

# Bounded Arithmetic and Constant Depth Frege Proofs

Samuel R. Buss\*

Department of Mathematics  
University of California, San Diego  
La Jolla, CA 92093-0112  
sbuss@math.ucsd.edu

April 28, 2004

## Abstract

We discuss the Paris-Wilkie translation from bounded arithmetic proofs to bounded depth propositional proofs in both relativized and non-relativized forms. We describe normal forms for proofs in bounded arithmetic, and a definition of  $\Sigma'$ -depth for PK-proofs that makes the translation from bounded arithmetic to propositional logic particularly transparent.

Using this, we give new proofs of the witnessing theorems for  $S_2^1$  and  $T_2^1$ ; namely, new proofs that the  $\Sigma_1^b$ -definable functions of  $S_2^1$  are polynomial time computable and that the  $\Sigma_1^b$ -definable functions of  $T_2^1$  are in Polynomial Local Search (PLS). Both proofs generalize to  $\Sigma_i^b$ -definable functions of  $S_2^i$  and  $T_2^i$ .

## 1 Introduction

From its inception, bounded arithmetic has been intended to connect to low-level complexity classes. Parikh's definition [17] of  $I\Delta_0$  was intended to relate to the linear-time hierarchy. The introduction of the  $\Omega_1$  axiom by Wilkie and Paris [22] and the corresponding introduction of the smash ( $\#$ ) function by Nelson [16] were originally motivated by the need to arithmetize the syntax of metamathematics, but these were quickly recognized as axiomatizations of the growth-rate of polynomial time functions. The

---

\*Supported in part by NSF grant DMS-0100589.

modern formulation of bounded arithmetic in its “ $S_2^i$ ” and “ $T_2^i$ ” forms by Buss [3, 4] included a complete characterization of the proof theoretic strengths of a hierarchy of theories in terms of the polynomial time hierarchy.

A second connection between theories of bounded arithmetic and computational complexity is via the connection between provability in theories of bounded arithmetic and provability in propositional logic. There are two distinct kinds of connections between bounded arithmetic and propositional proofs. The first is due to Steve Cook [7] who provided a translation between PV and polynomial-size extended Frege ( $e\mathcal{F}$ ) proofs. (By [3], the theory PV is conservative over  $S_2^1$ , so the same translation applies to  $S_2^1$ -proofs.) This approach has been extended by a number of people, including Dowd [9] and Krajíček-Pudlák [15], to apply a number of theories, including all the fragments  $S_2^i$  and  $T_2^i$ . Analogous translations for  $NC^1$  have been given by Arai [1] and Cook and Morioka [8]. The second connection was initiated by Paris and Wilkie [18]. In this approach, a proof in bounded arithmetic is transformed into a propositional proof (a Frege proof) where the formulas all have constant depth, with “depth” measured in terms of alternations of AND’s and OR’s. It is this second connection that we will be exploring in the present paper, and we present more details below.

In recent years, there has been a large research effort aimed at establishing upper bounds and especially lower bounds on the size of propositional proofs. On the other hand, research in fragments of bounded arithmetic has not received a comparable level of attention. The present author believes, however, that bounded arithmetic should be kept in mind while doing propositional proof complexity: if nothing else, it provides a touchstone or metric which allows us to evaluate the quality of the research in propositional proof complexity.

The outline of the present paper is as follows: Section 2 quickly introduces theories of bounded arithmetic, and discusses normal forms for proofs in  $S_2^i$  and  $T_2^i$  that are useful for the Paris-Wilkie translations. We assume some familiarity with fragments of bounded arithmetic, for this, the reader may consult [3, 10, 13]. Section 3 discusses bounded depth Frege systems, called  $\Sigma'$ -depth  $d$  PK-proof systems, which are tailored to work well for translating from bounded arithmetic theories. Section 4 contains the theorems about the Paris-Wilkie translation from fragments of bounded arithmetic to the PK-proof systems. The material in this section is fairly conventional, but there are a couple new aspects; most importantly, the Paris-Wilkie translation is applied not only to “relativized” theories  $S_2^i(\alpha)$  and  $T_2^i(\alpha)$ , but also to the unrelativized theories  $S_2^i$  and  $T_2^i$ . Section 5 gives new proofs for the “Main Theorems” for the theories  $S_2^1$  and  $T_2^1$ ; namely, that

their provably total functions are precisely the polynomial time computable functions and the projections of polynomial local search (PLS) functions. These new proofs are based on first translating to the setting of constant depth PK-proofs.

## 2 Proofs in theories of bounded arithmetic

The traditional language of bounded arithmetic includes the function and relation symbols  $0$ ,  $S$ ,  $+$ ,  $\cdot$ ,  $\#$ ,  $\lfloor \frac{1}{2}x \rfloor$ ,  $|x|$ , and  $\leq$ . To these can be added the symbols  $\beta(i, w)$  and  $\langle \rangle$  and  $*$ , where  $\beta(i, w)$  is the Gödel beta function, where  $\langle \rangle$  is the empty sequence, and where the  $*$  function concatenates an element to a sequence, so

$$\langle x_1, \dots, x_k \rangle * y = \langle x_1, \dots, x_k, y \rangle.$$

Adding these symbols and their defining equations yields a conservative extension of the theories  $S_2^i$  and  $T_2^i$ , for  $i \geq 1$  [3]. The particular formulation of the sequence coding functions is not terribly important, but they should be definable by polynomial size formulas.<sup>1</sup>

