数理解析研究所講究録
976 巻 1997 年 1-12

Bounded Arithmetic vs. Propositional Calculus

Noriko H. Arai (新井 紀子)
Department of Computer Science, Hiroshima City University
151 Ozuka, Asaminami-ku, Hiroshima 731-31 Japan

1 Introduction

In [11], Cook and Reckhow showed a close relation between the relative efficiency of propositional calculi and P=?NP problem, though it is rather unrealistic to dream to show the inequality P$\neq$NP by showing that there is no super system for propositional logic.

However, recent researches have revealed that the study of lengths of proofs in propositional calculi may benefit substantially to solve other open problems in the computational complexity such as P=?NC^1. It was Cook's result [9] which revealed the fact that certain systems of bounded arithmetic bridges the hierarchy of computational complexity and that of propositional calculus. In [9], he introduced an equational system PV as a theory of polynomial time functions analogous to the theory of primitive recursive functions, PRA. PV contains a schema which allows function symbols to be introduced for every polynomial time computable function and an induction schema to be applied for open formulas in PV. He showed that any PV-proof can be translated into polynomial-size eF-proofs and that PV is able to prove the formalized consistency of eF: PV can prove that "A is a tautology" when A has a polynomial-size eF-proof.

Buss introduced the system S_2^i as the formal foundation for polynomial-time computable functions [5]. It has a finite set of function symbols, a set of axioms on the functions and the length induction on Σ_i^p-predicates, whereas PV has an infinite set of function symbols and the induction on open formulas. Buss showed that $S_2 \stackrel{def}{=} \bigcup_{i=0}^{\infty} S_2^i$ corresponds with the polynomial time hierarchy [20] in the sense that every $\square_i^p$-functions is Σ_i^b-definable in S_2^i, and the converse holds true: every Σ_i^b-definable function in S_2^i is in $\square_i^p$. Later, it was shown that the polynomial time hierarchy provably collapses if and only if S_2 does, or equivalently if and only if S_2 is finitely axiomatizable [17], [7]. In particular, the following relations hold:

1. S_2^1 is a system which characterizes the functions in P as Σ_1^b-definable functions.

2. Any S_2^1 proof of bounded formula is translatable into polynomial-size eF proofs [6], [3].

3. S_2^1 proves the consistency of eF.

Here rises an interesting question: what systems of bounded arithmetic characterize the functions in the classes of computational complexity such as AC^0 and NC^1, and to what propositional calculi are they translatable? The answers are partly known: there does exist a bounded arithmetic which characterize functions in AC^0 and it is translatable into a well-known propositional calculus, bounded depth Frege.

It was conceived that the class of problems solved by bounded depth circuits (AC^0) is closely related to the class of tautologies having polynomial-size bounded depth Frege proofs. At the same time, it had been strongly predicted that the class of problems (and functions) related to "counting" would draw the line separating AC^0 and NC^1. Among them were the parity problem and the pigeonhole principle. In 1983, Ajtai showed that the parity problem gives the superpolynomial lowerbound for AC^0 [1]. Later the lowerbound was improved to exponential [22], [13].

There rose a totally different interest in the field of bounded arithmetic: what is the weakest bounded arithmetic which proves the fact that there are infinitely many primes? The famous Euclid's proof for the existence of infinitely many primes uses the function !, though the next prime of p is bounded by polynomial of p.

The system $\mathrm{I}\Delta_0$ is defined as a bounded arithmetic with the language of Peano arithmetic and the induction on the class of bounded formulas. Woods showed that $\mathrm{I}\Delta_0$ proves the existence of infinitely many primes if it proves the (Δ_0-) pigeonhole principle [21]. In [18], they showed that proofs in the relativised $\mathrm{I}\Delta_0$ to a new relation symbol R are translatable to polynomial-size bounded depth Frege proofs. Along the line, Ajtai showed that the pigeonhole principles do not have polynomial-size bounded depth Frege proofs and that $\mathrm{I}\Delta_0(R)$ does not prove the pigeonhole principle simultaneously [2].

There are a few attempts to find a suitable system of bounded arithmetic which characterizes the functions in NC^1 or ALOGTIME. In [4], Arai introduced a system called AID which is an analogue to S^1_2, and in [8], Clote introduced ALV that of PV. Accordingly, NC^1 (ALOGTIME), AID (ALV) and Frege will enjoy the similar relations that P, S^1_2 (PV) and eF do [10].

The map of hierarchies of propositional calculi, bounded arithmetic and complexity classes, shown in the literature, can be sketched as follows: for systems below the horizontal line, lowerbounds are known.

extended Frege Frege + substitution Frege + renaming	$\cdots$	PV S^1_2	$\cdots$	P
$\Downarrow$		$\Downarrow$		$\Downarrow$
Frege, LK, NK	$\cdots$	AID ALV	$\cdots$	ALOGTIME
$\Downarrow \not\Uparrow$		$\Downarrow \not\Uparrow$		$\Downarrow \not\Uparrow$
bounded depth Frege	$\cdots$	$\mathrm{I}\Delta_0(f)$	$\cdots$	AC^0

In this paper, we give a technique to translate bounded S^1_2-proofs into polynomial-size eF proofs, which is called the *linewise translation*. When a bounded normal form S^1_2-proof is given, the proof can be viewed as a pile of computations with the free variables in the end sequent as its input. Since it is a bounded proof, every non-parameter variable a in the proof must be eliminated as a bound variable bounded by a term t. Hence, the range of a does not exceed t. We can inductively compute the bound of a in terms of parameter variables. Then, we are ready to compute the polynomial space bound for the computation associated with each line of the proof. Now, it is ready to be translated into polynomial-size eF proofs almost automatically.

