Aula 11: Algebraic Laws, Congruences and Axiomatizations

Interaction & Concurrency Course Unit: Reactive Systems Module

May 17, 2023

Some Laws for Strong Bisimulation

Some laws of the choice operator

For any $P, Q, R \in Proc$:

- $P + (Q + R) \sim (P + Q) + R$ (associativity)
- $P + Q \sim Q + P$ (commutativity)
- $P + Nil \sim P$ (identity)
- $P + P \sim P$ (idempotency)

Some laws of the parallel operator:

For any $P, Q, R \in Proc$:

- $P \mid (Q \mid R) \sim (P \mid Q) \mid R$ (associativity)
- $P \mid Q \sim Q \mid P$ (commutativity)
- $P \mid Nil \sim P$ (identity)

Expansion Law

Let $P = \sum_{i=1}^{n} a_i.P_i$ and $Q = \sum_{k=1}^{n} b_k.Q_k$

Then:

$$P \mid Q \ \sim \ \sum_{i=1}^{n} a_i.(P_i \mid Q) \ + \ \sum_{k=1}^{n} b_k.(P \mid Q_k) \ + \ \sum_{i,\ k,\ b_k = \overline{a_i}} \tau.(P_i \mid Q_k)$$

Some laws of restriction:

For any $P \in Proc$,

- $Nil \backslash \{a\} \sim Nil$
- $(P \backslash \{b\}) \backslash \{a\} \sim (P \backslash \{a\}) \backslash \{b\}$ if $a \neq b$
- $(P \backslash \{a\}) \backslash \{a\} \sim P \backslash \{a\}$
- $(a.P) \backslash \{b\} \sim a.(P \backslash \{b\})$ if $a \neq b$ and $a \neq \overline{b}$
- $(P + Q) \backslash S \sim P \backslash S \ + \ Q \backslash S$

Exercício:
$A = a.A + b.B$ $\quad A[c/a]$
$B = c.d.A + a.B$

1º renomear c em B (ficamos com B')

$B' = B[e/c] = e.d.A + a.B'$
$A' = a.A' + b.B'$

já podemos fazer a substituição $A'[c/a]$

$A' = c.A' + b.B'$
$B' = e.d.A' + c.B'$

Syntactic substitution definitions

- $Nil[b/a] = Nil$
- $(a.P)[b/a] = b.(P[b/a])$
- $(\overline{a}.P)[b/a] = \overline{b}.(P[b/a])$
- $(c.P)[b/a] = c.(P[b/a])$ if $c \neq b, a$
- $(P + Q)[b/a] = P[b/a] + Q[b/a]$
- $(P \mid Q)[b/a] = P[b/a] \mid Q[b/a]$
- $(P\backslash\{c\})[b/a] = (P[b/a])\backslash\{c\}$ if $c \neq b, a$
- $(P\backslash\{a\})[b/a] = P\backslash\{a\}$
- $(P\backslash\{b\})[b/a] = P\backslash\{b\}$ if a is not a free name of P, otherwise
  $(P\backslash\{b\})[b/a] = ((P[c/b])[b/a])\backslash\{c\}$
  with c not a free name nor a bound name of P.

Additional laws of restriction:

For any $P, Q \in Proc$

- $P\backslash\{a\} \sim P$ if a is not a free name of P
- $(P\backslash\{a\}) \mid Q \sim (P \mid Q)\backslash\{a\}$ if a is not a free name of Q
- $P \mid (Q\backslash\{a\}) \sim (P \mid Q)\backslash\{a\}$ if a is not a free name of P
- $P\backslash\{a\} \sim (P[b/a])\backslash\{b\}$ if b is not a free name nor a bound name of P

