Integer Square Root (M0)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
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: $\models_I \{x = c\} T_0 \{y_1 = \sqrt{c}\}$

Steps

(1) Select C

(2) Select a formula for each element of C

(3) Find the paths for proving

(4) Prove the correctness of the paths

- Select $C = \{beg, test, end\}$
- Select q_{beg}, q_{end}, q_{test} as follows.

$$\begin{array}{ll} q_{beg} & x = c \\ q_{end} & y_1 = \sqrt{c} \\ q_{test} & x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \end{array}$$

- Find the Paths

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \\ (test, end) \end{array}$$

- Prove the Correctness

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \\ \models_I vc(q_{test}, (test, end), q_{end}) \end{array}$$

Integer Square Root (M1)

$B = (\{0, 1, 2, 3, \ldots, +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
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: $\models_I [true] T_0 [true]$

Steps
(1) Select C
(2) Select a formula for each element of C
(3) Find the paths for proving
(4) Prove the correctness of the paths (a)
(5) Select C'
(6) Select $(W, \sqsubseteq)$
(7) Select a function $g_c : \Sigma \rightarrow W$ for each c of C'
(8) Find the paths for proving
(9) Prove the correctness of the paths (b)

- Select $C = \{beg, test\}$
- Select $q_{beg},\ q_{test}$

$$\begin{array}{ll} q_{beg} & true \\ q_{test} & y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2*y_1+1 \end{array}$$

- Find the Paths

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \end{array}$$

- Prove the Correctness

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \end{array}$$

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- Select $g_{test} : \Sigma \to W$

$$g_{test}(\sigma) = \sigma(x) + 1 - \sigma(y_3)$$

- Find the Paths

$$(test, loop, inloop, test)$$

- Prove the Correctness

$$I(q_{test})(\sigma) = true \wedge (\sigma \to^{(test,loop,inloop,test)} \sigma') \\ \to \\ g_{test}(\sigma') < g_{test}(\sigma)$$

i.e., (for simplicity, the symbol σ is omitted)

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

Integer Square Root (M1a)

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

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: $\models_I [x \geq 0]\, T_0 [true]$

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

$$\begin{array}{ll} q_{beg} & x \geq 0 \\ q_{test} & y_2 \geq 0 \end{array}$$

- Find the Paths

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \end{array}$$

- Prove the Correctness

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \end{array}$$

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- Select $g_{test} : \Sigma \to W$

$$g_{test}(\sigma) = \begin{cases} \sigma(x) + 1 - \sigma(y_3) & \sigma(y_3) \leq \sigma(x) \\ 0 & \end{cases}$$

- Find the Paths

$$(test, loop, inloop, test)$$

- Prove the Correctness

$$I(q_{test})(\sigma) = true \wedge (\sigma \to^{(test,loop,inloop,test)} \sigma') \\ \to \\ g_{test}(\sigma') < g_{test}(\sigma)$$

i.e.,

$$y_2 \geq 0 \wedge (y_3 \leq x) \to x + 1 - (y_2 + y_3 + 2) < x + 1 - y_3$$

i.e.,

$$y_2 \geq 0 \wedge (y_3 \leq x) \to 0 < x + 1 - y_3$$

Integer Square Root (M2)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
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: $\models_I [true]T_0[true]$

Steps

(1) Select C

(2) Select a formula q_c for each c of C

(3) Find the paths for proving

(4) Prove the correctness of the paths (a)

(5) Select C'

(6) Select $(W \subseteq D, I_0(\sqsubseteq))$;
Select w and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$

(7) Select a term t_c for each c of C' and prove $q_c \rightarrow w_x^{t_c}$

(8) Find the paths for proving

(9) Prove the correctness of the paths (b)

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

$$\begin{array}{ll} q_{beg} & true \\ q_{test} & y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1 \end{array}$$

- Find the Paths

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \end{array}$$

- Prove the Correctness

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \end{array}$$

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
  Select $w = true$, and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
- Select $t_{test} = x + 1 - y_3$, and prove $q_{test} \rightarrow w_x^{t_{test}}$
- Find the Paths

$$(test, loop, inloop, test)$$

- Prove the Correctness

$$\models_I vc(q_{test} \wedge t_{test} = v, (test, loop, inloop, test), t_{test} < v)$$

i.e.,

$$\begin{array}{l} y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge \\ x + 1 - y_3 = v \\ \rightarrow \\ ((y_3 \leq x) \rightarrow x + 1 - (y_2 + y_3 + 2) < v) \end{array}$$

Integer Square Root (M2a)

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

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: $\models_I [x \geq 0]\, T_0 [true]$

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

$$\begin{array}{ll} q_{beg} & x \geq 0 \\ q_{test} & y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_2 \geq 1 \end{array}$$

- Find the Paths

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \end{array}$$

- Prove the Correctness

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \end{array}$$

- Select$(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
  Select$w = (x \geq 0)$, and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
- Select $C' = \{test\}$
- Select $t_{test} = x + 1 - y_3 + y_2$, and prove $q_{test} \rightarrow w_x^{t_{test}}$
- Find the Paths

$$(test, loop, inloop, test)$$

- Prove the Correctness

$$\models_I vc(q_{test} \wedge t_{test} = v, (test, loop, inloop, test), t_{test} < v)$$

i.e.,

$$\begin{array}{l} y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_2 \geq 1 \wedge \\ x + 1 - y_3 + y_2 = v \\ \rightarrow \\ ((y_3 \leq x) \rightarrow x + 1 - (y_2 + y_3 + 2) + (y_2 + 2) < v) \end{array}$$