Weak Theories of Arithmetic for Computational Complexity: A Gentle Introduction

Sendai Logic Seminar, May 2, 2012, Tohoku University

Naohi Eguchi

Mathematical Institute, Tohoku University, Japan
eguchi@math.tohoku.ac.jp

Abstract. In this talk we will discuss about proof-theoretic approaches to computational complexity in terms of weak theories of arithmetic as known as theories of *bounded arithmetic*, which was initiated by Samuel Buss. We will start with classical facts on primitive recursive functions, and then go into discussion about polynomial time functions and polynomial space functions, including a recent challenge by the speaker.

1 Introduction

One goal in computational complexity theory is to classify problems, predicates or functions depending on their intrinsic computational difficulty. Given a problem, it is natural to ask how much computing resources we need to solve it. To date we have made much progress in classifying problems into *complexity classes*. The class **P** of problems decidable in polynomial time has been accepted as the most central complexity class along with a crucial open question "$\mathbf{P} \neq \mathbf{NP}$?". The class **PSPACE** of problems decidable in polynomial space is known together with another crucial open question "$\mathbf{P} \neq \mathbf{PSPACE}$?".

Machine-independent approaches to computational complexity have been developed characterising complexity classes by conceptual measures from proof theory. The proof-theoretic approaches to computational complexity started with introduction of a first order theory S^1_2 of *bounded arithmetic*, which characterises the class **P**, by S. Buss in [2]. In [2] a second order theory U^1_2 of bounded arithmetic, which characterises the class **PSPACE** is also introduced. More recently, in [5] A. Skelley introduces a third order theory W^1_1 of bounded arithmetic, or more precisely a three sorted theory in the sense of S. Cook and P. Nguyen [4], which characterises the class **PSPACE**. In a draft [1] Toshiyasu Arai[1] and the speaker propose a new second order theory $T^{1,\mathsf{seq}}_2$ of bounded arithmetic for the class **PSPACE**. This talk aims to give a brief introduction to theories S^1_2 and $T^{1,\mathsf{seq}}_2$. Mostly we will follow notations and conventions given in the chapter [3] by S. Buss of "Handbook of Proof Theory".

[1] Graduate School of Science, Chiba University, Japan.

2 A classical proof-theoretic characterisation of primitive recursive function

We start with a classical proof-theoretic characterisation of the class of primitive recursive functions. We assume reader's familiarity with standard first order theories of arithmetic. In particular we assume that the languages of these theories contain the constant symbol 0 and the successor function symbol S. For every natural number m we will write $\underline{m}$ to denote the term $S^m(0)$. Let $\mathrm{I}\Sigma_i$ denote the fragment of Peano arithmetic PA with induction restricted to Σ^0_i-formulas. For a class Φ of formulas, let Φ-IND denote the schema of induction with respect to a Φ-formula A:

$$A(0) \wedge \forall x(A(x) \to A(S(x))) \to \forall x A(x) \qquad (\Phi\text{-IND})$$

Definition 1. *Let T be a theory of arithmetic such that $\mathrm{I}\Sigma_1 \subseteq T$, Φ a set of formulas, $k \geq 0$ a natural number, and $f : \mathbb{N}^k \to \mathbb{N}$ be a k-ary function. Then, we say f is* Φ-definable in T *if there exists a formula $A_f(x_1, \ldots, x_k, y) \in \Phi$ which enjoys the following conditions.*

1. *All free variables appearing in $A_f(x_1, \ldots, x_k, y)$ are indicated.*
2. *For all $\boldsymbol{m} = m_1, \ldots, m_k, n \in \mathbb{N}$, $n = f(\boldsymbol{m})$ holds if and only if $\mathbb{N} \models A_f(\underline{\boldsymbol{m}}, \underline{n})$, where $\mathbb{N}$ denotes a standard model of theories of first order arithmetic.*
3. *$T \vdash \forall \boldsymbol{x} \exists! y A_f(\boldsymbol{x}, y)$, where $\boldsymbol{x} = x_1, \ldots, x_k$.*

Theorem 1 (Parsons '70, Mints '73, Buss [2] and Takeuti '87). *A function f is Σ^0_1-definable in $\mathrm{I}\Sigma_1$ if and only if f is primitive recursive.*

