Structure and Definability in General Bounded Arithmetic Theories

Chris Pollett

May 22, 1997

Overview

1. Background
   (a) Complexity Classes
   (b) Bounded Arithmetic Theories
      i. Classical Theories: R^i_2, S^i_2, T^i_2
   (c) Known Results
2. New Results
   (a) New Theories: $\widehat{T}^{i,\tau}_2$, $\widehat{C}^{i,|\tau|}_2$
   (b) Definability Results:
      i. Local Search and Machine Classes.
      ii. Results for R^i_2, T^i_2, $\widehat{T}^{i,\tau}_2$, $\widehat{C}^{i,|\tau|}_2$.
   (c) Structural Results:
      i. $\widehat{T}^{i,\tau\#}_2 \preceq_{B(\widehat{\Sigma}^b_{i+1})} \widehat{T}^{i+1,|\tau|}_2 \preceq_{B(\widehat{\Sigma}^b_{i+2})} \widehat{C}^{i+1,|\tau|}_2$
      ii. Weak Equalities $\Rightarrow PH \downarrow$
      iii. Oracle Separations

The Polynomial Hierarchy (PH)

$$
\begin{array}{ccccc}
 & & \vdots & & \\
 & & \mathbf{\Delta^p_3} & & \\
 & \rotatebox{45}{$\subseteq$} & & \rotatebox{-45}{$\supseteq$} & \\
\mathbf{\Pi^p_2} & & & & \mathbf{\Sigma^p_2} \\
 & \rotatebox{-45}{$\supseteq$} & & \rotatebox{45}{$\subseteq$} & \\
 & & \mathbf{\Delta^p_2} & & \\
 & \rotatebox{45}{$\subseteq$} & & \rotatebox{-45}{$\supseteq$} & \\
\mathbf{co\text{-}NP} & & & & \mathbf{NP} \\
 & \rotatebox{-45}{$\supseteq$} & & \rotatebox{45}{$\subseteq$} & \\
 & & \mathbf{P} & &
\end{array}
$$

$\mathbf{P = \Delta^p_1}$ = deterministic poly-time rel'ns.

$\mathbf{NP = \Sigma^p_1}$ = nondeterministic p-time rel'ns.

$\mathbf{\Delta^p_{i+1} = P^{\Sigma^p_i}}$ add Σ^p_i oracle set

$\mathbf{\Sigma^p_{i+1} = NP^{\Sigma^p_i}}$ add Σ^p_i oracle set

$\mathbf{\Pi^p_i = co - \Sigma^p_i}$ = complements of Σ^p_i rel'ns.

<u>**Open:**</u> Does PH collapse? Does $P = NP$?

Complexity into Logic

$\mathbf{L_2} := \{0,\ Sx = x+1,\ +,\ \cdot,\ \leq,\ \dot{-},\ |x|,\ \lfloor \frac{x}{2^i} \rfloor,$
$x\#y = 2^{|x||y|}\}.$

The Bounded Arithmetic Hierarchy is:

$\mathbf{\Sigma_0^b} = \mathbf{\Pi_0^b}$ are the sharply bounded formulas. i.e., Quantifiers are of form $\exists x \leq |t|$ or $\forall x \leq |t|$.

$\mathbf{\Sigma_i^b} \supset \Pi_{i-1}^b$ closed under $\wedge, \vee, \forall x \leq |t|, \exists x \leq t$.

$\mathbf{\Pi_i^b} \supset \Sigma_{i-1}^b$ closed under $\wedge, \vee, \exists x \leq |t|, \forall x \leq t$.

$\mathbf{\hat{\Sigma}_i^b}$, $\mathbf{\hat{\Pi}_i^b}$ are the prenex formulas in Σ_i^b, Π_i^b. i.e., a $\hat{\Sigma}_i^b$-formula is of the form

$$(\exists x_1 \leq t_1)(\forall x_2 \leq t_2) \cdots (Q_i x_i \leq t_i)(Q_{i+1} x_{i+1} \leq |t_{i+1}|)A$$

where A is open.

It turns out $\hat{\Sigma}_i^b = \Sigma_i^b = \Sigma_i^p$ and $\hat{\Pi}_i^b = \Pi_i^b = \Pi_i^p$.

Bounded Arithmetic Theories

Bounded arithmetic theories are theories using axiom schemas restricted to the bounded arithmetic hierarchy. We will be talking about definability in such theories and their connections with PH. Our base theory is:

BASIC := a finite list of open axioms for L_2.

Defining Functions in a Theory

A **multifunction** is a total relation. Let Ψ be a set of L_2-formulas.

