Inference rule for total correctness of while-loop

(vii)
$$\frac{[\alpha(x) \wedge B(x)] \wedge [0 \leq E(x) = T] \;\{S\}\; [\alpha(x)] \wedge [0 \leq E(x) < T]}{\alpha(x) \wedge [0 \leq E(x)] \{\text{while } B(x) \text{ do } S\} [\alpha(x) \wedge \neg B(x)] \wedge [0 \leq E(x)]}$$

- $\alpha(x)$ is loop-invariant
- $E(x)$ is a positive integer, called loop-variant, that decreases monotonically.
  In previous example, $f(x) \equiv f(w,b) = w+b$.

Example (factorial computation):

$[i, f = 1, 1]$ — pre-cond.
while $i < n$ do $i, f \Leftarrow i+1, f*i$. (S)
$[f = n!]$ — post. cond.
($i < n$: guard)

Loop-variant $E(i,f)$ can be taken to be $n-i$
Loop-invariant $\alpha(i,f)$ can be taken to be $[f = i!]$.

$[f = i!] \wedge [\underbrace{n-i > 0}_{\text{guard}}] \;\{i, f \Leftarrow i+1, f*i\}\; [f = i!]$ — loop-inv.

Also, $[\underbrace{n-i > 0}_{\text{guard}}] \wedge [0 \leq n-i = T] \;\{i, f \Leftarrow i+1, f*i\}\; [0 \leq n-i < T]$ — loop-variant

Applying rule (vii) we get post-condition:

$[f = i!] \wedge [0 \leq n-i] \{\text{while } \ldots\} [f = i!] \wedge [0 \leq n-i] \wedge \neg [0 < n-i]$
$\equiv [n-i = 0] \equiv [n = i]$
$\equiv [f = n!]$

- No mechanical procedure exist for finding loop-inv. or loop-variant.