Principles for Software Composition

Roberto Bruni

http://www.di.unipi.it/~bruni/

PSC 2023/24 (375AA, 9CFU)

18b - CCS strong bisimulation
CCS syntax

\[ p, q ::= \begin{array}{ll}
\text{nil} & \text{inactive process} \\
\text{x} & \text{process variable (for recursion)} \\
\mu.p & \text{action prefix} \\
p\backslash\alpha & \text{restricted channel} \\
p[\phi] & \text{channel relabelling} \\
p + q & \text{nondeterministic choice (sum)} \\
p|q & \text{parallel composition} \\
\text{rec } x. \; p & \text{recursion}
\end{array} \]

(operators are listed in order of precedence)
CCS op. semantics

Act) \[ \mu . p \xrightarrow{\mu} p \]

Res) \[ p \xrightarrow{\mu} q \quad \mu \not\in \{ \alpha, \overline{\alpha} \} \]
\[ p \setminus \alpha \xrightarrow{\mu} q \setminus \alpha \]

Rel) \[ p \xrightarrow{\mu} q \]
\[ p[\phi] \xrightarrow{\phi(\mu)} q[\phi] \]

SumL) \[ p_1 \xrightarrow{\mu} q \]
\[ p_1 + p_2 \xrightarrow{\mu} q \]

SumR) \[ p_2 \xrightarrow{\mu} q \]
\[ p_1 + p_2 \xrightarrow{\mu} q \]

ParL) \[ p_1 \xrightarrow{\mu} q_1 \]
\[ p_1 | p_2 \xrightarrow{\mu} q_1 | p_2 \]

Com) \[ p_1 \xrightarrow{\lambda} q_1 \]
\[ p_2 \xrightarrow{\overline{\lambda}} q_2 \]
\[ p_1 | p_2 \xrightarrow{\tau} q_1 | q_2 \]

ParR) \[ p_2 \xrightarrow{\mu} q_2 \]
\[ p_1 | p_2 \xrightarrow{\mu} p_1 | q_2 \]

Rec) \[ p[\mathrm{rec} \ x. \ p/x] \xrightarrow{\mu} q \]
\[ \mathrm{rec} \ x. \ p \xrightarrow{\mu} q \]
Bisimulation game
From your forms

(over 8 answers)
Bisimulation game

two processes \( p, q \) and two opposing players

Alice, the attacker, aims to prove \( p \) and \( q \) are not equivalent

Bob, the defender, aims to prove \( p \) and \( q \) are equivalent

the game is turn based, at each turn:

Alice chooses one process and one of its outgoing transitions

Bob must reply with a transition of the other process, matching the label of the transition chosen by Alice

at the next turn, if any, the players will consider the equivalence of the target processes of the chosen transitions
Bisimulation game

Alice wins if, at some stage, she can make a move that Bob cannot match.

Bob wins in all other cases:
- if Alice cannot find a move
- if the game does not terminate

Alice has a winning strategy if she can make a move that Bob cannot match; or if she can make a move that no matter what Bob replies, at the next turn she wins; or so the like after any (finite) number of moves ...

Alice has a winning strategy if she can disprove the equivalence of $p$ and $q$ in a finite number of moves.
Bisimulation game

Alice plays

Bob can only reply

Alice plays

Bob cannot reply

Alice wins!
CCS
Strong bisimulation
Strong bisimulation

the notion of bisimulation is not restricted to CCS processes it applies to any LTS

in the following we recall Milner’s original definition of strong bisimulation relation

to keep in mind

there are many strong bisimulation relations

we are interested in the largest such relation, called strong bisimilarity

to prove that two processes are strong bisimilar it is enough to show they are related by a strong bisimulation
Strong bisimulation

\( \mathcal{P} \) set of processes

\( R \subseteq \mathcal{P} \times \mathcal{P} \) a binary relation

we write \( p R q \) when \( (p, q) \in R \)