The theories  $S_2^i$  and  $T_2^i$  are formulated using the sequent calculus, LKB, which includes rules for bounded quantifiers. Quantifiers of the form  $(Qx \leq t)$  are called *bounded quantifiers*, and ones of the form  $(Qx \leq |t|)$  are called *sharply bounded quantifiers*. Formulas that contain only (sharply) bounded quantifiers are called (sharply) bounded formulas. The set  $\Delta_0^b = \Sigma_0^b = \Pi_0^b$  is the set of sharply bounded formulas. For  $i \geq 0$ , the classes  $\Sigma_i^b$  and  $\Pi_i^b$  of bounded formulas are defined by counting alternations of bounded quantifiers, ignoring the sharply bounded ones. The theories  $S_2^i$  and  $T_2^i$  are usually defined using the  $\Sigma_i^b$ -PIND and  $\Sigma_i^b$ -IND rules, respectively, which are

$$\Sigma_i^b\text{-PIND: } A(0) \wedge (\forall x)(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow (\forall x)(A(x)),$$

and

$$\Sigma_i^b\text{-IND: } A(0) \wedge (\forall x)(A(x) \rightarrow A(x+1)) \rightarrow (\forall x)(A(x)).$$

For the purpose of simplifying the translation from bounded arithmetic, we now introduce some well-known syntactically restricted versions of bounded arithmetic. A formula is said to be a *form restricted  $\Sigma_1^b$  formula* if it has the form

$$(\exists x \leq t)(\forall y \leq |s|)B,$$

---

<sup>1</sup>Alternatively, the MSP and LSP functions could be used instead of the more powerful sequence coding functions, c.f. [19].

where  $B$  is quantifier-free and possibly one or both of the quantifiers are omitted. In particular, every quantifier-free formula is form restricted  $\Sigma_1^b$ . The class of *form restricted  $\Pi_1^b$  formulas* is defined dually. For  $i > 1$ , a formula is *form restricted  $\Sigma_i^b$*  (resp., *form restricted  $\Pi_i^b$* ), if either it is form restricted  $\Pi_{i-1}^b$  (resp., form restricted  $\Sigma_{i-1}^b$ ) or it consists of a single bounded existential (resp., bounded universal quantifier) in front of a form restricted  $\Pi_{i-1}^b$  (resp., form restricted  $\Sigma_{i-1}^b$ ) formula.

Because the extra  $\beta$  function and sequence coding functions are included in the language, every  $\Sigma_i^b$  (resp.,  $\Pi_i^b$ ) formula is equivalent to a form restricted  $\Sigma_i^b$  (resp.,  $\Pi_i^b$ ) formula. Furthermore, this equivalence can be proved in  $S_2^i$  (and, in  $T_2^i$ ) using induction on only form restricted  $\Sigma_1^b$  formulas; to prove this, see the methods of [3]. From this it follows, using free cut elimination (c.f., Takeuti [20]), that if  $A$  is a form restricted  $\Sigma_i^b$  formula that is a consequence of  $S_2^i$  or  $T_2^i$ , then there is a proof  $P$  of  $A$  in that theory such that every formula in  $P$  is a form restricted  $\Sigma_i^b$  formula.

Let  $P$  be a proof in  $S_2^i$  or  $T_2^i$ . The variables  $\vec{a}$  which occur freely in the endsequent of  $P$  are called the *parameter variables* of  $P$ . A quantifier ( $Qx \leq t$ ) appearing in  $P$  is said to be *restricted by parameter variables* provided the term  $t$  contains no variables other than parameter variables. A free variable  $z$  in  $P$  is said to be restricted by parameter variables iff either (a) it is a parameter variable or (b) every cedent which contains an occurrence of  $z$  also contains an antecedent formula of the form  $z \leq t(\vec{a})$  bounding  $z$  in terms of the parameter variables  $\vec{a}$ . From Buss [3] or Takeuti [21], it is known that if a proof  $P$  contains only bounded quantifiers, then it can be converted into a proof of the same endsequent such that all quantifiers and all variables in  $P'$  are restricted by parameter variables. Now, the proof  $P'$  cannot be obtained in polynomial time from  $P$  since it may be exponentially larger;<sup>2</sup> however, the quantifier complexity of the formulas in  $P'$  is no greater than the quantifier complexity of formulas in  $P$ .

**Definition** Let  $P$  be a proof in a theory of bounded arithmetic. The proof  $P$  is said to be a *restricted- $\Sigma_i^b$  proof* provided (a) every formula in  $P$  is a form restricted  $\Sigma_i^b$  formula, (b) every quantifier in  $P$  is bounded and is restricted by parameter variables of  $P$ , and (c) all free variables in  $P$  are restricted by parameter variables.

**Theorem 1** *Let  $i \geq 1$  and  $R$  be one of the theories  $S_2^i$  or  $T_2^i$ . Further let  $A$  be a form restricted  $\Sigma_i^b$  formula which is a consequence of  $R$ . Then, there*

---

<sup>2</sup>For a construction that makes the proof exponentially larger when restricting by parameter variables, see [5].

is a restricted- $\Sigma_i^b$   $R$ -proof of  $A$ .

As discussed above, the theorem follows from the constructions in Buss [3].

### 3 Bounded depth PK-proof systems

This section formulates bounded depth PK-proofs in a manner optimized for translating from bounded arithmetic. Our main sources for the constructions are the definition of  $\Sigma$ -depth  $d$  proofs by Krajíček [12] and the subsequent definition of  $\Theta$ -depth  $d$  proofs by Beckmann and Buss [2]. Both these definitions use a size parameter, a function  $S(n)$ . When the bottom fanin of a formula is less than  $\log S(n)$ , then it does not count toward the  $\Sigma$ -depth, and counts only  $\frac{1}{2}$  towards the  $\Theta$ -depth. The size parameter  $S(n)$  is generally an upper bound on the size of PK-proofs.

The PK proof system we use is a Tait-style system (not a Gentzen-style system). Each line of the proof is called a *cedent*, and consists of a finite set of formulas. The intended meaning of the cedent is the disjunction of the formulas appearing in it. We use capital Greek letters,  $\Gamma$ ,  $\Delta$ , etc., to denote cedents.

Formulas are formed from propositional variables  $p$ , negated propositional variables  $\bar{p}$ , and unbounded fanin conjunctions ( $\bigwedge$ ) and disjunctions ( $\bigvee$ ). The formulas  $p$  and  $\bar{p}$  are called *literals*. If  $\varphi$  is a formula, the negation of  $\varphi$  is denoted  $\bar{\varphi}$  and is obtained from  $\varphi$  by replacing each literal by its negation and interchanging conjunctions and disjunctions.

