

---

## Cours MALG & MOVEX

### Vérification d'une annotation

---

Dominique Méry  
Telecom Nancy, Université de Lorraine

---

### Année universitaire 2023-2024

- ① Correction
- ② Règles appliquées sur les séquents

## ① Correction

## ② Règles appliquées sur les séquents

① Correction

② Règles appliquées sur les séquents

## Ecriture du contrat

---

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

On définit un contrat comme suit :

```
variables x, y, z
requires x0 = 3 ∧ y0 = z0+x0 ∧ z0 = 2.x0
ensures xf = 3 ∧ yf = xf+6
begin
    ℓ1 : x = 3 ∧ y = z+x ∧ z = 2·x
    y := z+x
    ℓ2 : x = 3 ∧ y = x+6
end
```

## Conditions de vérification du contrat

---

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

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

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

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

On établit les trois conditions pour valider le contrat :

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

## Preuve du pas induct

---

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

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

## Preuve du pas inductif

---

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

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

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

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

- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge \text{TRUE} \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $\vdash pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge \text{TRUE} \wedge (x', y', z') = (x, z+x, z) \Rightarrow Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0) \wedge Q_1(x_0, y_0, z_0, x, y, z) \wedge \text{TRUE} \wedge (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $pre(x_0, y_0, z_0), Q_1(x_0, y_0, z_0, x, y, z), \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x_0 = 3 \wedge y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, Q_1(x_0, y_0, z_0, x, y, z), \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x_0 = 3 \wedge y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, x = 3 \wedge y = z+x \wedge z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash Q_2(x_0, y_0, z_0, x', y', z')$
- ▶  $x_0 = 3 \wedge y_0 = z_0 + x_0, z_0 = 2 \cdot x_0, x = 3 \wedge y = z+x \wedge z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash x' = 3 \wedge y' = x' + 6$



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

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

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

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

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



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

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

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

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

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

- ▶  $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$ 
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash z+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.x+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.3+3 = 3+6$

- ▶  $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$ 
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash z+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.x+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.3+3 = 3+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 9 = 9$

- ▶  $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$ 
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x' + 6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash y' = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash z+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.x+x = x+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 2.3+3 = 3+6$
  - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, \text{TRUE}, (x', y', z') = (x, z+x, z) \vdash 9 = 9$
  - Réflexivité de l'égalité.

## ① Correction

## ② Règles appliquées sur les séquents