

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
- $\mathcal{L}_A^1 = \{0, 1, +, \cdot, \leq, =\}$ $\mathcal{L}_A^2 = \mathcal{L}_A^1 \cup \{|\cdot|_2, \in_2\}$ Smash: $x \# y = 2^{|x| \cdot |y|}$
- Σ_i^b : i alternations of bd. 1st order Q's, outermost existential
- Σ_i^B : Count 2nd order Q's
- Φ -IND: $\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x+1)) \rightarrow \forall x \leq t \phi(x)$ $(\phi \in \Phi)$
- Φ -PIND: $\phi(0) \wedge \forall x(\phi(\lfloor \frac{x}{2} \rfloor) \rightarrow \phi(x)) \rightarrow \forall x \leq t \phi(x)$ $(\phi \in \Phi)$

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_2^1, V_2^1
- Buss-Krajíček-Takeuti 1993: U_2^i, V_2^i
- 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, $\Delta_1^b - CR$
- P, eFrege, S_2^1 / PV
- PLS, G_1 , T_2^1
- \square_i^p , G_i^* , S_2^i
- PSPACE, G , U_2^1
- 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_2^i vs. V^i

- S_2^i [Buss]: $\mathcal{L}_A^1 \cup \{\#, | \cdot |_1, [\cdot]_2\}$, BASIC, Σ_i^b -PIND. \square_i^p functions Σ_i^b -definable in S_2^i . Very technical (e.g. $|\text{BASIC}|=32$)
- V^i [Zambella]: \mathcal{L}_A^2 , 14 axioms + strict- Σ_i^B -IND + comprehension. Σ_i^B -defines \square_i^p -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 , 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]: $\mathcal{L}_A^2 \cup \{\#, | \cdot |_1, \lfloor \cdot \rfloor_2\}$, BASIC, Σ_1^b -PIND. Σ_1^B -defines PSPACE (number-)functions
- G [Dowd]: Propositional sequent calculus with Σ_∞^q formulas (propositional quantifiers)
- Σ_0^B theorems of U_2^1 translate to polysize families of G proofs [Krajíček-Takeuti] but very difficult even to state (Cook style, numbers \longrightarrow 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]

- Σ_i^B formulas defined analogously to Σ_i^b counting second-order quantifiers
- Σ_0^B -Comprehension
- Σ_i^B -PIND (-IND)
- Language includes $|\cdot|_1$, $\lfloor \cdot / 2 \rfloor$, “smash”: $x \# y = 2^{|x| \cdot |y|}$
- Σ_i^B -definable **number**-functions exactly $\text{PSPACE}^{\Sigma_{i-1}^B}$ ($\text{EXP}^{\Sigma_{i-1}^B}$)
- 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.
- $(\Sigma_0^{exp})^\diamond = \text{EXP}^\diamond$, $(\Sigma_{i+1}^{exp})^\diamond = (\text{NEXP}^\diamond)^{(\Sigma_i^{exp})^\diamond}$. Contrast with $\Sigma_{i+1}^{exp} = \text{NEXP}^{\Sigma_i^p}$ (unbounded queries).
- $\text{P}^\diamond \neq \text{NP}^\diamond$.
- Savitch's works so $\text{PSPACE}^\diamond = \text{NPSPACE}^\diamond$.
- Complexity classes P^\diamond , PSPACE^\diamond , \square_i^{exp} , etc. agree with ordinary counterparts when restricted to strings.

Third-Order Computation

- $(\Sigma_i^{exp})^\diamond = (\Sigma_i - time(exp))^\diamond$ and is represented by $\Sigma_i^{\mathcal{B}}$ -formulas.
- $(\Sigma_i^{exp})^\diamond = (\Pi_i^{exp})^\diamond$ 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:
 $I = \{0, 1, x + y, x \cdot y, 1^x, |X|, s_0(X), s_1(X), \text{bit}(x, Y), X \frown Y, X \in \mathcal{Y}\}$
- Limited recursion: $\tilde{f}(0, \dots) = \tilde{g}(\dots)$, $\tilde{f}(x + 1, \dots) = \tilde{h}(x, \tilde{f}(x, \dots), \dots)$ and either $\tilde{f}(x, \dots) \leq l(x, \dots)$ or $|\tilde{f}(x, \dots)| \leq l(x, \dots)$
- Limited doubling recursion: $\tilde{f}(0, \tilde{y}, \dots) = \tilde{g}(\tilde{y}, \dots)$, $\tilde{f}(x + 1, \tilde{y}, \dots) = \tilde{f}(x, \tilde{f}(x, \tilde{y}, \dots), \dots)$ and either $\tilde{f}(x, \tilde{y}, \dots) \leq l(x, \dots)$ or $|\tilde{f}(x, \tilde{y}, \dots)| \leq l(x, \dots)$
- Limited 3-comprehension: $\mathcal{F}(\dots)(X) \leftrightarrow (|X| \leq g(\dots) \wedge h(X, \dots) = 0)$

Recursion-Theoretic Characterizations

- Closure of I under composition, limited 3-comprehension and limited recursion is 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 FEXP^+
 - (limited doubling recursion restricted to number- and string-valued functions gives FPSPACE^+)

Third-Order Theories W_1^i (TW_1^i)

- $\mathcal{L}_A^3 = \{0, 1, +, \cdot, |\cdot|_2, \in_2, \in_3, \leq, =_1, =_2\}$ (**Note: third sort unbounded**)
- Axioms of V^0 ; Strict $\forall^2 \Sigma_i^{\mathcal{B}}$ -IND
- $\Sigma_0^{\mathcal{B}}$ -3COMP: $(\exists \mathcal{Y})(\forall Z \leq s(\bar{x}, \bar{X}))[\phi(\bar{x}, \bar{X}, \bar{\mathcal{X}}, Z) \leftrightarrow \mathcal{Y}(Z)]$
- $\Sigma_0^{\mathcal{B}}$ -2COMP: $(\exists Y \leq t(\bar{x}, \bar{X}))(\forall z \leq s(\bar{x}, \bar{X}, Y))[\phi(\bar{x}, \bar{X}, \bar{\mathcal{X}}, z) \leftrightarrow Y(z)]$
(Y, \mathcal{Y} not free in ϕ)

TW_1^i has (strict) $\Sigma_i^{\mathcal{B}}$ -SIND (string induction) instead.

Definability and Witnessing Theorems

- For $i \geq 1$ the $(\square_i^{exp})^+$ functions (of all input and output sorts) are $\Sigma_i^{\mathcal{B}}$ -definable in TW_1^i .
- The $(FPSPACE^{(\Sigma_{i-1}^{exp})^\diamond})^+$ functions (of all sorts) are $\Sigma_i^{\mathcal{B}}$ -definable in W_1^i ($i \geq 1$).
- Corresponding witnessing theorems for $\Sigma_i^{\mathcal{B}}$ -definable functions of these theories ($i \geq 1$).
- These theorems are analogous to the ones by Buss, Krajíček and Takeuti for U_2^i and V_2^i .

Application of the Function Calculus

- HW_1^0 is W_1^0 with $\Sigma_0^{\mathcal{B}}$ -HRC:

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

where $\phi(Y, \mathcal{X}) \in \Sigma_0^{\mathcal{B}}$, 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