Cook's PV II: Buss' theories and Propositional proofs

Enriching PV

Definition 1. Let PV_1 be the theory in the language of PV consisting of all provable statements of PV, the $BASIC$ axioms and for each open formula $\varphi(x)$ define a function $h(b,u)$ by

- $h(b,0) = (0,b)$
- if $h(b,\lfloor u/2 \rfloor) = (x,y)$ and $u > 0$, then

$$h(b,u) = \begin{cases} (\lceil (x+y)/2 \rceil, y) & \text{if } \lceil (x+y)/2 \rceil < y \wedge \varphi(\lceil (x+y)/2 \rceil) \\ (x, \lceil (x+y)/2 \rceil) & \text{if } x < \lceil (x+y)/2 \rceil \wedge \neg\varphi(\lceil (x+y)/2 \rceil) \\ (x,y) & \text{otherwise,} \end{cases}$$

and a PV_1-axiom

$$(\varphi(0) \wedge \neg\varphi(b) \wedge h(b,b) = (x,y)) \to (x+1 = y \wedge \varphi(x) \wedge \neg\varphi(y)).$$

Exercise 2. Show that PV_1 proves induction for open formulas.

Exercise 3. For $A \in \Sigma_1^b$ we have $\mathrm{PV}_1 \vdash \mathrm{Witness}_A^{1,\overline{a}}(w,\overline{a}) \to A(\overline{a})$.

Theorem 4 (Buss' witnessing restated)**.** Assume $\varphi(x,y) \in \Sigma_1^b$ and

$$S_2^1 \vdash (\forall \overline{x})\varphi(\overline{x}),$$

then there is a PV-function symbol $f(x)$ such that

$$\mathrm{PV}_1 \vdash \mathrm{Witness}_{\varphi}^{1,x}(f(\overline{x}),\overline{x}).$$

Exercise 5. Show that for every $\varphi \in \Sigma_1^b$ we have

$$S_2^1 \vdash (\forall \overline{x})\varphi(\overline{x}) \implies \mathrm{PV}_1 \vdash (\forall \overline{x})\varphi(\overline{x}).$$

Enriching S_2^1

Definition 6. The theory $S_2^1(\mathrm{PV})$ is the extension of S_2^1 in the language of PV by all equations provable in PV and by the polynomial induction axioms for all $\Sigma_1^b(\mathrm{PV})$-formulas.

Fact 7 (Definability of computation in PV_1)**.** For every polynomial-time clocked Turing machine M

$$\mathrm{PV}_1 \vdash (\forall x)(\exists! w)\mathrm{Comp}_M(x,w),$$

where Comp_M is the natural formula stating that w is a computation of M on input x.

Exercise 8. We say a formula $\varphi \in \Sigma_1^b$ is $\Delta_1^b(S_2^1)$, or Δ_1^b in S_2^1, if there is $\psi \in \Pi_1^b$ such that

$$S_2^1 \vdash \varphi(x) \leftrightarrow \psi(x),$$

in which case we also have $\psi \in \Delta_1^b(S_2^1)$.

Exercise 9 (Provable **NP**$\cap$**coNP** is **P**)**.** Show that if $\varphi \in \Sigma_1^b$ is in fact $\Delta_1^b(S_2^1)$, then the set $\varphi(\mathbb{N}) \in \mathbf{P}$.

Exercise 10. Show that S_2^1 proves Δ_1^b-*induction*. That is, whenever

$$S_2^1 \vdash \varphi(x) \leftrightarrow \psi(x),$$

for some $\varphi \in \Sigma_1^b$ and $\psi \in \Pi_1^b$, then actually S_2^1 proves

$$(\varphi(0) \wedge (\forall x)(\varphi(x) \to \varphi(x+1))) \to (\forall x)(\varphi(x)).$$

Exercise 11. For $\varphi \in \Sigma_1^b$, we have

$$\mathrm{PV}_1 \vdash (\forall x)\varphi(x) \implies S_2^1(\mathrm{PV}) \vdash (\forall x)\varphi(x).$$

Exercise 12. For φ in the language of $BASIC$, we have

$$S_2^1(\mathrm{PV}) \vdash \varphi \iff S_2^1 \vdash \varphi.$$

Theorem 13. For $\varphi(x) \in \Sigma_1^b$, we have

$$S_2^1 \vdash (\forall x)\varphi(x) \iff \mathrm{PV}_1 \vdash (\forall x)\varphi(x).$$

Partial Answer 14. Every submodel of a model $M \models \Sigma_1^b(S_2^1)$ closed under PV-symbols is a model of S_2^1.

Propositional proofs

Definition 15. A circuit of input size n is a labeled directed acyclic graph with n sources (inputs) and exactly one sink (output), such that every non-source vertex is labeled by either $\wedge$ or by $\vee$.

A family of circuits $\{C_n\}_{n=0}^{\infty}$ is a sequence of circuits such that C_n has n inputs. We say it is of polynomial size if there is a polynomial p such that the number of vertices of C_n is at most $p(n)$.

The class of sets decidable by polynomial size circuits is denoted $\mathbf{P}/poly$.

Exercise 16. $\mathbf{P} \subseteq \mathbf{P}/poly$

Exercise 17 (Limited extension)**.** Show that for every circuit $C(\overline{x})$ there is a CNF $A(\overline{x}, \overline{y})$, which is at most polynomially larger, such that for every $b \in \{0,1\}^n$ we have

$$C(\overline{b}) = 1 \iff A(\overline{b}, \overline{y}) \in \mathrm{SAT}.$$

Definition 18. Let t, s be PV symbols. We define the Cook's translation of this equation as a sequence of CNFs $\{||t = s||_n\}_{n=0}^{\infty}$ where $||t = s||^n$ is the natural CNF expressing that the circuits computing t and s on n bits are equal.

Theorem 19 (Cook)**.** Let $\mathrm{PV} \vdash t = s$, then $\mathrm{EF} \vdash_* ||t = s||^n$.

Corollary 20. Let $\varphi(x) \in \Pi_1^b$. Then $S_2^1 \vdash (\forall x)\varphi(x) \implies \mathrm{EF} \vdash_* ||t = s||^n$.