

---

# Cours MALG & MOVEX

## Vérification d'une annotation

---

Dominique Méry  
Telecom Nancy, Université de Lorraine  
(5 mai 2025 at 12:42 A.M.)

---

Année universitaire 2024-2025

---

$$\begin{aligned} \ell_1 : x = 3 \wedge y = z+x \wedge z = 2 \cdot x \\ y := z+x \\ \ell_2 : x = 3 \wedge y = x+6 \end{aligned}$$

On définit un contrat comme suit :

```
variables x, y, z
requires  $x_0 = 3 \wedge y_0 = z_0 + x_0 \wedge z_0 = 2 \cdot x_0$ 
ensures  $x_f = 3 \wedge y_f = x_f + 6$ 
begin
   $\ell_1 : x = 3 \wedge y = z+x \wedge z = 2 \cdot x$ 
   $y := z+x$ 
   $\ell_2 : x = 3 \wedge y = x+6$ 
end
```

On pose les assertions suivantes à partir de l'annotation :

- ▶  $pre(x_0, y_0, z_0) \stackrel{def}{=} x_0 = 3 \wedge y_0 = z_0 + x_0 \wedge z_0 = 2 \cdot x_0$
- ▶  $prepost(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = x + 6$
- ▶  $Q_1(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = z + x \wedge z = 2 \cdot x$
- ▶  $Q_2(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = x + 6$

On pose les assertions suivantes à partir de l'annotation :

- ▶  $pre(x_0, y_0, z_0) \stackrel{def}{=} x_0 = 3 \wedge y_0 = z_0 + x_0 \wedge z_0 = 2 \cdot x_0$
- ▶  $prepost(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = x + 6$
- ▶  $Q_1(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = z + x \wedge z = 2 \cdot x$
- ▶  $Q_2(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \wedge y = x + 6$

On établit les trois conditions pour valider le contrat :

- ▶ (init)  $pre(x_0, y_0, z_0) \wedge (x, y, z) = (x_0, y_0, z_0) \Rightarrow Q_1(x_0, y_0, z_0, x, y, z)$
- ▶ (concl)  $pre(v_0) \wedge Q_2(x_0, y_0, z_0, x, y, z) \Rightarrow prepost(x_0, y_0, z_0, x, y, z)$
- ▶ (induct)  
 $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$



► 
$$pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$$

- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$

- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$



- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0), Q_1(x_0, y_0, z_0, x, y, z), TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$

- MALG & MOVEX 4/6

## Preuve du pas induct

- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0), Q_1(x_0, y_0, z_0, x, y, z), TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x_0 = 3 \wedge y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, Q_1(x_0, y_0, z_0, x, y, z), TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x_0 = 3 \wedge y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, x = 3 \wedge y = z + x \wedge z = 2 \cdot x, TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$

- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge TRUE \wedge (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0), Q_1(x_0, y_0, z_0, x, y, z), TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x0 = 3 \wedge y0 = z0 + x0, z0 = 2.x0, Q_1(x_0, y_0, z_0, x, y, z), TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x0 = 3 \wedge y0 = z0 + x0, z0 = 2.x0, x = 3 \wedge y = z+x \wedge z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x0 = 3 \wedge y0 = z0 + x0, z0 = 2.x0, x = 3 \wedge y = z+x \wedge z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x' = 3 \wedge y' = x' + 6$



►  $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, x = 3, y = z + x, z = 2 \cdot x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \wedge y' = x' + 6$

- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \wedge y' = x' + 6$
- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$

- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \wedge y' = x' + 6$
- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$ 
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$



- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \wedge y' = x' + 6$
- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$ 
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x = 3$

- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \wedge y' = x' + 6$
- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$ 
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x = 3$
  - $x = 3$  est une hypothèse à gauche. Le séquent est valide.



►  $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, x = 3, y = z + x, z = 2 \cdot x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$

- ▶  $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$ 
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$

- $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$
- $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x + 6$

- $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$
- $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x' + 6$
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash y' = x + 6$
  - $x0 = 3, y0 = z0 + x0, z0 = 2.x0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash z + x = x + 6$









