Bounded Reverse Mathematics

Stephen Cook
(joint work with Phuong Nguyen)
June 21, 2007

“Reverse Mathematics” introduced in [Fr76],...

Subsystems of Second Order Arithmetic [Sim99]

Goal of Reverse Mathematics:
“Given a theorem τ of ordinary mathematics, what is the weakest natural subsystem $S(\tau)$ of $\mathbf{Z}_2$ in which τ is provable?”

However the weakest system in Simpson’s book is RCA_0, in which all primitive recursive functions are provably total.

“Finite Reverse Mathematics” from [Friedman 99,01] considers weaker systems, but this has not been pursued.

Our Goal: Concentrate on theorems involving concepts of smaller complexity, especially the polynomial space and below.

Our specific goal: Classify these theorems based on the computational complexity of the concepts needed to prove them.

This is a fundamental question of **Proof Complexity**. Closely related to propositional proof complexity.

Side Benefit: Simplify Proofs
(Razborov greatly simplified the proof of Hastad's Switching Lemma)

Complexity Classes for this talk:

$\mathbf{AC^0} \subset \mathbf{AC^0}(2) \subset \mathbf{TC^0} \subseteq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC} \subseteq \mathbf{P}$

Complexity Questions:
$\mathbf{AC^0}(6) = \mathbf{TC^0} = \ldots = \mathbf{P} = \mathbf{NP} = \mathbf{PH}$??

Proof Complexity (Reverse Math) Questions:
(1) Given a theorem, what is the least complexity class containing enough concepts to prove the theorem?

Examples:
pigeonhole principle ($\mathbf{TC^0}$, not $\mathbf{AC^0}$)
discrete Jordan curve theorem ($\mathbf{AC^0}$ or $\mathbf{AC^0}(2)$)
st-connectivity principle ($\mathbf{AC^0}$ or $\mathbf{AC^0}(2)$)
matrix identities ($\mathbf{P}$ – what about $\mathbf{NC}$?)
prime factorization theorem ($\mathbf{P}$ – Buss's $\mathbf{S}^1_2$)

(2) Can the correctness of an algorithm solving a problem in a given complexity class be proved using only concepts in that class?

Positive Examples:

Natural complete problems

$Parity(X)$	$\mathbf{V^0}(2)$
$numones(X)$	$\mathbf{TC^0}$
$Directed\text{-}Reach(z, Y)$	$\mathbf{NL}$
$MCVP$	$\mathbf{P}$

Possible Negative Examples:

computing the determinant	$\mathbf{NC}^2$ vs $\mathbf{P}$
prime recognition	$\mathbf{P}$ vs **PH**
L = **SL**	**SL** vs **P**
SL = co**SL**	**SL** vs **P**

But $\mathbf{NL} = co\mathbf{NL}$ is provable with **NL** reasoning. [C,Kol 04]

Goal: For each complexity class, introduce a *cononical* minimal logical theory which captures reasoning using concepts in that class.

History:
C 1975 Introduced an equational theory $\mathbf{PV}$ (like Skolem's **PRA**) for reasoning about polynomial time. **PV** has function symbols for all polytime functions
$f : \mathbb{N}^k \to \mathbb{N}$ with equational axioms based on Cobham's Theorem.

Buss ca 1983 (**Independently of [C 75]**) thought up the theory $\mathbf{S}^1_2$ for polytime.
Theorem: [Buss 86] The Σ^b_1 theorems of **QPV** and $\mathbf{S}^1_2$ are essentially the same.

Question Can **PV** and $\mathbf{S}^1_2$ be modified to capture small complexity classes?

Difficulty: Their vocabulary contains $x{\cdot}y$, which is NOT in $\mathbf{AC^0}$ or $\mathbf{AC^0}(2)$.

Solution: Use two-sorted theories.

