Inference rule for loop - Ctnd.

- $\alpha(x) \wedge B(x) \rightarrow wlp_S(\alpha(x))$ — establish loop-inv.

$(0 \leq E(x) = T) \wedge B(x) \rightarrow wlp_S(0 \leq E(x) < T)$ — establish loop.-variant

---

$\alpha(x) \wedge (0 \leq E(x))$ $\{$while $B(x)$ do $S\}$ $\alpha(x) \wedge (0 \leq E(x)) \wedge \neg B(x)$

Example (factorial program).

1. $[x \geq 0]$ — pre-condition
2. $[1 = 0!] \wedge [0 \leq x]$
   $y := 1;$
3. $[y = 0!] \wedge [0 \leq x]$
   $z := 0;$
4. $[y = z!] \wedge [0 \leq x - z]$
   while $(z \neq x)$ do $z := z+1;\ y := y * z;$
5. $[y = z!] \wedge [0 \leq x - z] \wedge [z = x]$
6. $[y = x!]$ — post-condition

The program proof requires these proofs.

- 4 & 5 require loop-invariant & loop-variant:

  $[y = z!] \wedge [z \neq x] \rightarrow [y * (z+1) = (z+1)!]$ — (A)

  $[0 \leq x - z = T] \wedge [z \neq x] \rightarrow [0 \leq x - (z+1) < T].$ — (B)

- 1 → 2, ie.,

  $[x \geq 0] \rightarrow [1 = 0!] \wedge [0 \leq x]$ — (C)

- 5 → 6, i.e.,

  $[y = z!] \wedge [0 \leq x - z] \wedge [z = x] \rightarrow [y = x!]$ — (D)

(A) - (D) can be encoded in PVS and proved.