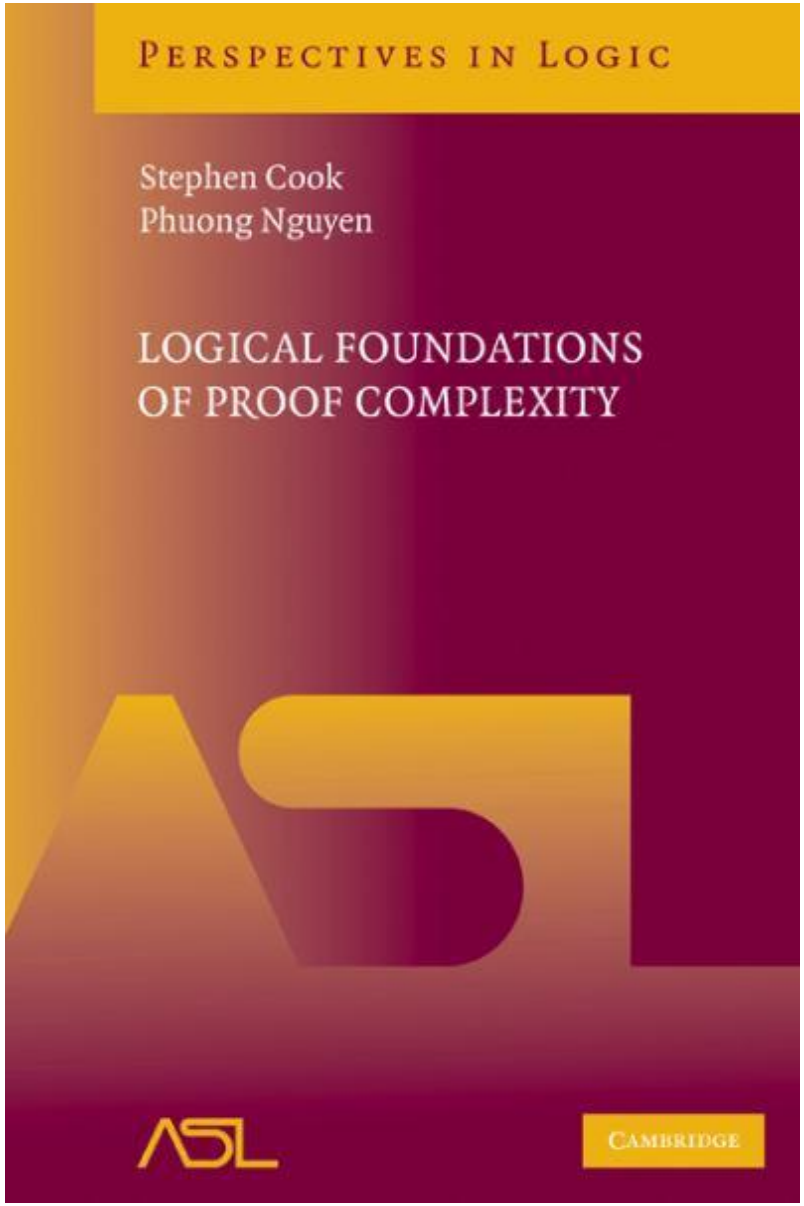
Bounded Reverse Mathematics

Stephen Cook

Department of Computer Science
University of Toronto
Canada

The Banff Workshop on Proof Complexity 2011

Reference


PERSPECTIVES IN LOGIC
Stephen Cook
Phuong Nguyen
LOGICAL FOUNDATIONS
OF PROOF COMPLEXITY
ASL
CAMBRIDGE

- "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

test Concentrate on theorems involving concepts of smaller complexity, especially the polynomial hierarchy 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.

Motivation

- Shed light on complexity classes
- Simplify Proofs
  (Razborov greatly simplified the proof of Hastad's Switching Lemma)

Our Goal

test Concentrate on theorems involving concepts of smaller complexity, especially the polynomial hierarchy 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.