\( R \) is a strong bisimulation if

\[
\forall p, q. \ (p, q) \in R \Rightarrow
\begin{cases}
\forall \mu, p'. \ p \xrightarrow{\mu} p' & \Rightarrow \exists q'. \ q \xrightarrow{\mu} q' \land p' R q' \\
\forall \mu, q'. \ q \xrightarrow{\mu} q' & \Rightarrow \exists p'. \ p \xrightarrow{\mu} p' \land p' R q'
\end{cases}
\]

intuitively: if two processes are related, then for any move of Alice, Bob can find a move that leads to related processes i.e., Bob has a winning strategy
Example

\[ \emptyset \text{ is a strong bisimulation} \]

\[ \text{Id} \triangleq \{(p, p) \mid p \in \mathcal{P}\} \text{ is a strong bisimulation} \]

any graph isomorphism defines a strong bisimulation

\[ \mathcal{R}_f \triangleq \{(p, f(p))\} \]
Example

\[ \text{rec } x. \alpha.x \rightarrow \text{rec } x. \alpha.\alpha.x \]

\[ \text{rec } x. \alpha.x \rightarrow \alpha.\text{rec } x. \alpha.\alpha.x \]

\[ R \triangleq \left\{ (\text{rec } x. \alpha.x, \text{rec } x. \alpha.\alpha.x), (\text{rec } x. \alpha.x, \alpha.\text{rec } x. \alpha.\alpha.x) \right\} \]

Unlike graph isomorphisms, the same process can be related to many processes.
Example

\[
\begin{align*}
B_0^2 & \quad \text{out} \quad \text{in} \quad B_0^1 | B_0^1 \\
B_1^2 & \quad \text{out} \quad \text{in} \quad B_1^1 | B_0^1 \\
B_2^2 & \quad \text{out} \quad \text{in} \quad B_2^1 | B_1^1
\end{align*}
\]

\[
\mathbf{R} \triangleq \left\{ (B_0^2, B_0^1 | B_0^1), (B_1^2, B_1^1 | B_0^1), (B_0^2, B_1^1 | B_0^1), (B_1^2, B_1^1 | B_1^1) \right\}
\]
Union

Lemma  If $R_1$ and $R_2$ are strong bisimulations, then $R_1 \cup R_2$ is a strong bisimulation.

proof.  take $(p, q) \in R_1 \cup R_2$

take $p \xrightarrow{\mu} p'$ we want to find $q \xrightarrow{\mu} q'$ with $(p', q') \in R_1 \cup R_2$

since $(p, q) \in R_1 \cup R_2$ we have $p R_i q$ for some $i \in \{1, 2\}$

since $R_i$ is a strong bisimulation and $p \xrightarrow{\mu} p'$

we have $q \xrightarrow{\mu} q'$ with $p' R_i q'$ and hence $(p', q') \in R_1 \cup R_2$

take $q \xrightarrow{\mu} q'$ we want to find $p \xrightarrow{\mu} p'$ with $(p', q') \in R_1 \cup R_2$

analogous to the previous case
Inverse

**Lemma** If $R$ is a strong bisimulation, then $R^{-1} \triangleq \{(q, p) \mid p \mathrel{R} q\}$ is a strong bisimulation.

**proof.** Take $(q, p) \in R^{-1}$.

Take $q \xrightarrow{\mu} q'$ we want to find $p \xrightarrow{\mu} p'$ with $(q', p') \in R^{-1}$.

Since $(q, p) \in R^{-1}$ we have $p \mathrel{R} q$.

Since $R$ is a strong bisimulation and $q \xrightarrow{\mu} q'$

we have $p \xrightarrow{\mu} p'$ with $p' \mathrel{R} q'$ and hence $(q', p') \in R^{-1}$.

Take $p \xrightarrow{\mu} p'$ we want to find $q \xrightarrow{\mu} q'$ with $(q', p') \in R^{-1}$.

analogous to the previous case.

