Considérations de sémantique sur les (L)TS

Complément au cours sur les algèbres de processus

Pascal Poizat

http://www.lami.univ-evry.fr/˜poizat/enseignement-fr.php

Université d'Evry Val d'Essonne

Maîtrise Informatique, Génie Logiciel 2

2003 – 2004

version 0.1

Un système de transition ST est un triplet $(S, \longrightarrow)$ où

- S est un ensemble (états)
- $\longrightarrow \subseteq S \times S$ (transitions)

Une définition proche est celle des automates qui est souvent donnée sous la forme (S, S_0, T) où $S_0 \subseteq S$ (états initiaux) et où T correspond à $\longrightarrow$.

Plusieurs extensions possibles des systèmes de transitions (ST/TS)

- en associant un ensemble de propositions P au système et en valuant ces propositions dans $\{vrai, faux\}$ au niveau des états
  Structures de Kripke $SK = (S, \rightarrow)$
  (ou $(S, P, \rightarrow)$ si on explicite P)
  avec $S \subseteq 2^P$
  Servent de modèles en logiques temporelles basées états (CTL,LTL)

Plusieurs extensions possibles des systèmes de transitions (ST/TS)

- en associant des étiquettes prises dans un alphabet A aux transitions
  Systèmes de transitions étiquettées $LTS = (S, \rightarrow)$ (ou $(S, A, \rightarrow)$)
  avec $\rightarrow \subseteq S \times A \times S$
  Servent de modèles en algebres de processus (CCS,FSP,...) et logiques temporelles à actions (ACTL,..)

Plusieurs extensions possibles des systèmes de transitions (ST/TS)

- en construisant une abstraction des états et des transitions lorsqu'elles sont étiquettées : STS. Hors du cadre ici.

De nombreuses A.P. existent.

- sémantique opérationnelle (règles SOS, obtention d'un LTS)
- sémantique de bissimulation (CCS)
- sémantique de "failures-divergences" (CSP)
- et de nombreux autres outils disponibles : traces, traces finies, ... qui peuvent définir autant de (classes d')équivalences
  - ➠ treillis de ces équivalences : voir chap. 1 du HPA.

Ce cours peut donc être vu comme un complément au cours sur les algèbres de processus.

- $(Q, A, \rightarrow)$, un LTS avec
  - $\tau \in A$
  - $s \in (A - \{\tau\})^*$ séquence d'actions visibles
  - ϵ, séquence vide
- $q, q_i, \ldots$: élements de Q

- $\forall q,\ q \stackrel{\epsilon}{\Longrightarrow} q$
- $q \stackrel{s}{\Longrightarrow} q'$ ssi $s = a.s_r$, $\exists q'',\ q \stackrel{\hat{a}}{\Longrightarrow} q'' \wedge q'' \stackrel{s_r}{\Longrightarrow} q'$
- $q \stackrel{s}{\Longrightarrow}$ ssi $\exists q'$, $q \stackrel{s}{\Longrightarrow} q'$
- l'ensemble des traces de q, noté $L(q)$ est : $\{s \mid q \stackrel{s}{\Longrightarrow}\}$

intuition : ensemble des actions visibles que le système peut faire (! il existe aussi une déf. avec $q \xrightarrow{a} q'$)

préordre (de test) : $P \sqsubseteq_L Q$ ssi $L(P) \subseteq L(Q)$

```
cwb-nc :  le -S may P Q
```

équivalence : $P =_L Q$ si $L(P) = L(Q)$ ou encore $P \sqsubseteq_L Q \wedge Q \sqsubseteq_L P$

```
cwb-nc :  eq -S may P Q
```

- q refuse B, avec $B \subseteq (A - \{\tau\})$,
  ssi $|B| < \infty$ et $\forall b \in B,\ \nexists q',\ q \stackrel{b}{\Longrightarrow} q'$

intuition : ensemble fini d’actions visibles qu’un état ne peut faire / dans lequel il ne peut s’engager (! idem)

- q divergent ($q \uparrow$) si
  $\exists q_0, q_1, \ldots,\ q_0 = q \wedge \forall i \geq 0,\ q_i \xrightarrow{\tau} q_{i+1}$
- q diverge sur s ($q \uparrow s$) si $\exists s'$ (eventuellement vide), $s = s' \hat{}\, s_r$ (préfixe), et $\exists q'$ tel que $q \overset{s'}{\Longrightarrow} q'$ et $q' \uparrow$
- q converge sur s ($q \downarrow s$) si $q \uparrow s$ n'est pas vrai
- q totalement convergent ($q \downarrow$) si $\forall s,\ q \downarrow s$

intuition : état divergent s'il peut s'engager dans une séquence infinie d'actions internes, divergence sur une séquence si en cours d'exécution il y a possibilité d'entrer dans un état divergent.

s une séquence d'actions visibles et $B \subseteq A$ fini,
$< s, B >$ échec pour q si

- soit $q \uparrow s$
- soit $\exists q', \; q \stackrel{s}{\Longrightarrow} q' \wedge q'$refuse$B$

intuition : séquence d'action et ens. d'actions offertes qu'un état peut échouer à faire (soit en divergent au cours de la séquence, soit en arrivant dans un état en fin de séquence qui ne peut offrir les actions).
préordre : $P \sqsubseteq_F Q$ ssi $F(Q) \subseteq F(P)$

```
cwb-nc :  le -S must P Q
```

équivalence : $P =_F Q$ ssi $P \sqsubseteq_F Q \wedge Q \sqsubseteq_F P$

```
cwb-nc :  eq -S must P Q
```

- $\sqsubseteq_L$ et $\sqsubseteq_F$ sont des préordres (ie reflex. + trans.) sur $\mathcal{P}$
- + petit pour $\sqsubseteq_L$ = - d'exécutions possibles
- + petit pour $\sqsubseteq_F$ = + de possibilités d'échecs
  dans ce cas, échecs résultants du nondéterminisme
  ou de la divergence, le + non déterministe ou
  divergent un système est, le + d'échecs il y a

Commentaires (2)

- $\mathcal{D} = \tau.\mathcal{D}$ est le plus petit élement pour $\sqsubseteq_L$ et $\sqsubseteq_F$
- dans de nombreuses A.P., $\sqsubseteq_L$ et $\sqsubseteq_F$ sont des précongruences :
  $P \sqsubseteq Q \Rightarrow \forall C[\_],\ C[P] \sqsubseteq C[Q]$
- en CCS : vrai pour $\sqsubseteq_L$ mais pas pour $\sqsubseteq_F$ (tjs pb de τ p/r $+$)

➡ identifier la plus large précongruence $\sqsubseteq_F^C$ contenue dans $\sqsubseteq_F$ pour CCS:

$$P \sqsubseteq_F^C Q \Leftrightarrow P \sqsubseteq_F Q \wedge (P \stackrel{\tau}{\not\longrightarrow} \Rightarrow Q \stackrel{\tau}{\not\longrightarrow})$$

Prendre $A1 - A4, EXP$ plus :

$$
\begin{array}{llcl}
(F1) & a.X + a.Y & = & a.(\tau.X + \tau.Y) \\
(F2) & X + \tau.Y & \leq & \tau.(X + Y) \\
(F3) & a.X + \tau.(a.Y + Z) & = & \tau.(a.X + a.Y + Z) \\
(F4) & \tau.X & \leq & X \\
(F5) & \tau.X + \tau.Y & \leq & X
\end{array}
$$

- sert à prouver $\leq$ et pas $=$!
- $=$ raccourci pour $\leq$ dans les deux sens