The rules of inference are as follows. First, the logical initial cedents are the *Neg* and *Taut*

$$\text{Neg: } p, \bar{p} \quad \text{and} \quad \text{Taut: } \Gamma$$

where in the *Taut* inference,  $\Gamma$  is any tautology. (We shall restrict the use of *Taut* axioms; note that the *Neg* axioms are a special case of the *Taut* axioms.) Second, if the proof is a proof of  $\mathcal{A} \vDash \Gamma$ , where  $\mathcal{A}$  is a set of cedents, then the following non-logical axioms are allowed:  $\Delta$  and  $\bigvee \Delta$  for any cedent  $\Delta \in \mathcal{A}$ . (This convention comes from [2].) Third, the following rules of inference are allowed:

$$\begin{array}{ll} \bigvee: \frac{\Gamma, \varphi_{i_0}}{\Gamma, \bigvee_{i \in \mathcal{I}} \varphi_i}, \text{ where } i_0 \in \mathcal{I} & \bigwedge: \frac{\Gamma, \varphi_i \text{ for all } i \in \mathcal{I}}{\Gamma, \bigwedge_{i \in \mathcal{I}} \varphi_i} \\ \text{Weakening: } \frac{\Gamma}{\Gamma, \Delta} & \text{Cut: } \frac{\Gamma, \varphi \quad \Gamma, \bar{\varphi}}{\Gamma} \end{array}$$

Given the above axioms and rules of inference, the notion of PK-proof is defined in the usual way. Proofs can be either tree-like or sequence-like but, unless stated otherwise, are presumed to be tree-like. Proof size will be measured by the number of occurrences of symbols in the proof; a proof is said to have size  $S$  provided it has  $\leq S$  many symbols.

**Definition** Let  $S$  be a proof size parameter (size upper bound). The formulas that have  $\Sigma'$ -depth  $d$  with respect to  $S$  are inductively defined as follows:

- a. If  $\varphi$  has size  $\leq \log S$ , then  $\varphi$  has  $\Sigma'$ -depth 0.
- b. If  $\varphi$  has  $\Sigma'$ -depth  $d$ , then it has  $\Sigma'$ -depth  $d'$  for all  $d' > d$ .
- c. If  $\varphi_i$  has  $\Sigma'$ -depth  $d$  for all  $i \in \mathcal{I}$ , then  $\bigvee_{i \in \mathcal{I}} \varphi_i$  and  $\bigwedge_{i \in \mathcal{I}} \varphi_i$  have  $\Sigma'$ -depth  $(d + 1)$ .

When talking about  $\Sigma'$ -depth, we usually omit mention of the proof size parameter  $S$ , but it is always implicitly included.

We can now state the restrictions that will be placed on the *Taut* axioms; namely, the *Taut* axioms are allowed only for cedents  $\Gamma$  such that  $\bigvee \Gamma$  has  $\Sigma'$ -depth 0; i.e., only for cedents that have size at most  $\log S$ .

**Definition** Let  $S$  be a size parameter. Let  $P$  be an PK-proof. We say that  $P$  is a  $\Sigma'$ -depth  $d$  proof of size  $S$  provided that the following hold:  $P$  has  $\leq S$  symbols, every formula in  $P$  has  $\Sigma'$ -depth  $d$ , and every *Taut* axiom has size  $\leq \log S$ .

Krajíček [12] defined a notion of  $\Sigma$ -depth  $d$  which is almost identical to the notion of  $\Sigma'$ -depth  $d$ . His definition differed only in the base case of  $d = 0$ , as he required  $\varphi$  to be a disjunction or conjunction of  $\leq \log S$  literals. It is not hard to see that, for  $d \geq 1$ , the notions of  $\Sigma$ -depth and  $\Sigma'$  coincide semantically at least, because a  $\Sigma'$ -depth  $d$  formula may be translated into a  $\Sigma$ -depth  $d$  formula by expressing its  $\Sigma'$ -depth 0 subformulas in disjunctive or conjunctive normal form. It has become common to refer to  $\Sigma$ -depth  $d$  formulas as formulas of depth  $(d + \frac{1}{2})$ . Beckmann and Buss [2] use the name  $\Theta$ -depth  $d$  where  $d$  is any half integer to unify the notions of depth and  $\Sigma$ -depth. Our definition of PK-proofs of  $\Sigma'$ -depth  $d$  corresponds to what Beckmann-Buss refers to as  $(d + \frac{1}{2})$ -LK-proofs.

It is worth remarking about the *Taut* axioms that they do not add much to the provability strength of PK-proofs. Since a *Taut* axiom has size bounded by  $\log S$ , it can be proved outright by a proof of size  $O(S \log S)$

using only *Neg* axioms. Thus, if *Taut* axioms were disallowed, it would only change proof size polynomially (and for us, polynomial changes in proof size are unimportant).

We are usually interested in asymptotic results. Thus, we will have a family of proofs, indexed by  $n$ . The  $n$ th proof  $P_n$  will be size bounded by  $S(n)$ , and will prove some statement  $\mathcal{A}_n \vDash \varphi_n$ , for some set  $\mathcal{A}_n$  of cedents and some formula  $\varphi_n$ , where possibly  $\mathcal{A}_n$  is empty or  $\varphi_n$  is the empty cedent. When translating from bounded arithmetic,  $P_n$  will be a proof about the property holding for parameter variables of  $\leq n$  bits in length.

## 4 Translating from bounded arithmetic to PK

We now describe the transformation from bounded arithmetic  $S_2^d$ - or  $T_2^d$ -proofs,  $d \geq 1$ , into PK-proofs of  $\Sigma^1$ -depth  $d$ . Suppose  $P$  is a proof in bounded arithmetic. W.l.o.g., there is a single parameter variable  $x$  for  $P$ . We choose an integer  $n$ , which will be an upper bound on  $|x|$ , and the translation to propositional logic will then apply to values for  $x$  such that  $|x| \leq n$ .