T can **Ψ-define the multifunction** $f(x)$, if
$T \vdash \forall x \exists y A_f(x, y)$ where $A_f \in \Psi$ and
$\mathbb{N} \models A_f(x, y) \Leftrightarrow f(x) = y$.

T can **Ψ-define the function** $f(x)$ if
$T \vdash \forall x \exists ! y A_f(x, y)$ where $A_f \in \Psi$ and
$\mathbb{N} \models A_f(x, f(x))$.

Example: A Σ_1^b-definable multi-fn in $BASIC$:

$$f(x) = y \Leftrightarrow$$
$$(\exists w)(\exists z)(y \leq 4(x+1) \wedge y = w \cdot z \wedge w, z > 1)$$

Example: $f(x) = x + 2$ is an open-definable fn in $BASIC$.

Def'n: A formula A is $\mathbf{\Delta_i^b}$ **in** $\mathbf{T}$ iff $T \vdash A \Leftrightarrow A^\Sigma$ and $T \vdash A \Leftrightarrow A^\Pi$ where $A^\Sigma \in \Sigma_i^b$ and $A^\Pi \in \Pi_i^b$. The formula A is $\mathbf{\hat{\Delta}_i^b}$ **in** $\mathbf{T}$ if $A^\Sigma \in \hat{\Sigma}_i^b$ and $A^\Pi \in \hat{\Pi}_i^b$

Idea: $\hat{\Delta}_i^b$ is what theory proves is $\hat{\Sigma}_i^b \cap \hat{\Pi}_i^b$

Axiom Schemas

τ - set of 1-ary terms (**iterms**).
Ψ - set of formulas.
Write $|\tau|$ for set of iterms $|\ell|$ where $\ell \in \tau$.

We form theories from $BASIC$ with schemas below. Here IND is for induction, $REPL$ for replacement, and $COMP$ for comprehension.

$\mathbf{\Psi}$**-IND**$^{\tau}$:

$$\alpha(0) \wedge (\forall x)(\alpha(x) \supset \alpha(Sx)) \supset (\forall x)\alpha(\ell(x))$$

$\mathbf{\Psi}$**-REPL**$^{|\tau|}$:

$$\forall x \leq |\ell(s)| \exists y \leq t\alpha(x,y) \Leftrightarrow \exists w \leq 2(t^* \# \ell(s)) \\ \forall x \leq |\ell(s)| \alpha(x, \dot{\beta}(x, |t^*|, t, w)))$$

$\mathbf{\Psi}$**-COMP**$^{|\tau|}$:

$$(\exists w)(\forall x \leq |\ell(b)|)(\alpha(v,x) \Leftrightarrow Bit(x,w) = 1)$$

Here $\alpha \in \Psi$, $\ell \in \tau$, and $s, t \in L_2$.

Classical Bounded Arithmetic Theories

$\mathbf{T_2^i} = BASIC + \Sigma_i^b\text{-}IND^{\{id\}}$
$\mathbf{S_2^i} = BASIC + \Sigma_i^b\text{-}IND^{\{|id|\}}$
$\mathbf{R_2^i} = BASIC + \Sigma_i^b\text{-}IND^{\{||id||\}}$

Some facts about them

- $S_2^{i-1} \subseteq R_2^i \subseteq S_2^i \subseteq T_2^i \preceq_{\Sigma_{i+1}^b} S_2^{i+1}$ (Bu,Al,Ta)
- $T_2^i = S_2^{i+1}$ implies $\Sigma_{i+2}^p = \Pi_{i+2}^b$.(KPT)
- Σ_{i+1}^b-definable functions of S_2^{i+1} and T_2^i are precisely the p-time functions with access to a Σ_i^p-oracle, $FP^{\Sigma_i^p}$. (Buss, Krajicek)
- Σ_{i+1}^b-definable multifunctions of S_2^i is the class $FP^{\Sigma_i^p}(wit, \log)$. (Krajicek)
- Σ_1^b-functions of R_2^1 are FNC, the class of poly-size polylog depth circuits and those of T_2^1 are projections of polynomial local search problems (PLS).(Al,Cl,BK)
- $S_2^2(\alpha)$ can't prove PRNGs exist.(Ra,Wi)

Questions

- Is $S_2^i \preceq_{\Sigma_{i+1}^b} R_2^{i+1}$? What makes one bounded arithmetic theory conservative over another? Can the $T_2^i \preceq_{\Sigma_{i+1}^b} S_2^{i+1}$ result be strengthened?

- For $i > 1$ what are the Σ_i^b-multifunction of T_2^i?

