

Dev. ⑨

# Sémantique axiomatique de la factorielle

927 : Preuves d'algos. 930 : sémantique.

FACT :=  $Y \leftarrow 1$ ; while  $X \neq 1$  do  $Y \leftarrow Y \times X$ ;  $X \leftarrow X - 1$  done

mq:  $\{ \sigma(X) = m \wedge m > 0 \} \text{FACT} \{ \sigma(Y) = m! \}$

→ Pour simplifier les notations on écrira  $X$  au lieu de  $\sigma(X)$ .

Quel invariant pour la boucle while ?

INV =  $X > 0 \wedge Y \times X! = m!$

Déroulons le programme:

$$\frac{\text{(aff)}}{\{ \text{INV} \} \{ \} \{ Y \leftarrow Y \times X \} \{ \text{INV} \} \{ \} \{ X \leftarrow X - 1 \} \{ \text{INV} \} \}$$

$$\frac{\text{INV} \wedge X \neq 1 \downarrow \text{INV} [X-1/X] [Y \times X / Y]}{\{ \text{INV} [X-1/X] [Y \times X / Y] \} \{ Y \leftarrow Y \times X; X \leftarrow X - 1 \} \{ \text{INV} \}}$$

$$\frac{\text{(aff)} \quad \frac{\frac{X = m \wedge m > 0 \downarrow \text{INV} [1/Y]}{\text{INV} [1/Y]} \quad \frac{\text{INV} [1/Y] \{ Y \leftarrow 1 \} \{ \text{INV} \}}{\{ X = m \wedge m > 0 \} \{ Y \leftarrow 1 \} \{ \text{INV} \}}}{\text{INV} \wedge X \neq 1 \{ Y \leftarrow Y \times X; X \leftarrow X - 1 \} \{ \text{INV} \}} \quad \frac{\text{INV} \{ \} \text{idem} \{ X = 1 \wedge \text{INV} \}}{X = 1 \wedge \text{INV} \Rightarrow Y = m!}}{\{ \text{INV} \} \text{while } X \neq 1 \text{ do } Y \leftarrow Y \times X; X \leftarrow X - 1 \text{ done} \{ Y = m! \}}$$


---


$$\{ X = m \wedge m > 0 \} \text{FACT} \{ Y = m! \}$$

Et par connectio- de la logique de Hoare, FACT est correcte. □