The usual convention for a bounded arithmetic proof  $P$  is that it is formulated in the sequent calculus. However, we convert it into a Tait-style proof by the simple expedient of negating all formulas that appear in the antecedent, those plus the formulas in the succedent form a cedent in a Tait-style proof, which we call  $P_{\text{Tait}}$ . The sequent calculus rules become Tait calculus rules in the obvious fashion.

We start by describing the translation of quantifier-free formulas. Each variable  $u$  is bounded by the parameter variable, and thus there is an upper bound  $n_u$  on the number of bits in the binary representation of the value of  $u$ . (Note  $n_x = n$ .) We use propositional variables  $p_{u,i}$ , with  $0 \leq i < n_u$ , to represent the bits of  $u$ . Now, given any atomic formula  $\varphi(\vec{u})$  over the language of bounded arithmetic, there is a polynomial-size propositional formula  $\llbracket \varphi \rrbracket_n$  which is the translation of  $\varphi(\vec{u})$ . The formula  $\llbracket \varphi \rrbracket_n$  involves the propositional variables  $p_{u_k,i}$  for the bits of the free variables appearing in  $\varphi$ , and the value of  $\llbracket \varphi \rrbracket_n$  gives the truth value of  $\varphi$ . It is well-known how to form the formulas  $\llbracket \varphi \rrbracket_n$  (c.f., [13]): the key point is that polynomial size propositional formulas may be used to describe the effects of the functions and predicates of bounded arithmetic. Because of the fact we have the *Taut* axioms, the details of the formation of these propositional formulas is not particularly important.

The translations  $\llbracket \varphi \rrbracket_n$  of quantifier-free formulas are size  $n^{O(1)}$ , i.e.,

polynomial-size. They are defined by letting  $\llbracket \varphi \wedge \psi \rrbracket_n$  be  $\llbracket \varphi \rrbracket_n \wedge \llbracket \psi \rrbracket_n$ , letting  $\llbracket \varphi \vee \psi \rrbracket_n$  be  $\llbracket \varphi \rrbracket_n \vee \llbracket \psi \rrbracket_n$ , and letting  $\llbracket \neg \varphi \rrbracket_n$  be  $\overline{\llbracket \varphi \rrbracket_n}$ . We will be constructing proofs of size  $S(n) = 2^{n^{O(1)}}$ ; thus, these formulas will be  $\Sigma'$ -depth 0.

Second, we describe the translation of the sharply bounded formulas in  $P_{\text{Tait}}$ . These have the form  $(\forall y \leq |s|)B$  or  $(\exists y \leq |s|)B$ . Because the term  $s$  contains only parameter variables as variables, and since the parameter variables have at most  $n$  bits, we can find a bound  $n_y = n^{O(1)}$  such that  $|s| \leq n_y$  for all values of parameter variables with binary length  $\leq n$ . Then, we translate the formula  $(\forall y \leq |s|)B$  to

$$\llbracket (\forall y \leq |s|)B \rrbracket_n = \bigwedge_{i=0}^{n_y} \llbracket y \leq |s| \rightarrow B \rrbracket_n / (y \mapsto i). \quad (1)$$

The last notation, “ $\psi / (y \mapsto i)$ ” means replace the variables  $p_{y,i}$  representing the bits of  $y$  by constants 0 or 1 as given by the bits of the integer  $i$ .<sup>3</sup> The propositional formula (1) has size only  $n^{O(1)}$ . Thus, it has  $\Sigma'$ -depth 0 for suitably large  $S(n) = 2^{n^{O(1)}}$ . Existential sharply bounded formulas are translated similarly, but using a disjunction instead of a conjunction.

Third, we describe the translation of a formula with a general bounded quantifier, say  $(\forall y \leq t)B$ . By the fact  $t$  contains only parameter variables, we can find an integer  $n_y = n^{O(1)}$  such  $|t| \leq n_y$  whenever the parameter variables have length  $\leq n$ . The formula is then translated to

$$\llbracket (\forall y \leq t)B \rrbracket_n = \bigwedge_{i=0}^{2^{n_y}-1} \llbracket y \leq t \rightarrow B \rrbracket_n / (y \mapsto i). \quad (2)$$

A dual construction works for bounded existential quantifiers.

It is clear that this translation maps  $\Sigma_d^b$  and  $\Pi_d^b$  bounded arithmetic formulas to  $\Sigma'$ -depth  $d$  propositional formulas.

So far, we have discussed how to translate individual formulas. Next, we discuss how cedents of  $P_{\text{Tait}}$  are translated. Given a cedent  $\Gamma$ , let  $\vec{y} = y_1, \dots, y_k$  be the non-parameter variables in the cedent. For each  $y_i$ , there is a formula  $\neg y_j \leq t_j$  in the cedent where  $t_j$  involves only parameter variables. Find, for each  $j$ , a integer  $n_j = n^{O(1)}$  such that  $|t_j| \leq n_j$  holds

---

<sup>3</sup>The subscript  $n$  in the notation indicates that the parameter variable,  $x$ , has  $\leq n$  bits in its binary representation. Other variables such as  $y$  may have more bits. In (1),  $y$  will have  $n_y = O(|n|)$  bits. In (2),  $y$  will have  $n_y = n^{O(1)}$  bits, i.e., polynomially many bits.

whenever the parameter variables have values of length  $\leq n$ . Then, for each choice of values  $i_1 < 2^{n_1}, \dots, i_k < 2^{n_k}$ , form the sequent

$$\llbracket \Gamma \rrbracket_n / (y_1 \mapsto i_1, \dots, y_k \mapsto i_k).$$

The notation  $\llbracket \Gamma \rrbracket_n$  indicates forming the cedent by taking the propositional translation of each formula in  $\Gamma$ . Note that each cedent of  $P$  has become a large number of cedents; the total number of propositional cedents is easily calculated to be  $O(2^{n^{O(1)}})$ . Also note that the only free variables in the translated cedents are the propositional variables  $p_{x,i}$  associated with the parameter variable  $x$ .

