# Formal Reasoning Using Low-Complexity Concepts

Lecture 2: The theory $\mathbf{V^0}$ and the $\mathbf{V}^i$ Hierarchy

Book Reference: Chapters 4,5

Stephen Cook

Fall School, Prague

September, 2008

We base our theories on a **Two-Sorted** ("second-order") language $\mathcal{L}_A^2$ [Zambella 96]

NOTE: The natural inputs for Turing machines and circuits are finite strings.

"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

**Definitions:** $\Sigma_0^B$ formula: All number quantifiers bounded.
No string quantifiers. (Free string variables allowed.)

$\Sigma_1^B$ formula has the form

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

$k \geq 0$, $\varphi$ is $\Sigma_0^B$.

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

$\Sigma_1^1$ is the class of formulas

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

$\Sigma_i^B$ formulas begin with at most $i$ blocks of bounded string quantifiers $\exists\forall\exists$... followed by a $\Sigma_0^B$ formula.

**Note:** $\Sigma_i^B$ 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. [Similarly for two-sorted **P**]

**Representation Theorem** [BIS,I,Wrathall]
(a) The $\Sigma_0^B$ formulas $\varphi(\vec{x}, \vec{X})$ represent precisely the relations $R(\vec{x}, \vec{X})$ in $\mathbf{AC^0}$.

(b) The $\Sigma_1^B$ formulas represent precisely the **NP** relations.

(c) The $\Sigma_i^B$ formulas, $i \geq 1$, represent precisely the $\Sigma_i^p$ 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 $\Sigma_0^B$ formulas

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

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

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

**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 $\Sigma_0^B$ 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 $\mathbf{S}_2^i$.

**Theories** $\mathbf{V}^i, i = 0, 1, 2, ...$ ($\mathbf{V^0}$ captures $\mathbf{FAC^0}$)
(All our theories extend $\mathbf{V^0}$)
**2-BASIC Axioms:**

**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)

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

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

$\mathbf{V^0}$ proves the following
(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 $\mathbf{V}^i$ proves (using $\Sigma_i^B$-COMP)

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

and

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

where $\varphi(x)$ is any $\Sigma_i^B$-formula (with parameters).

## Provably Total Functions

**Definition** Let $\mathcal{T}$ be a theory and let $\Phi$ be a set of $\mathcal{L}$-formulas in $\mathcal{T}$. A function $F$ is $\Phi$-*definable* in $\mathcal{T}$ if there is a formula $\varphi$ in $\Phi$ s.t.

$$\mathcal{T} \vdash \forall \vec{x} \forall \vec{X} \exists ! Y \varphi(\vec{x}, \vec{X}, Y)$$

and

$$Y = F(\vec{x}, \vec{X}) \leftrightarrow \varphi(\vec{x}, \vec{X}, Y)$$

$F$ is *provably total* in $\mathcal{T}$ if $F$ is $\Phi$-definable in $\mathcal{T}$, when $\Phi = \Sigma_1^1$. (If $\mathcal{T}$ is a single-sorted theory, then we take $\Phi = \Sigma_1$.)

**Quiz:** What are the provably total functions in the following single-sorted theories?
**TA** (True Arithmetic)?
**PA** ?
$\mathbf{I}\Sigma_1$? (Induction over $\Sigma_1$ formulas)
$\mathbf{I}\Delta_0$? (Induction over bounded formulas)

We say that $\mathcal{T}$ *captures* the function class **FC** if the provably total functions in $\mathcal{T}$ are precisely **FC**. (**FC** is the function class associated with **C**).

For $i \geq 1$, $\mathbf{V}^i$ is "isomorphic" to Buss's single-sorted $\mathbf{S}_2^i$.

**Facts:**
$\mathbf{V^0}$ captures $\mathbf{FAC^0}$ (we will show this)
$\mathbf{V}^1$ captures **FP** [Buss 86] (cut elim.)

**Definition:** A theory is $p$-*bounded* if it can be axiomatized by formulas of the form $\forall\varphi$, where all quantifiers in $\varphi$ are bounded (or length-bounded) by polynomials.

All theories we consider are $p$-bounded (including $\mathbf{V}^i$).

