Fragments of bounded arithmetic

Chun-Yu "Max" Lin

Department of Logic, Faculty of Arts, Charles University

April 14, 2023

Definition

A theory of **bounded arithmetic** is a subtheory of Peano Arithmetic (PA) which is axiomatized by Π_1-formulas. These theories are typically weaker than strong subtheories of PA but stronger than Q and R.

Two approaches :

- Theories involved $I\Delta_0$ and $I\Delta_0 + \Omega_1$.
- Theories such as S_2^i and T_2^i.

Motivation : Give us a rich perspective on and a different approach to questions in low-level computational complexity.

$I\Delta_0$ and Ω_n

Theorem (Parikh,1971)

Let $A(\vec{x},y)$ be a Δ_0-formula and that $I\Delta_0 \vdash (\forall\vec{x})(\exists y)A(\vec{x},y)$. Then there is a term $t(\vec{x})$ such that $I\Delta_0 \vdash (\forall\vec{x})(\exists y \leq t)A(\vec{x},y)$.

Define $logx$ to be the greatest y such that $2^y \leq x$. We define $\omega_1(x,y) = x^{logy}$. From Parikh's theorem, ω_1 is not Σ_1-definable in $I\Delta_0$.
Stronger theory : $I\Delta_0 + \Omega_1$
One can extend the definition of ω_1 toward ω_n for $n \geq 1$ as $\omega_{n+1}(x,y) = 2^{\omega_n(logx,logy)} = 2^{\omega_n(|x|,|y|)}$.

Definition

$\Omega_1 : (\forall x)(\forall y)(\exists z)(z = \omega_1(x,y))$, $\Omega_n : (\forall x)(\forall y)(\exists z)(z = \omega_n(x,y))$

From Parikh's theorem, $I\Delta_0 + \Omega_n \nvdash \Omega_{n+1}$

$I\Delta_0$ and Ω_n

Proposition (Bennett,1962;Gaifman and Dimitracopoulos, 1982)

The graph of the exponentiation $\{(x, y, z)|x^y = z\}$ *is* Δ_0*-definable in* $I\Delta_0$.

S_2^i and T_2^i

- Have close connection to polynomial time complexity classes
- Have close connection to propositional proof systems

Language : $0, S, +, \cdot, \leq, |x|, \lfloor \frac{1}{2}x \rfloor, x\#y$

Definition

$\Delta_0^b = \Sigma_0^b = \Pi_0^b$: set of sharply bounded formulas. For $i \geq 1$,

- If A and B are Σ_1^b-formulas, then so ar $A \vee B$,$A \wedge B$. If A is a Π_i^b-formula and B is a Σ_i^b-formula, then $A \rightarrow B$ and $\neg A$ are Σ_i^b-formulas.
- If A is a Π_{i-1}^b-formula, then A is a Σ_i^b-formula.
- If A is a Σ_i^b-formula and t is a term, then $(\forall x \leq |t|)A$ is a Σ_i^b-formula.
- If A is a Σ_i^b-formula, and t is a term, then $(\exists x \leq t)A$ is a Σ_i^b-formula. Note that this quantifier may be sharply bounded.

The classes Π_i^b are defined dually.

Why including $\#$?

1. Gives a natural bound to the Gödel number for a formula $A(t)$ in terms of product of the numbers of symbols in A and in t.

2. Quantifier exchange property :

$(\forall x \leq |a|)(\exists y \leq b)A(x,y) \leftrightarrow (\exists w \leq SqBd(a,b))(\forall x \leq |a|)$
$(A(x,\beta(x+1,y)) \wedge (\beta(x+1,y) \leq b)$ where SqBd is a term involving $\#$.
This allows sharply bounded quantifers to be pushed inside non-sharply bounded quantifiers.