The next two theorems describe the well-known Paris-Wilkie translation from bounded arithmetic to propositional logic. The notion of a *polynomial time uniform* proof is defined analogously to the definition of a uniform circuit. We won't define this notion completely, but merely state that a polynomial time uniform proof is a proof that can be effectively described by and traversed by a polynomial time procedure. Note that a polynomial time uniform proof can be exponentially big: the uniformity means that there are polynomial time algorithms for describing the structure of the proof and the formulas in the proof. This is similar to the way the "connection language" of circuits can be used to uniformly define a family of circuits.

The *height* of a proof is the maximum number of cedents along any branch of the proof tree.

**Theorem 2** *Let  $i \geq 1$ . Suppose  $A(x)$  is a form restricted  $\Sigma_i^b$  formula of bounded arithmetic. Let  $\llbracket A \rrbracket_n$  denote the propositional translation of  $A$ ;  $\llbracket A \rrbracket_n$  has free variables  $p_{x,i}$ , for  $i < n$ .*

- a. *Suppose  $S_2^i \vdash A$ . Then there is a function  $S(n) = 2^{n^{O(1)}}$  such that, for all  $n$ ,  $\llbracket A \rrbracket_n$  has a  $\Sigma'$ -depth  $i$  proof of size  $S(n)$ . Furthermore, this proof has height  $O(\log \log S(n))$  and contains only  $O(1)$  many formulas in each cedent. In addition, the proof is polynomial-time uniform.*
- b. *Suppose  $T_2^i \vdash A$ . Then there is a function  $S(n) = 2^{n^{O(1)}}$  such that, for all  $n$ ,  $\llbracket A \rrbracket_n$  has a  $\Sigma'$ -depth  $i$  proof of size  $S(n)$ . Furthermore, this proof has height  $O(\log S(n))$  and contains only  $O(1)$  many formulas per cedent. In addition, the proof is polynomial-time uniform.*

**Proof** The proof is based on the above constructions: For any  $n$ , apply the translation  $\llbracket \Gamma \rrbracket_n$  to each sequent  $\Gamma$  in the proof  $P_{\text{Tait}}$ , then combine these into a valid PK-proof. Recall that each cedent in  $P_{\text{Tait}}$  becomes multiple



or

$$\bigwedge_{i=0}^{t_{\text{Max}}} (\llbracket t = \underline{i} \rrbracket_n \rightarrow q_i) \quad (4)$$

where  $\llbracket t = \underline{i} \rrbracket_n$  is the polynomial size formula that states that the value of  $t$  is the integer  $i$ .

We want to define a new notion of  $\Sigma^\alpha$ -depth, which generalizes the notion of  $\Sigma'$ -depth to formulas that contain subformulas of the forms (3) or (4). For this, define  $\bar{\alpha}$ -Boolean formulas to be propositional formulas in the language containing Boolean literals, constants 0 and 1, unbounded connectives  $\bigvee$  and  $\bigwedge$ , and a new unbounded connective  $\bar{\alpha}$  with the restriction that no occurrence of  $\bar{\alpha}$  may be in the scope of another occurrence of  $\bar{\alpha}$ .

An  $\bar{\alpha}$ -Boolean formula  $\chi$  can be converted into an ordinary Boolean formula  $\chi'$  by replacing each subformula  $\bar{\alpha}(b_1, \dots, b_m)$  by

$$\bigvee_{i=0}^{2^m-1} (\bigwedge_j b_j^{(i_j)} \wedge q_i),$$

where each  $b_j$  is a Boolean formula and where  $b_j^{(i_j)}$  is either  $b_j$  or  $\bar{b}_j$  depending on whether the  $j$ th bit of the binary representation of  $i$  is 1 or 0, respectively. If  $\chi$  has size  $m$ , then we say  $\chi'$  has  $\alpha$ -size  $m$ . If  $\chi'$  cannot be obtained in this way, it is defined to have  $\alpha$ -size equal to infinity.

This allows the following definition of  $\Sigma^\alpha$ -depth, which generalizes the notion of  $\Sigma'$ -depth.<sup>4</sup>

**Definition** Let  $S$  be a proof size parameter (size upper bound). The formulas that have  $\Sigma^\alpha$ -depth  $d$  with respect to  $S$  are inductively defined as follows:

- a. If  $\varphi$  has  $\alpha$ -size  $\leq \log S$ , then  $\varphi$  has  $\Sigma'$ -depth 0.
- b. If  $\varphi$  has  $\Sigma^\alpha$ -depth  $d$ , then it has  $\Sigma^\alpha$ -depth  $d'$  for all  $d' > d$ .
- c. If  $\varphi_i$  has  $\Sigma^\alpha$ -depth  $d$  for all  $i \in \mathcal{I}$ , then  $\bigvee_{i \in \mathcal{I}} \varphi_i$  and  $\bigwedge_{i \in \mathcal{I}} \varphi_i$  have  $\Sigma^\alpha$ -depth  $(d + 1)$ .

**Theorem 3** Let  $i \geq 1$ . Suppose  $A(x)$  is a form restricted  $\Sigma_i^b(\alpha)$  formula of bounded arithmetic possibly involving  $\alpha$ . Let  $\llbracket A \rrbracket_n$  denote the propositional translation of  $A$ .  $\llbracket A \rrbracket_n$  has free variables  $p_{x,i}$ , for  $i < n$  and  $q_i$  for  $i < 2^{n^{O(1)}}$ .

<sup>4</sup>It is possible to define  $\Sigma^\alpha$ -size in a more general fashion, but this needlessly adds major difficulties to the details of translating from bounded arithmetic to propositional proofs. Thus we prefer the ad-hoc, but direct, approach used in this definition.