16
Composition

**Lemma** If \( R_1 \) and \( R_2 \) are strong bisimulations, then \( R_2 \circ R_1 \triangleq \{(p, q) \mid \exists r. p \ R_1 r \land r \ R_2 q\} \) is a strong bisimulation.

**proof.** take \( (p, q) \in R_2 \circ R_1 \)

take \( p \xrightarrow{\mu} p' \) we want to find \( q \xrightarrow{\mu} q' \) with \( (p', q') \in R_2 \circ R_1 \)

since \( (p, q) \in R_2 \circ R_1 \) we have \( p \ R_1 r \land r \ R_2 q \) for some \( r \)

since \( R_1 \) is a strong bisimulation and \( p \xrightarrow{\mu} p' \)

we have \( r \xrightarrow{\mu} r' \) with \( p' \ R_1 r' \)

since \( R_2 \) is a strong bisimulation and \( r \xrightarrow{\mu} r' \)

we have \( q \xrightarrow{\mu} q' \) with \( r' \ R_2 q' \) and hence \( (p', q') \in R_2 \circ R_1 \)

take \( q \xrightarrow{\mu} q' \) we want to find \( p \xrightarrow{\mu} p' \) with \( (p', q') \in R_2 \circ R_1 \)

analogous to the previous case.
Notation

\[ R_2 \circ R_1 \triangleq \{(p, q) \mid \exists r. \ p \ R_1 \ r \land r \ R_2 \ q\} \]

sometimes written

\[ R_1 R_2 \]
CCS
Strong bisimilarity
Strong bisimilarity

often denoted $\sim$ in the literature
we use $\sim$ to remark it is a congruence relation

$p \sim q \iff \exists R$ a strong bisimulation with $(p, q) \in R$

i.e. Bob has a winning strategy

i.e. $\sim \triangleq \bigcup_{R \text{ s.b.}} R$

a strong bisimulation is not necessarily an equivalence
is strong bisimilarity an equivalence relation?
# Equivalence relation

$\equiv$

<table>
<thead>
<tr>
<th>Property</th>
<th>Condition</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflexive</td>
<td>$\forall p \in P$</td>
<td>$p \equiv p$</td>
</tr>
<tr>
<td>Symmetric</td>
<td>$\forall p, q \in P$</td>
<td>$p \equiv q \Rightarrow q \equiv p$</td>
</tr>
<tr>
<td>Transitive</td>
<td>$\forall p, q, r \in P$</td>
<td>$p \equiv q \land q \equiv r \Rightarrow p \equiv r$</td>
</tr>
</tbody>
</table>
Induced equivalence

Any relation $R$ induces an equivalence relation $\equiv_R$

$\equiv_R$ is the smallest equivalence that contains $R$

<table>
<thead>
<tr>
<th>$p$ $R$ $q$</th>
<th>$p$ $\equiv_R$ $q$</th>
<th>$p$ $\equiv_R$ $p$</th>
<th>$q$ $\equiv_R$ $p$</th>
<th>$p$ $\equiv_R$ $q$</th>
<th>$q$ $\equiv_R$ $r$</th>
<th>$p$ $\equiv_R$ $r$</th>
</tr>
</thead>
</table>

**Lemma** if $R$ is a strong bisimulation,
then $\equiv_R$ is a strong bisimulation
Induced partition

Any equivalence relation induces a partition of processes into equivalence classes

\[[p]_\equiv = \{ q \mid p \equiv q \}\]

if $\equiv_R$ is a strong bisimulation

\[q \in [p]_\equiv \land p \xrightarrow{\mu} p' \Rightarrow \exists q' \in [p']_\equiv . q \xrightarrow{\mu} q'\]

instead of listing all pairs of $\equiv_R$
we list only its equivalence classes
Example

\[ R \triangleq \left\{ (B_0^2, B_0^1 | B_0^1), (B_1^2, B_1^1 | B_1^1), (B_2^2, B_1^1 | B_1^1) \right\} \]

