1 Review: Structural Congruence

Definition of Structural Congruence [$\equiv$]:

1. α-conversion
2. Re-order sums
3. $P|0 \equiv P$, $P|Q \equiv Q|P$, $P|(Q|R) \equiv (P|Q)|R$
4. $\mathsf{new}\ a\ (P|Q) \equiv (\mathsf{new}\ a\ Q)|P$ if $a \notin \mathsf{fv}(P)$, $\mathsf{new}\ a\ 0 \equiv 0$, $\mathsf{new}\ a, b\ P \equiv \mathsf{new}\ b, a\ P$
5. $A\langle\vec{b}\rangle \equiv \{\vec{b}/\vec{a}\}P_A$ where $A(\vec{a}) = P_A$

2 CCS

2.1 Definitions

$$
\begin{array}{rll}
\mathcal{L} ::= \mathcal{N} \cup \overline{\mathcal{N}} & \lambda, \mu, \ldots & \text{Labels} \\
\mathsf{Act} ::= \mathcal{L} \cup \{\tau\} & \alpha, \beta, \ldots & \text{Actions} \\
P ::= A\langle a_1, \ldots, a_n\rangle \;\Big|\; \sum_{i \in I} \alpha_i.P_i \;\Big|\; P_1|P_2 \;\Big|\; \mathsf{new}\ a\ P & P, Q, \ldots & \text{Processes}
\end{array}
$$

2.2 Operational Semantics Rules

$$
\frac{}{(a.P + M)|(\overline{a}.Q + N) \to P|Q}\ \text{React} \qquad \frac{P \to P'}{P|Q \to P'|Q}\ \text{Par} \qquad \frac{P \to P'}{\mathsf{new}\ a\ P \to \mathsf{new}\ a\ P'}\ \text{Res}
$$

$$
\frac{}{\tau.P + M \to P}\ \text{Tau} \qquad \frac{Q \equiv P \quad P \to P' \quad P' \equiv Q'}{Q \to Q'}\ \text{Struct}
$$

2.3 Example: Lottery

Suppose we wish to model a lottery. There is a set of N balls with outcomes written on them, and we want to non-deterministically choose a ball, output its outcome, and reset to the initial state. We can use the following definitions:

$$
\begin{aligned}
\text{Lottery} &= \tau.b_1.\text{Lottery} + \ldots + \tau.b_n.\text{Lottery} \\
\text{Main} &= (\text{Lottery}|\overline{b_1}.P_1| \ldots |\overline{b_n}.P_n)
\end{aligned}
$$

This definition simulates a one-ball lottery. The process Lottery picks a ball i and sends the corresponding action b_i, which reacts with the corresponding parallel observer process $\overline{b_i}.P_i$, triggering the appropriate reward process P_i. We could also extend this to a multi-ball lottery by adding more actions to the observer processes: $\overline{b_i}.\overline{b_j}.\overline{b_k}.P_{ijk}$. However, we must take care to avoid having a b_i possibly interact with the wrong $\overline{b_i}$ in a process; i.e., if the second ball drawn is b_i, we don't want that action to react with a process that has $\overline{b_i}$ as its first action.

We can also use the following alternative definitions:

$$
\begin{aligned}
A(a,b,c) &= \overline{a}.C\langle a,b,c\rangle \\
B(a,b,c) &= \overline{b}.C\langle a,b,c\rangle \\
C(a,b,c) &= \tau.B\langle a,b,c\rangle + c.A\langle a,b,c\rangle \\
A_i &= A\langle a_i, b_i, a_{i+1}\rangle && \text{for } i \in \{1,2,3\}, \text{ with } 3+1=1 \\
B_i &= B\langle a_i, b_i, a_{i+1}\rangle \\
C_i &= C\langle a_i, b_i, a_{i+1}\rangle \\
L_1 &= \mathsf{new}\ a_1,a_2,a_3\ (C_1|A_2|A_3) \\
L_2 &= \mathsf{new}\ a_1,a_2,a_3\ (A_1|C_2|A_3) \\
L_3 &= \mathsf{new}\ a_1,a_2,a_3\ (A_1|A_2|C_3)
\end{aligned}
$$