Two-Sorted Theories ("Second Order Arithmetic") Standard for formalizing analysis (e.g. [Sim99])
In bounded arithmetic: [Buss 86], [Zambella 96]

"number" variables $x, y, z...$ (range over $\mathbb{N}$)

"string" variables $X, Y, Z...$
range over finite subsets of $\mathbb{N}$
(arbitrary subsets of $\mathbb{N}$ for analysis)

Language $\mathcal{L}_A^2 = [0, 1, +, \cdot, |\ |; \in, \leq, =_1, =_2]$

Standard model $\mathbb{N}_2 = \langle \mathbb{N}, \text{finite}(\mathbb{N}) \rangle$

$0, 1, +, \cdot, \leq, =$ usual meaning over $\mathbb{N}$

$$|X| = \begin{cases} 1 + \text{sup}(X) & \text{if } X \neq \emptyset \\ 0 & \text{if } X = \emptyset \end{cases}$$

$x \in X$ (set membership)

number terms $s, t, u...$ defined as usual
only string terms are variables $X, Y, Z, ...$

Notation: $X(t) \equiv t \in X$, t a term

Definitions: Σ_0^B formula: All number quantifiers bounded.
No string quantifiers. (Free string variables allowed.)

Σ_1^B formula has the form

$$\exists Y_1 \leq t_1 ... \exists Y_k \leq t_k \ \phi$$

$k \geq 0$, ϕ is Σ_0^B.

$\exists X \leq t \ \phi$ stands for $\exists X(|X| \leq t \wedge \phi)$, where t does not involve X.

Σ_1^1 is the class of formulas

$$\exists \vec{Y} \phi \qquad \phi \in \Sigma_0^B$$

Σ_i^B formulas begin with at most i blocks of bounded string quantifiers $\exists\forall\exists$... followed by a Σ_0^B formula.

Note: Σ_i^B corresponds to **strict** $\Sigma_i^{1,b}$.

Two-Sorted Complexity Classes

In general, number inputs $x, y, z...$ are presented in unary.
String inputs $X, Y, Z, ...$ are presented as bit strings.

Definition A relation $R(\vec{x}, \vec{X})$ is in $\mathbf{AC^0}$ iff some ATM (alternating Turing machine) accepts R in time $O(\log n)$ with a constant number of alternations.

Representation Theorem [BIS,I,Wrathall]
(a) The Σ_0^B formulas $\phi(\vec{x}, \vec{X})$ represent precisely the relations $R(\vec{x}, \vec{X})$ in $\mathbf{AC^0}$.

(b) The Σ_1^B formulas represent precisely the **NP** relations.

(c) The Σ_i^B formulas, $i \geq 1$, represent precisely the Σ_i^p relations.

Function Classes and Bit Graphs

Definition If **C** is a class of relations, then the function class **FC** contains

(a) All p-bounded number-valued functions $f(\vec{x}, \vec{X})$ s.t. its graph

$$G_f(y, \vec{x}, \vec{X}) \equiv (y = f(\vec{x}, \vec{X}))$$

is in **C**.

(b) All p-bounded string-valued functions $F(\vec{x}, \vec{X})$ such that its bit graph

$$B_F(i, \vec{x}, \vec{X}) \equiv F(\vec{x}, \vec{X})(i)$$

is in **C**.

p-bounded means for some polynomial $q(\vec{x}, \vec{X})$:
$f(\vec{x}, \vec{X}) \leq q(\vec{x}, |\vec{X}|)$
$|F(\vec{x}, \vec{X})| \leq q(\vec{x}, |\vec{X}|)$

All functions in $\mathbf{FAC^0}$ must have graphs (or bit graphs) representable by Σ_0^B formulas

Example: $Plus(X,Y) = X + Y$ (binary $+$)
$Plus \in \mathbf{FAC^0}$

$$Plus(X,Y)(i) \equiv X(i) \oplus Y(i) \oplus Carry(X,Y,i)$$

$$\begin{aligned} Carry(i,X,Y) \;&\equiv\; \exists j < i[X(j) \wedge Y(j) \wedge \\ &\qquad \forall k < i(j < k \supset (X(k) \vee Y(k))] \end{aligned}$$

NON-Examples:
$X \cdot Y$ (binary multiplication) NOT in $\mathbf{FAC^0}$.
$Parity(X) \equiv X$ has an odd number of ones.
$Parity \notin \mathbf{AC^0}$ (Ajtai, FSS)
$Parity(X)$ NOT representable by a Σ_0^B formula.

Hierarchy of Theories $\mathbf{V^0} \subset \mathbf{V}^1 \subseteq \mathbf{V}^2 \subseteq ...$
All have underlying vocabulary $\mathcal{L}_A^2$
For $i \geq 1$, $\mathbf{V}^i$ is "RSUV" isomorphic to $\mathbf{S}_2^i$.