3. Connection with polynomial time and the polynomial time hierarchy:

- All terms $t(x)$ have polynomial growth rate (bounded by $2^{|x|^c}$ with some constant c)
- Σ_i^b- and Π_i^b-formulas define exactly the predicates in the classes Σ_i^p and Π_i^p at the i-th level of the polynomial time hierarchy

Axiom-BASIC

$$
\begin{array}{ll}
a \le b \supset a \le Sb & |a| = |b| \supset a\#c = b\#c \\
a \ne Sa & |a| = |b| + |c| \supset a\#d = (b\#d) \cdot (c\#d) \\
0 \le a & a \le a + b \\
a \le b \wedge a \ne b \leftrightarrow Sa \le b & a \le b \wedge a \ne b \supset \\
a \ne 0 \supset 2 \cdot a \ne 0 & \qquad S(2 \cdot a) \le 2 \cdot b \wedge S(2 \cdot a) \ne 2 \cdot b \\
a \le b \vee b \le a & a + b = b + a \\
a \le b \wedge b \le a \supset a = b & a + 0 = a \\
a \le b \wedge b \le c \supset a \le c & a + Sb = S(a + b) \\
|0| = 0 & (a + b) + c = a + (b + c) \\
|S0| = S0 & a + b \le a + c \leftrightarrow b \le c \\
a \ne 0 \supset |2 \cdot a| = S(|a|) \wedge |S(2 \cdot a)| = S(|a|) & a \cdot 0 = 0 \\
a \le b \supset |a| \le |b| & a \cdot (Sb) = (a \cdot b) + a \\
|a\#b| = S(|a| \cdot |b|) & a \cdot b = b \cdot a \\
0\#a = S0 & a \cdot (b + c) = (a \cdot b) + (a \cdot c) \\
a \ne 0 \supset 1\#(2 \cdot a) = 2 \cdot (1\#a) & S0 \le a \supset (a \cdot b \le a \cdot c \leftrightarrow b \le c) \\
\qquad \wedge 1\#(S(2 \cdot a)) = 2 \cdot (1\#a) & a \ne 0 \supset |a| = S(|\lfloor \frac{1}{2} a \rfloor|) \\
a\#b = b\#a & a = \lfloor \frac{1}{2} b \rfloor \leftrightarrow 2 \cdot a = b \vee S(2 \cdot a) = b
\end{array}
$$

Remark 1

This choice is not entirely optimal.

Axioms for T_2^i and S_2^i

Induction Axioms : Let Φ be a set of formulas.

- Φ-IND : $A(0) \land (\forall x)(A(x) \to A(Sx)) \to (\forall x)A(x)$.
- Φ-PIND : $A(0) \land (\forall x)(A(\lfloor \frac{1}{2}x \rfloor) \to A(x)) \to (\forall x)A(x)$.
- Φ-LIND : $A(0) \land (\forall x)(A(x) \to A(Sx)) \to (\forall x)A(|x|)$.
- Φ-LMIN : $(\exists x)A(x) \to (\exists x)(A(x) \land (\forall y)(|y| < |x| \to \neg A(y)))$

Definition

S_2^i : BASIC + Σ_i^b-PIND.
T_2^i : BASIC + Σ_i^b-IND
$S_2 = \cup_i S_2^i$ $T_2 = \cup_i T_2^i$

Bootstrapping and Σ_i^b-definable functions

Definition

A predicate symbol $R(\vec{x})$ is Δ_i^b-defined by a theory T if there is a Σ_i^b-formula $\phi(\vec{x})$and a Π_i^b-formula $\psi(\vec{x})$ such that R has defining axiom $R(\vec{x}) \leftrightarrow \phi(\vec{x})$ and $T \vdash (\forall \vec{x})(\phi \leftrightarrow \psi)$.

Definition

Let T be a theory of arithmetic. A function symbol $f(\vec{x})$ is Σ_i^b-defined by T if it has a defining axiom $y = f(\vec{x}) \leftrightarrow \phi(\vec{x}, y)$ where ϕ is a Σ_i^b formula with all free variables indicated and $T \vdash (\forall \vec{x})(\exists! y)(\phi(\vec{x}, y))$

Theorem (Buss,1986)

Let BASIC $\subseteq T$ Let T be extended to a theory T^+ in an enlarged language L^+ by adding Δ_1^b-defined predicate symbols, Σ_1^b-defined function symbols and their defining equations. Let A be a Σ_i^b(respectively, a Π_i^b)-formula in L^+ Then

- *T^+ is conservative over T*
- *there is a formula A^- in the language of T such that A^- is in Σ_i^b(respectively, Π_i^b) and $T^+ \vdash (A \leftrightarrow A^-)$.*

Proof

Theorem 2: Let R be a fragment of Bounded Arithmetic. Suppose R can Σ_1^b–define the function f. Let R^* be the theory obtained from R by adding f as a new function symbol and adding the defining axiom for f. Then, if $i>0$ and B is a $\Sigma_i^b(f)$– (or a $\Pi_i^b(f)$–) formula, there is a $B^* \in \Sigma_i^b$ (or Π_i^b, respectively) such that $R^* \vdash B^* \leftrightarrow B$.

