Concurrency 5 = CCS (3/4)

Examples, and axiomatization

Pierre-Louis Curien (CNRS – Université Paris 7)

MPRI concurrency course 2004/2005 with :

Jean-Jacques Lévy (INRIA-Rocquencourt)
Eric Goubault (CEA)
James Leifer (INRIA - Rocq)
Catuscia Palamidessi (INRIA - Futurs)

Specification and weak bisimulation

\[
H = g \cdot H' \quad H' = p \cdot H
\]
\[
J = in \cdot S \quad S = \overline{g} \cdot U
\]
\[
U = \overline{p} \cdot F \quad F = \overline{ou} \cdot J
\]

We have : \((\nu g, h)(J \mid J \mid H) \approx K \mid K\). Their first actions are the same :

\[
(\nu g, h)(J \mid J \mid H) \mathcal{R} K \mid K \quad (\nu g, h)(S \mid J \mid H) \mathcal{R} D \mid K
\]
\[
(\nu g, h)(J \mid S \mid H) \mathcal{R} K \mid D \quad (\nu g, h)(S \mid S \mid H) \mathcal{R} D \mid D
\]

The only possible sequence of actions out of, say, \((\nu g, h)(S \mid S \mid H)\) is :

\[
(\nu g, h)(S \mid S \mid H) \xrightarrow{\tau} (\nu g, h)(S \mid U \mid H') \xrightarrow{\tau} (\nu g, h)(S \mid U \mid H') \xrightarrow{\overline{ou}} (S \mid J \mid H)
\]

Hence we complete \(\mathcal{R}\) with :

\[
(\nu g, h)(S \mid U \mid H') \mathcal{R} D \mid D \quad (\nu g, h)(S \mid F \mid H) \mathcal{R} D \mid D
\]
\[
(\nu g, h)(J \mid U \mid H') \mathcal{R} K \mid D \quad (\nu g, h)(J \mid F \mid H) \mathcal{R} K \mid D
\]
\[
(\nu g, h)(U \mid J \mid H') \mathcal{R} D \mid K \quad (\nu g, h)(F \mid J \mid H) \mathcal{R} D \mid K
\]
CCS encodings (1/4)

(Thanks to Catuscia Palamidessi for the encodings of this lecture).

Here is a specification $P$ of (up to) $n$ readers in parallel and (at most) one writer:

$$R = \overline{p_R} \cdot \text{read} \cdot \overline{v_R}$$
$$W = \overline{p_W} \cdot \text{write} \cdot \overline{v_W}$$

$$S_0 = p_R \cdot S_1 + p_W \cdot v_W \cdot S_0$$
$$S_k = p_R \cdot S_{k+1} + v_R \cdot S_{k-1} \quad (0 < k < n)$$
$$S_n = v_R \cdot S_{n-1}$$

in

$$(\nu p_R, v_R, p_W, v_W)(S_0 | R | \cdots | R | W | \cdots | W) \quad \text{(arbitrarily many readers and writers)}$$

If $P \xrightarrow{s} (\nu p_R, v_R, p_W, v_W)P'$, then there are two cases:

- $P' = S_i | Q$ : then up to $i$ threads of $Q$ can perform read and no thread can perform write.

- $P' = (v_W \cdot S_0) | Q$ : then no thread of $Q$ can perform read and at most one thread can perform write.
CCS encodings (2/4)

The dining philosophers can be encoded by a closed linking (cf. previous lecture) of \( n \) copies of the following process \( \text{Phil}_{n,p,a} \) (each philosopher holds its left fork at the beginning)

\[
\begin{align*}
\text{Phil}_{n,p,a} &= \tau \cdot \text{Phil}_{h,p,a} + \tau \cdot \text{Phil}_{n,p,a} + c_L \cdot \text{Phil}_{n,a,a} \\
\text{Phil}_{n,a,p} &= \text{symmetric} \\
\text{Phil}_{n,a,a} &= \tau \cdot \text{Phil}_{n,a,a} + \tau \cdot \text{Phil}_{h,a,a} \\
\text{Phil}_{h,a,a} &= c_L \cdot \text{Phil}_{h,p,a} + c_R \cdot \text{Phil}_{h,a,p} \\
\text{Phil}_{h,p,a} &= c_L \text{Phil}_{h,a,a} + c_R \cdot \text{Phil}_{h,a,p} \\
\text{Phil}_{h,a,p} &= \text{symmetric} \\
\text{Phil}_{h,p,p} &= \text{eat} \cdot \text{Phil}_{n,p,p} \\
\text{Phil}_{n,p,p} &= c_L \cdot \text{Phil}_{n,a,p} + c_R \cdot \text{Phil}_{n,p,a}
\end{align*}
\]

