Programming Language Theory

Imperative Language Constructs: Annotated Programs

游書泓

2020 邏輯、語言與計算暑期研習營

1 Residual

Precondition: $\exists y.\, [0 \le y < n] \star (l_\mathrm{r} \hookrightarrow y)$

if $!l_\mathrm{r} \ge n/2$ then

$\{\, \exists y.\, [y \ge n/2] \star [0 \le y < n] \star (l_\mathrm{r} \hookrightarrow y) \,\}$

$l_\mathrm{r} := !l_\mathrm{r} - n/2$

$\{\, \exists y.\, [y \ge n/2] \star [0 \le y < n] \star (l_\mathrm{r} \hookrightarrow y - n/2) \,\}$

$\{\, \exists y'.\, [0 \le y' < n/2] \star (l_\mathrm{r} \hookrightarrow y') \,\}$

else

$\{\, \exists y.\, [y < n/2] \star [0 \le y < n] \star (l_\mathrm{r} \hookrightarrow y) \,\}$

()

$\{\, \exists y.\, [0 \le y < n/2] \star (l_\mathrm{r} \hookrightarrow y) \,\}$

Postcondition: $\exists y.\, [0 \le y < n/2] \star (l_\mathrm{r} \hookrightarrow y)$

2 Summation

For any positive integer n, the following program fragment computes the sum from 0 to $n-1$.

$$\sum_{i=0}^{n-1} i = 0 + 1 + \cdots + (n-1) = \frac{(n-1)n}{2}$$

When proving the summation formula by induction, the inductive step for $n := m+1$ involves adding the last term m to the induction hypothesis.

$$\sum_{i=0}^{(m+1)-1} i = \left(\sum_{i=0}^{m-1}\right) + m = \frac{(m-1)m}{2} + m = \frac{(m+1)m}{2}.$$

A similar pattern emerges as the loop invariant. Since loops can be regarded as a form of tail-recursive functions and that recursion and induction coincide, the usage of inductive properties carries over.

Precondition: $[n > 0] \star (l_\mathrm{i} \hookrightarrow \_) \star (l_\mathrm{S} \hookrightarrow \_)$

$l_\mathrm{i} := 0;$

$\{\, [n > 0] \star (l_\mathrm{i} \hookrightarrow 0) \star (l_\mathrm{S} \hookrightarrow \_) \,\}$

$l_\mathrm{S} := 0;$

$\{\, [n > 0] \star (l_\mathrm{i} \hookrightarrow 0) \star (l_\mathrm{S} \hookrightarrow 0) \,\}$

$\left\{ \exists m.\, [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m) \star \left(l_\mathrm{S} \hookrightarrow \frac{(m-1)m}{2}\right) \right\}$

while $l_i < n$ do

$\left\{ \exists m.\, [m < n] \star [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m) \star \left(l_\mathrm{S} \hookrightarrow \frac{(m-1)m}{2}\right) \right\}$

$l_\mathrm{S} := !l_\mathrm{i} + !l_\mathrm{S};$

$\left\{ \exists m.\, [m < n] \star [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m) \star \left(l_\mathrm{S} \hookrightarrow m + \frac{(m-1)m}{2}\right) \right\}$

$\left\{ \exists m.\, [m < n] \star [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m) \star \left(l_\mathrm{S} \hookrightarrow \frac{(m+1)m}{2}\right) \right\}$

$l_\mathrm{i} := !l_\mathrm{i} + 1$

$\left\{ \exists m.\, [m < n] \star [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m+1) \star \left(l_\mathrm{S} \hookrightarrow \frac{(m+1)m}{2}\right) \right\}$

$\left\{ \exists m'.\, [m' < n+1] \star [m' \leq n+1] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m') \star \left(l_\mathrm{S} \hookrightarrow \frac{m'(m'-1)}{2}\right) \right\}$

$\left\{ \exists m'.\, [m' \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m') \star \left(l_\mathrm{S} \hookrightarrow \frac{(m'-1)m'}{2}\right) \right\}$

$\left\{ \exists m.\, [m \geq n] \star [m \leq n] \star [n > 0] \star (l_\mathrm{i} \hookrightarrow m) \star \left(l_\mathrm{S} \hookrightarrow \frac{(m-1)m}{2}\right) \right\}$

Postcondition: $[n > 0] \star (l_\mathrm{i} \hookrightarrow n) \star \left(l_\mathrm{S} \hookrightarrow \frac{(n-1)n)}{2}\right)$

3 Factorial

Precondition: $[n > 0] \star (l_{\mathrm{i}} \hookrightarrow \_) \star \left(l_{\mathrm{prod}} \hookrightarrow \_\right)$

$l_{\mathrm{i}} := n;$

$\{\, [n > 0] \star (l_{\mathrm{i}} \hookrightarrow n) \star (l_{\mathrm{prod}} \hookrightarrow \_) \,\}$

