Integer Square Root (P1)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

beg:	$(y_1, y_2, y_3) := (0, 1, 1)$; goto test
test:	if $(y_3 \leq x)$ goto loop else goto end
loop:	$(y_1, y_2) := (y_1 + 1, y_2 + 2)$; goto inloop
inloop:	$y_3 := y_3 + y_2$; goto test

Prove: $\models_I \{x \geq 0\} T_0 \{y_1 = \sqrt{x}\}$

Assume a computation is as follows.

$(beg, \sigma_0)(test, \sigma_1)(loop, \sigma_2)(inloop, \sigma_3)(test, \sigma_4)(loop, \sigma_5)\cdots$
$(test, \sigma_{n-1})(end, \sigma_n)\cdots$

There are n transitions, and $l_n = end$

Need $(y_1 = \sqrt{x})(\sigma_n)$, i.e., $\sigma_n(y_1) = \sqrt{\sigma_n(x)}$

We have
$\sigma_n = \sigma_{n-1}$ and
$\neg(\sigma_n(y_3) \leq \sigma_n(x))$ (implied by $(test, \sigma_{n-1}) \rightarrow (end, \sigma_n)$).

If there exists φ' such that $\varphi'(\sigma_{n-1})$ and

$$\neg(\sigma_n(y_3) \leq \sigma_n(x)) \wedge \varphi'(\sigma_n) \rightarrow \sigma_n(y_1) = \sqrt{\sigma_n(x)}$$

Then we have

$$\sigma_n(y_1) = \sqrt{\sigma_n(x)}$$

Let φ' be

$$x = \sigma_0(x) \wedge y_1^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = (y_1 + 1)^2$$

We have $\neg(\sigma_n(y_3) \leq \sigma_n(x)) \wedge \varphi'(\sigma_n) \rightarrow \sigma_n(y_1) = \sqrt{\sigma_n(x)}$

Remain to prove $\varphi'(\sigma_{n-1})$, i.e.,

$$\begin{array}{l} \sigma_{n-1}(x) = \sigma_0(x) \wedge \\ \sigma_{n-1}(y_1)^2 \leq \sigma_{n-1}(x) \wedge \\ \sigma_{n-1}(y_2) = 2 * \sigma_{n-1}(y_1) + 1 \wedge \\ \sigma_{n-1}(y_3) = (\sigma_{n-1}(y_1) + 1)^2 \end{array}$$

This can be proved by induction.

The label of σ_{n-1} is *test*.

We prove for all k, when σ_k has *test* as the label:

$$\begin{array}{l} \sigma_k(x) = \sigma_0(x) \wedge \\ \sigma_k(y_1)^2 \leq \sigma_k(x) \wedge \\ \sigma_k(y_2) = 2 * \sigma_k(y_1) + 1 \wedge \\ \sigma_k(y_3) = (\sigma_k(y_1) + 1)^2 \end{array}$$

(1) $k = 0$, the label is BEG, ok.

(2) $k = 1$, the label is *test*, we have
$\sigma_1(y_1) = 0, \sigma_1(y_2) = 1, \sigma_1(y_3) = 1, \sigma_1(x) = \sigma_0(x)$ and $\sigma_0(x) \geq 0$.
Therefore

$$\begin{array}{l} \sigma_k(x) = \sigma_0(x) \wedge \\ \sigma_k(y_1)^2 \leq \sigma_k(x) \wedge \\ \sigma_k(y_2) = 2 * \sigma_k(y_1) + 1 \wedge \\ \sigma_k(y_3) = (\sigma_k(y_1) + 1)^2 \end{array}$$

(3) Suppose that $k \leq i$, the goal holds.
Let $k = i + 1$ and $i \geq 1$.
No proof is needed if the label is not *test*.
Suppose that the label is *test* and we have $k \geq 4$.
Then

$$(test, \sigma_{k-3}) \Rightarrow (loop, \sigma_{k-2})$$
$$(loop, \sigma_{k-2}) \Rightarrow (inloop, \sigma_{k-1})$$
$$(inloop, \sigma_{k-1}) \Rightarrow (test, \sigma_k)$$

Therefore

$$\begin{aligned}
\sigma_k &= \sigma_{k-1}[y_3/I(y_2 + y_3)(\sigma_{k-1})] \\
\sigma_{k-1} &= \sigma_{k-2}[y_1/I(y_1 + 1)(\sigma_{k-2}][y_2/I(y_2 + 2)(\sigma_{k-2})] \\
\sigma_{k-2} &= \sigma_{k-3} \wedge I(y_3 \leq x)(\sigma_{k-3})
\end{aligned}$$

Therefore

$$\begin{aligned}
&\sigma_k(x) = \sigma_{k-3}(x) = \sigma_0(x) \\
&(\sigma_k(y_1))^2 = (\sigma_{k-3}(y_1) + 1)^2 = \sigma_{k-3}(y_3) \leq \sigma_{k-3}(x) = \sigma_k(x) \\
&\sigma_k(y_2) = \sigma_{k-3}(y_2) + 2 = 2 * \sigma_{k-2}(y_1) + 3 = 2 * \sigma_k(y_1) + 1 \\
&\sigma_k(y_3) = \sigma_{k-3}(y_2) + \sigma_{k-3}(y_3) + 2 = (\sigma_{k-3}(y_1) + 2)^2 = (\sigma_k(y_1) + 1)^2
\end{aligned}$$

Therefore, for all k, when the label of σ_k is *test*, we have

$$\begin{aligned}
&\sigma_k(x) = \sigma_0(x) \wedge \\
&\sigma_k(y_1)^2 \leq \sigma_k(x) \wedge \\
&\sigma_k(y_2) = 2 * \sigma_k(y_1) + 1 \wedge \\
&\sigma_k(y_3) = (\sigma_k(y_1) + 1)^2
\end{aligned}$$