- For $i > 1$ what are the Σ_i^b- and Σ_{i+1}^b-definable multifunctions of R_2^i? Does the trend $FP^{\Sigma_i^p}$ for T_2^i, $FP^{\Sigma_i^p}(wit, \log)$ for S_2^i continue to $FP^{\Sigma_i^p}(wit, \log\log)$ for R_2^i?

- What relativized separations occur between these theories? From (Kraj,KPT) known

$$S_2^i(\alpha) \subsetneq T_2^i(\alpha) \subsetneq S_2^{i+1}(\alpha).$$

New Theories

EBASIC $:= BASIC$ +3 open axioms enabling ordered pairs.

Thm $EBASIC \subseteq R^0_2$.

If restrict to prenex formulas can perform witnessing argument in extensions of $EBASIC$. Let τ be a set of iterms.

$\hat{\mathbf{T}}^{\mathbf{i},\tau}_{\mathbf{2}} := EBASIC + \hat{\Sigma}^b_i\text{-}IND^{\tau}$
$\hat{\mathbf{C}}^{\mathbf{i},|\tau|}_{\mathbf{2}} := EBASIC + open\text{-}IND^{|\tau|} + \hat{\Pi}^b_i\text{-}REPL^{|\tau|}$

We call $\hat{T}^{i,\tau}_2$ and $\hat{C}^{i,|\tau|}_2$ **prenex theories**. We write id for the identity term $id(a) := a$. We define cl to be the set of closed iterms. So $EBASIC = \hat{T}^{i,cl}_2$.

Thm
(1) $T^i_2 = \hat{T}^{i,\{id\}}_2$, $S^i_2 = \hat{T}^{i,\{|id|\}}_2$,
(2) $R^i_2 = \hat{T}^{i,\{||id||\}}_2 + \hat{\Pi}^b_{i-1}\text{-}REPL^{\{|id|\}}$
(3) $\hat{T}^{i,\{||id||\}}_2 \preceq_{B(\hat{\Sigma}^b_{i+1})} R^i_2$.

Definability Results

(Buss, Allen, Krajicek + new)

	Σ_i^b	Δ_i^b	Σ_{i+1}^b	Δ_{i+1}^b
T_2^i	$\pi LS_{\{id\}}^{B_{i,2}}$ *	$\pi LS_{\{id\}}^{B_{i,2}}$ rel'ns*	$FP^{\Sigma_i^p}$	Δ_{i+1}^p
S_2^i	$FP^{\Sigma_{i-1}^p}$	Δ_i^p	$FP^{\Sigma_i^p}(wit, \log)$	$P^{\Sigma_i^p}(\log)$
R_2^i	$FNC^{\Sigma_{i-1}^p}$ $(i > 1)$*	$NC^{\Sigma_{i-1}^p}$ $(i > 1)$*	$FP^{\Sigma_i^p}(wit, \log^{(2)})$ * $\widehat{R}_2^i$	$P^{\Sigma_i^p}(\log^{(2)})$ * $\widehat{R}_2^i$

A '*' indicates a new result. Also show for $k > 2$, $\widehat{\Delta}_{i+k}^b$-preds of $\widehat{R}_2^i$,S_2^i,T_2^i are $P^{\Sigma_{i+k-1}^p}(1)$.

$\pi\mathbf{LS}_{\{\mathbf{id}\}}^{\mathbf{B_{i,2}}}$ are multifunctions computable as local optima to a new set of search problems we define. For $i > 1$, $B_{i,2} = FP^{\Sigma_i^p}(wit, 1)$. Cost, feasible answer set, and nbhd multifunction are in $B_{i,2}$. Cost is a fn and nbhd single-valued at optima. The id means any cost bdd by a $id(L_2) = L_2$-term.

Structural Results

(Buss, Allen, Krajicek +new)

(a)

$$
\begin{array}{llcl}
\widehat{T}_2^{i,\{2^{p(\|x\|)}\}} \preceq_{B(\widehat{\Sigma}^b_{i+1})^*} & R_2^{i+1} & \subseteq & S_2^{i+1} \subseteq T_2^{i+1} \\
 & \cup\!| & & \curlyvee\!| B(\Sigma^b_{i+1}) \\
\qquad\quad \searrow\!\!\!\!\!\!\succeq & \tilde{S}_2^i & \subseteq & \tilde{T}_2^i \\
 & \curlyvee\!| B(\widehat{\Sigma}^b_{i+1})^+ & & \curlyvee\!| B(\widehat{\Sigma}^b_{i+1})^+ \\
\qquad\quad R_2^i \subseteq & S_2^i & \subseteq & T_2^i
\end{array}
$$

