Formal Reasoning Using Low-Complexity Concepts

Lecture 4: The $\mathbf{V}^i$ and $\mathbf{TV}^i$ Hierarchies
and the
Quantified Propositional Calculus
Chapters 7,8,10

Stephen Cook
Fall School, Prague
September, 2008

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]
$\mathbf{VNL} = \mathbf{V}$-$\mathbf{Krom}$ [Kolokolova]
$\mathbf{VP} = \mathbf{TV}^0 = \mathrm{V}^1$-HORN

Theories for Polynomial Time

1) Equivalent theories over $\mathcal{L}_A^2$

$\mathbf{VP} \qquad = \mathbf{V^0} + \{MCVP\}$

$\mathbf{TV}^0 \qquad = \mathbf{V^0} + \Sigma_0^B$-String-IND

$\mathbf{V}^1$-HORN $\qquad = \mathbf{V^0} + \Sigma_1^B$-HORN-COMP

2) **VPV** $\qquad$ = universal conservative extension of above based on Cobham's Theorem

3) $\mathbf{V}^1 \qquad = \mathbf{V^0} + \Sigma_1^B$-COMP

FACTS
(i) $\mathbf{VP} \subseteq \mathbf{V}^1$, and $\mathbf{VP}$ and $\mathbf{V}^1$ have the same Σ_1^B-theorems.

(ii) $\mathbf{V}^1 \vdash \Sigma_1^B$-**REPL**, but if $\mathbf{VP} \vdash \Sigma_1^B$-**REPL** then integers can be factored in BPP [CoTh]. If $\mathbf{VP} = \mathbf{V}^1$ then PH collapses [KPT].

The $\mathbf{TV}^i$ Hierarchy

$\mathbf{TV}^i$ is the two-sorted analog of Buss's $\mathbf{T}^i_2$.

Notation: We treat X as the binary number $\sum_i X(i)2^i$

$S(X)$ is the binary successor function (in $\mathbf{FAC^0}$).

$\varnothing$ is the empty set (i.e. binary 0)

String Induction Axiom: Φ-SIND

$$[\varphi(\varnothing) \wedge \forall X(\varphi(X) \supset \varphi(S(X))] \ \supset \ \varphi(Y)$$

where φ is in Φ.

(Note: Can eliminate S and $\varnothing$ from SIND scheme using $\mathbf{\Sigma}^B_0$ formulas).

Definition: For $i \geq 0$, $\mathbf{TV}^i$ is the theory over $\mathcal{L}^2_A$ whose axioms are those of $\mathbf{V^0}$ together with $\mathbf{\Sigma}^B_i$-SIND.

Theorem $\mathbf{TV}^i$ proves Σ_i^B-SMIN and Σ_i^B-SMAX.

Theorem: $\mathbf{TV}^0 = \mathbf{VP}$. The Σ_1^B-definable functions in $\mathbf{TV}^0$ comprise **FP** (polytime).

Proof sketch: Rephrase SIND by

$$(\varphi(\emptyset) \wedge \neg\varphi(Y)) \supset \exists X \leq |Y|(\varphi(X) \wedge \neg\varphi(S(X)) \tag{1}$$

To show $\mathbf{VPV}$ proves (1) use binary search. (So $\mathbf{TV}^0 \subseteq \mathbf{VP}$.)

To show polytime functions can be defined in $\mathbf{TV}^0$ use Σ_0^B-SMAX to show $\mathbf{TV}^0$ can solve a bit recursion problem.

The Σ_1^B-definable functions in $\mathbf{TV}^1$ have no known nice characterization. However the Σ_1^B-definable *total search problems* do.

A total search problem $Q(\vec{x}, \vec{X})$ is like a multivalued function. Think of $Q(\vec{x}, \vec{X})$ as a non-empty set of strings. Solving $Q(\vec{x}, \vec{X})$ means finding some Z in $Q(\vec{x}, \vec{X})$.