\[ \equiv R \triangleq \left\{ (B_0^2, B_0^2), (B_0^2, B_0^1 | B_0^1), (B_1^1 | B_0^1, B_0^1), (B_1^1 | B_1^1, B_1^1 | B_1^1), (B_0^1 | B_0^1, B_0^1 | B_0^1), (B_1^1 | B_1^1, B_1^1 | B_1^1), \ldots \right\} \]
Example

\[ R \triangleq \left\{ (B_0^2, B_0^1 | B_0^1), (B_1^2, B_1^1 | B_0^1), (B_2^2, B_1^1 | B_1^1) \right\} \]

\[ \equiv R \triangleq \left\{ \{B_0^2, B_0^1 | B_0^1\}, \{B_1^2, B_0^1 | B_1^1, B_1^1 | B_0^1\}, \{B_2^2, B_1^1 | B_1^1\} \right\} \]
Bisimulation check
Example

\[
\equiv_R \triangleq \left\{ \{ B^2_0, B^1_0 | B^1_0 \}, \{ B^2_0, B^1_0 | B^1_0, B^1_0 | B^1_0 \}, \{ B^2_1, B^1_1 | B^1_1, B^1_1 | B^1_0 \}, \{ B^2_2, B^1_1 | B^1_1 \} \right\}
\]
**TH.** Strong bisimilarity is an equivalence relation

**proof.**

**reflexive** \( Id \subseteq \sim \)

**symmetric** assume \( p \sim q \) we want to prove \( q \sim p \)

\( p \sim q \) means there is a s.b. \( R \) with \( (p, q) \in R \)

then \( (q, p) \in R^{-1} \) and \( R^{-1} \) is a s.b.

thus \( (q, p) \in R^{-1} \subseteq \sim \) i.e. \( q \sim p \)

**transitive** assume \( p \sim q \quad q \sim r \) we want to prove \( p \sim r \)

\( p \sim q \) means there is a s.b. \( R_1 \) with \( (p, q) \in R_1 \)

\( q \sim r \) means there is a s.b. \( R_2 \) with \( (q, r) \in R_2 \)

then \( (p, r) \in R_2 \circ R_1 \) and \( R_2 \circ R_1 \) is a s.b.

thus \( (p, r) \in R_2 \circ R_1 \subseteq \sim \) i.e. \( p \sim r \)

28
**TH.** Strong bisimilarity is a strong bisimulation

*proof.*

take $p \simeq q$

take $p \xrightarrow{\mu} p'$ we want to find $q \xrightarrow{\mu} q'$ with $p' \simeq q'$

$p \simeq q$ means there is a s.b. $R$ with $(p, q) \in R$

since $R$ is a strong bisimulation and $p \xrightarrow{\mu} p'$

we have $q \xrightarrow{\mu} q'$ with $(p', q') \in R$

since $R \subseteq \simeq$ we have $p' \simeq q'$

take $q \xrightarrow{\mu} q'$ we want to find $p \xrightarrow{\mu} p'$ with $p' \simeq q'$

follows from previous case (strong bisimilarity is symmetric)
Cor. Strong bisimilarity is the **largest** strong bisimulation

**proof.**

strong bisimilarity is a strong bisimulation (previous TH.)

by definition

\[ \sim \triangleq \bigcup_{\mathcal{R}, \text{s.b.}} \mathcal{R} \]

any other strong bisimulation is included in \( \sim \)
**TH.** Recursive definition of strong bisimilarity

\[ \forall p, q. p \simeq q \iff \begin{cases} \forall \mu, p'. p \xrightarrow{\mu} p' \implies \exists q'. q \xrightarrow{\mu} q' \land p' \simeq q' \\ \land \\ \forall \mu, q'. q \xrightarrow{\mu} q' \implies \exists p'. p \xrightarrow{\mu} p' \land p' \simeq q' \end{cases} \]