Motivation

- Should be clear to logicians
- Shed light on complexity classes
- Simplify Proofs
  (Razborov greatly simplified the proof of Hastad's Switching Lemma)
- Propositional Proof Systems (PHP example)

Theories for Polytime reasoning:

- **PV** [Cook 1975] Equational theory with function symbols for all polytime functions $f : \mathbb{N}^k \to \mathbb{N}$. Inspired by Skolem's Primitive Recursive Arithmetic (1923).
- **PV** functions introduced via Cobham's 1963 characterization of polytime functions: The least class containing initial functions and closed under composition and limited recursion on notation. **Rule:** Induction on notation
- **PV Nowadays** refers to a first-order theory with polytime function symbols as before, and **universal axioms** based on Cobham's theorem.

Theorem

PV *proves the induction scheme for open formulas* φ*:*

$$[\varphi(0) \wedge \forall x(\varphi(x) \supset \varphi(x+1))] \supset \forall y \varphi(y)]$$

Proof: Use binary search.

PV Witnessing Theorem:

If $\mathbf{PV} \vdash \forall \vec{x} \exists y \varphi(\vec{x}, y)$, where φ is open (i.e. expresses a polytime predicate) then there is a polytime f such that

$$\mathbf{PV} \vdash \forall \vec{x} \varphi(\vec{x}, f(\vec{x}))$$

Proof.

Immediate from Herbrand Theorem. □

- $\mathbf{S}^1_2$ [Buss 86] Finitely axiomatizable first-order theory, including an INDUCTION SCHEME for **NP** formulas.
- **Theorem:**[Buss 86] **PV** and $\mathbf{S}^1_2$ prove the same $\forall\exists\varphi$ theorems, where φ expresses a polytime predicate.
- **Theorem:**[KPT91],[Buss95],[Zam96] If $\mathbf{S}^1_2 \subseteq \mathbf{PV}$ then the polynomial hierarchy collapses.
- V_1-Horn [CoKol 03] A finitely-axiomatizable theory. **PV** is a conservative extension.
- $\mathbf{VP}, \mathbf{TV^0}$ [Nguyen], [Cook] Different axiomatizations of V_1-Horn.

PV is a ROBUST MINIMAL THEORY for **P**.

Theses: ('Polytime proof' means PV proof.)

1. 'Natural' polytime algorithms usually have polytime correctness proofs.
2. Combinatorial theorems of interest in computer science often have polytime proofs.
   - Kuratowski's Theorem
   - Hall's Theorem
   - Menger's Theorem
   - Linear Algebra (Cayley-Hamilton, determinant,...)
   - Extended Euclidean Algorithm

Possible Counter-Example to 1): Primes in **P**. [AKS 04] Correctness: $\neg Prime(n) \wedge n \geq 2 \supset \exists d(1 < d < n \wedge d|n)$
By Witnessing Theorem, provable in **PV** implies factoring in polytime. (Applies to any polytime algorithm for Primes.)

Possible counterexample to 2):
Fermat's Little Theorem:

$$\text{Prime}(n) \wedge 1 \leq a < n \;\rightarrow\; a^{n-1} \equiv 1 (\text{mod}\, n)$$

Contrapositive:

$$\forall a, n \exists d < n (a^{n-1} \not\equiv 1 (\text{mod}\, n) \;\rightarrow\; d \neq 1 \wedge d | n)$$

Thus if **PV** proves this then by the witnessing theorem d can be found from a, n in time polynomial in $|n|$.
This leads to a probabilistic polytime algorithm for factoring.

Some Complexity Classes

$$\mathbf{AC^0} \subset \mathbf{AC^0}(2) \subset \mathbf{AC^0}(6) \subseteq \mathbf{TC^0} \subseteq$$
$$\subseteq \mathbf{NC^1} \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PH}$$

Embarrassing Complexity Question

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

This motivates studying (apparently) small complexity classes.

Some Complexity Classes

$$\mathbf{AC^0} \subset \mathbf{AC^0}(2) \subset \mathbf{AC^0}(6) \subseteq \mathbf{TC^0} \subseteq$$
$$\subseteq \mathbf{NC^1} \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PH}$$

Embarrassing Complexity Question

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

This motivates studying (apparently) small complexity classes.