(b)

$$T_2^{i-1}(\alpha) \not\supseteq_{\widehat{\Delta}^b_{i+1}(\alpha)*} R_2^i(\alpha) \subsetneq_{\widehat{\Delta}^b_{i+1}(\alpha)*}$$
$$S_2^i(\alpha) \subsetneq_{\widehat{\Delta}^b_{i+1}(\alpha)} T_2^i(\alpha)$$

(c) $R_2^i(\alpha) \subsetneq_{\widehat{\Delta}^b_i(\alpha)*} T_2^{i-1}(\alpha)$

(d) $T_2^{i-1} = R_2^i$ implies $\Sigma^p_{i+3} = \Pi^p_{i+3}$. *

- A '$*$' indicates a new result.
- A '+' indicates $\preceq_{\Sigma^b_{i+1}}$ previously known.
- $\tilde{S}$ and $\tilde{T}$ means Σ^b_{i+1}-$REPL^{\{|id|\}}$ added.
- Collapse and oracle separations follow from our definability results.

Closing iterms under a base function

A set τ of iterms is called **product closed** if whenever $s(x)$ and $t(x)$ are terms in τ there is a iterm $(s \cdot t)$ in τ and a term r in L_2 such that $(s \cdot t)(r(x)) = s(x) \cdot t(x)$. We write $\dot{\tau}$ to denote the product closure of τ. This is defined inductively.

A class τ of iterms is called **smash closed** if the following additional conditions is satisfied whenever $s(x)$ and $t(x)$ are iterms in τ there is a term $(s\#t)$ in τ and a term r in L_2 such that $(s\#t)(r(x)) = s(x)\#t(x)$. We write $\tau^{\#}$ to denote the smash closure of τ. This is defined inductively.

Examples of Product and Smash Closure

An example of a product closed and smash closed set of iterms is $\{id\}$ since $id(x \cdot x) = id(x) \cdot id(x)$ and $id(x\#x) = id(x)\#id(x)$.

$\{|id|\}$ is product closed but not smashed closed.

The class of terms of the form $2^{p(||x||)}$ where p is a polynomial; however, is smash closed and product closed. To see this consider $2^{p_1(||x||)}$ and $2^{p_2(||x||)}$ where p_1 and p_2 are polynomials. Then

$$2^{p_1(||x||)} \# 2^{p_2(||x||)} = 2^{p_1(||x||) \cdot p_2(||x||)}$$

and the right hand side is also a term of the form $2^{p(||x||)}$. A similar argument works for product closure.

Definability Results

	$\hat{\Sigma}^b_i$	$\hat{\Sigma}^b_{i+1}$	$\hat{\Sigma}^b_{i+k}$
$\hat{T}^{i,\tau}_2$	$\pi LS_\tau^{FP^{\Sigma^p_{i-1}}(wit,1)}$	$FP^{\Sigma^p_i}(wit, \lvert\tau\rvert)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$
$\hat{C}^{i,\lvert\tau\rvert}_2$	$\pi LS_{\lvert\tau\rvert}^{FP^{\Sigma^p_{i-1}}(wit,1)}$	$FP^{\Sigma^p_i}(wit, \lvert\lvert\tau\rvert\rvert)$	$FP^{\Sigma^p_{i+k-1}}(wit, 1)$

	$\hat{\Delta}^b_i$	$\hat{\Delta}^b_{i+1}$	$\hat{\Delta}^b_{i+k}$
$\hat{T}^{i,\tau}_2$	$\pi LS_\tau^{FP^{\Sigma^p_{i-1}}(wit,1)}$ rel'ns	$P^{\Sigma^p_i}(\lvert\tau\rvert)$	$P^{\Sigma^p_{i+k-1}}(1)$
$\hat{C}^{i,\lvert\tau\rvert}_2$	$\pi LS_{\lvert\tau\rvert}^{FP^{\Sigma^p_{i-1}}(wit,1)}$ rel'ns	$P^{\Sigma^p_i}(\lvert\lvert\tau\rvert\rvert)$	$P^{\Sigma^p_{i+k-1}}(1)$

The π means we map out a block of bits of a sol'n to LS problem.

Other Definability Results

$\hat{\Delta}^b_{i+1}$-predicates in $\hat{T}^{i,\tau}_2$ are provably equivalent to formulas of form

$$(\exists x \leq \ell(a))(A(x,a) \wedge \neg B(x,a))$$

where $\ell \in \tau$ and $A,B \in \hat{\Sigma}^b_i$.