Third-Order Computation and Bounded Arithmetic

Alan Skelley
Academy of Sciences of the Czech Republic

July 4, 2006
Outline

- Background
- The second-order viewpoint
- Some second-order theories
- Third-order computation
- EXP-time hierarchy theories
Background about Bounded Arithmetic

- Originally, theories of arithmetic with weakened induction

- $\mathcal{L}_A^1 = \{0, 1, +, \cdot, \leq, =\} \quad \mathcal{L}_A^2 = \mathcal{L}_A^1 \cup \{| \cdot |_2, \in_2\} \quad \text{Smash: } x \# y = 2|x|\cdot|y|

- $\Sigma_i^b$: $i$ alternations of bd. 1st order Q’s, outermost existential

- $\Sigma_i^B$: Count 2nd order Q’s

- $\Phi-$IND: $\phi(0) \land \forall x (\phi(x) \rightarrow \phi(x + 1)) \rightarrow \forall x \leq t\phi(x) \quad (\phi \in \Phi)$

- $\Phi-$PIND: $\phi(0) \land \forall x (\phi([x/2]) \rightarrow \phi(x)) \rightarrow \forall x \leq t\phi(x) \quad (\phi \in \Phi)$
What’s the Point of Bounded Arithmetic?

• Connections to complexity theory
  – define functions and relations in a theory
  – witness quantifiers in a theorem

• Connections to propositional proof systems:
  – translate theorems into families of propositional proofs
  – prove reflection principles for proof systems
  – proof system strength related to provability of reflection

• Apply strong tools of logic and model theory to complexity
Bounded Arithmetic History

• Parikh 1971: $I\Delta_0$

• Paris and Wilkie 1980's: $I\Delta_0 + \Omega_1$

• Paris-Wilkie-Woods 1988: PHP vs. primes

• Cook 1975: PV and EF

• Buss 1986: $S_2, U^1_2, V^1_2$

• Buss-Krajíček-Takeuti 1993: $U^i_2, V^i_2$

• Takeuti, Razborov 1993: RSUV isomorphism

• KPT 91 + Buss 95, Zambella 96: $S_2$ collapses iff $S_2 \vdash "PH collapses"

• Now many examples of B.A. Theory vs. Complexity Class vs. Pf. System
Examples of (Class, System, Theory)

- $NC^1$, Frege, AID
- $TC^0$, $TC^0$-Frege, $\Delta^b_1 - CR$
- $P$, eFrege, $S^1_2$ / PV
- PLS, $G_1$, $T^1_2$
- $\Box^p_i$, $G^*_i$, $S^i_2$
- PSPACE, $G$, $U^1_2$
- Many more exotic examples of theories
What’s Wrong with this Picture?

• Theories vary greatly in language, method of capturing complexity classes

• Capturing small classes problematic in arithmetic e.g. $AC^0$, $TC^0$ vs. multiplication

• Propositional translations of first-order theories complicated due to strong language

Solution: Unified second-order viewpoint
Motivation for Second-Order: $S^i_2$ vs. $V^i$

- $S^i_2$ [Buss]: $L^1_A \cup \{#, \cdot, 1, \lfloor \cdot \rfloor \}$, BASIC, $\Sigma^b_i$-PIND. $\Box^p_i$ functions $\Sigma^b_i$-definable in $S^i_2$. Very technical (e.g. $|\text{BASIC}|=32$)

- $V^i$ [Zambella]: $L^2_A$, 14 axioms + strict-$\Sigma^B_i$-IND + comprehension. $\Sigma^B_i$-defines $\Box^p_i$-fns (of strings represented by sets)

- Second-order “viewpoint” eliminates ’#’, simplifies bootstrapping

- RSUV isomorphism [Razborov, Takeuti]
Some Second-Order Theories

- $V^0 = 2\text{-BASIC} + \Sigma_0^B\text{-COMP} (AC^0, \text{bounded-depth Frege})$ [CK]

- $VTC^0 = V^0 + \text{NUMONES}$ [CN]
  - NUMONES = “string have counting arrays”
  - RSUV-isomorphic to $\Delta_1^b - CR$