- \( n/h \) stand for “not hungry” / “hungry”, \( a/p \) for absent / present (second and third index for first and second fork, respectively)

- under the linking, \( c_R \) (resp. \( c_L \)) is (privately) identified with the \( c_L \) (resp. \( c_R \)) of the right (resp. left) neighbour
CCS encodings (3/4)

We show, at any stage: **Fairness** ⇒ **Progress**

**Fairness** A hungry philosopher, or a philosopher who has just eaten, is not ignored forever.

**Progress** If at least one philosopher is hungry, then eventually one of the hungry philosophers will eat.

By contradiction: Suppose $P$ is the state of the system in which one philosopher at least is hungry, and suppose that there is an infinite fair evolution $P \xrightarrow{\tau} \cdots$ that makes no progress. Then:

Step 1: Eventually, all philosophers hold at most one fork. No philosopher at any stage can be in state $(h, p, p)$, since by fairness eventually this philosopher will eat. If at some stage a philosopher is in state $(n, p, p)$, then by fairness this philosopher will eventually give one of his forks. No philosopher at any stage can be in state $(n, p, p)$ unless it was already in this state in $P$, since the only way to enter this state is after eating. Hence all the $(n, p, p)$ states will eventually disappear.
CCS encodings (4/4)

Step 2: Eventually, all philosophers hold exactly one fork. This is because if one philosopher had no fork, then another one would hold two ($n$ forks for $n – 1$ philosophers).

Step 3: When this happens, our philosopher is still hungry (he cannot revert to non-hungry unless he eats), say it is in state $(h, p, a)$, and eventually by Fairness it is his turn. The transition $(h, p, p)$ is forbidden. Hence he gives his fork to the left neighbour. Only a hungry philosopher receives forks, hence the neighbour is in state $(h, p, a)$, but then makes the transition $(h, p, p)$ which is also forbidden.

Exercice 1 Show that the system can never deadlock.
Strong axiomatization (1/4)

For finitary CCS (no recursion, finite guarded sums), $P \sim Q$ iff $A_1 \vdash P = Q$, where $A_1$ is:

1. $\Sigma_{i \in I} \mu_i \cdot P_i = \Sigma_{i \in I} \mu_{f(i)} \cdot P_{f(i)}$ (permutation)
2. $\Sigma_{i \in I} \mu_i \cdot P_i + \mu_j \cdot P_j = \Sigma_{i \in I} \mu_i \cdot P_i$ ($j \in I$) (idempotency)
3. $P | Q = \Sigma \{ \mu \cdot (P' \mid Q) \mid P \xrightarrow{\mu} P' \} + \Sigma \{ \mu \cdot (P \mid Q') \mid Q \xrightarrow{\mu} Q' \}
   + \Sigma \{ \tau \cdot (P' \mid Q') \mid P \xrightarrow{\alpha} P' \text{ and } Q \xrightarrow{\alpha} Q' \}$ (expansion)
4. $(\nu a) (\Sigma_{i \in I} \mu_i \cdot P_i) = \Sigma_{\{ j \in I \mid \mu_j \neq a, \alpha \}} \mu_j \cdot (\nu a)P_j$

Exercice 2 Show that $A_1 \vdash (\nu b)(a \cdot (b|c) + \tau \cdot (b|\bar{b} \cdot c)) = \tau \cdot \tau \cdot c \cdot 0 + a \cdot c \cdot 0$. 
Strong axiomatization (2/4)

First step: each process is provably equal to a synchronization tree (guarded sums only), using only

\[
(3) \quad P | Q = \sum \{ \mu \cdot (P' | Q) | P \xrightarrow{\mu} P' \} + \sum \{ \mu \cdot (P | Q') | Q \xrightarrow{\mu} Q' \} \\
+ \sum \{ \tau \cdot (P' | Q') | P \xrightarrow{\alpha} P' \text{ and } Q \xrightarrow{\overline{\alpha}} Q' \}
\]

\[
(4) \quad (\nu a) (\sum_{i \in I} \mu_i \cdot P_i) = \sum_{j \in I | \mu_j \neq a, \overline{a}} \mu_j \cdot (\nu a) P_j
\]