3 A first order theory S^1_2 of bounded arithmetic for P

First order theories of bounded arithmetic are defined over the first order predicate logic. For definitions we follow Buss [3]. We fix the language $\mathcal{L}^b_A$ of these theories as follows. The logical symbols of $\mathcal{L}^b_A$ consist of the usual first-order symbols, including propositional connectives, quantifiers and the equality $=$. The non-logical symbols of $\mathcal{L}^b_A$ include 0, S, $+$, $\cdot$, and $\leq$. Further $\mathcal{L}^b_A$ includes a unary function symbol $\lfloor \frac{x}{2} \rfloor$ for division by 2, a unary function symbol $|x|$ for the function such that $|x| = \lceil \log_2(x+1) \rceil$, and a binary function symbol $\#$ for the smash function $x \# y = 2^{|x| \cdot |y|}$.

A *bounded quantifier* is of the form $\forall x(x \leq t \to \cdots)$ or $\exists x(x \leq t \wedge \cdots)$ for some term t not involving x. These can be abbreviated as $(\forall x \leq t)(\cdots)$ and $(\exists x \leq t)(\cdots)$, respectively. A usual quantifier is called an unbounded quantifier. A *sharply bounded quantifier* is of the form $(Qx \leq |t|)(\cdots)$ for some $Q \in \{\forall, \exists\}$ and for some term t.

The non-logical axioms of theories of bounded arithmetic include the set BASIC of *basic* axioms. The set BASIC consists of axioms which define each

function and predicate symbol in $\mathcal{L}_A^b$. For the detailed definition of BASIC, we kindly refer the readers to Buss [3].

Theories of bounded arithmetic are defined by imposing some constrains on variations of induction schemes in such a way that induction is allowed only for formulas from specific sets Σ_i^b or Π_i^b $(i \geq 0)$. Let $i \geq 0$. The sets Σ_i^b and Π_i^b $(i \geq 0)$ of formulas are simultaneously defined as follows.

1. $\Sigma_0^b := \Pi_0^b$ is the set of formulas in which all quantifiers are sharply bounded.
2. The set Σ_i^b is closed under $\vee$ and $\wedge$.
3. If $A \in \Pi_i^b$ and $B \in \Sigma_i^b$, then $\{A \to B, \neg A\} \subseteq \Sigma_i^b$.
4. $\Pi_i^b \subseteq \Sigma_{i+1}^b$.
5. If $A \in \Sigma_i^b$ and t is a term, then $\{(\forall x \leq |t|)A, (\exists x \leq |t|)A\} \subseteq \Sigma_i^b$.
6. If $A \in \Sigma_i^b$ and t is a term, then $(\exists x \leq t)A \in \Sigma_i^b$.
7. The set Π_i^b is defined dually to Σ_i^b.

Definition 2. $T_2^i = \mathsf{BASIC} + \Sigma_i^b\text{-}\mathsf{IND}$. $(i \geq 0)$

In contrast to the Φ-IND schema, Φ-PIND is the schema, for a Φ-formula A,

$$A(0) \wedge \forall x(A(\lfloor \tfrac{x}{2} \rfloor) \to A(x)) \to \forall x A(x). \qquad (\Phi\text{-}\mathsf{PIND})$$

Definition 3. $S_2^i = \mathsf{BASIC} + \Sigma_i^b\text{-}\mathsf{PIND}$. $(i \geq 0)$

Theorem 2 (Buss [2]). *For all $i \geq 0$, $T_2^i \subseteq S_2^{i+1} \subseteq T_2^{i+1}$.*

Let us extend Definition 1 by replacing "$\mathrm{I}\Sigma_1 \subseteq T$" by "$S_2^1 \subseteq T$".

Theorem 3 (Buss [2]). *A function f is Σ_1^b-definable in S_2^1 if and only if f is polynomial time computable.*

This theorem can be generalised to each level of the polynomial hierarchy. Let $\mathbf{FP}$ denote the class of functions computable in polynomial time and $\Sigma_i^{\mathbf{P}}$ denote the i-th class of the polynomial hierarchy, i.e., $\Sigma_0^{\mathbf{P}} = \mathbf{P}$, $\Sigma_1^{\mathbf{P}} = \mathbf{NP}, \ldots$. Then a hierarchy $\square_i^{\mathbf{P}}$ $(i \geq 0)$ is defined by $\square_0^{\mathbf{P}} = \mathbf{FP}$ and $\square_{i+1}^{\mathbf{P}}$ is the class of functions computable in polynomial time using oracles from $\Sigma_{i+1}^{\mathbf{P}}$, i.e, $\square_i^{\mathbf{P}} = \mathbf{FP}^{\Sigma_i^{\mathbf{P}}}$.