Both of the above finitely axiomatizable; corollary for $\Delta_1^b - CR$

- $VNC^1 (NC^1), VL (L), VNL (NL)$, all obtained similarly by adding principles related to the class; all are “minimal” (have universal conservative extensions of a certain kind)
Existing Technology for PSPACE and Above

- $U_2^1$ [Buss]: $L^2_A \cup \{\#, |, |_1, |_{\frac{1}{2}}\}$, BASIC, $\Sigma^b_1$-PIND. $\Sigma^B_1$-defines PSPACE (number-)functions

- $G$ [Dowd]: Propositional sequent calculus with $\Sigma^q_\infty$ formulas (propositional quantifiers)

- $\Sigma^B_0$ theorems of $U_2^1$ translate to polysize families of $G$ proofs [Krajíček-Takeuti] but very difficult even to state (Cook style, numbers $\rightarrow$ variables)

- Strings in $U_2^1$ are exponentially larger than (number) inputs to the PSPACE function, allowing reasoning about computations
Second-Order Theories $U_2^i$ and $V_2^i$ [B]

- $\Sigma_i^B$ formulas defined analogously to $\Sigma_i^b$ counting second-order quantifiers
- $\Sigma_0^B$-Comprehension
- $\Sigma_i^B$-PIND (-IND)
- Language includes $| \cdot |_1$, $\lfloor \cdot / 2 \rfloor$, “smash”: $x \# y = 2^{\lfloor x \cdot |y|}$
- $\Sigma_i^B$-definable number-functions exactly PSPACE$^{\Sigma_i^{B-1}}$ (EXP$^{\Sigma_i^{B-1}}$)
- Translation of $\Sigma_0^B(U_2^1)$ theorems into polynomial-sized $G$ proofs [KT]
Third-Order Viewpoint and Computation

- 3 sorts: numbers, strings and superstrings (intended to be exponentially different in size)

- Computation by TMs with “oracle” access to superstrings, polynomially bounded output (string lengths, numbers).

- Resource bounds ignore superstrings.

- Output superstrings to write-only tape or “by query” to allow exponential-size output.

- Relativize with bounded queries to third-order predicate.
Third-Order Viewpoint and Computation

- FPSPACE\(^+\), PSPACE\(^\diamond\), FEXP\(^+\), EXP\(^\diamond\), NEXP\(^\diamond\), etc. as expected.

- \((\Sigma^\text{exp}_0)^\diamond = \text{EXP}^\diamond\), \((\Sigma^\text{exp}_{i+1})^\diamond = (\text{NEXP}^\diamond)(\Sigma^\text{exp}_i)^\diamond\). Contrast with \(\Sigma^\text{exp}_{i+1} = \text{NEXP}^\Sigma^p_i\) (unbounded queries).

- \(P^\diamond \neq NP^\diamond\).

- Savitch’s works so PSPACE\(^\diamond\) = NPSPACE\(^\diamond\).

- Complexity classes \(P^\diamond\), PSPACE\(^\diamond\), \(\Box^\text{exp}_i\), etc. agree with ordinary counterparts when restricted to strings.
Third-Order Computation

• $(\Sigma^\text{exp}_i)^\diamond = (\Sigma_i - \text{time}(\exp))^{\diamond}$ and is represented by $\Sigma^B_i$-formulas.

• $(\Sigma^\text{exp}_i)^\diamond = (\Pi^\text{exp}_i)^\diamond$ implies the collapse of the hierarchy, contrary to what is known in the ordinary setting.

• Function calculus with nice properties (classes closed under composition, etc.).