Proof: The defining axiom for f is

$$f(\vec{x})=y \leftrightarrow A(\vec{x},y)$$

where A is a Σ_1^b–formula. Let B be a bounded formula containing the symbol f. We first define the formula B_1 as follows: suppose f occurs in a term which bounds a quantifier, say $(Qx \le s)D$ is a subformula of B where the term s involves f. Replace each occurrence of $f(\vec{r})$ in

s by the term $t(\vec{r})$. (t is the bound in the Σ_1^b–definition of f, see the definition above.) This yields a term s'. Now, $(\exists x \leq s)D$ is provably equivalent to $(\exists x \leq s')(x \leq s \wedge D)$ and $(\forall x \leq s)D$ is provably equivalent to $(\forall x \leq s')(x \leq s \supset D)$. By repeating this procedure, we can form B_1 so that

(1) $R^* \vdash B \leftrightarrow B_1$, and

(2) B_1 does not contain f appearing in any term which bounds a quantifier.

We next obtain a formula B_2 in prenex normal form by applying prenex operations to B_1 so that $R^* \vdash B_2 \leftrightarrow B_1$. Furthermore, if B is a Σ_i^b– (or a Π_i^b–) formula, then so are B_1 and B_2.

Let the mantissa of B_2 be D; that is to say, suppose

$$B_2 = (Q_1 x_1 \leq s_1) \cdots (Q_n x_n \leq s_n) D$$

where D is an open formula. Let $f(\vec{r})$ be a term appearing in D. Obtain D' by replacing $f(\vec{r})$ everywhere in D by a new variable z. Define

$$D_A = (\forall z \leq t(\vec{r}))(A(\vec{r}, z) \supset D')$$

and

$$D_E = (\exists z \leq t(\vec{r}))(A(\vec{r}, z) \wedge D').$$

Let $D^\forall$ and $D^\exists$ be their respective prenex normal forms. Then $D^\forall$ is a $\Pi_1^b(f)$–formula and $D^\exists$ is a $\Sigma_1^b(f)$–formula, and

$$R^* \vdash (D \leftrightarrow D^\forall) \wedge (D \leftrightarrow D^\exists).$$

Define B_3 from B_2 by replacing the mantissa D by either $D^\forall$ or $D^\exists$, whichever is appropriate. We can do this so that B_3 has the same alternation of (non-sharply) bounded quantifiers as B_2. Also,

$$R^* \vdash B_3 \leftrightarrow B_2.$$

B_3 was formed from B_2 so that all occurrences of the term $f(\vec{r})$ were eliminated. By iterating this procedure, we obtain B_4 from B_3, B_5 from B_4, and so on, until all occurrences of f have been eliminated. We let B^* be the B_i such that $i \geq 2$ and f does not appear in B_i.

Every single function and predicate symbol which was claimed to be Σ_1-definable or Δ_1-definable in $I\Delta_0$ is likewise Σ_i^b-definable or Δ_i^b-definable in S_2^1, T_2^1, BASIC $+ \Pi_1^b$-PIND, BASIC $+ \Sigma_1^b$-LIND, BASIC $+ \Pi_1^b$-LIND and BASIC $+ \Pi_1^b$-IND.

Theorem (Buss,1986)

Let $i \geq 1$

1. *T_2^i proves Π_i^b-IND and $T_2^i \models S_2^i$.*
2. *S_2^i proves Σ_i^b-LIND, Π_i^b-PIND and Π_i^b-LIND.*

Definition (Cobham,1965)

The polynomial time function on $\mathbb{N}$ are inductive defined by

1. The following function are polynomial time :
   - The nullary constant function 0.
   - The successor function S(x)
   - The doubling function D(x)=2x
   - The conditional function $Cond(x,y,z) = \begin{cases} y & \text{if } x = 0 \\ z & \text{otherwise.} \end{cases}$
2. The projection functions are polynomial time functions; the composition of polynomial time functions is a polynomial time function.
3. If g is a $(n-1)$-ary polynomial time function and h is a $(n+1)$-ary polynomial time function and p is a polynomial, then the following function f, defined by limited iteration on notation from g and h , is also polynomial time : $f(0,\vec{x}) = g(\vec{x})$
   $f(z,\vec{x}) = h(z,\vec{x},f(\lfloor \frac{1}{2}z \rfloor,\vec{x}))$ for $z \neq 0$ provided $|f(z,\vec{x})| \leq p(|z|,|\vec{x}|)$

Notation

The class of polynomial time functions is denoted as $\square_1^p$, and the class of polynomial time predicates is denoted Δ_1^p.