2 Translation of S_2^1 proofs to polynomial-size extended Frege proofs

Now we present our translation algorithm from S_2^1 into eF. We first follow Buss' original definitions [6].

Definition 1 Let t be a term of S_2^1. The *bounding polynomial* $q_t(n)$ of t is defined inductively by:

1. $q_0(n) = 1$
2. $q_a(n) = n$ for any variable a
3. $q_{s(t)}(n) = q_t(n) + 1$
4. $q_{t+u}(n) = q_t(n) + q_u(n)$
5. $q_{t \cdot u}(n) = q_t(n) + q_u(n)$
6. $q_{t \# u}(n) = q_t(n) \cdot q_u(n) + 1$
7. $q_{|t|}(n) = q_{\lfloor \frac{1}{2} t \rfloor}(n) = q_t(n)$

Proposition 1 *If $t(a_1, \ldots, a_k)$ is a term and $x_1, \ldots, x_k$ are variables ranging over natural numbers of length $\leq n$, then the following holds;*

1. $|t(\vec{x})| \leq q_t(n)$,
2. $q_t(n) \geq n$ *if* $var(t) \neq \emptyset$.

Definition 2 Let A be a bounded formula of S_2^1. The *bounding polynomial* q_A of A is inductively defined by:

1. $q_{t=u} = q_{t \leq u} = q_t + q_u$
2. $q_{A \wedge B} = q_{A \vee B} = q_{A \supset B} = q_A + q_B$
3. $q_{\neg A} = q_A$
4. $q_{(\exists x \leq t)A}(n) = q_{(\forall x \leq t)A}(n) = q_t(n) + q_A(n + q_t(n))$

Proposition 2 *The bounded formula $A(x_1, \ldots, x_k)$ where $|x_i| \leq n$, only refers to numbers of length $\leq q_A(n)$.*

Proposition 3 *[5] Let A be a bounded formula in S_2^i ($i \geq 1$) and $\vec{a}$ be the list of free variables in A. Suppose that S_2^i proves A, then there is a bounded S_2^i proof of A such that it is free-cut free, free variable normal form.*

Note that translating S_2^i proofs into free variable normal proofs increases the size of proofs only linearly. On the contrary, producing free-cut free proofs requires superexponential function in general. However, it makes only the difference of constant when we focus on only one S_2^i proof. Without loss of generality, we only consider free-cut free, free variable normal form S_2^i proofs.

Now we are going to define a bounding term $tm(b; P)$ for a free variable b in an S_2^1 proofs so that b ranges over natural numbers bounded by $tm(b; P)$ in P.

Definition 3 Let P be a bounded, free-cut free and free variable normal form proof in S_2^1. Let b be a variable occurring in P. The *bounding term* $tm(b; P)$ of b is inductively defined by:

1. $tm(b;P) = b$ if b is a parameter variable.

2. Otherwise, let I denote the unique elimination inference of b in P. For every free variable a, of which elimination inference appears below I, assume that $tm(a;P)$ is already defined. Note that I is one of

   Σ_1^b-PIND
   $$\frac{\Gamma, A(\lfloor \frac{1}{2}b \rfloor) \longrightarrow A(b), \Delta}{\Gamma, A(0) \longrightarrow A(u), \Delta}$$

   $(\forall \leq: right)$
   $$\frac{b \leq u, \Gamma \longrightarrow \Delta, C(b)}{\Gamma \longrightarrow \Delta, (\forall x \leq u)C(x)}$$

   or
   $(\exists \leq: left)$
   $$\frac{b \leq u, A(b), \Gamma \longrightarrow \Delta}{(\exists x \leq u)A(x), \Gamma \longrightarrow \Delta}.$$

   where $u = u(\vec{a})$. Since $\vec{a}$ occur free in u, either they are parameter variables or their elimination inferences appear below I.

   Define $tm(b;P) = u(\vec{a}/tm(\vec{a};P))$.

For a technical reason, we extend the language of S_2^1 by introducing a new set of free variables, b^k $(k = 0, 1, 2, \ldots)$. Intuitively, it means a free variable ranging over of length less than or equal to k. The elimination inference of b^k must be one of Σ_1^b-PIND, $((\forall \leq) : right)$ or $((\exists \leq) : left)$ as shown above. Furthermore, k must be greater or equal to the length of $u(\vec{a}/tm(\vec{a};P))$ so that k is large enough for b^k to be replaced by the term u.

Lemma 1 *Suppose that P is a free-cut free, free variable normal form S_2^1 proof of a bounded formula $A(\vec{a})$. When we replace every free variable b by $b^k (k = q_{tm(b;P)}(n))$, we again obtain a well-formed S_2^1 proof in the extended language.*

(Proof.) Obvious from the definition of $tm(b;P)$.