2-BASIC Axioms for $\mathbf{V}^i, i \geq 0$ [Zam96]

B1. $x + 1 \neq 0$
B2. $x + 1 = y + 1 \supset x = y$
B3. $x + 0 = x$
B4. $x + (y + 1) = (x + y) + 1$
B5. $x \cdot 0 = 0$
B6. $x \cdot (y + 1) = (x \cdot y) + x$
B7. $(x \leq y \wedge y \leq x) \supset x = y$
B8. $x \leq x + y$
B9. $0 \leq x$
B10. $x \leq y \vee y \leq x$
B11. $x \leq y \leftrightarrow x < y + 1$
B12. $x \neq 0 \supset \exists y \leq x(y + 1 = x)$
L1. $X(y) \supset y < |X|$
L2. $y + 1 = |X| \supset X(y)$
SE. $[|X| = |Y| \wedge \forall i < |X|(X(i) \leftrightarrow Y(i))] \supset X = Y$

Also $\mathbf{V}^i$ needs $\mathbf{\Sigma_i^B}$-COMP (Comprehension)

$$\exists Z \leq y \forall j < y[Z(j) \leftrightarrow \phi(j, \vec{x}, \vec{X})]$$

where $\phi(j, \vec{x}, \vec{X})$ is a $\mathbf{\Sigma_i^B}$ formula without Z.

Theorem $\mathbf{V^0}$ proves
(because $|X| = 1+$ largest element of X...)

X-MIN

$$0 < |X| \supset \exists x < |X|(X(x) \wedge \forall y < x \neg X(y))$$

and X-IND

$$[X(0) \wedge \forall y < z(X(y) \supset X(y+1))] \supset X(z)$$

Therefore for $i = 0, 1, 2, ...$
$\mathbf{V}^i$ proves (using Σ_i^B-COMP)

Σ_i^B-IND: $\quad [\phi(0) \wedge \forall x(\phi(x) \supset \phi(x+1))] \supset \forall z \phi(z)$

and

Σ_i^B-MIN: $\quad \exists x \phi(x) \supset \exists x[\phi(x) \wedge \neg \exists y(y < x \wedge \phi(y))]$

where $\phi(x)$ is any Σ_i^B-formula (with parameters).

Fact: $\mathbf{V^0}$ is a conservative extension of $\mathbf{I\Delta_0}$.
Thus $\mathbf{V^0}$ proves all the usual properties of
$x + y, x \cdot y, |x|, Bit(i, x)$.

Fact: $\mathbf{V}^i$ is finitely axiomatizable ($i \geq 0$).

Pairing Function: $\langle x, y\rangle$ is a **term** of $\mathcal{L}_A^2$.

$$\langle x, y\rangle =_{def} (x+y)(x+y+1)+2y$$

$\mathbf{V^0}$ proves $(x, y) \mapsto \langle x, y\rangle$ is one-one $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

A **two-dimensional array** is represented by a string X. Define

$$X(i, j) = X(\langle i, j\rangle)$$

Then $X^{[i]}$ is row i of the array X. We bit-define the string function $X^{[i]}$ by

$$X^{[i]}(j) \leftrightarrow j < |X| \wedge X(i, j)$$

Example: $PHP(n, X)$ (Pigeonhole Principle)
This is a $\mathbf{\Sigma}_0^B$ formula.
Think $X(i, j)$ means pigeon $i \longrightarrow$ hole j.

$$\begin{array}{l}\forall i \leq n \exists j < n X(i, j) \supset \\ \exists i \leq n \exists j \leq n \exists k < n (i < j \wedge X(i, k) \wedge X(j, k))\end{array}$$

Theorem: (Ajtai) $\mathbf{V^0}$ does not prove $PHP(n, X)$.

$\mathbf{V^0}$ is like $\mathbf{I\Delta_0}(R)$

$\overline{\mathbf{V^0}}$: A universal conservative extension of $\mathbf{V^0}$ (In the spirit of **PV**.)

The vocabulary $\mathcal{L}_{\mathbf{FAC^0}}$ of $\overline{\mathbf{V^0}}$ has function symbols for all (and only) functions in $\mathbf{FAC^0}$. The axioms of $\overline{\mathbf{V^0}}$ consist entirely of universal formulas, and comprise a version of **2-BASIC** axioms of $\mathbf{V^0}$ together with the defining axioms for all new function symbols.