Theorem (Buss,1986)

1. *Every polynomial time function is Σ_1^b-definable in S_2^1.*
2. *Every polynomial time predicate (i.e. its characteristic function is polynomial time) is Δ_1^b-definable in S_2^1.*

Proof.

Boostraping S_2^1 sufficiently to intensionally introduce sequence coding function and prove this theorem by induction on the construction of polynomial time computability. □

Theorem (Buss,1986)

Let $i \geq 1$.

1. $T_2^i \supseteq S_2^i$.
2. $S_2^i \supseteq T_2^{i-1}$.

Proof.

For (1), it suffices to show Σ_i^b-PIND follows from Σ_i^b-LIND over BASIC with $i \geq 1$. We sketch the proof here. To prove PIND for $A(x)$(with c a free variable) $A(0) \wedge (\forall x)(A(\lfloor \frac{1}{2} x \rfloor) \to A(x)) \to A(c)$ use LIND on $B(i) := A(t(i))$ for $t(i) := \lfloor c/2^{|c|-i} \rfloor$. For this, note that $B(0)$ and $B(|c|)$ are equivalent to $A(c)$ and $A(0)$. Also, $t(i) = \lfloor \frac{1}{2} t(i+1) \rfloor$, so $(\forall i)(B(i) \to B(i+1))$ follows from $(\forall x)(A(\lfloor \frac{1}{2} x \rfloor) \to A(x))$ □

Proof Cont.

The proof of (2) use a divide-and-conquer method. Fix $i \geq 1$ and a Σ^b_{i-1}-formula $A(x)$; prove that S^i_2 proves the IND-axiom for A. Assume that we have $A(0)$ and $(\forall x)(A(x) \rightarrow A(x+1))$. Let $B(x,z)$ be the formula $(\forall w \leq x)(\forall y \leq z+1)(A(w \dot{-} y) \rightarrow A(w))$. B is equivalent to a Π^b_i-formula. By the definition of b, it follows that $(\forall x)(\forall z)(B(x, \lfloor \frac{1}{2} z \rfloor) \rightarrow B(x,z))$ and hence by Π^b_i-PIND on $B(x,z)$ w.r.t z, we have $(\forall x)(B(x,0) \rightarrow B(x,x))$. $(\forall x)B(x,0)$ holds as it's equivalent to $(\forall x)(A(x) \rightarrow A(x+1))$, therefore $(\forall x)B(x,x)$ holds. This implies $(\forall x)(A(0) \rightarrow A(x))$.

Corollary (Buss,1986)

$S_2 = T_2$

Definition

The classes Δ_1^p and $\square_1^p$ have already been defined. Further define, by induction on i,

1. Σ_i^p is the class of predicate $R(\vec{x})$ definable by $R(\vec{x}) \leftrightarrow (\exists y) \leq s(\vec{x})(Q(\vec{x}, y))$ for some term s in ther language of bounded arithmetic, and some Δ_i^p predicate Q.
2. Π_i^p is the class of complements of predicates in Σ_i^p.
3. $\square_{i+1}^p$ is the class of predicates computable on a polynomial time Turing machine using an oracle from Σ_i^p.
4. Δ_i^p is the class of predicates which have characteristic function in $\square_{i+1}^p$.

1. Base classes $P = \Delta_1^p$ of polynomial time recognizable predicates.
2. $FP = \square_1^p$ of polynomial time computable functions.
3. $NP = \Sigma_1^p$ of predicates computable in nondeterministic polynomial time.
4. $coNP = \Pi_1^p$ of complement of NP predicates.

Theorem (Wrathall'76,Stockmeyer'76,Kent-Hodgson'82)

A predicate is Σ_i^p if and only if there is a Σ_i^b-formula which defines it.

Proof.