- a. Suppose  $S_2^i(\alpha) \vdash A$ . Then there is a function  $S(n) = 2^{n^{O(1)}}$  such that, for all  $n$ ,  $\llbracket A \rrbracket_n$  has a  $\Sigma^\alpha$ -depth  $i$  proof of size  $S(n)$ . Furthermore, this proof has height  $O(\log \log S(n))$  and contains only  $O(1)$  many formulas in each cedent. In addition, the proof is polynomial-time uniform.
- b. Suppose  $T_2^i(\alpha) \vdash A$ . Then there is a function  $S(n) = 2^{n^{O(1)}}$  such that, for all  $n$ ,  $\llbracket A \rrbracket_n$  has a  $\Sigma^\alpha$ -depth  $i$  proof of size  $S(n)$ . Furthermore, this proof has height  $O(\log S(n))$  and contains only  $O(1)$  many formulas per cedent. In addition, the proof is polynomial-time uniform.

The proof of Theorem 3 is very similar to the proof of Theorem 2; we leave the proof to the reader.

## 5 New proofs for witnessing theorems

We now use the Paris-Wilkie translation as refined in Theorem 2 to prove the “main” witnessing theorems for  $S_2^1$  and  $T_2^1$ . We then also generalize the proofs to get witnessing theorems for  $S_2^i$  and  $T_2^i$ . With the exception of the theorem for  $T_2^i$  with  $i > 1$ , these witnessing theorems are not new; they were first proved for  $S_2^i$  by Buss [3] and for  $T_2^1$  by Buss-Krajíček [6]. The novelty is that we prove them via the Paris-Wilkie translation to propositional logic.

We start with the “Main Theorem” for  $S_2^1$ .

**Theorem 4** (Buss [3]) *Suppose that  $A(x, y) \in \Sigma_1^b$  and that  $S_2^1$  proves  $(\forall x)(\exists y)A(x, y)$ . Then there is a polynomial time function  $f(x) = y$  such that for all  $x \in \mathbb{N}$ ,  $A(x, f(x))$  holds.*

**Proof** By a well-known theorem of Parikh [17],  $S_2^1$  can also prove  $(\exists y \leq s(x))A(x, y)$  for some term  $s$ . Now,  $x$  is the parameter variable. Applying Theorem 2(a) yields a  $\Sigma'$ -depth 1 proof; adding a *Cut* to the end of this proof turns the proof into a refutation  $R$  of the formula

$$\llbracket (\forall y \leq s(x)) \neg A(x, y) \rrbracket. \tag{5}$$

The refutation  $R$  ends with the empty cedent.

We shall describe a polynomial time procedure that is given a particular value for  $x$  (i.e., settings for the propositional variables  $p_{x,i}$ ) and traverses the refutation  $R$  until it arrives at a false initial cedent. Of necessity this false initial cedent is the cedent (5), and when it is reached, the procedure will know a value  $y$  that falsifies the cedent. This value for  $y$  will be the value of  $f(x)$ .

We shall describe the action of this procedure informally; however, the refutation  $R$  has a polynomial time uniform structure, since it was obtained by translating a bounded arithmetic proof. Therefore, this informal description can be carried out by a polynomial time procedure. To clarify the exact structure of proof, we specify that whenever a cut occurs on a  $\Sigma'$ -depth 1 formula  $\varphi$  that the right upper cedent contains  $\varphi$  if  $\varphi$  is a conjunction and contains  $\bar{\varphi}$  if  $\varphi$  is a disjunction. (This convention preserves the order of cut hypotheses in the order they appeared in the bounded arithmetic proof.)

The polynomial time procedure acts as follows: it starts at the root of the proof and traverses the proof upward, backtracking as needed as described below. At each stage, the procedure is at some cedent  $\Gamma$  in the proof that it believes to be false. In particular, every  $\Sigma'$ -depth 0 formula in  $\Gamma$  evaluates to have value *False*. (Recall that the variables  $p_{x,i}$  are the only variables in  $R$ , and the procedure has values for these.) Furthermore, for any formula in  $\Gamma$  which is a conjunction of  $\Sigma'$ -depth 0 formulas, the procedure knows of a particular conjunct which is false. For the formulas which are a disjunction of  $\Sigma'$ -depth 1 formulas, the procedure does not know for sure that they are false, it is merely tentatively assuming they are false.

We can now describe the algorithm used by the proof traversal procedure. At the beginning, the procedure is at the root of  $R$ , which is the empty cedent. Suppose the procedure is at the lower cedent of a cut inference

$$\frac{\Gamma, \varphi \quad \Gamma, \bar{\varphi}}{\Gamma}$$

If  $\varphi$  is  $\Sigma'$ -depth 0, then it can be evaluated as being either *True* or *False*. If it is true, the procedure proceeds to the right upper cedent, otherwise, it proceeds to the left upper cedent. Otherwise,  $\varphi$  is a disjunction by our assumption on how the upper cedents of *Cut*'s are ordered, so the algorithm makes the (tentative) assumption that  $\varphi$  is false and proceeds to the left upper cedent.

If the procedure is at the lower cedent of a  $\wedge$ -inference:

$$\frac{\Gamma, \psi_i \quad , \text{ for } i \in \mathcal{I}}{\Gamma, \bigwedge_{i \in \mathcal{I}} \psi_i}$$

the algorithm acts as follows. By assumption, the procedure knows a value  $i_0$  such that the conjunct  $\psi_{i_0}$  is false. The algorithm proceeds to the upper cedent  $\Gamma, \psi_{i_0}$  for this  $i_0$ .

If the procedure is at the lower cedent of a  $\vee$ -inference:

$$\frac{\Gamma, \psi_{i_0}}{\Gamma, \bigvee_{i \in \mathcal{I}} \psi_i}$$

the algorithm acts as follows. If  $\psi_{i_0}$  is false, it proceeds to the upper cedent. However, if it is true, the algorithm has discovered a disjunct of  $\varphi = \bigvee_{i \in \mathcal{I}} \psi_i$  which is true, contradicting the tentative assumption that  $\varphi$  was false. The procedure then backtracks down the path towards the root until it finds the *Cut* inference where the formula  $\varphi$  was added to the cedent. It then proceeds to the right upper cedent of the *Cut*, and saves the information about which conjunct of  $\bar{\varphi}$  is false.