The class PLS (Polynomial Local Search) of search problems was introduced by [Johnson/Papadimitriou/Yannakakis 88]

Definition: [Polynomial Local Search] A **PLS** problem Q is specified by the following:

1. A polytime relation $\varphi_Q(\vec{x}, \vec{X}, Z)$ and an $\mathcal{L}^2_A$-term $t(\vec{x}, \vec{X})$ satisfying the two conditions

$$\varphi_Q(\vec{x}, \vec{X}, \varnothing)$$
$$\varphi_Q(\vec{x}, \vec{X}, Z) \supset |Z| \leq t(\vec{x}, \vec{X})$$

   ($\varphi_Q(\vec{x}, \vec{X}, Z)$ means Z is a candidate solution for problem instance $(\vec{x}, \vec{X})$.)

2. Polytime string functions $P_Q(\vec{x}, \vec{X}, Z)$ and $N_Q(\vec{x}, \vec{X}, Z)$ satisfying the two conditions

$$\varphi_Q(\vec{x}, \vec{X}, Z) \supset \varphi_Q(\vec{x}, \vec{X}, N_Q(\vec{x}, \vec{X}, Z))$$
$$N_Q(\vec{x}, \vec{X}, Z) \neq Z \supset P_Q(Z) < P_Q(N_Q(\vec{x}, \vec{X}, Z))$$

   (N_Q is a heuristic for finding a neighbor of Z which increases the profit P_Q. $N_Q(\vec{x}, \vec{X}, Z) = Z$ is taken to mean that Z is locally optimal.

Then

$$Q(\vec{x}, \vec{X}) = \{Z \mid \varphi_Q(\vec{x}, \vec{X}, Z) \wedge N_Q(\vec{x}, \vec{X}, Z) = Z\}$$

Definition: A search problem Q_1 is *many-one* reducible to Q_2 (written $Q_1 \leq Q_2$) if there are polytime functions $\vec{f}, \vec{F}, G$ such that

$$G(\vec{x}, \vec{X}, Z) \in Q_1(\vec{x}, \vec{X})$$

for all

$$Z \in Q_2(\vec{f}(\vec{x}, \vec{X}), \vec{F}(\vec{x}, \vec{X}))$$

Definition: A search problem $Q(\vec{x}, \vec{X})$ is Φ-definable in a theory $\mathcal{T}$ if there is a formula $\psi_Q(\vec{x}, \vec{X}, Z)$ in Φ such that

$$\psi_Q(\vec{x}, \vec{X}, Z) \supset Z \in Q(\vec{x}, \vec{X})$$

and

$$\mathcal{T} \vdash \exists Z \psi_Q(\vec{x}, \vec{X}, Z)$$

Theorem:[Buss/Krajîček] A search problem Q is Σ_1^B-definable in $\mathbf{TV}^1$ iff Q is many-one reducible to some problem in **PLS**.

Proof $\Rightarrow$: Witnessing, using cut elimination.
Proof $\Leftarrow$: $\mathbf{TV}^1 \vdash \Sigma_1^B$-SMAX.

Theorem: For all $i \geq 0$

$$\mathbf{V}^i \subseteq \mathbf{TV}^i \subseteq \mathbf{V}^{i+1}$$

Proof: First inclusion: String IND is stronger than number IND.
Second inclusion generalizes $\mathbf{TV}^0 \subseteq \mathbf{V}^1$ (binary search).

Thus

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

Define

$$\mathbf{V}^\infty = \sum_i \mathbf{V}^i = \sum_i \mathbf{TV}^i$$

Theorem: [Buss] For $i \geq 0$ $\mathbf{V}^{i+1}$ is Σ^B_{i+1}-conservative over $\mathbf{TV}^i$.

This generalizes the case $i = 0$.
For $i = 1$, this says the Σ^B_1-definable search problems in $\mathbf{V}^2$ are the same as in $\mathbf{TV}^1$: those reducible to PLS.