($\Leftarrow$) Note that a sharply bounded formula defines a polynomial time predicate. Given a Σ_i^b-formula, one can use the quantifier exchange property to push sharply bounded quantifier inward and can use pairing functions to combine adjacent quantifiers; this transforms the formula into an equivalent formula which defines a Σ_i^p property.
($\Rightarrow$) Induction on i : For $i = 1$, from previous theorem, we have known every Δ_1^p-predicate is defined by both a Σ_1^p and a Π_1^p formula. For the first part of induction step, we assume that every Δ_i^p predicate is definable by both a Σ_i^b and Π_i^b-formula. Use this claim, we get every Σ_i^p predicate is definable by a Σ_i^b-formula. To prove the second part of induction step, we have to prove that every Δ_{i+1}^p-predicate is definable by both a Σ_{i+1}^b-formula and a Π_{i+1}^b-formula. To show this, it suffices to show that every $\square_{i+1}^p$-function has its graph defined by a Σ_i^b-formula. These are contents of next theorem. □

Theorem (Buss,1986)

$i \geq 1$.

1. *Every $\square_i^p$ function is Σ_i^b-definable in S_2^i.*
2. *Every Δ_i^p predicate is Δ_i^bdefinable in S_2^i*

Proof.

Induction on i. The base case has already been done. For (2), consider a Δ_i^p predicate $Q(\vec{x})$ with the characteristic function f in $\square_i^p$. By (1), it is defined by a Σ_i^b-formula A_f. Define $A(\vec{x})$ and $B(\vec{x})$ to be $A_f(x, 1)$ and $\neg A_f(x, 0)$. Then $S_2^i \vdash (\forall \vec{x})(A(\vec{x}) \leftrightarrow B(\vec{x}))$.

□

Proof of (1)

(1) If $f(\vec{x}, y)$ is a $\square^p_{i-1}$-function, then the characteristic function $\chi(\vec{x})$ of $(\exists y \le t(\vec{x}))(f(\vec{x}, y) = 0)$ is Σ^b_i-definable. To prove this, we have by the induction hypothesis that $f(\vec{x}, y) = z$ is equivalent to a Σ^b_{i-1} formula $A(\vec{x}, y, z)$. The Σ^b_i-definition of $\chi(\vec{x})$ is thus[6]

$$\chi(\vec{x}) = z \ \Leftrightarrow \ (z = 0 \wedge (\exists y \le t)A(\vec{x}, y, 0)) \vee (z = 1 \wedge \neg(\exists y \le t)A(\vec{x}, y, 0))$$

which is clearly equivalent to a Σ^b_i-formula by prenex operations.
(2) If functions g and $\vec{h}$ have graph definable by Σ^b_i-formulas, then so does their composition. As an example of how to prove this, suppose $f(\vec{x}) = g(\vec{x}, h(\vec{x}))$; then the graph of f can be defined by

$$f(\vec{x}) = y \ \Leftrightarrow \ (\exists z \le t_h(\vec{x}))(h(\vec{x}) = z \wedge g(\vec{x}, z) = y),$$

where t_h is a term bounding the function h.
(3) If f is defined by limited iteration from g and h with bounding polynomial p, and g and h have Σ^b_i-definable graphs, then so does f. To prove this, show that $f(z, \vec{x}) = y$ is expressed by the formula

$$(\exists w \le SqBd(2^{p(|z|,|\vec{x}|)}, z))[\beta(|z| + 1, \vec{x}) = y \wedge \beta(1, w) = g(\vec{x}) \wedge$$
$$\wedge (\forall i < |z|)(\beta(i + 2, w) = \min\{h(\lfloor \tfrac{z}{2^{|z| \dot- i \dot- 1}} \rfloor, \vec{x}, \beta(i + 1, w)), 2^{p(|i+1|,|\vec{x}|)}\})].$$

Here the term $SqBd(\cdots)$ has been chosen sufficiently large to bound the size of the sequence w encoding the steps in the computation of $f(z, \vec{x})$. The formula is clearly in Σ^b_i, and the theory S^i_2 can prove the existence and uniqueness of w by PIND induction up to z. □

Theorem (Buss,1990)

Let $i \geq 1$.

1. *Every $\square_i^p$ function is Σ_i^b-definable in T_2^{i-1}.*
2. *Every Δ_i^p predicate is Δ_i^b-definable in T_2^{i-1}.*

Remark 2 (Krajíček-Pudlák-Takeuti'91,Buss'95,Zambella'96)

If $T_2^i = S_2^{i+1}$ for some $i \geq 1$, then the polynomial time hierarchy collapses provably in T_2.