**Parikh's Theorem:**[1971] If $\mathcal{T}$ is $p$-bounded and

$$\mathcal{T} \vdash \exists Y \varphi(\vec{x}, \vec{X}, Y)$$

where quantifiers in $\varphi$ are $p$-bounded then there is a polynomial term $t(\vec{x}, |\vec{X}|)$ such that

$$\mathcal{T} \vdash \exists Y \leq t \varphi(\vec{x}, \vec{X}, Y)$$

**Corollary:** A function is $\Sigma_1^1$-definable in a $p$-bounded theory $\mathcal{T}$ iff it is $\Sigma_1^B$-definable in $\mathcal{T}$.

For $i > 1$ the $\Sigma_1^B$-definable functions of $\mathbf{V}^i$ do not seem to have a nice characterization, although their $\Sigma_1^B$-definable "**NP** search problems" do [BK,KST,ST].

For example a search problem is $\Sigma_1^B$-definable in $\mathbf{V}^2$ iff it is reducible to a polynomial local search problem. [Buss, Krajíček ]

Buss proved (for $i \geq 1$) that the $\Sigma_i^B$-definable functions in $\mathbf{V}^i$ comprise $\mathbf{FP}^{\Sigma_{i-1}^P}$.

We want to show $\mathbf{V^0}$ captures $\mathbf{FAC^0}$.
One direction is easy:

**Theorem:** Every function in $\mathbf{FAC^0}$ is $\Sigma_1^B$-definable in $\mathbf{V^0}$.

**Proof:** If $F \in \mathbf{FAC^0}$ then the bit graph of $F$ is in $\mathbf{AC^0}$. Hence

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

where $\varphi$ is $\Sigma_0^B$. Thus

$$Y = F(\vec{x}, \vec{X}) \leftrightarrow |Y| \leq t \wedge \forall i < t(Y(i) \leftrightarrow \varphi(i))$$

Then

$$\mathbf{V^0} \vdash \exists Y \leq t \quad RHS$$

by $\Sigma_0^B$-COMP.

(We've shown that $F$ is $\Sigma_0^B$-definable in $\mathbf{V^0}$.)

For the converse (only $\mathbf{FAC^0}$ functions are $\Sigma_0^B$-definable in $\mathbf{V^0}$) it suffices to prove

**Witnessing Theorem for $\mathbf{V^0}$:** If

$$\mathbf{V^0} \vdash \exists \vec{Y} \varphi(\vec{x}, \vec{X}, \vec{Y})$$

where $\varphi$ is $\Sigma_0^B$ then there are $\mathbf{FAC^0}$ functions $\vec{F}$ such that

$$\forall \vec{x}, \vec{X} \varphi(\vec{x}, \vec{X}, \vec{F}(\vec{x}, \vec{X}))$$

Proof 1: [Buss] cut elimination

Proof 2: Apply the Herbrand Theorem to a universal conservative extension $\overline{\mathbf{V^0}}$ of $\mathbf{V^0}$.

$\mathcal{T}$ is *universal* if it can be axiomatized by universal formulas $\forall\varphi$, where $\varphi$ is open.

**Herbrand Theorem:** If $\mathcal{T}$ is a universal two-sorted theory and $\mathcal{T}$ proves $\exists Y \varphi(\vec{x}, \vec{X}, Y)$, where $\varphi$ is open, then there exist string terms $T_1(\vec{x}, \vec{X}), ..., T_n(\vec{x}, \vec{X})$ such that $\mathcal{T}$ proves

$$\varphi(\vec{x}, \vec{X}, T_1) \vee ... \vee \varphi(\vec{x}, \vec{X}, T_n)$$

## Proof of the Witnessing Theorem

We will define $\overline{\mathbf{V^0}}$ to be a universal conservative extension of $\mathbf{V^0}$ whose function symbols stand for the functions in $\mathbf{FAC^0}$.