Remark 1. $\bigcup_{i \geq 0} \Sigma_i^{\mathbf{P}} \subseteq \mathbf{PSPACE}$.

Theorem 4 (Buss [2]). *For every $i \geq 0$ a function f is Σ_i^b-definable in S_2^i if and only if f belongs to $\square_i^{\mathbf{P}}$.*

Corollary 1. *For every $i \geq 0$ a predicate (or equivalently a problem) is Δ_i^b-definable in S_2^i if and only if it belongs to $\Sigma_i^{\mathbf{P}}$.*

4 Why second order notions for PSPACE?

Let **FPS** denote the class of functions computable in polynomial space. Thanks to the following fact, we can discuss about classes **FP** and **FPS** of functions instead of classes **P** and **PSPACE** of problems.

Fact 1 $\mathbf{FP} \neq \mathbf{FPS} \Longleftrightarrow \mathbf{P} \neq \mathbf{PSPACE}$.

In cantrast to a (possible) gap between **P** and **NP**, it is known **PSPACE** = **NPSPACE**. W. Savitch's proof of this fact is based on an observation that **PSPACE** computations allow computation sequences of exponential lengths. However the exponential is an *infinitary* notion in first order bounded arithmetic. Hence, in order to capture **PSPACE** computations, it is natural to extend first order theories S^i_2 and T^i_2 of bounded arithmetic to second order ones, cf. Fig. 1.

	Polynomials	Exponentials
Predicativity	Predicative	Impredicative
Model Theory	Standard	Nonstandard
1st order Bounded Arithmetic	finite	infinite
2nd order Bounded Arithmetic	1st order elements	2nd order elements

Fig. 1. Relationship between polynomials and exponentials.

5 A new second order theory $T^{1,\mathsf{seq}}_2$ for PSPACE

We extend the language $\mathcal{L}^b_A$ to $\mathcal{L}^{\mathsf{seq}}_A$ by adding second order variables $X, Y, Z, \ldots$, a function constant $\emptyset$, a unary function symbol $|\cdot|$, binary function symbols $\cdot(\cdot)$ and App. We write $\mathcal{T}(\mathcal{L})$ denote the set of all the terms over a language $\mathcal{L}$.

Definition 4. *The set $\mathcal{T}(\mathcal{L}^{\mathsf{seq}}_A)$ of $\mathcal{L}^{\mathsf{seq}}_A$ terms is partitioned into $\mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$ and $\mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$. The sets $\mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$ and $\mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$ of terms simultaneously as follows.*

1. $\mathcal{T}(\mathcal{L}^b_A) \subseteq \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$.
2. *If $f \in \mathcal{L}^b_A$ is a function symbol of arity k and $t_1, \ldots, t_k \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$, then $f(t_1, \ldots, t_k) \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$.*
3. *$X \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$ for each second order variable X.*
4. *$\emptyset \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$.*
5. *If $U \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$, then $|U| \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$.*
6. *If $t \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$ and $U \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$, then $U(t) \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$.*
7. *If $U \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$ and $t \in \mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$, then $\mathsf{App}(t, U) \in \mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$.*

We use $s, t, \ldots$ to denote elements of $\mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$ while $U, V, W, \ldots$ to denote elements of $\mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$. Intuitively, each element of $\mathcal{T}^b(\mathcal{L}^{\mathsf{seq}}_A)$ denotes a natural number while each element of $\mathcal{T}^{\mathsf{seq}}(\mathcal{L}^{\mathsf{seq}}_A)$ denotes a finite sequence of natural numbers. More precisely, we extend a standard semantic $\cdot^{\mathbb{N}}$ for closed terms in $\mathcal{T}(\mathcal{L}^b_A)$ to a semantic for closed terms in $\mathcal{T}(\mathcal{L}^{\mathsf{seq}}_A)$ as follows.

