Raisonnement compositionnel

Motivation

- Les systèmes sont souvent construits à partir d'éléments plus simples.
  Exemple: Peterson $P = P_1 \| P_2$.
- But: prouver des propriétés de P à partir de propriétés de P_1 et de P_2.

Paradigme “hypothèses garanties”

- Paradigme "hypothèses garanties”.
- Formules.
  1. Notation: triplets

$$< g > M < f > .$$

où f et g sont des formules temporelles et M un système.

  2. Sémantique: si M est une partie d’un système qui vérifie g alors le système vérifie f.
     Exemple typique: $< g > M' < f >$, $< true > M < g >$ permet d’affirmer $< true > M \| M' < f >$.

Composition de structures

- A partir des structures de Kripke

  1. $M_1 = (S^1, S_0^1, R^1, L^1)$ sur AP_1,
  2. $M_2 = (S^2, S_0^2, R^2, L^2)$ sur AP_2,

  on définit

  $$M_1 ||| M_2 = (S, S_0, R, L)$$

  sur AP par

  1. $AP = AP_1 \cup AP_2$
  2. $S = \{(s, s') | L^1(s) \cap AP_2 = L^2(s') \cap AP_1\}$
  3. $S_0 = (S_0^1 \times S_0^2) \cap S$
  4. $L((s, s')) = L_1(s) \cup L_2(s)$
  5. $R((s, s'), (t, t'))$ ssi $R^1(s, t)$ et $R^2(s', t')$.

Règles d'inférence

- Exemple de règle valide:

$$\frac{< True > \quad M \quad < g > \qquad < g > \quad M' \quad < f >}{< True > \quad M|||M' \quad < f >}$$

- Exemple de règle non valide:

$$\frac{\begin{array}{ll} < g > & M \quad < f > \\ < f > & M' \quad < g > \end{array}}{M|||M' \models f \wedge g}$$

Contre Exemple:

$$M \equiv wait(y = 1); x := 1$$

$$M' \equiv wait(x = 1); y := 1$$

$$g \equiv \forall \diamond y = 1$$

$$f \equiv \forall \diamond x = 1$$

Résultats

- Théorème 1: pour tout M, M', on a $M|||M' \leq^S M$.
  Démonstration: exercice élémentaire.
- Théorème 2: pour tout M, M', M'', on a $M \leq^S M''$ implique $M|||M' \leq^S M''|||M'$.
  Démonstration: exercice élémentaire.
- Théorème 3: pour tout M, on a $M \leq^S M|||M$.
  Démonstration: exercice élémentaire.

Résultats (suite)

- Théorème 4: pour toute formule g ACTL, on peut construire une structure de Kripke τ_g telle que pour toute structure de Kripke M,

$$M \models g \text{ si et seulement si } M \leq^S \tau_g.$$

Démonstration: laissée en exercice*.

- Conséquence: $M \models g$ ssi $M \equiv^S M|||\tau_g$.
Démonstration: On a toujours $M|||\tau_g \leq^S M$. $M \leq^S \tau_g$ implique $M \leq^S M|||M \leq^S M|||\tau_g$. Réciproquement $M \equiv^S M|||\tau_g$ implique $M \leq^S M|||\tau_g \leq \tau_g$.

Résultats (suite)

- Théorème 5: si
  1. $M \leq^S M'$,
  2. $M' \models f$,
  3. f ACTL,

  alors $M \models f$.

Raisonnement par hypothèses garant

Exemple de règle: (f, g formules ACTL, M,A systèmes).

$$\frac{< true > M < A > \quad < A > M' < g > \quad < g > M < f >}{< true > M|||M' < f >}$$

Ce que cela signifie:

$$\frac{M \leq^S A \quad A|||M' \models g \quad g\ formule\ ACTL \quad \tau_g|||M \models f \quad f\ formule\ ACTL}{M|||M' \models f}$$

Démonstration de la règle

1. $M \leq^S A$ par hypothèse
2. $M||M' \leq^S A||M'$ par Théorème 2
3. $A||M' \models g$ par hypothèse
4. $A||M' \leq^s \tau_g$ par Théorème 4
5. $M||M' \leq^s \tau_g$ par 2.,4., et transitivité de $\leq^s$
6. $M||M||M' \leq^s \tau_g||M$ par Théorème 2
7. $\tau_g||M \models f$ par hypothèse
8. $M||M||M' \models f$ par 6.,7., préservation $\forall CTL$
9. $M \leq^S M||M'$ par Théorème 3
10. $M||M' \leq^S M||M||M'$ par 9., Théorème 2
11. $M||M' \models f$