Cook's PV

Context

Theorem 1. Let $\varphi(x,y) \in \Sigma_1^b$ and

$$S_2^1 \vdash (\forall x)(\exists y)\varphi(x,y),$$

then there is $f \in \mathbf{FP}$ such that

$$\mathbb{N} \models (\forall x)\varphi(x, f(x)).$$

Rhetorical question 2. Can we add every such f to the language of S_2? Does this change power of S_2^1?

Rhetorical question 3. Subsets of $\mathbb{N}$ definable in Σ_1^b are exactly **NP**, but it does not necessarily hold that Δ_0^b-definable sets are precisely the **P** sets. Can we expand the language of S_2 to make this true?

Rhetorical question 4. The theory S_2^1 seems to correspond to polynomial-time (**P**) reasoning, but it still has (a weak form) of Σ_1^b (**NP**) induction, is this necessary for the witnessing theorem to hold?

Question 5. Is every substructure of $M \models S_2^1$ also a model of S_2^1?

Cobham's Theorem

Definition 6. We define the bit-succesor functions $s_0, s_1 : \mathbb{N} \to \mathbb{N}$ as

$$\begin{aligned} s_0(x) &= 2x \\ s_1(x) &= 2x+1. \end{aligned}$$

Definition 7. Let $g, h_0, h_1, l : \mathbb{N} \to \mathbb{N}$, we say f is defined by *limited recusion on notation* (LRN) if it satisfies:

$$\begin{aligned} f(\overline{x}, 0) &= g(\overline{x}) \\ f(\overline{x}, s_0(y)) &= h_0(\overline{x}, y, f(\overline{x}, y)) \\ f(\overline{x}, s_1(y)) &= h_1(\overline{x}, y, f(\overline{x}, y)) \\ f(\overline{x}, y) &\leq l(\overline{x}, y). \end{aligned}$$

Theorem 8 (Cobham)**.** The class **FP** of polynomial time functions is the smallest class of functions containing projections, the constant 0, s_0, s_1, $x\#y$ and closed under

- composition
- limited recursion on notation.

Exercise 9. Show that the function concatenating the binary representations of numbers x and y is in **FP** by Cobham's theorem.

Exercise 10. Show that we can get a function outside **FP** by (un)limited recursion on notation, that is, by recursion on notation without any bound for the resulting function.

The Definition of PV

"The definition of the theory PV (for polynomially verifiable) is rather complex, as its language, axioms and derivations are introduced simultaneously and in infinitely many steps." – Jan Krajíček in [Proof complexity, 2019]

Definition 11. PV is an equational theory, which we define by simultaneously providing a definition for rank k function symbols and PV-derivations for each $k \in \mathbb{N}$.

1. Function symbols of rank 0 are constant 0, unary s_0, s_1, $\mathrm{Tr}(x)$ and binary $x \frown Y$, $x\#y$ and $\mathrm{Less}(x, y)$.
2. Defining equations of rank 0 are:

$$\begin{aligned}
&\mathrm{Tr}(0) = 0\\
&\mathrm{Tr}(s_i(x)) = x, i \in \{0, 1\}\\
&x \frown 0 = x\\
&x \frown s_i(y) = s_i(x \frown y), i \in \{0, 1\}\\
&x\#0 = 0\\
&x\#s_i(y) = x \frown (x\#y), i \in \{0, 1\}\\
&\mathrm{Less}(x, 0) = x\\
&\mathrm{Less}(x, s_i(y)) = \mathrm{Tr}(\mathrm{Less}(x, y)), i \in \{0, 1\}.
\end{aligned}$$

3. PV rules are

$$\frac{t = u}{u = t} \tag{R1}$$

$$\frac{t = u \quad u = v}{t = v} \tag{R2}$$

$$\frac{t_1 = u_1 \dots t_k = u_k}{f(t_1, \dots, t_k) = f(u_1, \dots, u_k)} \tag{R3}$$

$$\frac{t = u}{t(x/v) = u(x/v)}, \tag{R4}$$

and if $E_1, \dots E_6$ are two pairs of the first three equations from the definition of (LRN), E_1, E_2, E_3 for f_1 and E_4, E_5, E_6 for f_2 then the following is a PV rule

$$\frac{E_1, \dots, E_6}{f_1(x, \overline{y}) = f_2(x, \overline{y})}. \tag{R5}$$

4. PV derivations of rank k are sequences of equalities $E_1,\dots,E_t$ in which every function symbol is of rank $\leq k$ and every E_i is either a defining equation of rank $\leq k$ or derived from some earlier equations by one of the PV-rules.

5. Let t be a term consisting of function symbols of rank $\leq k$, then f_t is a function symbol of rank $k+1$ and $f_t = t$ is a defining equation of rank $k+1$.

6. The rest of $k+1$ function symbols are defined as follows. If g, h_0, h_1, l_0, l_1 are function symbols of rank $\leq k$ and $\pi_i, i \in \{0,1\}$ are PV derivations of rank k of the equality

$$\mathrm{Less}(h_i(\overline{x}, y, z), z \frown l_i(\overline{x}, y)) = 0,$$

then $f_{\mathrm{LRN}(g,h_0,h_1,l_0,l_1,\pi_0,\pi_1)}$ is a function symbol of rank $k+1$ with the first three equations from the definition of (LRN) being the definiting equations of rank $k+1$.

Exercise 12. Prove in PV that the function $f(x) = 0$ and the function

$$g(0) = 0$$
$$g(s_i(x)) = g(x)$$

are equal.

Exercise 13. Show that there is a PV-function $S(x)$ computing $x \mapsto x+1$.

Exercise 14. Show that there is a PV-function $x + y$ computing addition of x and y.

Exercise 15 (Possibly involved)**.** Show that $\mathrm{PV} \vdash x + y = y + x$.

Definition 16. Let $S^1_2(\mathrm{PV})$ denote the extension of the theory S^1_2 in the language containing all PV function symbols, with the defining equations of PV as new axioms and polynomial induction for Σ^b_1 formulas in the new language.

Theorem 17 (Buss, 1986)**.** For every φ in the language of S_2:

$$S^1_2(\mathrm{PV}) \vdash \varphi \iff S^1_2 \vdash \varphi,$$

that is $S^1_2(\mathrm{PV})$ is *conservative* over S^1_2.