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 $\mathbf{AC^0}(2)$)
matrix identities ($\mathbf{P}$ – what about $\mathbf{NC}$?)
prime factorization theorem ($\mathbf{S}^1_2$ but not $\mathbf{PV}$?)

Circuit Complexity Classes

Problems are specified by a (uniform) poly-size family $\langle C_n \rangle$ of Boolean circuits.
C_n solves problems with input length n.

- $\mathbf{AC^0}$: bounded depth, unbounded fan-in $\wedge, \vee$.
  Contains binary $+$ but not parity or $\times$
- $\mathbf{AC^0}(2)$: allow unbounded fan-in parity gates.
  Cannot count mod 3 [Raz 87],[Smo 87]
- $\mathbf{AC^0}(6)$: allow unbounded fan-in mod 6 gates.
  Might be all of $\mathbf{PH}$. (Contains $\times$??)
- $\mathbf{TC^0}$: allow threshold gates.
  Contains binary $\times$
- $\mathbf{NC^1}$: circuits must be trees (formulas).

Propositional Proof Systems

Definition

- A prop proof system is a polytime function F from $\{0,1\}^*$ onto tautologies.
- If $F(X) = A$ then F is a proof of A.
- We say F is *poly-bounded* if every tautology of length n has a proof of length $n^{O(1)}$.

Easy Theorem

A poly-bounded prop proof system exists iff **NP** = **coNP**.

Propositional Proof Systems

Definition

- A prop proof system is a polytime function F from $\{0,1\}^*$ onto tautologies.
- If $F(X) = A$ then F is a proof of A.
- We say F is *poly-bounded* if every tautology of length n has a proof of length $n^{O(1)}$.

Easy Theorem

A poly-bounded prop proof system exists iff **NP** = **coNP**.

Example

Frege Systems (Hilbert systems)
Finiteley many axiom schemes and rule schemes.
Must be sound and implicationally complete.
All Frege systems are essentially equivalent.
Gentzen's propositional **LK** is an example.

Propositional Proof Systems

Definition

- A prop proof system is a polytime function F from $\{0,1\}^*$ onto tautologies.
- If $F(X) = A$ then F is a proof of A.
- We say F is *poly-bounded* if every tautology of length n has a proof of length $n^{O(1)}$.

Easy Theorem

A poly-bounded prop proof system exists iff **NP** = **coNP**.

Example

Frege Systems (Hilbert systems)
Finiteley many axiom schemes and rule schemes.
Must be sound and implicationally complete.
All Frege systems are essentially equivalent.
Gentzen's propositional **LK** is an example.

Embarrassing Fact

No nontrivial lower bounds known on proof lengths for Frege systems. (So maybe Frege systems are poly-bounded??)

Hard tautologies from combinatorial principles

Pigeonhole Principle

If $n+1$ pigeons are placed in n holes, some hole has at least 2 pigeons.

- Atoms p_{ij} (pigeon i placed in hole j)
  $1 \leq i \leq n+1,\ 1 \leq j \leq n$
- $\neg\mathrm{PHP}_n^{n+1}$ is the conjunction of clauses:
- $(p_{i1} \vee \ldots \vee p_{in})$ (pigeon i placed in some hole) $1 \leq i \leq n+1$
- $(\neg p_{ik} \vee \neg p_{jk})$ (pigeons i, j not both in hole k)
  $1 \leq i < j \leq n+1,\ 1 \leq k \leq n$
- $\neg\mathrm{PHP}_n^{n+1}$ is unsatisfiable: $O(n^3)$ clauses

Theorem (Buss)

PHP_n^{n+1} has polysize Frege proofs.
[$\mathbf{NC}^1$ can count pigeons and holes.]

Theorem (Ajtai)

PHP_n^{n+1} does not have polysize $\mathbf{AC}^0$-Frege proofs.
[$\mathbf{AC}^0$ cannot count.]