Congruences

Strong Bisimulation Equivalence is a Congruence

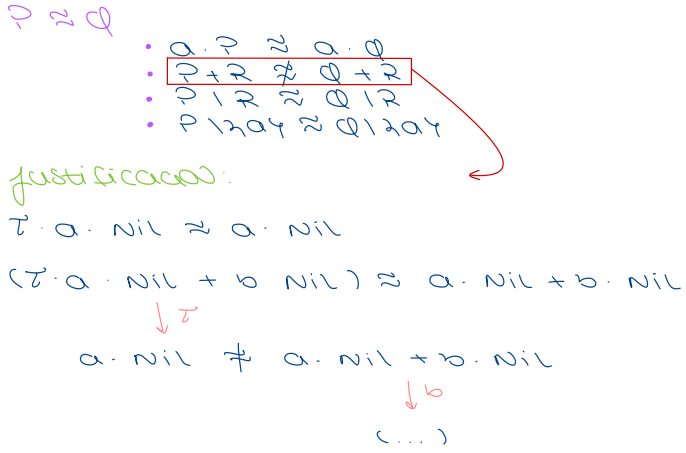
If $P \sim Q$, then:

- $a.P \sim a.Q$ for all $a \in Act$
- $P + R \sim Q + R$ for all $R \in Proc$
- $P \mid R \sim Q \mid R$ for all $R \in Proc$
- $P\backslash\{a\} \sim Q\backslash\{a\}$ for all $a \in \mathcal{A}$

Is Weak Bisimulation Equivalence a Congruence?

If $P \approx Q$, then:

- $a.P \approx a.Q$ for all $a \in Act$
- $P \mid R \approx Q \mid R$ for all $R \in Proc$
- $P\backslash\{a\} \approx Q\backslash\{a\}$ for all $a \in \mathcal{A}$
- But $P + R$ is not weakly bisimilar to $Q + R$.



Exercises suggested

1. (a) Let $A = a.A$. Prove $A \mid A \sim A$
   (b) Prove that, in general, idempotency of parallel composition does not hold for strong bisimulation : $P \mid P \nsim P$
2. Prove the following does not hold ($P, Q, R \in Proc$)
   (a) $a.(P + Q) \sim a.P + a.Q$
   (b) $(P + Q) \mid R \sim (P \mid R) + (Q \mid R)$
3. Show that we may have $P \approx Q$ but not $P + R \approx Q + R$

Axiomatization of Finite Processes

Behavioral equivalences for full CCS are undecidable. However, for the class of finite CCS processes decidability holds. It is possible to give algebraic characterization of bisimilarity, in the form of axiomatizations. Alternative proof method: instead of checking the behavioral equivalence on the associated LTS, we can reason using algebraic laws. A discussion of this topics is outside the scope of this year course. For illustrative purposes only, we briefly present a basic example.

Rules of equational deduction

1. Reflexivity:
$$\frac{}{t = t}$$
2. Symmetry:
$$\frac{t1 = t2}{t2 = t1}$$
3. Transitivity:
$$\frac{t1 = t2 \quad t2 = t3}{t1 = t3}$$
4. Substitutivity:
$$\frac{t_i = t_i'}{f(t1, \ldots, t_i, \ldots, tn) = f(t1, \ldots, t_i', \ldots, tn)}$$
   for any f and $1 \leq i \leq n$
5. Instantiation:
$$\frac{t1 = t2}{t1[\sigma] = t2[\sigma]}$$
   for any substitution σ.
6. Axioms (a sample for illustrative purposes):
   A1 $P + (Q + R) \sim (P + Q) + R$ (associativity of +)
   A2 $P + Q \sim Q + P$ (commutativity of +)
   A3 $P + Nil \sim P$ (identity of +)
   A4 $P + P \sim P$ (idempotency of +)