We associate with a process \( P \) the multi-set of the sizes of all its subterms \((\nu a) Q\) and \( Q_1 | Q_2 \). This multi-set decreases at each application of rules (3)-(4).
Strong axiomatization (3/4)

Second step: If \( P = \sum_{i=1}^{m} \alpha_i \cdot P_i \) and \( Q = \sum_{j=m+1}^{n} \alpha_j \cdot P_j \), and if \( P \sim Q \), then \( P \) and \( Q \) are provably equal, using only

\[
(1) \quad \sum_{i \in I} \mu_i \cdot P_i = \sum_{i \in I} \mu_{f(i)} \cdot P_{f(i)} \quad (f \text{ permutation})
\]

\[
(2) \quad \sum_{i \in I} \mu_i \cdot P_i + \mu_j \cdot P_j = \sum_{i \in I} \mu_i \cdot P_i \quad (j \in I)
\]

Induction on size(P)+size(Q) : Let \( \equiv \) be the equivalence relation on \( \{1, \ldots, n\} \) defined by \( i \equiv j \) iff \( \alpha_i = \alpha_j \) and \( P_i \sim P_j \).

By strong bisimilarity, each \( \equiv \) equivalence class contains at least one element of \([1, m]\) and at least one element of \([m + 1, n]\). Now for each of the equivalence classes we pick one representative in \([1, m]\) and one in \([m + 1, n]\). Call them \( p_1, \ldots, p_k \) and \( q_1, \ldots, q_k \), respectively. Then we have:

\[ \vdash \sum_{i=1}^{m} \alpha_i \cdot P = \sum_{l=1}^{k} \alpha_{p_l} \cdot P_{p_l} \quad \text{and} \quad \vdash \sum_{j=m+1}^{n} \alpha_j \cdot P_j = \sum_{l=1}^{k} \alpha_{q_l} \cdot P_{q_l} \]

with \( P_{p_l} \sim P_{q_l} \) for all \( l \), so we can apply induction.

(Note that the finiteness of sums is crucial.)
Weak axiomatization (1/6)

For finitary CCS, \( P \approx Q \) iff \( A_1 + A_2 \vdash P = Q \), where \( A_2 \) is:

\[
\begin{align*}
(\tau_0) & \quad P = \tau \cdot P \\
(\tau_1) & \quad \tau \cdot P + R = P + \tau \cdot P + R \\
(\tau_2) & \quad \alpha \cdot (\tau \cdot P + Q) + R = \alpha \cdot (\tau \cdot P + Q) + \alpha \cdot P + R
\end{align*}
\]

(In general, we do not have \( \vdash P + Q = \tau \cdot P + Q \).)
Weak axiomatization (2/6)

We can limit ourselves to synchronization trees (ST).

There is a notion of ST in fully standard form such that:

- each ST $P$ is provably equal (by $A_2$) to a ST in fully standard form
- if $P, Q$ are in fully standard form and $P \approx Q$, then $P$ and $Q$ are provably equal
Weak axiomatization (3/6)

Definition: $P = \sum_{i \in I} \mu_i \cdot P_i$ is in fully standard form if and only if

- each $P_i$ is in fully standard form and
- $\forall \mu, P' \ (P \vdash^\mu P'$ and $P' \neq P) \Rightarrow P \vdash^\mu P'$
Weak axiomatization (4/6)

Lemma: For any ST $P$, if $P \xrightarrow{\mu} P'$ and $P \neq P'$, then $\vdash P = P + \mu.P'$.