FACT: Each $\mathbf{V}^i$ and $\mathbf{TV}^i$ is finitely axiomatizable. Hence $\mathbf{V}^\infty$ is finitely axiomatizable iff $\mathbf{V}^\infty = \mathbf{V}^i$ for some i.

Recall $\mathbf{VPV}$ is a universal conservative extension of $\mathbf{VP} = \mathbf{TV}^0$, like $\overline{\mathbf{VP}}$ but based on Cobham's Theorem. $\mathbf{VPV}$ has function symbols for all polytime functions.

Define $\mathbf{VPV}^1 = \mathbf{VPV}$. In general we can define $\mathbf{VPV}^{i+1}$ to be a universal conservative extension $\mathbf{TV}^i$, in the style of $\mathbf{VPV}$. [KPT]

Denote the two-sorted polynomial hierarchy PH by

$$\mathbf{NP} = \Sigma_1^P \subseteq \Sigma_2^P \subseteq ...$$

Theorem: For $i \geq 0$ the following are equivalent for a string function F:

(i) F is in $\mathbf{FP}^{\Sigma_i^P}$.
(ii)F is Σ_{i+1}^B-definable in $\mathbf{TV}^i$.
(iii)F is Σ_{i+1}^B-definable in $\mathbf{V}^{i+1}$.
(iv)F is Σ_{i+1}^B-definable in $\mathbf{VPV}^{i+1}$.

Similarly for a number function f.

This generalizes the case $i = 0$.

Definition: A *witness query* Y to an oracle $\exists W \leq t\, R(Y,W)$ returns a witness $W \leq t$ satisfying $R(Y,W)$ if such exists, and otherwise returns "NO". For $i \geq 1$, $\mathbf{FP}^{\mathbf{\Sigma}_i^P}[wit, O(g(n)]$ is the class of search problems Q solvable by a polynomial time Turing machine that makes $O(g(n)$ witness queries to a $\mathbf{\Sigma}_i^P$ oracle $\exists W \leq t\, R(Y,W)$.

Notice that a witness query can be simulated by polynomial many Boolean queries, using binary search. However as far as we know, the class $\mathbf{FP}^{\mathbf{\Sigma}_i^P}[wit, O(g(n)]$ cannot be specified in terms of Boolean queries when $g(n)$ is $O(\log n)$.

Theorem:

(i) [Kraj] For $i \geq 1$, a search problem Q is $\mathbf{\Sigma}_{i+1}^B$-definable in $\mathbf{V}^i$ iff $Q \in \mathbf{FP}^{\mathbf{\Sigma}_i^P}[wit, O(\log n)]$.

(ii) [Pollett, Morioka] For $j \geq 2$ and $\mathbf{V^0} \subseteq \mathcal{T} \subseteq \mathbf{TV}^{j-2}$, a search problem Q is $\mathbf{\Sigma}_j^P$-definable in $\mathcal{T}$ iff $Q \in \mathbf{FP}^{\mathbf{\Sigma}_{j-1}^P}[wit, O(1)]$.

Quantified Propositional Calculus (QPC)

Formulas are built from

- propositional constants $\top, \bot$;
- free variables $p, q, r, \ldots$;
- bound variables $x, y, z, \ldots$;
- connectives $\wedge, \vee, \neg$;
- quantifiers $\exists, \forall$;
- parentheses (,);

according to the following rules:

(a) $\top$, $\bot$, and p are *atomic* formulas, for any free variable p;

(b) if φ and ψ are formulas, so are $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $\neg\varphi$;

(c) if $\varphi(p)$ is a formula, then $\forall x\varphi(x)$ and $\exists x\varphi(x)$ are formulas, for any free variable p and bound variable x.