Lemma 2 *Let P be a bounded, free-cut free and free variable normal form proof in S_2^1, and b be a variable occurring in P. Suppose that the lengths of parameter variables are bounded by n. Then, b ranges over of length $\leq q_{tm(b;P)}(n)$ in P.*

Definition 4 Let P be a bounded, free-cut free and free variable normal form proof in S_2^1 and $A(\vec{b})$ be a formula in P. The *bounding polynomial* $q_{(A;P)}$ *of A in P*, is defined by q_{A^*} where $A^* = A(\vec{b}/tm(\vec{b};P))$.

We take a polynomial function $p(n)$ as the *bounding polynomial of P* so that it dominates all the bounding polynomials of formulas in P.

For example, we can define the *bounding polynomial* p of P as follows: suppose that each $q_{(A;P)}$ is in the form $d_A^k \cdot x^k + \cdots + d_A^1 \cdot x + d_A^0$. Then,

$$p(x) = c_m \cdot x^m + \cdots + c_1 \cdot x + c_0$$

is defined by

$$c_i = \max\{d_A^i | A \text{ is a formula in } P\}.$$

Lemma 3 *Let P be a bounded, free-cut free and free variable normal form proof in S_2^1 of which parameter variables are $a_1, \dots, a_k$, and Q be a subproof of P. Let p and q be the bounding polynomials of P and Q, respectively. Suppose that $|a_i| \leq n$ for all $1 \leq i \leq k$, and that $|b| \leq q_{tm(b;P)}(n)$ for every non-parameter variable b in the end-sequent of Q. Then,*

1. *P only refers to the numbers of which length is $\leq p(n)$.*

2. *$p(n) \geq q(n)$ for all n.*

It is known that there are fan-out 1 polynomial-size family of Boolean circuits for computing the function symbols of the language of S_2^1: for each function symbol f in S_2^1, there is a polynomial function p_f such that the circuit $[\![f]\!]_n$ takes one or two inputs of length n to computes the function f, and the size of $[\![f]\!]_n$ is bounded by $p_f(n)$. Since they are fan-out 1 Boolean circuits, they are readily translated into Boolean formulas.

It is also known that there are polynomial-size extended Frege proofs for the BASIC axioms of S_2^1. We pick a polynomial function p_b to dominate these polynomials. If P is a bounded S_2^1 proof and p is the bounding polynomial of P, the number of bits necessary for computation carried out throughout in P is bounded by $p(n)$, where n is the length of inputs.

We define, for each term t, a vector of m propositional formulas $[\![t]\!]_m^n$ giving the first m bits of the value of t when its free variables are assigned values of length $\leq n$.

Definition 5

1. $[\![0]\!]_m^n$ is a sequence of m false formulas (for example $p \wedge \neg p$).

2. If a^k is a variable with $k \leq m$, $[\![a^k]\!]_m^n$ is a sequence of $m - k$ false formulas followed by propositional variables $v_{k-1}^{a^k}, \dots, v_0^{a^k}$. If a^k is a variable with $k > m$, $[\![a^k]\!]_m^n$ is $v_{m-1}^{a^k}, \dots, v_0^{a^k}$.

3. If a is a variable (without subscript), Then, $[\![a]\!]_m^n$ is $[\![a^n]\!]_m^n$.

4. $[\![t+u]\!]_m^n$ is $[\![+]\!]_m([\![s]\!]_m^n, [\![t]\!]_m^n)$ (the formulas corresponding to the circuit for addition applied to the output of $[\![t]\!]_m^n$ and $[\![u]\!]_m^n$.)

5. $[\![s(t)]\!]_m^n$, $[\![\lfloor \frac{1}{2}t \rfloor]\!]_m^n$, $[\![\, |t| \,]\!]_m^n$, $[\![t \sharp u]\!]_m^n$ and $[\![t \cdot u]\!]_m^n$ are defined similarly.

Definition 6 A first order formula is in negation-implication normal form (*NINF*) if every negation is applied to an atomic subformula and there is no implication. For a bounded formula A in *NINF* and m, we define the propositional formula $[\![A]\!]_m^n$ inductively as follows:

1. $[\![t = u]\!]_m^n$ is $EQ_{m-1}([\![t]\!]_m^n, [\![u]\!]_m^n)$, where

$$EQ_{m-1}(\vec{p}, \vec{q}) = \bigwedge_{k=0}^{m-1} (p_k \leftrightarrow q_k).$$

2. $[\![t \leq u]\!]_m^n$ is $LE_{m-1}([\![t]\!]_m^n, [\![u]\!]_m^n)$, where

$$LE_{m-1}(\vec{p}, \vec{q}) = \bigvee_{k=0}^{m-1} (\neg p_k \wedge q_k \wedge \bigwedge_{k>j\geq 0} (p_j \leftrightarrow q_j)).$$

3. $[\![\neg A]\!]_m^n$ is $\neg [\![A]\!]_m^n$ for A atomic.