We still need to prove that this procedure runs in polynomial time, that is, for only  $O(n^{O(1)})$  steps. The problem is that the proof is exponentially large because the  $\bigwedge$  inferences have many hypotheses. However, the procedure visits at most one hypothesis of each  $\bigwedge$ -inference. The set of cedents that are visited by the procedure during its traversal of the proof forms a tree in which each node has at most two children (e.g., a cedent derived by *Cut* inference may have two children in the traversal tree). This tree is of height  $O(\log n)$  since the proof has height  $O(\log n)$ . A binary tree of  $O(\log n)$  height has size at most  $O(n^{O(1)})$ , thus the procedure is polynomial time.

The procedure cannot terminate at any logical axiom since these always evaluate to the value *True*, nor will it stop at any internal cedent. Furthermore, it does depth-first search, and when it backtracks, it always moves rightward. Hence, it eventually reaches the cedent (5). When it reaches this, it knows a value for  $y$  that falsifies it. This value of  $y$  satisfies  $A(x, y)$ .  $\square$

The Witnessing Theorem 4 is usually stated in a stronger form stating that  $S_2^1$  can  $\Sigma_1^b$ -define the function  $f$  and can prove that  $(\forall x)A(x, f(x))$ . This stronger theorem can be proved by formalizing the proof of Theorem 4 in  $S_2^1$ . To do this, first note that Theorems 2 and 3 can be proved in  $S_2^1$ : the  $\Sigma'$ -depth or  $\Sigma^\alpha$ -depth PK-proofs of  $\llbracket A \rrbracket_n$  are not only polynomial-time uniform but *provably* polynomial-time uniform in the theory  $S_2^1$ . Second, the proof of Theorem 4 can be formalized in  $S_2^1$  in that  $S_2^1$  can prove the correctness of the polynomial time algorithm traversing the refutation  $R$ .

We next prove the ‘‘Main Theorem’’ for  $T_2^1$ . The class of Polynomial Local Search (PLS) functions was defined by Johnson, Papadimitriou and Yannakakis [11].

**Theorem 5** (Buss-Krajíček [6]) *Suppose  $A(x, y) \in \Sigma_1^b$  and that  $T_2^1$  proves  $(\forall x \leq t)(\exists y)A(x, y)$ . Then there is a Polynomial Local Search function  $f(x) = y$  such that for all  $x \in \mathbb{N}$ ,  $A(x, f(x))$  holds.*

**Proof** The proof uses exactly the same proof traversal procedure that was used for the proof of Theorem 4. The only thing that changes is that the procedure is no longer polynomial time since it may need to visit an exponential number of cedents in the inference. To formulate the traversal as a PLS procedure, we define a cost function on cedents in the refutation  $R$ . The cost is equal to the number of cedents above the current cedent plus the number of cedents to the right of the current cedent plus one. Clearly the cost decreases in each step of the procedure. At the end, we reach the initial cedent (5), which has cost 1. We add one more configuration that consists of the value for  $y$  such that  $A(x, y)$  holds and has cost 0.

The proofs of the previous two theorems can be relativized straightforwardly; this yields the following theorems for  $S_2^i$  and  $T_2^i$  with  $i > 1$ .

**Theorem 6** *Let  $i > 1$  and  $A(x, y) \in \Sigma_i^b$ .*

- a. *Suppose  $S_2^i \vdash (\forall x)(\exists y)A(x, y)$ . Then, there is a function  $f$  in  $\Pi_i^p = \text{FP}^{\Sigma_{i-1}^p}$  such that  $A(x, f(x))$  holds for all  $x \in \mathbb{N}$ . Here  $\text{FP}$  is the class of polynomial time functions, so  $\Pi_i^p$  is the class of functions computable in polynomial time relative to a  $\Sigma_{i-1}^p$ -oracle (i.e., relative to a set at the  $i$ th level of the polynomial time hierarchy).*
- b. *Suppose  $T_2^i \vdash (\forall x)(\exists y)A(x, y)$ . Then, there is a function  $f$  in  $\text{PLS}^{\Sigma_{i-1}^p}$  such that  $A(x, f(x))$  holds for all  $x \in \mathbb{N}$ .*

## 6 A translation to lower depth PK-proofs

The following theorem has been proved by Beckmann and Buss [2], based on earlier theorems of Krajíček and Razborov. Actually, [2] proved the theorem for  $\Sigma$ -depth and for  $\Theta$ -depth, not  $\Sigma'$ -depth, but the proofs apply also to  $\Sigma'$ -depth and  $\Sigma^\alpha$ -depth.

**Theorem 7** *Let  $d \in \mathbb{N}$ , and  $\{\mathcal{A}_n\}_n$  be a family of sets of cedents. Then the following conditions (1) and (2) are equivalent:*

- (1)  $\mathcal{A}_n$  has a  $\Sigma'$ -depth  $d$  PK-refutation of sequence-size quasi-polynomial in  $n$ , for all  $n$ .
- (2)  $\mathcal{A}_n$  has a  $\Sigma'$ -depth  $(d + 1)$  PK-refutation of tree-size quasi-polynomial in  $n$ , for all  $n$ .

*Furthermore, the following conditions (3) and (4) are equivalent:*

- (3)  $\mathcal{A}_n$  has  $\Sigma'$ -depth  $d$  PK-refutation of tree-size quasi-polynomial in  $n$ , for all  $n$ .
- (4)  $\mathcal{A}_n$  has a  $\Sigma'$ -depth  $(d + 1)$  PK-refutation which simultaneously has tree-size quasi-polynomial in  $n$  and height poly-logarithmic in  $n$ , for all  $n$ .

Although the paper [2] does not explicitly discuss uniformity of proofs, its proofs of the equivalences of Theorem 7 provide strongly constructive methods of transforming proofs that preserve the property of being polynomial uniform. From this, we get the following corollary, which is based on constructions of Krajíček [14].