Thus if $\mathbf{V^0}$ proves $\exists \vec{Y} \varphi(\vec{x}, \vec{X}, Y)$ then so does $\overline{\mathbf{V^0}}$, and in fact $\overline{\mathbf{V^0}}$ proves $\varphi \leftrightarrow \varphi'$ where $\varphi'$ is open, so $\overline{\mathbf{V^0}}$ proves

$$\exists Y \varphi'(\vec{x}, \vec{X}, Y)$$

so by Herbrand there are terms $T_1, ..., T_n$ so $\overline{\mathbf{V^0}}$ proves

$$\varphi(\vec{x}, \vec{X}, T_1) \vee ... \vee \varphi(\vec{x}, \vec{X}, T_n)$$

Define $F$ by cases as follows

$$F(\vec{x}, \vec{X}) = \begin{cases} T_1(\vec{x}, \vec{X}) & \text{if } \varphi'(\vec{x}, \vec{X}, T_1(\vec{x}, \vec{X})) \\ \vdots & \\ T_{n-1}(\vec{x}, \vec{X}) & \text{if } \varphi'(\vec{x}, \vec{X}, T_{n-1}(\vec{x}, \vec{X})) \\ T_n(\vec{x}, \vec{X}) & \text{otherwise} \end{cases}$$

It is easy to see that the bit graph of $F$ is defined by a $\Sigma_0^B$ formula, and witnesses $Y$ in $\varphi(\vec{x}, \vec{X}, Y)$.

It remains to show how to construct $\overline{\mathbf{V^0}}$, a universal conservative extension of $\mathbf{V^0}$ with function symbols for $\mathbf{FAC^0}$.

Suppose $\mathcal{T}$ is a theory and $F$ is a new string function which is definable in $\mathcal{T}$ using $\varphi$, so

$$\mathcal{T} \vdash \exists! Y \varphi(\vec{x}, \vec{X}, Y) \tag{1}$$
$$Y = F(\vec{x}, \vec{X}) \ \leftrightarrow \ \varphi(\vec{x}, \vec{X}, Y) \tag{2}$$

Then $\mathcal{T}(F)$ extends $\mathcal{T}$ by adding $F$ to the vocabulary of $\mathcal{T}$ and the formula (2) as a defining axiom for $F$.

**Lemma:** $\mathcal{T}(F)$ is a conservative extension of $\mathcal{T}$.

(Similarly we define $\mathcal{T}(f)$ for number functions $f$.)

We define the function symbols in $\overline{\mathbf{V^0}}$ using two schemes:

$$F_{\varphi(z),t}(\vec{x}, \vec{X})(z) \leftrightarrow (z < t(\vec{x}, \vec{X}) \wedge \varphi(z, \vec{x}, \vec{X}))$$

and (omitting $\vec{x}, \vec{X}$ and writing $f$ for $f_{\varphi(z),t}$)

$$f \leq t \wedge (f < t \supset \varphi(f) \wedge (v < f \supset \neg\varphi(v))$$

We apply these schemes when $\varphi(z)$ is open in a vocabulary extending $\mathcal{L}_A^2$, and $t$ is an $\mathcal{L}_A^2$-term.

Note that $F_{\varphi(z),t}$ is provably total by COMP applied to $\varphi$, and $f$ is provably total by the MIN principle applied to $\varphi$.

Also, the defining axiom for $f_{\varphi(z),t}$ implies

$$\exists z \le t \varphi(z, \vec{x}, \vec{X}) \leftrightarrow \varphi(f_{\varphi(z),t}(\vec{x}, \vec{X}))$$

so use of $f_{\varphi(z),t}$ allows us to eliminate bounded number quantifiers.

Two axioms in the set 2-BASIC for $\mathbf{V^0}$ (namely B12 for predecessor and SE for extensionality) have number quantifiers, so we introduce two new functions $pd$ and $f_{\mathbf{SE}}$ with appropriate defining axioms to give open versions of these axioms to form the set 2-BASIC' of open axioms (for $\overline{\mathbf{V^0}}$).