Example:

$$\forall x \exists y \Big((\neg y \vee (\neg x \wedge p)) \wedge (y \vee x \vee \neg p) \Big)$$

Definition: $\Sigma_0^q = \Pi_0^q$ is the class of quantifier-free formulas of QPC. For $i \geq 0$, Σ_{i+1}^q and Π_{i+1}^q are the smallest classes of QPC formulas satisfying

1. $\Sigma_i^q \cup \Pi_i^q \subseteq \Sigma_{i+1}^q \cap \Pi_{i+1}^q$
2. Σ_{i+1}^q is closed under $\vee$ and $\wedge$ and existential quantification
3. Π_{i+1}^q is closed under $\vee$ and $\wedge$ and universal quantification
4. If $A \in \Sigma_{i+1}^q$ then $\neg A \in \Pi_{i+1}^q$
5. If $A \in \Pi_{i+1}^q$ then $\neg A \in \Sigma_{i+1}^q$

For $i \geq 0$ every formula in Σ_{i+1}^q has a prenex form with at most i alternations of quantifiers, with the outermost quantifier being $\exists$. Similarly for Π_{i+1}^q with $\forall$. Checking the validity of a Σ_i^q sentence is Σ_i^p-complete, for $i \geq 1$. Checking validity of an arbitrary sentence is PSPACE-complete.

Recall Gentzen's sequent system **PK** for the propositional calculus.

PK is p-equivalent to Frege systems.

Recall a problem in the complexity class $\mathbf{NC}^1$ is solved by a polynomial size family of Boolean formulas.

Intuitively, the formulas in a polysize **PK** proof express $\mathbf{NC}^1$ concepts.

Theorem:[Arai] A Σ_0^B-theorem of the theory $\mathbf{VNC}^1$ can be translated into a tautology family with polysize **PK**-proofs.

Proof System G for QPC [KP]

G includes the axioms and rules for **PK**, where now formulas are QPC formulas. It also has the following four quantifier introduction rules:

$\forall$ introduction rules:

$$\forall\text{-left: } \frac{A(B), \Gamma \longrightarrow \Delta}{\forall x A(x), \Gamma \longrightarrow \Delta} \qquad \forall\text{-right: } \frac{\Gamma \longrightarrow \Delta, A(p)}{\Gamma \longrightarrow \Delta, \forall x A(x)}$$

$\exists$ introduction rules:

$$\exists\text{-left: } \frac{A(p), \Gamma \longrightarrow \Delta}{\exists x A(x), \Gamma \longrightarrow \Delta} \qquad \exists\text{-right: } \frac{\Gamma \longrightarrow \Delta, A(B)}{\Gamma \longrightarrow \Delta, \exists x A(x)}$$

Restriction: In the rules $\forall$-right and $\exists$-left, p is a free variable called an *eigenvariable* that must not occur in the bottom sequent. For the rules $\forall$-left and $\exists$-right, the formula B is called the *target* formula and may be any quantifier-free formula (with no bound variables).

Theorem: Every valid sequent of length n has a treelike G proof with $O(n2^n)$ sequents of length $O(n)$ with all cut formulas atomic.

The Systems $\mathbf{G}_i$ and $\mathbf{G}_i^*$

Definition:[KP, Kraj, modified by Morioka] For each $i \geq 0$, $\mathbf{G}_i$ is the subsystem of $\mathbf{G}$ in which cut formulas are restricted to $\Sigma_i^q \cup \Pi_i^q$. The system $\mathbf{G}_i^*$ is treelike $\mathbf{G}_i$.

Claim $\mathbf{G}_i^*$ and $\mathbf{G}_i$ are nonuniform analogs of $\mathbf{V}^i$ and $\mathbf{TV}^i$.

Theorem: [Kraj] For $i \geq 0$, $\mathbf{G}_{i+1}^*$ p-simulates $\mathbf{G}_i$, when the systems are restricted to proving $\Sigma_i^q \cup \Pi_i^q$ formulas. Treelike **G** p-simulates **G**.

