Zambella's Model-Theoretic Proof of the Buss Witnessing Theorem

Stephen A. Cook

February, 2001

First-order theories about polytime functions

For $a \in \mathbb{N}$, $|a| = \log_2(a+1)$ = length of a.

$\square_1^p$ = polytime functions $f : \mathbb{N}^k \to \mathbb{N}$.

$f(x_1, ..., x_n)$ computable in time
$(|x_1| + ... + |x_k|)^{O(1)}$

PV (Polynomially Verifiable) (Cook 75) is an equational theory.

$\mathcal{L}(\mathbf{PV})$ = function symbols for all polytime functions, based on Cobham's Theorem.

QPV (Quantified PV) is a first-order version (same language).

The axioms of **QPV** are defining equations for all function symbols in $\mathcal{L}(\mathbf{PV})$ plus

$$\textbf{PIND}: \phi(0) \wedge \forall x(\phi(\lfloor \frac{1}{2}x \rfloor) \to \phi(x)) \ \to \forall x \phi(x)$$

for every quantifier-free formula ϕ.

Theorem 1: QPV is axiomatized by its $\forall$-theorems.

Theorem: 2 QPV proves

$$\textbf{IND}: \phi(0) \wedge \forall x(\phi(x) \to \phi(x+1)) \ \to \forall x \phi(x)$$

for all quantifier-free ϕ.

Proof: Define f using binary search so that

$$QPV \vdash \phi(0) \wedge \neg\phi(x) \to \phi(f(x)) \wedge \neg\phi(f(x)+1)$$

This is a $\forall$-theorem of QPV implying **IND** (also **PIND**).

Theorem 3: (Witnessing for **QPV**) If $\phi(x, y)$ is quantifier-free and

$$\mathbf{QPV} \vdash \forall x \exists y \phi(x, y)$$

then for some (polytime) f in $\mathcal{L}(\mathbf{PV})$

$$\mathbf{QPV} \vdash \forall x \phi(x, f(x))$$

Example: $\mathbf{QPV} \not\vdash \forall x \exists y Exp(x, y)$ where $Exp(x, y) \leftrightarrow y = 2^x$.

Proof of Theorem: Prove the contrapositive.

Assume for all f in $\mathcal{L}(\mathbf{PV})$

$$\mathbf{QPV} \not\vdash \forall x \phi(x, f(x))$$

We find a model M^* of **QPV** such that

$$M^* \not\models \forall x \exists y \phi(x, y)$$

(so $\mathbf{QPV} \ \not\vdash \forall x \exists y \phi(x, y)$)

Let c be a new constant symbol.

CLAIM: $\mathbf{QPV} \cup \{\neg\phi(c, f(c)) \mid f \in \mathcal{L}(\mathbf{PV})\}$ is consistent. (Use compactness and def'n by cases.)

Thus let $M \models \mathbf{QPV} \cup \{\neg\phi(c, f(c)) \mid f \in \mathcal{L}(\mathbf{PV})\}$.

Define the substructure M^* of M by

$$|M^*| = \{f(c) \mid f \in \mathcal{L}(\mathbf{PV})\} \subseteq |M|$$

Thus $M^* \models \mathbf{QPV}$. (Why?)

Also $M^* \models \forall y \neg\phi(c, y)$
Thus $\mathbf{QPV} \not\vdash \forall x \exists y \phi(x, y)$. QED.

NOTE: The only properties of **QPV** needed are
1) It's a $\forall$-theory.
2) It's function symbols are closed under definition by q-f cases.

GOAL NOW: Prove witnessing for Buss's S^1_2.

S^1_2 has function symbols
$0, 1, +, \cdot, \lfloor \frac{1}{2}x \rfloor, |x|, 2^{|x|\cdot|y|}$

$S^1_2(\mathbf{PV})$ is a conservative extension of S^1_2.

The language of $S^1_2(\mathbf{PV})$ is $\mathcal{L}(\mathbf{PV})$.

The axioms of $S^1_2(\mathbf{PV})$ are the $\forall$-axioms of **QPV** together with **PIND** for Σ^b_1 formulas:

$$\phi(0) \wedge \forall x(\phi(\lfloor \frac{1}{2}x \rfloor) \to \phi(x)) \ \to \forall x \phi(x)$$

Definition: A Σ^b_1 formula in $\mathcal{L}(\mathbf{PV})$ has the form $\exists x \leq t \phi$ where ϕ is quantifier-free.

(Original definition involved "sharply-bounded quantifiers".)

FACT: The Σ^b_1 formulas represent precisely the **NP** relations in the standard model.

Theorem (Buss, Zambella). $S^1_2(\mathbf{PV})$ is NOT universally axiomatized unless the polynomial hierarchy collapses.

$\mathbf{QPV} \subseteq S^1_2(\mathbf{PV})$ (Inclusion proper unless PH collapses.)

Theorem 4 (Buss) $S^1_2(\mathbf{PV})$ is $\forall\Sigma_1$-conservative over **QPV**.

Corollary (Buss Witnessing for S^1_2) If

$$S^1_2(\mathbf{PV}) \vdash \forall x \exists y \phi(x,y)$$

where ϕ is quantifier-free then for some f in $\mathcal{L}(\mathbf{PV})$

$$\mathbf{QPV} \vdash \forall x \phi(x, f(x))$$

Proof: By above theorem and **QPV** witnessing.

