Embedding of $\mu$-measure 0 programs

**Def.** A certified program $P$, i.e. $M(P)\downarrow$, is **non-size-increasing w.r.t.** $X_i$ iff $M(P)[i] \leq 1_{n+1}[i]$.

Obviously, $\text{pop}(X_i)$ and $\text{nil}(X_i)$ are non-size-increasing w.r.t. $X_i$.

**Lemma (Non-Size-Increasing).** If a certified program $P$ contains only non-size-increasing BIs w.r.t. $X_i$, then $P$ is non-size-increasing w.r.t. $X_i$.

**Lemma (Embedding of Control).**
Let $P$ be any loop/stack program with certificate $Z := M(P)$.
Then for all $i, j \in \{1, \ldots, n\}$:
(a) $Z[i][j] \geq 1$ and $i \neq j \implies X_j \rightarrow P X_i$
(b) $Z[i][i] = \infty \implies X_i \rightarrow P X_i$ (top circle!)

**Theorem (Measure-0-Embedding).**
For every loop/stack program of $\mu$-measure 0, one has $M(P)\downarrow$.

---

Characterisation Theorems – 1

**Def.** General loop programs are loop programs that have arbitrary BIs which can be simulated (in binary) on a Turing machine in linear space, and are extended by the conditional if $X_i \leq X_j$ then $P_1$ else $P_2$ with expected operational semantics.

**Thm (FLINSPACE).** Certified general loop programs exactly compute the functions in FLINSPACE.

**Proof.** $\subseteq$ Holds by Base Theorem and Measure-0-Embedding.
$\supseteq$ By induction on the structure of certified general loop programs $P$, using the construction of bps in the ADD-Case and Else-Case for loops, and closure of $E_2$ under simultaneous bounded recursion, one obtains that $P$ computes functions in $E_2 = \text{FLINSPACE}$ only. $\square$
**Characterisation Theorems – 2**

**Def.** **String programs** are stack programs that have arbitrary BIs which can be simulated on a Turing machine in polynomial time.

**Thm (FP).** **Certified string programs** exactly compute the FP functions.

**Proof.** \(\Leftarrow\) Holds by **Base Theorem** and **Measure-0-Embedding**.

\(\Rightarrow\) Let \(P\) be a string program in \(X_1, \ldots, X_n\) such that \(M(P) \downarrow\). Following the construction in the proof of **Base Theorem** for stack programs, we prove for any standard simulation \(\text{sim}(P)\) of \(P\) on a Turing machine that

\[T_{\text{sim}(P)}(n) = O(n) + O(q_{\text{time}}(Q(n)) \cdot Q(n)) + O(Q(n))\]

for a polynomial \(q_{\text{time}}\) bounding the cost of \(\text{sim}(\text{imp})\) for each BI \(\text{imp}\) in \(P\), and \(Q(n) := q(n, \ldots, n)\) for some \(pb\ q\) on program \(\text{STEPS}(P)\):

---

**Characterisation Theorems – 3**

Let \(\text{steps}_p(\vec{w})\) denote the number of steps (execution of an BI) \(P\) performs on input \(\vec{w}\). Furthermore, for some new variable \(X_0\), define

\[\text{ADD} := X_0 + = X_1; \ldots; X_0 + = X_n.\]

and thus \(\text{STEPS}(p) := \text{nil}(X_0); \text{ADD}; P^\#\), where \(P^\#\) results from \(P\) by replacing each occurrence of a BI \(\text{imp}\) with \(\text{imp}; \text{ADD}\). Then we know:

1. \(\text{STEPS}(P)\) behaves on \(X_1, \ldots, X_n\) identical with \(P\).
2. In a run of \(P\) on input \(\vec{w}\), the size of \(X_0\) bounds the size of any \(X_1, \ldots, X_n\) (at any time).
3. \(\{ \vec{x} = \vec{w} \} \text{STEPS}(P) \{ \text{steps}_p(\vec{w}) \leq |X_0| \}\)

Thus, for a proof of (*), it remains to show \(M(\text{STEPS}(P)) \downarrow\).
Characterisation Theorems – 4

To see this, call a matrix $X^\# \in M_{n+1}[A]$ a **sharp form** of $X$, where $X \in M_n[A]$, iff there exist $*_1, \ldots, *_{n+1} \in A$ such that

$$X = \begin{pmatrix} S_1 \cdots S_n S_{n+1} \\ 0 \cdots 0 1 \end{pmatrix} \quad \text{and} \quad X^\# = \begin{pmatrix} 1 *_1 \cdots *_{n+1} \\ 0 S_1 \cdots S_n S_{n+1} \\ 0 0 \cdots 0 1 \end{pmatrix}$$

Now show for sharp forms $X^\#, Y^\#$ of $X, Y$:

(a) $X^\# \otimes Y^\#, X^\# \sqcup Y^\#$, $\hat{Y}^\#$ are sharp forms of $X \otimes Y, X \sqcup Y, \hat{Y}$, resp.

(b) $(X^\#)^+, (X^\#)^*, (\hat{Y}^\#)^*$ are sharp forms of $X^+, X^*, \hat{Y}^+$, resp.

Thus, using (a), (b) and $M(\text{ADD}) = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$, we obtain:

(c) $M(\text{imp; ADD})$ is a sharp form of $M(\text{imp})$.

(b) $M(\text{P}^\#)$ is a sharp form of $M(\text{P})$.

Thus, we obtain $M(\text{STEPS(P)}) \downarrow$, concluding the proof.

---

Characterisation Theorems – 5

**Def.** **Power String programs** are stack programs that have arbitrary BIs which can be simulated on a Turing machine in polynomial space, and are extended by the following loop statement (called **power loop**)

$$\text{repeat Pow}(X_h) [Q]$$

which executes the body $2^{|w|} - 1$ times whenever $w$ is initially stored in the control stack $X_h$.

**Thm (FPSPACE).** Certified power string programs exactly compute the functions in FPSPACE.

**Optimality**

**Fact** ([Kristiansen & N.]). There is no certification method for the psb-property that certifies all psb programs.

**Def.** A certificate $Z \in \mathcal{M}_n[A]$ for a program $P$ is honest, if there exist constants $\vec{m} \geq \vec{1}$ such that for all $i \neq j$ in $\{1, \ldots, n\}$,

\[
Z[i][i] \geq 1 \implies \{\vec{X} = \vec{s} \geq \vec{m}\} P \{\vec{|X|} \geq s_i\}
\]

\[
Z[i][j] \geq 1 \implies \{\vec{X} = \vec{s} \geq \vec{m}\} P \{\vec{|X|} \geq s_i + s_j\}
\]

\[
Z[i][i] = \infty \implies \{\vec{X} = \vec{s} \geq \vec{m}\} P \{\vec{|X|} \geq 2 \cdot s_i\}
\]

\[
Z[i][n+1] \geq 1 \implies \{\vec{X} = \vec{s} \geq \vec{m}\} P \{\vec{|X|} \geq s_i + 1\}.
\]

**Core programs** are built from honestly certified basic instructions by sequencing and loop statements.

**Thm (Optimality [Mehler & N.]).** For core programs $P$, one has $M(P) \downarrow$ if and only if $P$ is psb.