Definition 5. *We assume a primitive recursive sequencing of natural numbers:* $(m_0, \ldots, m_{l-1}) \mapsto \langle m_0, \ldots, m_{l-1}\rangle$. *Let* $^\frown$ *denote the concatenation with respect to this sequencing, i.e.,* $\langle m_0, \ldots, m_{l-1}\rangle^\frown\langle n_0, \ldots, n_{l'-1}\rangle$ *denote the sequence* $\langle m_0, \ldots, m_{l-1}, n_0, \ldots, n_{l'-1}\rangle$

1. $\emptyset^{\mathbb{N}} := \langle\rangle$.
2. $\mathsf{App}(t, U)^{\mathbb{N}} := U^{\mathbb{N}\frown}\langle t^{\mathbb{N}}\rangle$.
3. $|U|^{\mathbb{N}} = l$*: the length of the sequence* $U^{\mathbb{N}} = \langle m_0, \ldots, m_{l-1}\rangle$.
4. $U(t)^{\mathbb{N}} = m_{t^{\mathbb{N}}}$*: the* $t^{\mathbb{N}}$*-th entry of the sequence* $U^{\mathbb{N}} = \langle m_0, \ldots, m_{l-1}\rangle$ *if* $t^{\mathbb{N}} < l$, *otherwise* 0.

One could convince oneself that each of functions symbols $\emptyset$, $|\cdot|$, $\cdot(\cdot)$ and App defines a primitive recursive function. Indeed, each of them defines even a polynomial time function, cf. discussion in Buss [3, Section 1.2].

Definition 6. $\mathcal{L}_A^{\mathsf{seq}}$*-formulas are obtained by extending* $\mathcal{L}_A^b$*-formulas as follows.*

1. *Every* $\mathcal{L}_A^b$*-formula is an* $\mathcal{L}_A^{\mathsf{seq}}$*-formula.*
2. *If* A *is an* $\mathcal{L}_A^{\mathsf{seq}}$*-formula, then* QXA *is an* $\mathcal{L}_A^{\mathsf{seq}}$*-formula for each* $Q \in \{\forall, \exists\}$.

We introduce a set $\mathsf{BASIC}^{\mathsf{seq}}$ of axioms which define function symbols in $\mathcal{L}_A^{\mathsf{seq}}$.

Definition 7. *The set* $\mathsf{BASIC}^{\mathsf{seq}}$ *consists of the following formulas.*

1. $|\emptyset| = 0$.
2. $|\mathsf{App}(x, X)| = |X| + 1$.
3. $y < |X| \to \mathsf{App}(x, X)(y) = X(y)$.
4. $\mathsf{App}(x, X)(|X|) = x$.

Definition 8. *Let* $t, s \in \mathcal{T}^b(\mathcal{L}_A^{\mathsf{seq}})$ *be two terms and* $A(X)$ *an* $\mathcal{L}_A^{\mathsf{seq}}$*-formula. Then, we write* $(\exists X^{(t,s)})A(X)$ *instead of* $\exists X((\forall j < |X|)(X(j) \le t) \wedge |X| \le s \wedge A(X))$. *Accordingly, we write* $(\forall X^{(t,s)})A(X)$ *instead of* $\forall X((\forall j < |X|)(X(j) \le t) \wedge |X| \le s \to A(X))$. *A quantifier of the form* $(\exists X^{(t,s)})(\cdots)$ *or* $(\forall X^{(t,s)})(\cdots)$ *will be called a* bounded quantifier on sequences.

Definition 9. *For each* $i \ge 0$ *sets* Σ_i^{seq}, Π_i^{seq} *and* Δ_i^{seq} *of* $\mathcal{L}_A^{\mathsf{seq}}$*-formulas are simultaneously defined as follows.*

1. $\bigcup_{j\in\mathbb{N}} \Sigma_j^b \subseteq \Sigma_0^{\mathsf{seq}} := \Pi_0^{\mathsf{seq}}$.
2. *The set* Σ_i^{seq} *is closed under* $\vee$ *and* $\wedge$.
3. *If* $A \in \Pi_i^{\mathsf{seq}}$ *and* $B \in \Sigma_i^{\mathsf{seq}}$, *then* $\{A \to B, \neg A\} \subseteq \Sigma_i^{\mathsf{seq}}$.
4. $\Pi_i^{\mathsf{seq}} \subseteq \Sigma_{i+1}^{\mathsf{seq}}$.
5. *If* $A \in \Sigma_i^{\mathsf{seq}}$ *and* $t \in \mathcal{T}^b(\mathcal{L}_A^{\mathsf{seq}})$ *is a term, then* $\{(\forall x \le t)A, (\exists x \le t)A\} \subseteq \Sigma_i^{\mathsf{seq}}$.
6. *If* $A \in \Sigma_i^{\mathsf{seq}}$ *and* $t, s \in \mathcal{T}^b(\mathcal{L}_A^{\mathsf{seq}})$ *is two terms, then* $(\exists X^{(t,s)})A \in \Sigma_i^{\mathsf{seq}}$.
7. *The set* Π_i^{seq} *is defined dually to* Σ_i^{seq} *and* Δ_i^{seq} *is defined in an obvious way.*