- Thus the Pigeonhole Principle can be proved using $\mathbf{NC}^1$ concepts, but not using $\mathbf{AC}^0$ concepts.
- This motivates finding theories for the complexity classes $\mathbf{NC}^1$ and $\mathbf{AC}^0$.
- These should correspond to the propositional proof systems Frege and $\mathbf{AC}^0$-Frege.

Theories for Small Complexity Classes

Two-Sorted Theories

("Second Order Arithmetic") [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 $\mathbb{N}$

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

- $y \in X$ (set membership) (Write $X(y)$)
- 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

Definition

- Σ_0^B formula: All number quantifiers bounded.
  No string quantifiers. (Free string variables allowed.)
- Σ_1^B formula has the form

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

  $k \geq 0$, φ is Σ_0^B.
  $\exists X \leq t \ \varphi$ stands for $\exists X(|X| \leq t \wedge \varphi)$, where t does not involve X.
- Σ_1^1 is the class of formulas

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

- 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]

1. The Σ_0^B formulas $\varphi(\vec{x}, \vec{X})$ represent precisely the relations $R(\vec{x}, \vec{X})$ in $\mathbf{AC^0}$.
2. The Σ_1^B formulas represent precisely the **NP** relations.
3. 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

1. 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**.

2. 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 $+$), $Plus \in \mathbf{FAC^0}$

$$Plus(X, Y)(i) \equiv X(i) \oplus Y(i) \oplus Carry(X, Y, i)$$
$$Carry(i, X, Y) \equiv \exists j < i[X(j) \wedge Y(j) \wedge \forall k < i(j < k \supset (X(k) \vee Y(k))]$$

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 $\mathbf{V^0} \subset \mathbf{V^1} \subseteq \mathbf{V^2} \subseteq \ldots$

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 $\mathbf{\Sigma}^{\mathbf{B}}_{\mathbf{i}}$-COMP (Comprehension)

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

where $\varphi(j, \vec{x}, \vec{X})$ is a $\mathbf{\Sigma}^{\mathbf{B}}_{\mathbf{i}}$ formula without Z.

Theorem

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

$$X\text{-}MIN: \qquad 0 < |X| \supset \exists x < |X|(X(x) \wedge \forall y < x\, \neg X(y))$$
$$X\text{-}IND: \qquad [X(0) \wedge \forall y < z(X(y) \supset X(y+1))] \supset X(z)$$

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

$$\Sigma^B_i\text{-}IND: \qquad [\varphi(0) \wedge \forall x(\varphi(x) \supset \varphi(x+1))] \supset \forall z \varphi(z)$$
$$\Sigma^B_i\text{-}MIN: \qquad \exists x \varphi(x) \supset \exists x[\varphi(x) \wedge \neg\exists y(y < x \wedge \varphi(y))]$$

where $\varphi(x)$ *is any* Σ^B_i*-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 $x + y$, $x \cdot y$, $|x|$, $Bit(i, x)$.
- $\mathbf{V}^i$ is finitely axiomatizable ($i \geq 0$).

Propositional Translations of Σ_0^B-formulas

(See [C 75, PW 87])

- For each $n \in \mathbb{N}$, $\varphi(X)[n]$ is propositional formula expressing $\varphi(X)$ when $|X| = n$.
- The propositional variables of $\varphi(X)[n]$ are $p_0^X, \ldots, p_{n-1}^X$

Example

$Pal(X)$ says "X is a palindrome".

$$\forall y < |X|(X(y) \leftrightarrow X(|X| \dot{-} y \dot{-} 1))$$

Then $Pal(X)[4]$ is

$$(p_0^X \leftrightarrow p_3^X) \wedge (p_1^X \leftrightarrow p_2^X) \wedge (p_2^X \leftrightarrow p_1^X) \wedge (p_3^X \leftrightarrow p_0^X)$$

Theorem

1. *If $\varphi(X)$ is true then $\langle \varphi(X)[n] \rangle$ is a poly-size family of tautologies.*
2. *If $V^0 \vdash \varphi(X)$ then $\langle \varphi(X)[n] \rangle$ has polysize $\mathbf{AC^0}$-Frege proofs.*