4. $[\![A \wedge B]\!]_m^n$ is $[\![A]\!]_m^n \wedge [\![B]\!]_m^n$

5. $[\![A \vee B]\!]^n_m$ is $[\![A]\!]^n_m \vee [\![B]\!]^n_m$

6. $[\![(\exists x \le t)A(x)]\!]^n_m$ is $[\![b^k \le t \wedge A(b^k)]\!]^n_m$, where t is not of the form $|s|$ and b^k is a new free variable such that $k = q_t(n)$. b is called a *quantifier variable*

7. $[\![(\forall x \le t)A(x)]\!]^n_m$ is $[\![\neg b^k \le t \vee A(b^k)]\!]^n_m$,where t is not of the form $|s|$ and b^k is a new free variable such that $k = q_t(n)$. b is called a *quantifier variable.*

8. $[\![(\exists x \le |t|)A(x)]\!]^n_m$ is $\bigvee_{k=0}^{m-1} [\![\bar{k} \le |t| \wedge A(\bar{k})]\!]^n_m$, where $\bar{k}$ is a term with value k and length $\simeq \log k$.

9. $[\![(\forall x \le |t|)A(x)]\!]^n_m$ is $\bigwedge_{k=0}^{m-1} [\![\neg \bar{k} \le |t| \vee A(\bar{k})]\!]^n_m$.

For a sequent $A \to B$, we define $[\![A \to B]\!]^n_m$ by $[\![A]\!]^n_m \supset [\![B]\!]^n_m$.

Suppose that a given formula B occurs positively (resp. negatively) in an S^1_2 proof, P. We assign quantifier variables $\epsilon^b_0, \epsilon^b_1, \ldots$ (for an existential variable x) and $\mu^d_0, \mu^d_1, \ldots$ (for an universal variable y) to B so that we will assign different sequences of quantifier variables for x to distinct positive (resp. negative) occurrences of B in P but all positive (resp. negative) occurrences of B use the same sequence of quantifier variables for y.

Proposition 4 *For any bounded formula A, the propositional formula* $[\![A]\!]^n_m$ *is polynomial-size in* m, n.

3 Main theorem

For the time being, we extend the use of extension inference. A free variable p introduced by an extension rule, $p \leftrightarrow \phi$, can occur in the end-formula (sequent).

When p occurs in the end-formula ψ, we can transform it to a valid eF-proof by substituting every occurrence of p by ϕ.

Theorem 1 *Suppose that* $A(\vec{a^n})$ *is a bounded formula in* S^1_2 *and* $S^1_2 \vdash A(\vec{a^n})$. *Let* P *be a free-cut free, free variable normal form* S^1_2 *proof of* A *and* m *be the number of lines in* P. *Then, there are* eF*-proofs of* $[\![A]\!]^n_{q(n)}$ *where* $q(n)$ *is the bounding polynomial of* P. *The size of the proofs are bounded by* $c \cdot m \cdot q(n) \cdot p_b(n)$ *for some constant* c.

Replace every free variable b occurring in P by b^k, where $k = q_{tm(b;P)}(n)$. We still have a well-formed S^1_2 proof. In [6], they intend to show that for each sequent $A_1, \ldots, A_k \longrightarrow B_1, \ldots, B_l$ in P and for any n and $m > q(n)$, there is a polynomial-size eF-proof of $[\![A_1 \wedge \ldots \wedge A_k \to B_1 \vee \ldots \vee B_l]\!]^n_m$ by the induction of the number of proof lines of P. Intuitively, n stands for the length of inputs and m for the number of bits necessary for the computation. They let n and m vary as occasion demands in each induction step, however, it is not suggested how to assign numbers to n or m. It is quite vague why the whole translation procedure terminated in polynomial-time; unsuitable assignment of n or m can increase the size of the resulting eF proofs exponentially.

Our direct translation use a much simpler induction hypothesis: both n and m remain unchanged throughout in the proof. It helps clarifying the underlying situation.

(Proof of the main theorem.)

Base case:
Logical axioms and equality axioms: Straightforward.

Basic axioms of S_2^1: For each basic axiom, there are extended Frege proofs of size bounded by $p_b(n)$.

Induction step:

Case 1 ($\neg$-*right*) Suppose P ends with

$$\frac{\Gamma \longrightarrow \Delta, B}{\neg B, \Gamma \longrightarrow \Delta},$$

where B is atomic. By the induction hypothesis, there is a polynomial-size eF-proof of $[\![\Gamma \rightarrow \Delta \vee B]\!]^n_{q(n)}$. Note that $[\![\Gamma \rightarrow \Delta \vee B]\!]^n_{q(n)}$ is $[\![\Gamma]\!]^n_{q(n)} \supset [\![\Delta]\!]^n_{q(n)} \vee [\![B]\!]^n_{q(n)}$. From this, we can easily infer $[\![\neg B]\!]^n_{q(n)} \wedge [\![\Gamma]\!]^n_{q(n)} \supset [\![\Delta]\!]^n_{q(n)}$ in eF.

Case 2($\neg$-*left*) Similar to case 1.