• Recursion-theoretic characterization of P, PSPACE, EXP functions.
Recursion-Theoretic Characterizations

- **Initial functions:**
  \[ I = \{0, 1, x + y, x \cdot y, 1^x, |X|, s_0(X), s_1(X), \text{bit}(x, Y), X \rightarrow Y, X \in \mathcal{Y}\} \]

- **Limited recursion:**
  \[ \tilde{f}(0, \ldots) = \tilde{g}(\ldots), \tilde{f}(x + 1, \ldots) = \tilde{h}(x, \tilde{f}(x, \ldots), \ldots) \]
  and either \( \tilde{f}(x, \ldots) \leq l(x, \ldots) \) or \( |\tilde{f}(x, \ldots)| \leq l(x, \ldots) \)

- **Limited doubling recursion:**
  \[ \tilde{f}(0, \tilde{y}, \ldots) = \tilde{g}(\tilde{y}, \ldots), \tilde{f}(x + 1, \tilde{y}, \ldots) = \tilde{f}(x, \tilde{f}(x, \tilde{y}, \ldots), \ldots) \]
  and either \( \tilde{f}(x, \tilde{y}, \ldots) \leq l(x, \ldots) \) or \( |\tilde{f}(x, \tilde{y}, \ldots)| \leq l(x, \ldots) \)

- **Limited 3-comprehension:**
  \[ \mathcal{F}(..)(X) \leftrightarrow (|X| \leq g(\ldots) \land h(X, \ldots) = 0) \]
Recursion-Theoretic Characterizations

- Closure of $I$ under composition, limited 3-comprehension and limited recursion is \( \text{FPSPACE}^+ \)
  - (limited recursion restricted to number- and string-valued functions gives a version of P)

- Closure of $I$ under composition, limited 3-comprehension and limited doubling recursion is \( \text{FEXP}^+ \)
  - (limited doubling recursion restricted to number- and string-valued functions gives \( \text{FPSPACE}^+ \))
Third-Order Theories $W_i^1$ ($TW_i^1$)

- $\mathcal{L}_A^3 = \{0, 1, +, \cdot, |, \cdot|_2, \in_2, \in_3, \leq, =_1, =_2\}$ (Note: third sort unbounded)

- Axioms of $V^0$; Strict $\forall^2\Sigma_i^B$-IND

- $\Sigma_0^B$-3COMP: $(\exists Y)(\forall Z \leq s(\overline{x}, \overline{X}))[\phi(\overline{x}, \overline{X}, \overline{X}, Z) \leftrightarrow Y(Z)]$

- $\Sigma_0^B$-2COMP: $(\exists Y \leq t(\overline{x}, \overline{X}))(\forall z \leq s(\overline{x}, \overline{X}, Y))[\phi(\overline{x}, \overline{X}, \overline{X}, z) \leftrightarrow Y(z)]$
  ($Y, Y$ not free in $\phi$)

$TW_i^1$ has (strict) $\Sigma_i^B$-SIND (string induction) instead.
Definability and Witnessing Theorems

• For $i \geq 1$ the $(\square_i^{\text{exp}})^+$ functions (of all input and output sorts) are $\Sigma_i^B$-definable in $TW^i_1$.

• The $(\text{FPSPACE}^{(\Sigma_i^{\text{exp}})^{\diamond}})^+$ functions (of all sorts) are $\Sigma_i^B$-definable in $W^i_1$ ($i \geq 1$).

• Corresponding witnessing theorems for $\Sigma_i^B$-definable functions of these theories ($i \geq 1$).

• These theorems are analogous to the ones by Buss, Krajíček and Takeuti for $U^i_2$ and $V^i_2$. 
Application of the Function Calculus

- $HW_1^0$ is $W_1^0$ with $\Sigma^B_0$-HRC:

  $$\exists \mathcal{X} \phi^{\text{hrc}}(x, \mathcal{X}),$$

  where $\phi(Y, \mathcal{X}) \in \Sigma^B_0$, and

  $$\phi^{\text{hrc}}(S, \mathcal{X}) \equiv \forall Y \leq x(\mathcal{X}(Y) \leftrightarrow \phi(Y, \mathcal{X}^{Y/2})).$$

- Universal conservative extension $\overline{HW_1^0}$ of $HW_1^0$ defined with language of FPSPACE$^+$ functions

- Should work for FEXP$^+$ (and maybe $TTW_1^0$?) also
Conclusion

• Bounded arithmetic is important

• The second-order “viewpoint” unifies and clarifies presentation and notation

• Second-order theories are much more appropriate for smaller complexity classes

• Third-order theories are a natural extension of this viewpoint to larger complexity classes