



Cours MALG & MOVEX

Vérification d'une annotation

Dominique Méry Telecom Nancy, Université de Lorraine (22 avril 2025 at 7:53 A.M.)

Année universitaire 2024-2025

$$\begin{array}{l} \ell_1 : x = 3 \ \land \ y = z + x \ \land z = 2 \cdot x \\ y := z + x \\ \ell_2 : x = 3 \ \land \ y = x + 6 \end{array}$$

On définit un contrat comme suit :

variables x, y, z requires
$$x0=3 \land y0=z0+x0 \land z0=2.x0$$
 ensures $x_f=3 \land y_f=x_f+6$ begin
$$\ell_1: x=3 \ \land \ y=z+x \ \land z=2\cdot x$$
 $y:=z+x$
$$\ell_2: x=3 \ \land \ y=x+6$$
 end

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

- $ightharpoonup pre(x_0, y_0, z_0) \stackrel{def}{=} x0 = 3 \land y0 = z0 + x0 \land z0 = 2.x0$
- $ightharpoonup prepost(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \land y = x + 6$
- $ightharpoonup Q_1(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \ \land \ y = z + x \ \land z = 2 \cdot x$
- $Q_2(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \land y = x + 6$

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

- $ightharpoonup pre(x_0, y_0, z_0) \stackrel{def}{=} x0 = 3 \land y0 = z0 + x0 \land z0 = 2.x0$
- $ightharpoonup prepost(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \land y = x + 6$
- $ightharpoonup Q_1(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \ \land \ y = z + x \ \land z = 2 \cdot x$
- $Q_2(x_0, y_0, z_0, x, y, z) \stackrel{def}{=} x = 3 \land y = x + 6$

On établit les trois cpnditions pour valider le contrat :

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

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

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

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

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

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

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

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

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

- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \land y' = x' + 6$
- $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x' = 3$

- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \land y' = x' + 6$
- $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x' = 3$
 - x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 0
 - $2 \cdot x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$

- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \land y' = x' + 6$
- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$
 - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x' = 3$
 - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x = 3$

- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3 \land y' = x' + 6$
- $x_0 = 3, y_0 = z_0 + x_0, z_0 = 2.x_0, x = 3, y = z + x, z = 2.x, TRUE, (x', y', z') = (x, z + x, z) \vdash x' = 3$
 - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2 \cdot x, TRUE, (x', y', z') = (x, z+x, z) \vdash x' = 3$
 - $x0 = 3, y0 = z0+x0, z0 = 2.x0, x = 3, y = z+x, z = 2.x, TRUE, (x', y', z') = (x, z+x, z) \vdash x = 3$
 - x = 3 est une hypothèse à gauche. Le séquent est valide.

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

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

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

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

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

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

Vérification d'une annotation (22 avril 2025) (Dominique Méry)

✓ □ ➤ ✓ △ → ➤ → MALG & MOVEX ⋅ 6/6. ○

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

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