To see how this works, we start by expanding the definition of L_1:

$$L_1 = \mathsf{new}\ a_1,a_2,a_3\ (C_1|A_2|A_3) \equiv \mathsf{new}\ a_1,a_2,a_3\ (\tau.B\langle a_1,b_1,a_2\rangle + a_2.A\langle a_1,b_1,a_2\rangle|A_2|A_3)$$

Thus from L_1, we can take one of two actions: either τ, or a_2. In the latter case, we get (after a_2 reacts with $\overline{a_2}$ in A_2):

$$\mathsf{new}\ a_1,a_2,a_3\ (A\langle a_1,b_1,a_2\rangle|C\langle a_2,b_2,a_3\rangle|A_3) \equiv L_2$$

In the former case, we get:

$$\mathsf{new}\ a_1,a_2,a_3\ (b_1.C\langle a_1,b_1,a_2\rangle|A_2|A_3) \equiv \mathsf{new}\ a_1,a_2,a_3\ (b_1.C_1|A_2|A_3)$$

Once the b_1 reacts with an external observer process, we are left with L_1. Thus at each of the L_i, we can either draw a ball b_i or transition to L_{i+1}.

3 CCS as an LTS

3.1 Operational Semantics Rules

$$\frac{}{M + \alpha.P + N \xrightarrow{\alpha} P}\ \text{L-Sum} \qquad \frac{P \xrightarrow{\lambda} P' \quad Q \xrightarrow{\overline{\lambda}} Q'}{P|Q \xrightarrow{\tau} P'|Q'}\ \text{L-React} \qquad \frac{P \xrightarrow{\alpha} P' \quad \alpha \notin \{a, \overline{a}\}}{\mathsf{new}\ a\ P \xrightarrow{\alpha} \mathsf{new}\ a\ P'}\ \text{L-Res}$$

$$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}\ \text{L-Par L} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P|Q'}\ \text{L-Par R} \qquad \frac{\{\vec{b}/\vec{a}\}P_A \xrightarrow{\alpha} P' \quad A(\vec{a}) = P_A}{A\langle\vec{b}\rangle \xrightarrow{\alpha} P'}\ \text{L-Ident}$$

There are two important things to notice. The first is that we no longer make use of structural congruence; consequently, we now require separate rules for left- and right-parallel composition, and we need summands on both sides for the L-Sum rule. The second thing to notice is that in the L-React rule, since λ is internal to the process, we label the transition with τ so that λ is hidden from any external processes. Also, we still have α-equivalence for $\mathsf{new}\ a\ P$ expressions: $\mathsf{new}\ a\ P = \mathsf{new}\ b\ P\{b/a\}$ for any other label b.

3.2 Theorems

First, we want to show that even though we no longer have a structural congruence rule, structural congruence in fact still holds. We therefore have the following theorem:

Theorem 1. *If* $P \xrightarrow{\alpha} P'$ *and* $P \equiv Q$*, then* $\exists Q'$ *such that* $Q \xrightarrow{\alpha} Q'$ *and* $Q' \equiv P'$*.*

Proof. Here is a partial proof, containing only a few subcases. Proof by induction on $P \xrightarrow{\alpha} P'$. Case L-Par L: $P = P_1|P_2$, $P_1 \xrightarrow{\alpha} P_1'$, $P' = P_1'|P_2$. Consider $P \equiv Q$. We now look at all of the ways Q could be structurally congruent to P:

Subcase $Q = P_2|P_1$. Then let $Q' = P_2|P_1'$. By L-Par R, $Q \xrightarrow{\alpha} Q'$. ✓

Subcase $Q = Q_1|P_2$, $Q_1 \equiv P_1$. By the induction hypothesis, $\exists Q_1'$ such that $Q_1 \xrightarrow{\alpha} Q_1'$, $Q_1' \equiv P_1$. By L-Par L, $Q \xrightarrow{\alpha} Q_1'|P_2 \equiv P'$. Then let $Q' = Q_1'|P_2$. ✓ □

We would also like to show that the transitions in this system correspond to those in the original CCS:

Theorem 2. $P \rightarrow P'$ *iff* $P \xrightarrow{\tau}\equiv P'$ *(where* $\xrightarrow{\tau}\equiv$ *indicates relational composition of* $\xrightarrow{\tau}$ *and* $\equiv$*).*