**proof.**

\( \implies \) follows immediately because \( \simeq \) is a strong bisimulation

\[ \forall \mu, p'. p \xrightarrow{\mu} p' \implies \exists q'. q \xrightarrow{\mu} q' \land p' \simeq q' \]

\( \iff \) take \( p, q \) s.t.

\[ \begin{cases} \forall \mu, p'. p \xrightarrow{\mu} p' \implies \exists q'. q \xrightarrow{\mu} q' \land p' \simeq q' \\ \land \\ \forall \mu, q'. q \xrightarrow{\mu} q' \implies \exists p'. p \xrightarrow{\mu} p' \land p' \simeq q' \end{cases} \]

we want to prove \( p \simeq q \)

this is done by proving that \( R \triangleq \{(p, q)\} \cup \simeq \) is a s.b.

(see next slide)
\( \mathcal{R} \triangleq \{(p, q)\} \cup \simeq \) is a s.b.

Take \((r, s) \in \mathcal{R}\)

Take \(r \xrightarrow{\mu} r'\) we want to find \(s \xrightarrow{\mu} s'\) with \((r', s') \in \mathcal{R}\)

If \(r \simeq s\) then we can find \(s \xrightarrow{\mu} s'\) with \((r', s') \in \simeq \subseteq \mathcal{R}\)

Because \(\simeq\) is a strong bisimulation

If \((r, s) = (p, q)\) then \(p \xrightarrow{\mu} r'\) and

\[
\begin{align*}
\forall \mu, p'. p \xrightarrow{\mu} p' & \Rightarrow \exists q'. q \xrightarrow{\mu} q' \land p' \simeq q' \\
\forall \mu, q'. q \xrightarrow{\mu} q' & \Rightarrow \exists p'. p \xrightarrow{\mu} p' \land p' \simeq q'
\end{align*}
\]

Thus we can find \(q \xrightarrow{\mu} s'\) with \((r', s') \in \simeq \subseteq \mathcal{R}\)

Take \(s \xrightarrow{\mu} s'\) we want to find \(r \xrightarrow{\mu} r'\) with \((r', s') \in \mathcal{R}\)

Analogous to the previous case
CCS
Compositionality
Compositionality

recall that an equivalence \( \equiv \) is a congruence when

\[
\forall C[\cdot]. \ \forall p, q. \ p \equiv q \ \Rightarrow \ C[p] \equiv C[q]
\]

we can replace equivalent processes in any context without changing the abstract semantics
TH. Strong bisimilarity is a congruence

1. $\forall p, q. \ p \simeq q \Rightarrow \forall \mu. \ \mu.p \simeq \mu.q$
2. $\forall p, q. \ p \simeq q \Rightarrow \forall \alpha. \ p \setminus \alpha \simeq q \setminus \alpha$
3. $\forall p, q. \ p \simeq q \Rightarrow \forall \phi. \ p[\phi] \simeq q[\phi]$
4. $\forall p_0, q_0, p_1, q_1. \ p_0 \simeq q_0 \land p_1 \simeq q_1 \Rightarrow p_0 + p_1 \simeq q_0 + q_1$
5. $\forall p_0, q_0, p_1, q_1. \ p_0 \simeq q_0 \land p_1 \simeq q_1 \Rightarrow p_0 | p_1 \simeq q_0 | q_1$

let us omit quantification to make the statement more readable
TH. Strong bisimilarity is a congruence

1. \( p \simeq q \implies \mu.p \simeq \mu.q \)

2. \( p \simeq q \implies p\{\alpha\} \simeq q\{\alpha\} \)

3. \( p \simeq q \implies p[\phi] \simeq q[\phi] \)

4. \( p_0 \simeq q_0 \land p_1 \simeq q_1 \implies p_0 + p_1 \simeq q_0 + q_1 \)