$l_{\mathrm{prod}} := 1;$

$\{\, [n > 0] \star (l_{\mathrm{i}} \hookrightarrow n) \star (l_{\mathrm{prod}} \hookrightarrow 1) \,\}$

$\left\{ \exists m.\, [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{m!}\right) \right\}$

while $!l_{\mathrm{i}} \neq 0$ do

$\left\{ \exists m.\, [m \neq 0] \star [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{m!}\right) \right\}$

$l_{\mathrm{prod}} := !l_{\mathrm{prod}} \times !l_{\mathrm{i}};$

$\left\{ \exists m.\, [m \neq 0] \star [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{m!} \times m\right) \right\}$

$\left\{ \exists m.\, [m \neq 0] \star [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{(m-1)!}\right) \right\}$

$l_{\mathrm{i}} := !l_{\mathrm{i}} - 1$

$\left\{ \exists m.\, [m \neq 0] \star [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m - 1) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{(m-1)!}\right) \right\}$

$\left\{ \exists m'.\, [m' \neq -1] \star [-1 \leq m' \leq n-1] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m') \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{(m')!}\right) \right\}$

$\left\{ \exists m'.\, [0 \leq m' \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m') \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{(m')!}\right) \right\}$

$\left\{ \exists m.\, [m = 0] \star [0 \leq m \leq n] \star [n > 0] \star (l_{\mathrm{i}} \hookrightarrow m) \star \left(l_{\mathrm{prod}} \hookrightarrow \frac{n!}{m!}\right) \right\}$

Postcondition: $[n > 0] \star (l_{\mathrm{i}} \hookrightarrow 0) \star \left(l_{\mathrm{prod}} \hookrightarrow n!\right)$

4 Fast Exponentiation

$$\begin{aligned} n &= \underbrace{b_L 2^L + b_{L-1} 2^{L-1} + \cdots + b_m 2^m} \quad + \quad b_{m-1} 2^{m-1} + \cdots + b_0 2^0 \\ l_\mathrm{E} &\hookrightarrow a^{\lfloor n/2^m \rfloor} = a^{b_L 2^{L-m} + \cdots + b_{m+1} 2^1 + b_m 2^0} \\ l_\mathrm{b} &\hookrightarrow 2^m \end{aligned}$$

For any positive integer n and a, the fast exponentiation algorithm computes the value a^n using $O(\log n)$ number of multiplications.

Let the binary representation of n be $(b_L b_{L-1} \dots b_2 b_1 b_0)_2$. The exponentiation process iteratively computes a raised to the power of some prefix of the representation $(b_L \dots b_0)_2$. At each step, the partial exponentiation result equals $a^{(b_L \dots b_{m+1} b_m)_2}$ for some $0 \le m \le L$.

To connect the successive partial exponentiation results, consider the expression for extracting consecutive prefixes.

$$\begin{aligned} \left\lfloor \frac{n}{2^{m-1}} \right\rfloor &= \left\lfloor 2 \left(b_L 2^{L-m} + \cdots + b_m 2^0 \right) + b_{m-1} + \left(b_{m-2} 2^{-1} + \cdots + b_0 2^{-(m-1)} \right) \right\rfloor \\ &= 2 \left(b_L 2^{L-m} + \cdots + b_m 2^0 \right) + b_{m-1} \end{aligned}$$

The above equation can be further rewritten using $\lfloor n/2^m \rfloor$.

$$\left\lfloor \frac{n}{2^{m-1}} \right\rfloor \quad = \quad 2 \left\lfloor \frac{n}{2^m} \right\rfloor + b_{m-1} = 2 \left\lfloor \frac{n}{2^m} \right\rfloor + \left(\left\lfloor \frac{n}{2^{m-1}} \right\rfloor \bmod 2 \right)$$

Therefore if location l_E stores the partial exponentiation results, all we need is to compute either $(!l_\mathrm{E})^2$ or $(!l_\mathrm{E})^2 \times a$.

Precondition: $[n > 0] \star [a > 0] \star (l_\mathrm{b} \hookrightarrow \_) \star (l_\mathrm{E} \hookrightarrow \_)$

$l_\mathrm{b} := 1;$

(while $!l_\mathrm{b} \le n$ do

$\quad l_\mathrm{b} := 2 \times !l_\mathrm{b});$

$l_\mathrm{E} := 1;$

while $l_\mathrm{b} > 1$ do

$\quad l_\mathrm{E} := !l_\mathrm{E} \times !l_\mathrm{E};$

$\quad l_\mathrm{b} := !l_\mathrm{b}/2;$

$\quad$(if $(\lfloor n/l_\mathrm{b} \rfloor \bmod 2) = 1$ then

$\quad\quad l_\mathrm{E} := a \times !l_\mathrm{E}$

$\quad$ else ())

Postcondition: $[n > 0] \star [a > 0] \star (l_\mathrm{b} \hookrightarrow 1) \star (l_\mathrm{E} \hookrightarrow a^n)$

Let $H_0 \equiv [n > 0] \star [a > 0]$.