Let $\mathbb{N}$ denote a standard model of first order theories of arithmetic. We extend the standard validity $\mathbb{N} \models \cdot$ to the $\mathcal{L}_A^{\mathsf{seq}}$-sentences. Here we extend the notation for the numeral $\underline{m}$ corresponding to a natural number m to the notation $\underline{\langle m_0, \ldots, m_{l-1}\rangle}$ for the sequence of natural numbers $m_0, \ldots, m_{l-1}$ in an obvious way: $\underline{\langle\rangle} = \emptyset$, $\underline{\langle m_0, \ldots, m_{l-1}, m_l\rangle} = \mathsf{App}(\underline{m_l}, \underline{\langle m_0, \ldots, m_{l-1}\rangle})$.

Definition 10. *We write* $\mathbb{N} \models \exists X A(X)$ *if there exists a sequence* $\langle m_0, \ldots, m_{l-1} \rangle$ *of natural numbers* $m_0, \ldots, m_{l-1} \in \mathbb{N}$ *such that* $\mathbb{N} \models A(\underline{\langle m_0, \ldots, m_{l-1} \rangle})$. *The validity* $\mathbb{N} \models \forall X A(X)$ *is defined accordingly.*

Definition 11. $T_2^{i,\mathsf{seq}} = \mathsf{BASIC} + \mathsf{BASIC}^{\mathsf{seq}} + \Sigma_i^{\mathsf{seq}}\text{-}\mathsf{IND}$. $(i \geq 0)$

Theorem 5 ([1]). *A function* f *is* Σ_1^{seq}*-definable in* $T_2^{1,\mathsf{seq}}$ *if* f *is polynomial space computable.*

Conjecture 1. The "only if" direction of Theorem 5 also holds. Hence a predicate is Δ_1^{seq}-definable in $T_2^{1,\mathsf{seq}}$ if and only if it belongs to **PSPACE**.

6 Conclusion

We started with the classical fact that primitive recursive functions can be captured by $\mathrm{I}\Sigma_1$. The first order bounded arithmetic started with capturing the class **P** by a miniaturisation S_2^1 of $\mathrm{I}\Sigma_1$. In order to capture the class **PSPACE** it is natural to extend S_2^1 to second order theories. The speaker believes that a new second order theory $T_2^{1,\mathsf{seq}}$ captures the class **PSPACE**. What is new, or what is a challenge, in the formulation of $T_2^{1,\mathsf{seq}}$ compared to Buss's second order theory U_2^1 or Skelley's third order theory W_1^1 will be explained as follows.

	Induction Axioms	(Bit-) Comprehension Axioms
U_2^1	Φ-PIND	included
W_1^1	Φ-PIND	included
$T_2^{1,\mathsf{seq}}$	Φ-IND	not included

For future works it is natural to ask what complexity classes can be captured by $T_2^{i,\mathsf{seq}}$ in general, or by second order theories $S_2^{i,\mathsf{seq}}$ with Σ_i^{seq}-PIND defined in accordance with $T_2^{i,\mathsf{seq}}$.

References

1. T. Arai and N. Eguchi. A New Theory of Bounded Arithmetic for PSPACE Computations. in preparation.
2. S. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
3. S. Buss. Proof Theory of Arithmetic. In S. R. Buss, editor, *Handbook of Proof Theory*, pages 79–147. North Holland, Amsterdam, 1998.
4. S. Cook and P. Nguyen. *Logical Foundations of Complexity*. Cambridge University Press, 2010.
5. A. Skelley. A Third-order Bounded Arithmetic Theory for PSPACE. In *Proceedings of Computer Science Logic 2004, the 18th International Workshop of the EACSL, LNCS*, volume 3210, pages 340–354. Springer, Berlin, 2004.