**Definition:** The vocabulary $\mathcal{L}_{\mathbf{FAC^0}}$ for $\overline{\mathbf{V^0}}$ is the union of the sequence

$$\mathcal{L}_1 \subset \mathcal{L}_2 \subset ...$$

where $\mathcal{L}_1 = \mathcal{L}_A^2 \cup \{pd, f_{\mathbf{SE}}\}$ and
$\mathcal{L}_{n+1}$ is obtained from $\mathcal{L}_n$ by adding functions $f_{\varphi(z),t}$ and $F_{\varphi(z),t}$ for every open formula $\varphi(z)$ over $\mathcal{L}_n$ and every term $t$ over $\mathcal{L}_A^2$.

The axioms for $\overline{\mathbf{V^0}}$ (all of them open) consist of 2-BASIC' and the defining axioms for all function symbols in $\mathcal{L}_{\mathbf{FAC^0}}$.

**Lemma 1:** For every $\Sigma_0^B(\mathcal{L}_{\mathbf{FAC^0}})$-formula $\varphi$ there is an open $\mathcal{L}_{\mathbf{FAC^0}}$-formula $\varphi^+$ such that $\overline{\mathbf{V^0}} \vdash \varphi \leftrightarrow \varphi^+$. (**Proof:** Use $f_{\varphi(z),t}$)

**Lemma 2:** $\overline{\mathbf{V^0}}$ proves $\Sigma_0^B(\mathcal{L}_{\mathbf{FAC^0}})$-COMP.
**Proof:** By Lemma 1 we may assume $\varphi$ is open. Apply $F_{\varphi(z),t}$.

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

Let $\mathbf{V^0}(\mathcal{L}_0) = \mathbf{V^0}$ and for $n > 0$ let $\mathbf{V^0}(\mathcal{L}_n)$ be $\mathbf{V^0}$ extended by the defining axioms for functions in $\mathcal{L}_n$. Thus

$$\mathbf{V^0}(\mathcal{L}_0) \subset \mathbf{V^0}(\mathcal{L}_1) \subset \mathbf{V^0}(\mathcal{L}_2) \subset \ldots$$

and

$$\overline{\mathbf{V^0}} = \bigcup_n \mathbf{V^0}(\mathcal{L}_n)$$

To prove $\overline{\mathbf{V^0}}$ is a conservative over $\mathbf{V^0}$ it suffices (by compactness) to show $\mathbf{V^0}(\mathcal{L}_{n+1})$ is conservative over $\mathbf{V^0}(\mathcal{L}_n)$ for all $n$. For this it suffices to show the new functions in $\mathcal{L}_{n+1}$ are provably total in $\mathbf{V^0}(\mathcal{L}_n)$.

**Lemma 3:** For every open $\mathcal{L}_n$-formula $\varphi^+$ there is a $\Sigma_0^B$-formula $\varphi$ such that $\mathbf{V^0}(\mathcal{L}_n) \vdash \varphi^+ \leftrightarrow \varphi$.
(**Proof:** induction on $n$ and then structural induction on terms in $\varphi^+$), replacing new functions by their definitions.

**Corollary:** $\mathbf{V^0}(\mathcal{L}_n)$ proves COMP, IND, and MIN for open $\mathcal{L}_n$ formulas, and hence proves totality of $F_{\varphi(z),t}$ (by COMP) and $f_{\varphi(z),t}$ (by MIN). Conservativity follows.

**Corollary:** The function symbols in $\mathcal{L}_{\mathbf{FAC^0}}$ represent precisely $\mathbf{FAC^0}$.
(**Proof:** By Lemma 1 and the $\Sigma_0^B$ Representation Theorem it follows that every string function in $\mathbf{FAC^0}$ has the form $F_{\varphi(z),t}$. It is easy to see that every number function in $\mathbf{FAC^0}$ has the form $f_{\varphi(z),t}$. The other direction follows from Lemma 3.

**Corollary** $\mathbf{FAC^0}$ is closed under composition.

SUMMARY:

- $\overline{\mathbf{V^0}}$ is a universal conservative extension of $\mathbf{V^0}$.
- The function symbols in $\overline{\mathbf{V^0}}$ represent precisely the functions in $\mathbf{FAC^0}$.
- $\overline{\mathbf{V^0}}$ proves the COMP, IND, and MIN schemes for $\Sigma_0^B(\mathcal{L}_{\mathbf{FAC^0}})$ formulas.