Case 3($\vee$-*right*) Suppose P ends with

$$\frac{\Gamma \longrightarrow B, \Delta}{\Gamma \longrightarrow B \vee C, \Delta}.$$

By the induction hypothesis, there is a polynomial-size eF-proof of $[\![\Gamma \rightarrow B \vee \Delta]\!]^n_{q(n)}$. By definition, this is $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)} \vee [\![\Delta]\!]^n_{q(n)}$. From this, we can easily infer in eF that $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)} \vee [\![C]\!]^n_{q(n)} \vee [\![\Delta]\!]^n_{q(n)}$, which is $[\![\Gamma \rightarrow (B \vee C) \vee \Delta]\!]^n_{q(n)}$.

Case 4: ($\wedge$-*right*) Similar to case 3.

Case 5: (Structural rule) A structural rule is one of a weakening inference, an exchange inference and a contraction. If it is either a weakening or exchange, it is easy.
(Contraction)

$$\frac{\Gamma \longrightarrow B, B, \Delta}{\Gamma \longrightarrow B, \Delta}.$$

By induction hypothesis, there is a polynomial-size eF-proof of $[\![\Gamma \rightarrow B \vee B \vee \Delta]\!]^n_{q(n)}$, which is $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)} \vee [\![B]\!]^n_{q(n)} \vee [\![\Delta]\!]^n_{q(n)}$. If a (not sharply) bound variable x occurs in B, it is replaced by different quantifier variables b and c in the first and second occurrences of $[\![B]\!]^n_{q(n)}$, respectively. Suppose that $[\![b]\!]^n_m = \mu_{m-1}, \ldots, \mu_0$ and $[\![c]\!]^n_m = \nu_{m-1}, \ldots, \nu_0$. For each k, we introduce a new variable η_k by an extension rule:

$$\eta_k \leftrightarrow (([\![B]\!]^n_{q(n)}(\vec{\mu})) \wedge \mu_k) \vee (\neg([\![B]\!]^n_{q(n)}(\vec{\mu})) \wedge \nu_k).$$

Then, prove $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)}(\vec{\eta}) \vee [\![\Delta]\!]^n_{q(n)}$ from $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)}(\vec{\mu}) \vee [\![B]\!]^n_{q(n)}(\vec{\nu}) \vee [\![\Delta]\!]^n_{q(n)}$. $[\![\Gamma]\!]^n_{q(n)} \supset [\![B]\!]^n_{q(n)}(\vec{\eta}) \vee [\![\Delta]\!]^n_{q(n)}$ is $[\![\Gamma \rightarrow B \vee \Delta]\!]^n_{q(n)}$.

Case 6: ($\wedge$-*right*) Suppose P ends with

$$\frac{\Gamma \longrightarrow B, \Delta \quad \Gamma \longrightarrow C, \Delta}{\Gamma \longrightarrow B \wedge C, \Delta}.$$

We separate this inference into two steps:

$$\cfrac{\cfrac{\Gamma \longrightarrow B, \Delta \quad \Gamma \longrightarrow C, \Delta}{\Gamma, \Gamma \longrightarrow B \wedge C, \Delta, \Delta}}{\Gamma \longrightarrow B \wedge C, \Delta}$$

By the induction hypothesis, there are polynomial-size eF-proofs of $[\![\Gamma \longrightarrow B, \Delta, \Delta]\!]^n_{q(n)}$ and $[\![\Gamma \longrightarrow C, \Delta]\!]^n_{q(n)}$. From them, we can conclude $[\![\Gamma, \Gamma \longrightarrow B \wedge C, \Delta, \Delta]\!]^n_{q(n)}$ easily in eF. The rest is treated as in case 5.

Case 7:($\vee$-*left*) Similar to case 6.

Case 8:(($\exists \leq$)-*right*)

Case 8.a: (*sharply bounded*) Suppose that P ends with

$$\frac{\Gamma \longrightarrow B(s), \Delta}{s \leq |t|, \Gamma \longrightarrow (\exists x \leq |t|)B(x), \Delta}.$$

By induction hypothesis, there is a polynomial-size proof of $[\![\Gamma \rightarrow B(s) \vee \Delta]\!]^n_{q(n)}$. $[\![(\exists x \leq |t|)B(x) \vee \Delta]\!]^n_{q(n)}$ is $\bigvee_{m=0}^{q(n)-1} [\![\bar{m} \leq |t| \wedge B(\bar{m})]\!]^n_{q(n)}$ by the definition. Let $\vec{b}$ denote the quantifier variables occurring in $B(s)$. Let $\vec{c}$ be the free variables in t and $\vec{u}$ be bounding terms of $\vec{c}$ in P. Define $k = q_{|t|(\vec{c}/\vec{u})}(n)$. Then, the length of $|t|$ does not exceed k. For each $0 \leq m \leq k$, there are short eF-proofs of

$$[\![s = \bar{m}]\!]^n_{q(n)} \supset ([\![B(s)]\!]^n_{q(n)}(\vec{b_m}/\vec{b}) \leftrightarrow [\![B(\bar{m})]\!]^n_{q(n)}),$$

where $\vec{b_m}$ are quantifier variables used in $B(\bar{m})$. Combining these, we get eF-proofs of

$$[\![\Gamma]\!]^n_{q(n)} \supset \bigwedge_{m=0}^{k} [\![\neg(\bar{m} \leq |t|) \vee B(\bar{m}) \vee \Delta]\!]^n_{q(n)}.$$