Theorem: $\overline{\mathbf{V^0}}$ is a conservative extension of $\mathbf{V^0}$.

Witnessing (Finding Skolem functions)

Definition: Functions $\vec{F}$ *witness* $\exists \vec{Y} \phi(\vec{x}, \vec{X}, \vec{Y})$ in T if

$$T(\vec{F}) \vdash \phi(\vec{x}, \vec{X}, \vec{F}(\vec{x}, \vec{X}))$$

Theorem: (**Witnessing**) Suppose T is a universal theory which extends $\mathbf{V^0}$, and is defined over a language $\mathcal{L}$ and suppose that for every open formula $\alpha(i, \vec{x}, \vec{X})$ and term $t(\vec{x}, \vec{X})$ over $\mathcal{L}$ there is a function symbol F in $\mathcal{L}$ such that

$$T \vdash F(\vec{x}, \vec{X})(i) \leftrightarrow i < t \wedge \alpha(i, \vec{x}, \vec{X})$$

Then every theorem of T of the form $\exists \vec{Y} \alpha(\vec{x}, \vec{X}, \vec{Y})$, where α is open, is witnessed in T by functions in $\mathcal{L}$.

Proof: Follows from the Herbrand Theorem.

Corollary: Every Σ_1^1 theorem of $\overline{\mathbf{V^0}}$ (and $\mathbf{V^0}$) is witnessed in $\overline{\mathbf{V^0}}$ by functions in $\mathcal{L}_{\mathbf{FAC^0}}$.

Recall SubGoal: Introduce a minimal cononical theory **VC** for each complexity class **C**.

• **VC** has vocabulary $\mathcal{L}_A^2$.

• $\mathbf{VC} = \mathbf{V^0} + \{$one axiom$\}$ (finitely axiomatizable) [Nguyen: see Chapter 9]

• The Σ_1^B-definable functions in **VC** are those in **FC**.

• **VC** has a universal convervative extension $\overline{\mathbf{VC}}$ in the style of **PV**.

class	$\mathbf{AC^0}$	$\subset$	$\mathbf{AC^0}(2)$	$\subset$	$\mathbf{TC^0}$	$\subseteq$	$\mathbf{NC}^1$
theory	$\mathbf{V^0}$	$\subset$	$\mathbf{V^0}(2)$	$\subset$	$\mathbf{VTC}^0$	$\subseteq$	$\mathbf{VNC}^1$

class	$\mathbf{L}$	$\subseteq$	$\mathbf{NL}$	$\subseteq$	$\mathbf{NC}$	$\subseteq$	$\mathbf{P}$
theory	$\mathbf{VL}$	$\subseteq$	$\mathbf{VNL}$	$\subseteq$	$\mathbf{VNC}$	$\subseteq$	$\mathbf{VP} = \mathbf{TV}^0$

Theories VC for other classes C

Recall $\mathbf{VC} = \mathbf{V^0} + \mathbf{Axiom_C}$
where $\mathbf{Axiom_C} = (\mathbf{Complete_C}$ has a solution$)$

class	theory	$\mathbf{Complete_C}$
$\mathbf{AC^0}$	$\mathbf{V^0}$	none
$\mathbf{AC^0}(2)$	$\mathbf{V^0}(2)$	$Parity(X)$
$\mathbf{TC^0}$	$\mathbf{VTC}^0$	$numones(X)$
$\mathbf{NC}^1$	$\mathbf{VNC}^1$	tree-$MCVP$
$\mathbf{L}$	$\mathbf{VL}$	$UniConn(z, a, E)$
$\mathbf{NL}$	$\mathbf{VNL}$	$Conn(z, a, E)$
$\mathbf{P}$	$\mathbf{VP}$	$MCVP$

Robustness Theorems

$\mathbf{VTC}^0 \simeq \Delta_1^B$-**CR** [JP] (proved in [Nguyen])
$\mathbf{VNC}^1 \simeq \mathbf{AID}$ [Arai] (proved in [CM])
$\mathbf{VNC}^1 \simeq ALV \simeq ALV'$ [Clote] (proved by [Nguyen])
$\mathbf{VL} = \Sigma_0^B$-Rec [Zam97]
$\mathbf{VNL} = \mathbf{V\text{-}Krom}$ [Kolokolova]

Discrete Jordan Curve Theorem
[C,Nguyen LICS 07]

Original statement: A simple closed curve divides the plane into exactly two connected components.