Corollary If $\alpha(x), \beta(x)$ are Σ^b_1 and

$$S^1_2(\mathbf{PV}) \vdash \forall x(\alpha(x) \leftrightarrow \neg\beta(x))$$

then $\alpha(x)$ and $\beta(x)$ represent a polytime predicate.

Proof: Exercise.

Proof of Theorem 4 (this one due to Zambella JSL 96) It suffices to show

Claim 1: If M is any countable model for **QPV**, then there is a Σ_1-elementary extension M^* of M such that

$$M^* \models S^1_2(\mathbf{PV})$$

Definition $M \prec_{\Sigma_1} M^*$ iff for every q-f $\phi(x, \bar{y})$ and all parameters $\bar{c} \in M$

$$M \models \exists x \phi(x, \bar{c}) \text{ iff } M^* \models \exists x \phi(x, \bar{c})$$

Claim 2: For every countable model M for **QPV** there is M^* s. t. $M \prec_{\Sigma_1} M^*$ and for every q-f $\phi(x, y, \bar{z})$ and $\bar{d} \in M^*$ there is $f \in \mathcal{L}(\mathbf{PV})$ and $\bar{e} \in M^*$ s. t.

$$M^* \models \forall x \exists y \phi(x, y, \bar{d}) \to \forall x \phi(x, f(x, \bar{e}), \bar{d})$$

We will show **Claim 2** $\Longrightarrow$ **Claim 1**

Lemma: The structure M^* of Claim 2 is a model for $S^1_2(\mathbf{PV})$.

Proof: First note that $M^* \models \mathbf{QPV}$, because $M \models \mathbf{QPV}$ and $M \prec_{\Sigma_1} M^*$ and so $M \prec_{\Pi_1} M^*$, and $\mathbf{QPV}$ is axiomatized by Π_1 sentences.

Thus it suffices to show $M^* \models PIND$ for Σ^b_1 formulas. Thus suppose M^* satisfies (where $t = t(x)$)

$$\exists y \leq t\phi(0, y) \wedge \forall x(\exists y \leq t'\phi(\lfloor\frac{1}{2}x\rfloor, y) \rightarrow \exists y \leq t\phi(x, y))$$

where ϕ is quantifier-free. Then

$$M^* \models \forall x\forall z\exists y[(z \leq t' \wedge \phi(\lfloor\frac{1}{2}x\rfloor, z)) \rightarrow (y \leq t \wedge \phi(x, y))]$$

Thus by Claim 2 there is $f \in \mathcal{L}(\mathbf{PV})$ such that $M^* \models$

$$\forall x\forall z\ [(z \leq t' \wedge \phi(\lfloor\frac{1}{2}x\rfloor, z) \rightarrow (f(x, z) \leq t \wedge \phi(x, f(x, z)))]$$

Now define g by limited recursion on notation by

$g(0) = y_0$ (where $y_0 \leq t \wedge \phi(0, y_0)$)
$g(x) = f(x, g(\lfloor \frac{1}{2}x \rfloor))$
$g(x) \leq t(x)$

Then by $PIND$ in M^*

$$M^* \models \forall x[g(x) \leq t(x) \wedge \phi(x, g(x))]$$

so $M^* \models \forall x \exists y \leq t \phi(x, y)$

This proves the Lemma.

Claim 2: For every countable model M for **QPV** there is M^* s. t. $M \prec_{\Sigma_1} M^*$ and for every q-f $\phi(x, y, \bar{z})$ and $\bar{d} \in M^*$ there is $f \in \mathcal{L}(\mathbf{PV})$ and $\bar{e} \in M^*$ s. t.

$$M^* \models \forall x \exists y \phi(x, y, \bar{d}) \to \forall x \phi(x, f(x, \bar{e}), \bar{d}) \quad (1)$$

Proof of Claim 2: Define a Σ_1-elem chain

$$M = M_0 \prec_{\Sigma_1} M_1 \prec_{\Sigma_1} M_2 \prec_{\Sigma_1} \ldots$$

Let $M^* = \bigcup_k M_k$.
Thus $M \prec_{\Sigma_1} M^*$ (by model theory).

Enumerate formulas $\langle \phi_k(x, y, \bar{d}_k) \rangle$, $\bar{d}_k \in M_{k-1}$.

Make M_k satisfy (1) for ϕ_k.

Claim: $M_k \models$ (1) for $\phi_k \implies M^* \models$ (1) for ϕ_k

because (1) is an $\exists\Pi_1$ formula.

Construct M_{k+1} from M_k.

Fix $\phi = \phi_{k+1}, \bar{d} = \bar{d}_{k+1}$
Assume for all $f, \bar{e}$

$$M_k \not\models (1) \text{ for } \phi$$

Claim: For a new constant symbol c

$$Diag(M_k) \cup \{\neg\phi(c, f(c, \bar{e}), \bar{d}) \mid \bar{e} \in M_k, f \in \mathcal{L}(\mathbf{PV})\} \tag{2}$$

is consistent. (By compactness and def'n by cases.)

Let $M' \models (2)$ and define $M_k \subseteq M_{k+1} \subseteq M'$

$$|M_{k+1}| = \{f(c, \bar{e}) \mid \bar{e} \in M_k, f \in \mathcal{L}(\mathbf{PV})\} \subseteq |M'|$$

Then $M_k \prec_{\Sigma_1} M_{k+1}$ because $M_k \prec M'$.

$$M_{k+1} \not\models \exists y \phi(c, y, \bar{d}) \text{ (by (2))}$$

so $M_{k+1} \models (1)$ for $\phi = \phi_{k+1}$. QED