Then, given $P = \Sigma_{i \in I} \mu_i \cdot P_i$, first convert each $P_i$ to a fully standard form $P'_i$. Next, consider all $(\nu_j, P''_j)$ such that $P' = \Sigma_{i \in I} \mu_i \cdot P'_i \xrightarrow{\nu_j} P''_j$. Then

$$\vdash P = \Sigma_{i \in I} \mu_i \cdot P'_i = \Sigma_{i \in I} \mu_i \cdot P'_i + \Sigma_j \nu_j \cdot P''_j = Q'$$

and $Q'$ is in fully standard form:

- Each $P''_j$, being a subterm of some $P'_i$, is in fully standard form.
- Suppose $Q' \xrightarrow{\nu} Q''$, passing through $P''_j$:
  1. $\nu = \nu_{j_0} = \alpha$ and $P''_{j_0} \xrightarrow{\tau} Q''$. Then

$$\vdash P' \xrightarrow{\nu_{j_0}} P''_{j_0} \text{ and } P''_{j_0} \xrightarrow{\tau} Q'' \Rightarrow P' \xrightarrow{\nu} Q''$$

  2. $\nu_{j_0} = \tau$ and $P''_{j_0} \xrightarrow{\nu} P''$. Then we get also $P' \xrightarrow{\nu} Q''$.

Then by definition of $Q'$ we have $\nu = \nu_{j_1}$ and $Q'' = P''_{j_1}$ for some $j_1$. 


Weak axiomatization (5/6)

Proof of the lemma (by induction on size($P$)):

1. $P \xrightarrow{\mu} P'$. Then $P = P_1 + \mu \cdot P'$ and $\vdash P = P + \mu \cdot P'$ by idempotency.

2. $P \xrightarrow{\tau} P'' \xrightarrow{\mu} P'$ and $P' \neq P''$. Then $P = P_1 + \tau \cdot P''$, and hence $\vdash P = P + P''$ by ($\tau_1$). By induction we have $\vdash P'' = P'' + \mu \cdot P'$, so we conclude:

$$\vdash P = P + P'' = P + (P'' + \mu \cdot P') = (P + P'') + \mu \cdot P' = P + \mu \cdot P'$$

3. $\mu = \alpha$, $P \xrightarrow{\alpha} P'' \xrightarrow{\tau} P'$, and $P' \neq P''$. Then $P = P_1 + \alpha \cdot P''$, and by induction $\vdash P'' = P'' + \tau \cdot P'$. Hence, by ($\tau_2$):

$$\vdash P = P_1 + \alpha \cdot P'' = P_1 + \alpha \cdot (P'' + \tau \cdot P')$$
$$= P_1 + \alpha \cdot (P'' + \tau \cdot P') + \alpha \cdot P' = P + \alpha \cdot P'$$
Weak axiomatization (6/6)

If $P = \Sigma_{i \in I} \mu_i \cdot P_i$ and $Q = \Sigma_{j \in J} \nu_j \cdot Q_j$ are in fully standard form and $P \approx Q$, then we have “almost” $P \sim Q$.

Indeed, for every $P \overset{\mu_i}{\rightarrow} P_i$ there exists $Q'$ such that $Q' \approx P_i$ and $Q \overset{\mu_i}{\rightarrow} Q'$, and hence $Q \overset{\mu_i}{\rightarrow} Q'$, the only possible exception being when $\mu_i = \tau$ and $Q' = Q$.

We prove $\vdash P = Q$ by induction on $\text{size}(P) + \text{size}(Q)$. If the exceptional case does not apply, we proceed as for strong bisimulation and apply induction. Otherwise:

$$\exists i_0 \ (\mu_{i_0} = \tau \text{ and } P_{i_0} \approx Q \text{ and } \neg \exists j \ (\mu_j = \tau \text{ and } Q_j \approx P_{i_0}))$$

Now, we have:

$$(Q \approx \Sigma_{i \in I} \mu_i \cdot P_i \text{ and } \neg \exists j \ (\mu_j = \tau \text{ and } Q_j \approx P_{i_0})) \Rightarrow Q \approx \Sigma_{i \in I \setminus \{i_0\}} \mu_i \cdot P_i$$

Hence by induction $\vdash P_{i_0} = Q$ and $\vdash Q = \Sigma_{i \in I \setminus \{i_0\}} \mu_i \cdot P_i$, and we conclude with $(\tau_1)$ and $\boxed{\text{(}\tau_0\text{)}}$:

$$\vdash Q = \tau \cdot Q = Q + \tau.Q = \Sigma_{i \in I \setminus \{i_0\}} \mu_i \cdot P_i + \tau.P_{i_0} = P$$