(Hales gave a computer-verified proof involving 44,000 proof steps. His proof started with a discrete version.)

Discrete Setting: The curve consists of edges connecting grid points in the plane.

Case I: The curve is given as a set of edges such that every grid point has degree 0 or 2.

(Then there may be more than 2 connected components.)

Theorem: $\mathbf{V}^0(2)$ proves the following:
If B is a set of edges forming a curve and p_1, p_2 are two points on different sides of B, and R is a set od edges that connects p_1 and p_2, then B and R intersect.

Jordan Curve Cont'd

Case II: The curve is given as a sequence of edges.

Theorem: $\mathbf{V^0}$ proves that a curve given by a sequence of edges divides the plane into exactly two connected components.

Lemma: For each column in the planar grid, the edges of a closed curve alternate in direction.

(The proof is difficult in $\mathbf{V^0}$, since no counting is allowed, even mod 2.)

The quantifier complexity of theorems

Simplist: $\forall\Sigma_0^B$: $\forall\vec{x}\forall\vec{X}\phi$ where ϕ is Σ_0^B.

Examples:
- pigeonhole principle
- first part of JCT (at least two components)
- matrix identities: $AB = I \Rightarrow BA = I$

Σ_0^B facts translate into polysize tautolgy families. (Do they have polysize proofs???)

Next case: $\forall\Sigma_1^B$: $\forall\vec{x}\forall\vec{X}\exists\vec{Y} \leq \vec{t}\phi$ where ϕ is Σ_0^B.

Examples:
- second part of JCT (at most two components)
- existence of function values $Parity(X)$ etc.
- correctness of any prime recognition algorithm

$$\forall X\exists Y, Z[(\neg Prime(X) \wedge X \neq 1) \rightarrow X = Y \cdot Z \wedge X, Y \neq 1]$$

(So by Witnessing, correctness cannot be proved in **VP** unless factoring has a polytime algorithm.)

Theorems of higher quantifier complxity

$\forall\Sigma_2^B$: $\quad \forall\vec{x}\forall\vec{X}\exists\vec{Y} \le \vec{t}\forall\vec{Z} \le \vec{u}\phi$ where ϕ is Σ_0^B.

Example:
- induction axiom (or length max principle) for Σ_1^B formulas
- Prime Factorization Theorem for $\mathbf{N}$

Prime Factorization can be proved in $\mathbf{V}^1$ (i.e. $\mathbf{S}_2^1$) by the Σ_1^B length max principle [Jerabek]

Prime Factorization cannot be proved in **VPV** (i.e. PV), unless products of two primes can be factored in polytime (KPT witnessing)

Robustness of Theories

Many theories (first and second order) have been proposed for different complexity classes C. For a given C, they all have essentially the same $\forall\Sigma_0^B$ and $\forall\Sigma_1^B$ theorems. But they may not have the same $\forall\Sigma_2^B$ theorems.

Bounded Reverse Analysis

Ferreira [88,94,00,05,06] introduced a two-sorted system BTFA (Base Theory for Feasible Analysis) in which the functions definable on the first sort ($\{0,1\}^*$) are polytime.

BTFA together with various versions of Weak Konig's Lemma can prove the Heine-Borel Theorem for [0,1], and the max principle for continuous functions on [0,1].

Work to do: Tie in these theories more closely with the complexity theory of real functions [Friedman, Ko, Weirauch, Braverman ...]

Open Questions

Classify basic theorems graph theory, linear algebra, number theory, calculus according to the complexity of the concepts needed for their proof:

Hall's Theroem, Menger's Theorem, Kuratowski's Theorem, Cayley-Hamilton Theorem, Fermat's Little Theorem, Fundamental Theorem of Algebra, Fundamental Theorem of Calculus, ...

advertisement advertisement advertisement

Foundations of Proof Complexity: Bounded Arithmetic and Propositional Translations

Stephen Cook

Phuong Nguyen

Partial draft (300 pages) available on our web sites.

Comments and Corrections Welcome!