$l_{\mathrm{b}} := 1;$

$\{\, H_0 \star (l_{\mathrm{b}} \hookrightarrow 1) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

$\{\, \exists mL.\, [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

(while $!l_{\mathrm{b}} \le n$ do

$\{\, \exists mL.\, [2^m \le n] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

$l_{\mathrm{b}} := 2 \times !l_{\mathrm{b}}$

$\{\, \exists mL.\, [2^m \le n] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^{m+1}) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

$\left\{\, \exists m'L.\, [2^{m'-1} \le n] \star [2^L \le n < 2^{L+1}] \star [1 \le m' \le L+2] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{m'}\right) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\right\}$

$\left\{\, \exists m'L.\, [2^L \le n < 2^{L+1}] \star [0 \le m' \le L+1] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{m'}\right) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\right\}$);

$\{\, \exists mL.\, [2^m > n] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

$\{\, \exists L.\, [2^L \le n < 2^{L+1}] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{L+1}\right) \star (l_{\mathrm{E}} \hookrightarrow \_) \,\}$

$l_{\mathrm{E}} := 1;$

$\{\, \exists L.\, [2^L \le n < 2^{L+1}] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{L+1}\right) \star (l_{\mathrm{E}} \hookrightarrow 1) \,\}$

$\left\{\, \exists mL.\, [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^m \rfloor}\right) \,\right\}$

while $l_{\mathrm{b}} > 1$ do

$\left\{\, \exists mL.\, [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^m \rfloor}\right) \,\right\}$

$l_{\mathrm{E}} := !l_{\mathrm{E}} \times !l_{\mathrm{E}};$

$\left\{\, \exists mL.\, [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star \left(l_{\mathrm{E}} \hookrightarrow a^{2\lfloor n/2^m \rfloor}\right) \,\right\}$

$l_{\mathrm{b}} := !l_{\mathrm{b}}/2;$

$\left\{\, \exists mL.\, [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{2\lfloor n/2^m \rfloor}\right) \,\right\}$

(if $(\lfloor n/l_{\mathrm{b}} \rfloor \bmod 2) = 1$ then

$$\left\{ \begin{array}{l} \exists mL.\, [(\lfloor n/2^{m-1} \rfloor \bmod 2) = 1] \star [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star \\ \qquad (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{2\lfloor n/2^m \rfloor}\right) \end{array} \right\}$$

$l_{\mathrm{E}} := a \times !l_{\mathrm{E}}$

$$\left\{ \begin{array}{l} \exists mL.\, [(\lfloor n/2^{m-1} \rfloor \bmod 2) = 1] \star [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star \\ \qquad (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{1+2\lfloor n/2^m \rfloor}\right) \end{array} \right\}$$

$$\left\{ \begin{array}{l} \exists mL.\, [(\lfloor n/2^{m-1} \rfloor \bmod 2) = 1] \star [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star \\ \qquad (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^{m-1} \rfloor}\right) \end{array} \right\}$$

else

$$\left\{ \begin{array}{l} \exists mL.\, [(\lfloor n/2^{m-1} \rfloor \bmod 2) = 0] \star [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star \\ \qquad (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{2\lfloor n/2^m \rfloor}\right) \end{array} \right\}$$

()

$$\left\{ \begin{array}{l} \exists mL.\, [(\lfloor n/2^{m-1} \rfloor \bmod 2) = 0] \star [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star \\ \qquad (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^{m-1} \rfloor}\right) \end{array} \right\})$$

$\left\{\, \exists mL.\, [2^m > 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^{m-1}) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^{m-1} \rfloor}\right) \,\right\}$

$\left\{\, \exists m'L.\, [2^{m'+1} > 1] \star [2^L \le n < 2^{L+1}] \star [-1 \le m' \le L] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{m'}\right) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^{m'} \rfloor}\right) \,\right\}$

$\left\{\, \exists m'L.\, [2^L \le n < 2^{L+1}] \star [0 \le m' \le L+1] \star H_0 \star \left(l_{\mathrm{b}} \hookrightarrow 2^{m'}\right) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^{m'} \rfloor}\right) \,\right\}$

$\left\{\, \exists mL.\, [2^m \le 1] \star [2^L \le n < 2^{L+1}] \star [0 \le m \le L+1] \star H_0 \star (l_{\mathrm{b}} \hookrightarrow 2^m) \star \left(l_{\mathrm{E}} \hookrightarrow a^{\lfloor n/2^m \rfloor}\right) \,\right\}$