Integer Square Root (P2)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

beg:	$(y_1, y_2, y_3) := (0, 1, 1)$; goto test
test:	if $(y_3 \leq x)$ goto loop else goto end
loop:	$(y_1, y_2) := (y_1 + 1, y_2 + 2)$; goto inloop
inloop:	$y_3 := y_3 + y_2$; goto test

Prove: $\models_I [true] T_0 [true]$

Suppose that the program does not terminate:

$$(BEG, \sigma_0)(l_1, \sigma_1)(l_2, \sigma_2)(l_3, \sigma_3)(l_4, \sigma_4)(l_5, \sigma_5) \cdots$$

For all $k \geq 0$, we have
$l_{3k+1} = \mathit{test}$, $l_{3k+2} = \mathit{loop}$,$l_{3k+3} = \mathit{inloop}$ and $\sigma_{3k+1}(y_3) \leq x$
We prove for all $k \geq 0$
$\sigma_{3k+1}(y_3) \geq k$ and $\sigma_{3k+1}(x) = \sigma_0(x)$

- We have $\sigma_1(y_3) = 1$ and $\sigma_1(x) = \sigma_0(x)$.
  Therefore $\sigma_{3*0+1}(y_3) \geq 0$ and $\sigma_{3*0+1}(x) = \sigma_0(x)$.
- Suppose that for $k = i$,
  we have $\sigma_{3i+1}(y_3) \geq i$ and $\sigma_{3i+1}(x) = \sigma_0(x)$.
  We prove for $k = i+1$, we have $\sigma_{3(i+1)+1}(y_3) \geq i+1$ and $\sigma_{3i+1}(x) = \sigma_0(x)$.
  According to the previous calculation, we have

  $$\sigma_{3(i+1)+1}(x) = \sigma_{3(i+1)+1-3}(x) = \sigma_0(x)$$
  $$\sigma_{3(i+1)+1}(y_3) = \sigma_{3(i+1)+1-3}(y_2) + \sigma_{3(i+1)+1-3}(y_3) + 2 \geq i+1$$

  Therefore for $k = i+1$,
  we have $\sigma_{3(i+1)+1}(y_3) \geq i+1$ and $\sigma_{3i+1}(x) = \sigma_0(x)$

Therefore for all $k \geq 0$, we have $\sigma_{3k+1}(y_3) \geq k$ and $\sigma_{3k+1}(x) = \sigma_0(x)$.

Let $k = \sigma_0(x) + 1$. Then $\sigma_{3k+1}(y_3) \leq \sigma_{3k+1}(x)$ does not hold, and this contradicts to the supposition.

Integer Square Root (P3)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

beg:	$(y_1, y_2, y_3) := (0, 1, 1)$; goto test
test:	if $(y_3 \leq x)$ goto loop else goto end
loop:	$(y_1, y_2) := (y_1 + 1, y_2 + 2)$; goto inloop
inloop:	$y_3 := y_3 + y_2$; goto test

Prove: $\models_I [x \geq 0]\, T_0 [y_1 = \sqrt{x}]$

Lemma:
For all $\sigma \in \Sigma$ and all $0 \leq k \leq \sqrt{\sigma_0(x)}$, we have

$$(l_0 = beg, \sigma_0) \Rightarrow (l_{3k+1}, \sigma_{3k+1})$$

and

$$\begin{aligned}
&l_{3k+1} = test \\
&\sigma_{3k+1}(x) = \sigma_0(x) \\
&\sigma_{3k+1}(y_1) = k \\
&\sigma_{3k+1}(y_2) = 2k + 1 \\
&\sigma_{3k+1}(y_3) = (k + 1)^2
\end{aligned}$$

By induction.

- $k = 0$, ok.
- Suppose that for $k = i$ and $k \leq \sqrt{\sigma_0(x)}$, we have

$$\begin{aligned} &l_{3k+1} = test \\ &\sigma_{3k+1}(x) = \sigma_0(x) \\ &\sigma_{3k+1}(y_1) = k \\ &\sigma_{3k+1}(y_2) = 2k+1 \\ &\sigma_{3k+1}(y_3) = (k+1)^2 \end{aligned}$$

Then for $k = i + 1$ and $k \leq \sqrt{\sigma_0(x)}$, we have

$$\begin{aligned} &l_{3(i+1)+1} = test \\ &\sigma_{3(i+1)+1}(x) = \sigma_{3i+1}(x) = \sigma_0(x) \\ &\sigma_{3(i+1)+1}(y_1) = \sigma_{3i+1}(y_1) + 1 = i + 1 = k \\ &\sigma_{3(i+1)+1}(y_2) = \sigma_{3i+1}(y_2) + 2 = 2(i+1) + 1 = 2k + 1 \\ &\sigma_{3(i+1)+1}(y_3) = \sigma_{3i+1}(y_3) + \sigma_{3i+1}(y_2) + 2 = (i+2)^2 = (k+1)^2 \end{aligned}$$

Therefore the lemma holds.

Let $k = \sqrt{\sigma_0(x)}$
Then $\sigma_{3k+1}(y_3) = (k+1)^2 = (\sqrt{\sigma_0(x)}+1)^2 > \sigma_0(x) = \sigma_{3k+1}(x)$
Therefore

$$(l_0 = beg, \sigma_0) \stackrel{*}{\Rightarrow} (l_{3k+1}, \sigma_{3k+1}) \Rightarrow (end, \sigma_{3k+2})$$

and
$\sigma_{3k+2}(y_1) = \sigma_{3k+1}(y_1) = k = \sqrt{\sigma_0(x)}$