

S6.

$$\begin{array}{ll} x & \varphi(x) \\ z & \psi(x, z). \end{array}$$

$$v_0 [\varphi, \psi].$$

$$v_0 \leq v_1 \leq \dots \quad \text{if } \downarrow$$

Refinement rules:

$\downarrow_{\text{pre}}$        $\downarrow_{\text{post}}$

R Assignment.  $v : [\psi(v/e), \psi] \leq v \leftarrow e.$

R Seg. composition  $w : [\eta_1, \eta_2] \leq w, w_1 : [\eta_1, \gamma]$ .

$\gamma$  - middle point.  $w, w_2 : [\gamma, \eta_2]$ .

R Alternation  $w : [\eta_1, \eta_2] \leq$  IF  $g_i \rightarrow w, w_i : [\eta_1 \wedge g_i, \eta_2]$ .  
 $g_1, g_2, \dots, g_m$

$\downarrow$   
 $g_m \rightarrow w, w_m : [\eta_1 \wedge g_m, \eta_2]$

R Iteration.  $w : [\eta, \eta \wedge \text{TAG}] \leq \text{DO. } g_i \rightarrow w, w_i : [\eta \wedge g_i, \eta \wedge \text{TC}]$ .

$$G = g_1 \vee g_2 \vee \dots \vee g_m$$

$$\text{DO. } g_m \rightarrow w, w_m : [\eta \wedge g_m, \eta \wedge \text{TC}].$$

OD.

① Integer division : quotient & remainder

$$q : x \geq 0, y \geq 0.$$

$$\psi : x = q * y + r \wedge 0 \leq r < y$$

$$v_0 : [x \geq 0 \wedge y \geq 0, x = q * y + r \wedge 0 \leq r < y].$$

$$g : x = q * y + r \wedge 0 \leq r \xrightarrow{\text{R2}} v_1 : [x \geq 0 \wedge y \geq 0, x = q * y + r \wedge 0 \leq r] \xrightarrow{\text{R1}} [x = q * y + r \wedge 0 \leq r, x = q * y + r \wedge 0 \leq r < y].$$

$$v_2 (q, r) \leftarrow (0, x). \underbrace{[x = q * y + r \wedge 0 \leq r]}_m, \underbrace{(x = q * y + r \wedge 0 \leq r < y)}_m \xrightarrow{\text{R4}} \text{TAG} \Rightarrow G = r > y$$

$$(q, r) \in (0, x). \text{DO. } r > y \Rightarrow [\eta \wedge r > y, \eta \wedge \text{TC}]. \text{ OD. } \xrightarrow{\text{R5}}$$

$$v_4 (q, r) \in (0, x). \text{DO. } r > y \Rightarrow (r, q) \leftarrow (r - y, q + 1) \text{ OD. }$$

## S<sub>2</sub> Square root

φ:  $s \in \mathbb{N}$ .

ψ:  $n = \lceil \sqrt{s} \rceil$ .

$$n \leq \sqrt{s} < n+1 \quad |^2 \\ n^2 \leq s < n^2 + n + 1 \\ \frac{1}{2}$$

V<sub>0</sub>:  $[s \in \mathbb{N}, n^2 \leq s < q^2 \wedge q = n+1]$ .

δ:  $n^2 \leq s < q^2$ .

R<sub>2</sub>  $\Rightarrow$  V<sub>1</sub>:  $[s \in \mathbb{N}, n^2 \leq s < q^2]$

$[n^2 \leq s < q^2, n^2 < s < q^2 \wedge q = n+1]$ .

R<sub>3</sub>  $\Rightarrow$  V<sub>2</sub>:  $(n, q) \leftarrow (0, s+1)$ .

$\underbrace{[n^2 \leq s < q^2]}_n, \underbrace{n^2 < s < q^2}_{m} \wedge q = n+1$ .

R<sub>3</sub>  $\Rightarrow$   $(n, q) \leftarrow (0, s+1)$ .

DO.  $q \neq n+1 \rightarrow [m \wedge q \neq n+1, m \wedge t c] \text{ OD}$

V<sub>2</sub>  $(n, q) \leftarrow (0, s+1)$ .

DO  $q \neq n+1 \rightarrow \text{IF } s < p^2 \rightarrow q \leftarrow p$ .

FI.  $\square s \geq p^2 \rightarrow n \leftarrow p$ .

OD.