There are simple eF-proofs of $\neg(\bar{m} \leq |t|)$ for all $m \geq k$. Hence, we have $(\neg(\bar{m} \leq |t|) \vee B(\bar{m}) \vee \Delta) \leftrightarrow \Delta$ for $m \geq k$. Now we are ready to conclude

$$[\![s \leq |t| \wedge \Gamma]\!]^n_{q(n)} \supset \bigvee_{m=0}^{q(n)-1} [\![(\bar{m} \leq |t| \wedge B(\bar{m})) \vee \Delta]\!]^n_{q(n)}.$$

Use contraction to get

$$[\![s \leq |t| \wedge \Gamma \rightarrow (\exists x \leq |t|)B(x) \vee \Delta]\!]^n_{q(n)}.$$

Case 8.b (*not sharply bounded*) Suppose P ends with

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

By induction hypothesis, there is a polynomial-size eF-proof of $[\![\Gamma \rightarrow B(s) \vee \Delta]\!]^n_{q(n)}$. Let $\vec{c}$ be the free variables in t and $\vec{u}$ be bounding terms of $\vec{c}$ in P. Define $k = q_{t(\vec{c}/\vec{u})}(n)$. Then, the length of t does not exceed k in P. Let b be the quantifier variable used in the place of x in $(\exists x \leq t)B(x)$.

$$[\![b]\!]^n_{q(n)} = \underbrace{\bot, \ldots, \bot}_{q(n)-k}, \mu_{k-1}, \ldots, \mu_0,$$

where $\bot$ is an abbreviation for a false formula. Let ϕ^s_i be the formula giving the i^{th}-bit of s. We form the desired eF-proof as follows:

1. The definition of $\mu_i \leftrightarrow \phi^s_i$ for $0 \leq i \leq k-1$ and $\mu_j \leftrightarrow \bot$ for $k \leq j \leq q(n)-1$ by extension.

2. Derive $[\![s \le t \wedge \Gamma \to ((s \le t) \wedge B(s)) \vee \Delta]\!]^n_{q(n)}$ from $[\![\Gamma \to B(s) \vee \Delta]\!]^n_{q(n)}$.
3. Derive $[\![s \le t \wedge \Gamma \to ((b \le t) \wedge B(b)) \vee \Delta]\!]^n_{q(n)}$ by replacing some of ϕ^s_i and $\perp$ by μ_i according to the value of i.

Case 9: ($(\forall \le)$-*left*) Similar to case 8.

Case 10: ($(\forall \le)$-*right*)
In case 10, a^k is used as an eigenvariable in a bounded quantifier inference $(\forall x \le t)$. Note that lemma 1 guarantees that k is large enough to cover the range of the term t.

Case 10.a: (*Sharply bounded*) Suppose P ends with the inference

$$\frac{a^k \le |t|, \Gamma \longrightarrow B(a^k), \Delta}{\Gamma \longrightarrow (\forall x \le |t|)B(x), \Delta}.$$

where $k = q_{tm(a^k;P)}(n)$. By the induction hypothesis, there is a polynomial-size eF-proof $[\![a^k \le |t| \wedge \Gamma \to B(a^k) \vee \Delta]\!]^n_{q(n)}$. From them easily obtained $[\![\Gamma]\!]^n_{q(n)} \supset [\![a^k \le |t| \supset B(a^k)]\!]^n_{q(n)} \vee [\![\Delta]\!]^n_{q(n)}$. For $m \le q(n) - 1$, let $\phi^{\bar{m}}_i$ be the formula giving the i^{th}-bit of the natural number m. Use extension rule to replace $v^{a^k}_i$ by $\phi^{\bar{m}}_i$ for every $0 \le i \le k$ in $[\![a^k \le |t| \wedge \Gamma \to B(a^k) \vee \Delta]\!]^n_{q(n)}$. Then, we obtain $[\![\bar{m} \le |t| \wedge \Gamma \to B(\bar{m}) \vee \Delta]\!]^n_{q(n)}$. Combining these, we get eF-proofs of

$$[\![\Gamma]\!]^n_{q(n)} \supset \bigwedge_{m=0}^{q(n)-1} [\![\neg(\bar{m} \le |t|) \vee B(\bar{m})) \vee \Delta]\!]^n_{q(n)}.$$

Hence, we have

$$[\![\Gamma]\!]^n_{q(n)} \supset \bigwedge_{m=0}^{q(n)-1} [\![(\bar{m} \le |t| \to B(\bar{m})) \vee \Delta]\!]^n_{q(n)}.$$