Proof idea: Let the daglike proof $\pi = S_1, \ldots, S_n$. Then the sequents

$$\longrightarrow \forall A_{S_1}; \quad \longrightarrow (\forall A_{S_1} \wedge \forall A_{S_2}); \ldots; \quad \longrightarrow (\forall A_{S_1} \wedge \ldots \wedge \forall A_{S_n}); \quad \longrightarrow A_{S_n}$$

can be augmented to a treelike **G** proof. Here, if $S = A_1, \ldots A_k \longrightarrow B_1 \ldots B_\ell$ then A_S is

$$\neg A_1 \vee \ldots \vee \neg A_k \vee B_1 \vee \ldots \vee B_\ell$$

Theorem: [Morioka] $\mathbf{G}_i^*$ with cut formulas restricted to prenex $\mathbf{\Sigma}_i^q$ p-simulates $\mathbf{G}_i^*$.

Theorem: [Perron 08] For $i \geq 1$, $\mathbf{G}_i$ p-simulates $\mathbf{G}_{i+1}^*$ for all formulas. Hence $\mathbf{G}_i$ and $\mathbf{G}_{i+1}^*$ are p-equivalent for proving formulas in $\mathbf{\Sigma}_i^q \cup \mathbf{\Pi}_i^q$.

Quantified Propositional Translations

If $\varphi(X)$ is a general Σ_i^B formula then $\varphi(X)[n]$ is a Σ_i^q formula of size polynomial in n with variables $p_0^X, \ldots p_{n-1}^X$ which expresses $\varphi(X)$ when $|X| = n$.

More generally, if $\varphi(\vec{x}, \vec{X})$ is a bounded $\mathcal{L}_A^2$-formula then its QPC translation $\varphi(\vec{x}, \vec{X})[\vec{m}; \vec{n}]$ is valid iff

$$\mathbb{N}_2 \models \forall \vec{X}((\bigwedge |\vec{X}| = \vec{n}) \supset \varphi(\vec{m}, \vec{X}))$$

Theorem: [KP, Kraj] For $k \geq 1$ and For any bounded theorem $\varphi(\vec{x}, \vec{X})$ of $\mathbf{V}^i$ (resp. $\mathbf{TV}^i$) there is a polytime function F such that $F(\vec{m}, \vec{n})$ is a $\mathbf{G}_i^*$-proof (resp. $\mathbf{G}_i$-proof) of $\varphi(\vec{m}; \vec{n})$, for all $\vec{m}, \vec{n} \in \mathbb{N}$.

Note that this is true for all bounded formulas, not just Σ_i^B-formulas.

Reflection Principles

For a QPC proof system $\mathcal{F}$, the formula Σ_i^q-RFN$_{\mathcal{F}}$ is a $\forall\Sigma_i^B$ sentence which asserts that $\mathcal{F}$ is sound for proving Σ_i^q sentences.

Theorem: [KP, Kraj] $\mathbf{V}^i \vdash \Sigma_i^q\text{-RFN}_{\mathbf{G}_i^*}$
$\mathbf{TV}^i \vdash \Pi_{i+1}^q\text{-RFN}_{\mathbf{G}_i}$

Major Omission in these lectures:

Buss's use of free-cut-free ("anchored") LK proofs to get important results. For example

- Witnessing theorems for $\mathbf{V}^i$ and $\mathbf{TV}^i, i \geq 1$.

- Propositional Translation theorems.

- Simulation results concerning $\mathbf{G}_i$ and $\mathbf{G}_i^*$.

General Ideal: To get a nice anchored LK proof of a Σ_i^B-formula in $\mathbf{V}^i$, replace Σ_i^B-COMP by a rule for Σ_i^B-IND. Then all formulas in the formal proof are Σ_i^B.

Open Questions

Prove $\mathbf{VTC}^0$ (or even $\mathbf{V}^\infty$) can prove more Σ_0^B theorems than $\mathbf{V^0}(2)$. (This is related to propositional proof system lower bounds.)

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

Examples:
- Matrices: $AB = I \rightarrow BA = I$
- Reingold's Theorem: SL = L.

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