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: $PHP(y, X)$ (Pigeonhole Principle). This is a Σ_0^B formula.
Think $X(i, j)$ means pigeon $i \longrightarrow$ hole j.

$$\forall i \le y \exists j < y X(i, j) \supset$$
$$\exists i \le y \exists j \le y \exists k < y(i < j \wedge X(i, k) \wedge X(j, k))$$

$PHP(n, X)[\langle n + 1, n\rangle]$ is very close to the Pigeonhole tautologies PHP_n^{n+1}
Since these tautologies do not have polysize $\mathbf{AC^0}$-Frege proofs (Ajtai) it follows that $\mathbf{V^0}$ does not prove $PHP(y, X)$.

$\overline{\mathbf{V^0}}$: 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* $\mathbf{V^0}$.

Claim

$\overline{\mathbf{V^0}}$ is a **minimal** theory for $\mathbf{AC^0}$, just as **PV** is a **minimal** theory for **P**.

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 $\mathcal{L}_{\mathbf{FAC^0}}$.

Program: (with Phuong Nguyen: Book, Chapter 9)

Introduce a minimal canonical theory **VC** for each complexity class **C**.

- **VC** has vocabulary $\mathcal{L}_A^2$.
- $\mathbf{VC} = \mathbf{V^0} + \{\text{one axiom}\}$ (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-$MCVP$
$\mathbf{L}$	$\mathbf{VL}$	$UniConn(z, a, E)$
$\mathbf{NL}$	$\mathbf{VNL}$	$Conn(z, a, E)$
$\oplus\mathbf{L}$	$\mathbf{V} \oplus \mathbf{L}$	$DET(2)$
$\#\mathbf{L}$	$\mathbf{V}\#\mathbf{L}$	DET
$\mathbf{P}$	$\mathbf{VP}$	$MCVP$

Robustness Theorems

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

Discrete Jordan Curve Theorem [Nguyen/Cook 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 of edges that connects* p_1 *and* p_2*, then* B *and* R *intersect.*

Jordan Curve Cont'd

Theorem [Buss]

$\mathbf{V^0}$ cannot prove the previous version of JCT.

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 (Provable in $\mathbf{V^0}$)

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

Simplest: $\forall\Sigma^B_0$: $\forall\vec{x}\forall\vec{X}\phi$ where ϕ is Σ^B_0.

Examples:

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

$\forall\Sigma^B_0$ facts translate into polysize tautology families. (Do they have polysize proofs???)

Next case: $\forall\Sigma^B_1$: $\forall\vec{x}\forall\vec{X}\exists\vec{Y} \leq \vec{t}\varphi$ where φ is Σ^B_0.

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 complexity

$\forall\Sigma^B_2$: $\forall\vec{x}\forall\vec{X}\exists\vec{Y} \leq \vec{t}\forall\vec{Z} \leq \vec{u}\phi$ where ϕ is Σ^B_0.

Example:

- induction axiom (or length max principle) for Σ^B_1 formulas
- Prime Factorization Theorem for **N**

Prime Factorization can be proved in $\mathbf{V}^1$ (i.e. $\mathbf{S}^1_2$) by the Σ^B_1 length max principle [Jerabek]

Prime Factorization cannot be proved in **VPV** (i.e. PV), unless products of two primes can be factored in random 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 $\forall\Sigma^B_0$ and $\forall\Sigma^B_1$ theorems. But they may not have the same $\forall\Sigma^B_2$ 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, Kawamura, ...]

Conclusion and Open Questions

- It should be easier to separate theories than complexity classes. For example, if we can't show

$$\mathbf{AC^0}(6) \neq \mathbf{P}$$

maybe we can show

$$\mathbf{V^0}(6) \neq \mathbf{VP}$$

- Classify basic theorems graph theory, linear algebra, number theory, calculus according to the complexity of the concepts needed for their proof:
Hall's Theorem, Menger's Theorem, Kuratowski's Theorem, Cayley-Hamilton Theorem, Fermat's Little Theorem, Fundamental Theorem of Algebra, Fundamental Theorem of Calculus, ...