Use the method in case 3 to contract multiple occurrences of Δ's and get

$$[\![\Gamma \to (\forall x \le |t|)B(x) \vee \Delta]\!]^n_{q(n)}.$$

Case 10.b (*Nonsharply bounded*) Suppose P ends with

$$\frac{a^k \le t, \Gamma \longrightarrow B(a^k), \Delta}{\Gamma \longrightarrow (\forall x \le t)B(x), \Delta},$$

where $k = q_{tm(a^k;P)}(n)$. By the induction hypothesis, there is a polynomial-size eF-proof of $[\![a^k \le t \wedge \Gamma \to B(a^k) \vee \Delta]\!]^n_{q(n)}$. From this easily obtained $[\![\Gamma \to \neg(a^k \le t) \vee B(a^k) \vee \Delta]\!]^n_{q(n)}$. Since P is free variable normal form, the eigenvariable a^k appears only as indicated above. Infer

$$[\![\Gamma]\!]^n_{q(n)} \supset ([\![\neg(a^k \le t) \vee B(a^k)]\!]^n_{q(n)} \vee [\![\Delta]\!]^n_{q(n)}),$$

which is

$$[\![\Gamma \to (\forall x \le t)B(x) \vee \Delta]\!]^n_{q(n)}.$$

Case 11: (($\exists \leq$)-*left*) Similar to case 10.

Case 12: (Cut) Suppose P ends with

$$\frac{\Gamma \longrightarrow \Delta, B \quad B, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Lambda, \Delta}.$$

Note that B must be Σ_1^b. Without loss of generality, we can assume that $B = (\exists x \leq t)C(x)$, where C is Σ_0^b. Let $\vec{c}$ be the free variables in t and $\vec{u}$ be bounding terms of $\vec{c}$ in P. Define $k = q_{t(\vec{c}/\vec{u})}(n)$. Then, the length of t does not exceed k. By the induction hypothesis, there are polynomial-size proofs of $[\![\Gamma \to \Delta \vee B]\!]^n_{q(n)}$ and $[\![B \wedge \Pi \to \Lambda]\!]^n_{q(n)}$. Now suppose that $[\![B]\!]^n_{q(n)}$ in $[\![\Gamma \to \Delta \vee B]\!]^n_{q(n)}$ has quantifier variable b and $[\![B]\!]^n_{q(n)}$ in $[\![B \wedge \Pi \to \Lambda]\!]^n_{q(n)}$ has quantifier variable d for the same bound variable x. We can assume that $[\![b]\!]^n_{q(n)} = \underbrace{\bot, \ldots, \bot}_{q(n)-k}, \mu^b_{k-1}, \ldots, \mu^b_0$. Since d is introduced by extension as in case 11: there is an ($\exists \leq$)-*left* inference I in P such that

$$\frac{a \leq t, C(a), \Gamma \longrightarrow \Delta}{(\exists x \leq t)C(x), \Gamma \longrightarrow \Delta}\, I$$

and that a is an eigenvariable of I and $[\![a]\!]^n_{q(n)} = \underbrace{\bot, \ldots, \bot}_{q(n)-k}, v^a_{k-1}, \ldots, v^a_0$. Then, replace v^a_i by μ^b_i. Now we have the same translation of B in its left and right occurrences, and we are ready to make a cut inference in eF. We obtain a polynomial-size eF-proof of $[\![\Gamma \wedge \Pi \to \Lambda \vee \Delta]\!]^n_{q(n)}$. Here, it is crucial that the cut-formula is Σ_1^b.

Case 13: (Σ_1^b-PIND) Suppose P ends with

$$\frac{B(\lfloor \frac{1}{2} b^k \rfloor), \Gamma \longrightarrow \Delta, B(b^k)}{B(0), \Gamma \longrightarrow \Delta, B(t)}\, I$$

where $k = q_{tm(b^k;P)}$. Let By lemma 1, the length of t does not exceed k. Suppose that ϕ^t_i ($i < k$) is a formula giving the i^{th}-bit of t. (For $i \geq k$, set $\phi^t_i \leftrightarrow \bot$.) Use extension rule to replace $v^{b^k}_i$ by ϕ^t_{i-j} for $0 \leq j \leq k$. Then, we obtain

$$[\![B(\lfloor \frac{t}{2^{j+1}} \rfloor) \wedge \Gamma \to \Delta \vee B(\lfloor \frac{t}{2^j} \rfloor)]\!]^n_{q(n)}.$$

Combining these together by cut inferences, and using the technique in case 12, we obtain

$$[\![B(0) \wedge \Gamma \to \Delta, B(t)]\!]^n_{q(n)}.$$

□

We can shrink the size of the end-sequent of eF proofs by deleting the contents of unnecessary higher bits.

Lemma 4 *Let A be a bounded formula in S^1_2 For every $m \geq q_A(n)$, there is a simple proof of*

$$[\![A]\!]^n_{q(n)} \supset [\![A]\!]^n_m.$$

Corollary 1 *Suppose that $A(\vec{a^n})$ is a bounded formula in S^1_2 and $S^1_2 \vdash A(\vec{a^n})$. Let P be a free-cut free, free variable normal form S^1_2 proof of $A(\vec{a})$ and m be the number of lines in P. Then, there are eF-proofs of $[\![A]\!]^n_{q_A(n)}$. The size of the proofs are bounded by $c \cdot m \cdot q(n) \cdot p_b(n)$ for some constant c.*

4 Translation of other bounded arithmetic to propositional calculi

We can extend our technique to translate bounded proofs of other bounded arithmetic to polynomial size propositional proofs.