Example

Proof that $\{A1, A2, A3, A4\} \vdash a.Nil + (p.P + a.Nil) = a.Nil + b.P$

(1)	$x + y = y + x$	$Axiom\ A2$
(2)	$b.P + a.Nil = a.Nil + b.P$	$Instantiation\ of\ (1)$
(3)	$a.Nil + (p.P + a.Nil) = a.Nil + (a.Nil + b.P)$	$Substitutivity\ of\ (2)$
(4)	$x + (y + z) = (x + y) + z$	$Axiom\ A1$
(5)	$(a.Nil + a.Nil) + b.P = a.Nil + (a.Nil + b.P)$	$Instantiation\ of\ (4)$
(6)	$x + x = x$	$Axiom\ A4$
(7)	$a.Nil + a.Nil = a.Nil$	$Instantiation\ of\ (6)$
(8)	$(a.Nil + a.Nil) + b.P = a.Nil + b.Nil$	$Substitutivity\ of\ (7)$
(9)	$a.Nil + (p.P + a.Nil) = a.Nil + (a.Nil + b.P)$	$Transitivity\ of\ (3)\ and\ (5)$
(10)	$a.Nil + (p.P + a.Nil) = a.Nil + b.P$	$Transitivity\ of\ (8)\ and\ (9)$

Errata of Aceto et al. 2007 (only relevant corrections for this course)

pp. 26 Definition 2.3

- add a third condition on relabelling function: $f(a) \neq \tau$
- the set L of labels should be from $\mathcal{A}$ and not from $\mathcal{L}$.

pp. 91 $f : S \to S$ should be $f : 2^S \to 2^S$

pp. 148 b) ... $q \in [p']_\sim$ should be $q' \in [p']_\sim$

References

Aceto, Luca et al. (2007). *Reactive Systems - Modelling, Specification and Verification*. Cambridge University Press.

$(P + Q) \mid R \overset{?}{\sim} (P \mid R) + (Q \mid R)$

É escolhido um dos processos (choice)

são bissimilares?

Suponhamos que:

$P \overset{def}{=} a \cdot Nil$

$Q \overset{def}{=} b \cdot Nil$

$R \overset{def}{=} c \cdot Nil$

$(P + Q) \mid R$

$(a \cdot Nil + b \cdot Nil) \mid c \cdot Nil \quad (S)$

- $\xrightarrow{a}$ (S_1): $Nil \mid c \cdot Nil$
  - $\xrightarrow{c}$ (S_4): $Nil \mid Nil$
- $\xrightarrow{b}$ (S_2): $Nil \mid c \cdot Nil$
  - $\xrightarrow{c}$ (S_5): $Nil \mid Nil$
- $\xrightarrow{c}$ (S_3): $(a \cdot Nil + b \cdot Nil) \mid Nil$
  - $\xrightarrow{a}$ (S_6): $Nil \mid Nil$
  - $\xrightarrow{b}$ (S_7): $Nil \mid Nil$

$(P \mid R) + (Q \mid R)$

$(a \cdot Nil \mid c \cdot Nil) + (b \cdot Nil \mid c \cdot Nil) \quad (t)$

- $\xrightarrow{a}$ (t_1): $Nil \mid c \cdot Nil$
  - $\xrightarrow{c}$ (t_5): $Nil \mid Nil$
- $\xrightarrow{c}$ (t_2): $a \cdot Nil \mid Nil$
  - $\xrightarrow{a}$ (t_6): $Nil \mid Nil$
- $\xrightarrow{b}$ (t_3): $Nil \mid c \cdot Nil$
  - $\xrightarrow{c}$ (t_7): $Nil \mid Nil$
- $\xrightarrow{c}$ (t_4): $b \cdot Nil \mid Nil$
  - $\xrightarrow{b}$ (t_8): $Nil \mid Nil$

(s, t)

$s \xrightarrow{a} s_1$ $\quad t \xrightarrow{a} t_1$ ✓

$s \xrightarrow{b} s_2$ $\quad t \xrightarrow{b} t_3$ ✓

$s \xrightarrow{c} s_3$ $\quad t \xrightarrow{c} t_2$ or $t \xrightarrow{c} t_4$

(s_1, t_1)

$s_1 \xrightarrow{c} s_4$ $\quad t_1 \xrightarrow{c} t_5$

(s_2, t_3)

$s_2 \xrightarrow{c} s_5$ $\quad t_3 \xrightarrow{c} t_7$

(s_3, t_2)

$s_3 \xrightarrow{a} s_6$ $\quad t_2 \xrightarrow{a} t_6$

$s_3 \xrightarrow{b} s_7$ $\quad t_2 \not\xrightarrow{b}$ $\quad \therefore s \not\sim t$