**Theorem 8** *Let  $d \geq 2$ . Suppose  $A$  is a form restricted  $\Sigma_d^b$  formula and that  $T_2^d \vdash A$ . Without loss of generality,  $A$  has the form*

$$(\exists y \leq t(x))(\forall z \leq r(x))C(x, y, z)$$

where  $C$  is form restricted  $\Sigma_{d-2}^b$ . Let  $n_t = n^{O(1)}$  bound  $|t(x)|$  and  $n_r = n^{O(1)}$  bound  $|r(x)|$  for all  $x < 2^n$ . Then the set  $\mathcal{A}_n$  of cedents

$$\left\{ \llbracket y \leq t(x) \rightarrow (z \leq r(x) \wedge \neg C(x, y, z)) \rrbracket_n / (y \mapsto i, z \mapsto j) : j < 2^{n_r} \right\},$$

for  $i < 2^{n_t}$ , has a  $\Sigma'$ -depth  $d - 2$  PK-refutation which is polynomial time uniform.

The intuition behind this theorem is that the cedents in  $\mathcal{A}_n$  express the negation of  $\llbracket A \rrbracket_n$ . Loosely speaking, the theorem states that if  $A \in \Sigma_d^b$  is provable by  $T_2^d$  then the negations of  $\llbracket A \rrbracket_n$  have polynomial size PK-refutations of  $\Sigma'$ -depth  $(d - 2)$ .

**Proof** Let  $B(x, y) = (\forall z \leq r(x))C(x, y, z)$ . Theorem 2 implies that

$$\llbracket (\exists y \leq t)B(x, y) \rrbracket_n$$

has a  $\Sigma'$ -depth  $d$  refutation of size  $S(n)$ , of height  $O(\log S(n))$ , with  $O(1)$  many formulas per cedent, for some  $S(n) = 2^{n^{O(1)}}$ . Adding a cut, we change this to a refutation of

$$\llbracket (\forall y \leq t)\neg B(x, y) \rrbracket_n. \tag{6}$$

This formula is a conjunction of disjunctions, so by expanding the conjunction into multiple cedents and then expanding each disjunction by simply

separating formulas by commas, we can derive (6), using  $\vee$  inferences combined with a single  $\wedge$  inference. from the  $2^{n_t}$  many cedents

$$\left\{ \llbracket y \leq t \rightarrow (z \leq r \wedge \neg C(x, y, z)) \rrbracket_n / (y \mapsto i, z \mapsto j) : j < 2^{n_r} \right\}.$$

This proof still is  $\Sigma'$ -depth  $d$  and has height  $O(\log S(n))$ , and is now a refutation of a set of cedents of  $\Sigma'$ -depth  $(d - 2)$  formulas. Now Theorem 8 follows from Theorem 7.  $\square$

**Acknowledgements.** This paper was written on the occasion of the Takeuti Symposium in Kobe, December 2003. I wish to thank T. Arai and J. Krajíček for forcing me to write this paper.

## References

- [1] T. ARAI, *A bounded arithmetic AID for Frege systems*, Annals of Pure and Applied Logic, 103 (2000), pp. 155–199.
- [2] A. BECKMANN AND S. R. BUSS, *Separation results for the size of constant-depth propositional proofs*. Typeset manuscript, 2003.
- [3] S. R. BUSS, *Bounded Arithmetic*, Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.
- [4] ———, *A conservation result concerning bounded theories and the collection axiom*, Proceedings of the American Mathematical Society, 100 (1987), pp. 709–716.
- [5] ———, *Bounded arithmetic, cryptography and complexity*, Theoria, 63 (1997), pp. 147–167.
- [6] S. R. BUSS AND J. KRAJÍČEK, *An application of Boolean complexity to separation problems in bounded arithmetic*, Proc. London Math. Society, 69 (1994), pp. 1–21.
- [7] S. A. COOK, *Feasibly constructive proofs and the propositional calculus*, in Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.
- [8] S. A. COOK AND T. MORIOKA, *Quantified propositional calculus and a second-order theory for  $NC^1$* . Typeset manuscript, 2004.

- [9] M. DOWD, *Propositional representation of arithmetic proofs*, in Proceedings of the 10th ACM Symposium on Theory of Computing, 1978, pp. 246–252.
- [10] P. HÁJEK AND P. PUDLÁK, *Metamathematics of First-order Arithmetic*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1993.
- [11] D. S. JOHNSON, C. H. PAPADIMITRIOU, AND M. YANNAKAKIS, *How easy is local search?*, J. Comput. System Sci., 37 (1988), pp. 79–100.
- [12] J. KRAJÍČEK, *Lower bounds to the size of constant-depth propositional proofs*, Journal of Symbolic Logic, 59 (1994), pp. 73–85.
- [13] ———, *Bounded Arithmetic, Propositional Calculus and Complexity Theory*, Cambridge University Press, Heidelberg, 1995.
- [14] ———, *On the weak pigeonhole principle*, Fundamenta Mathematica, 170 (2001), pp. 123–140.
- [15] J. KRAJÍČEK AND P. PUDLÁK, *Quantified propositional calculi and fragments of bounded arithmetic*, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik, 36 (1990), pp. 29–46.
- [16] E. NELSON, *Predicative Arithmetic*, Princeton University Press, 1986.
- [17] R. J. PARIKH, *Existence and feasibility in arithmetic*, Journal of Symbolic Logic, 36 (1971), pp. 494–508.
- [18] J. B. PARIS AND A. J. WILKIE,  *$\Delta_0$  sets and induction*, in Open Days in Model Theory and Set Theory, W. Guzicki, W. Marek, A. Pelc, and C. Rauszer, eds., 1981, pp. 237–248.
- [19] C. POLLETT, *Arithmetic Theories with Prenex Normal Form Induction*, PhD thesis, University of California, San Diego, 1997.
- [20] G. TAKEUTI, *Proof Theory*, North-Holland, Amsterdam, 2nd ed., 1987.
- [21] ———, *Bounded arithmetic and truth definition*, Annals of Pure and Applied Logic, (1988), pp. 75–104.
- [22] A. J. WILKIE AND J. B. PARIS, *On the scheme of induction for bounded arithmetic formulas*, Annals of Pure and Applied Logic, 35 (1987), pp. 261–302.