In the translation given in the previous section, the crutial reason why we needed eF but not Frege to translate S^1_2 proofs was that we cannot literally translate non-sharply bounded formulas in S^1_2 to polynomial-size propositional formulas. Unlike sharply bounded quantifiers which are ready to be translated into polynomial-size conjunctions or disjunctions of propositional formulas,non-sharply bounded quantifiers require a superpolynomial function, $n^{O(\log n)}$, to be expressed as conjunctions and disjunctions. To avoid $n^{O(\log n)}$, we have to pick an instance s satisfying $s \leq t \wedge A(s)$ to express $(\exists x \leq t)A(x)$, that requires us to introduce the use of extension. That means every bounded S^0_2 proofs are translatable to polynomial-size Frege proofs. (By choozing appropriate language, it is translatable to polynomial-size bounded depth Frege proofs.)

It is also quite clear that every bounded T^1_2 proofs are translatable to eF proofs of size $n^{O(\log n)}$. The reason why it reqires $n^{O(\log n)}$ is that Σ^b_1-IND is decomposed to $n^{O(\log n)}$-many but not polynomially-many cuts.

The same technique also can be used to extend the result in [15].

Corollary 2 *Let $i \geq 1$ and $A(\vec{a})$ be a bounded formula. Assume that*

$$T^i_2 \vdash A(\vec{a}).$$

Then, there is a polynomial function p such that if every parameter variables of A has the length $\leq n$, and $\|A\|^{p(n)}_n$ has polynomial-size G_i-proofs.

Corollary 3 *Let $i \geq 1$ and $A(\vec{a})$ be a bounded formula. Assume that*

$$S^i_2 \vdash A(\vec{a}).$$

Then, there is a polynomial function p such that if every parameter variables of A has the length $\leq n$, and $\|A\|^{p(n)}_n$ has polynomial-size G^*_i-proofs.

References

[1] M. Ajtai, "Σ^1_1-formulae on finite structures", *Annals of Pure and Applied Logic*, Vol.24 (1983) 1-48.

[2] M. Ajtai, "The complexity of the pigeonhole principle", *29th Annual Symposium on the Foundations of Computer Science* (1988) 346-55.

[3] N. H. Arai, "Translation of S^1_2 proofs into polynomial-size extended Frege proofs", *submitted.*

[4] T. Arai, "Frege system, ALOGTIME and bounded arithmetic", manuscript (1991).

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

[6] S. R. Buss et al., *Weak Formal Systems and Connections to Computational Complexity*, Student-written lecture notes for topics course at U.C.Berkley, January-May, 1988.

[7] S. R. Buss, "Relating the bounded arithmetic and polynomial time hierarchies, *Annals of Pure and Applied Logic*, Vol.75 (1995) 67-77.

[8] P. Clote, "On polynomial size Frege proofs of certain combinatorial principles", in *Arithmetic, Proof Theory, and Computational Complexity*, Clarendon Press, Oxford (1993) 162-84.

[9] S. A. Cook, "Feasibly constructive proofs and the propositional calculus", *Proc. 7th A.C.M. Symposium on the Theory of Computation* (1975) 83-97.

[10] S. A. Cook, "Relating the provable collaspe of P to NC^1 and the power of logical theories", *preprint* (1996).

[11] S. A. Cook and R. Reckhow, "On the lengths of proofs in the propositional calculus", *Proc. 6th ACM Symposium on Theory of Computing* (1974) 135-148.

[12] S. A. Cook and R. A. Reckhow, "The relative efficiency of propositional proof systems", *J. Symbolic Logic*, Vol.44 (1979) 36-50.

[13] J. T. Håstad *Computational Limitaions for Small-Depth Circuits*, The MIT Press, Cambridge, London, 1986.

[14] M. Kikuchi, "On Buss and Turán's extensions of Haken's results", preprint.

[15] J. Krajíček and P. Pudlák, "Quantified propositional calculus and fragments of bounded arithmetic", *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, Vol.36 (1990) 29-46.

[16] J. Krajíček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge University Press, Cambridge, 1995.

[17] J. Krajíček, P. Pudlák and G. Takeuti, "Bounded arithmetic and the polynomial hierarchy", *Annals of Pure and Applied Logic*, Vol.52 (1991) 143-153.

[18] J. Paris and A. Wilkie, "Counting problems in bounded arithmetic", in: *Methods in Mathematical Logic*, Lecture Notes in Mathematics Vol.1130 (Springer, Berlin, 1985) 317-340.

[19] J. B. Paris, A. J. Wilkie and A. R. Woods, "Provability of the pigeonhole principle and the existence of infinitely many primes", *Journal of Symbolic Logic*, Vol.53 (1988) 1235-44.

[20] L. J. Stockmeyer, "The polynomial-time hierarchy", *Theoretical Computer Science*, Vol.3 (1976) 1-22.

[21] A. Woods, "Some problems in logic and number theory and their connections", Ph.D. Thesis, Manchester University (1981).

[22] A. Yao, "Separating the polynomial-time hierarchy by oracles", *Proc. 26th Annual IEEE Symposium on Foundation of Computer Science* (1985) 1-10.