5. \( p_0 \simeq q_0 \land p_1 \simeq q_1 \implies p_0|p_1 \simeq q_0|q_1 \)

proof technique:
“guess” a relation large enough to contain all pairs of interest; show that it is a bisimulation relation; then it is contained in the strong bisimilarity relation
**TH.** Strong bisimilarity is a congruence (3)

take $\mathcal{R} \triangleq \{ (p[\phi], q[\phi]) \mid p \simeq q \}$

we show that $\mathcal{R}$ is a strong bisimulation relation

take $(p[\phi], q[\phi]) \in \mathcal{R}$ (i.e. with $p \simeq q$)

take $p[\phi] \xrightarrow{\mu} p'$ we want to find $q[\phi] \xrightarrow{\mu} q'$ with $(p', q') \in \mathcal{R}$

by rule rel) it must be $p \xrightarrow{\mu'} p''$ $\mu = \phi(\mu')$ $p' = p''[\phi]$ 

since $p \simeq q$ then $q \xrightarrow{\mu'} q''$ with $p'' \simeq q''$

by rule rel) $q[\phi] \xrightarrow{\phi(\mu')} q''[\phi]$

take $q' = q''[\phi]$ so that $(p', q') = (p''[\phi], q''[\phi]) \in \mathcal{R}$

take $q[\phi] \xrightarrow{\mu} q'$ we want to find $p[\phi] \xrightarrow{\mu} p'$ with $(p', q') \in \mathcal{R}$

analogous to the previous case
TH. Strong bisimilarity is a congruence (4)

Take $R \triangleq \{(p_0 + p_1, q_0 + q_1) \mid p_0 \sim q_0 \land p_1 \sim q_1\}$

we show that $R$ is a strong bisimulation relation

take $(p_0 + p_1, q_0 + q_1) \in R$ (i.e. with $p_0 \sim q_0 \land p_1 \sim q_1$)

take $p_0 + p_1 \xrightarrow{\mu} p'$ we need $q_0 + q_1 \xrightarrow{\mu} q'$ with $(p', q') \in R$

if rule suml) was used: $p_0 \xrightarrow{\mu} p'$

since $p_0 \sim q_0$ then $q_0 \xrightarrow{\mu} q'$ with $p' \sim q'$

by rule suml) $q_0 + q_1 \xrightarrow{\mu} q'$

but unfortunately $(p', q') \in \sim$ not necessarily $(p', q') \in R$

how can we repair the proof?
**TH.** Strong bisimilarity is a congruence (4)

Take $R \triangleq \{(p_0 + p_1, q_0 + q_1) \mid p_0 \simeq q_0 \land p_1 \simeq q_1\} \cup \simeq$

we show that $R$ is a strong bisimulation relation

Take $(p_0 + p_1, q_0 + q_1) \in R$ (i.e. with $p_0 \simeq q_0 \quad p_1 \simeq q_1$)

Take $p_0 + p_1 \xrightarrow{\mu} p'$ we need $q_0 + q_1 \xrightarrow{\mu} q'$ with $(p', q') \in R$

if rule suml) was used: $p_0 \xrightarrow{\mu} p'$

since $p_0 \simeq q_0$ then $q_0 \xrightarrow{\mu} q'$ with $p' \simeq q'$

by rule suml) $q_0 + q_1 \xrightarrow{\mu} q'$

then $(p', q') \in \simeq \subseteq R$

how can we repair the proof?

(no need to check the pairs in $\simeq$)

- fill in the missing details
- sumr)
- $q_0 + q_1$ moves
CCS: some laws

\[ p + \text{nil} \simeq p \]
\[ p + q \simeq q + p \]
\[ p + (q + r) \simeq (p + q) + r \]
\[ p + p \simeq p \]

\[ p|\text{nil} \simeq p \]
\[ p|q \simeq q|p \]
\[ p|(q|r) \simeq (p|q)|r \]

how to prove them? find a strong bisimulation for each of them

\[ \text{nil} \setminus \alpha \simeq \text{nil} \]
\[ (\mu.p) \setminus \alpha \simeq \text{nil} \quad \text{if } \mu \in \{\alpha, \overline{\alpha}\} \]
\[ (\mu.p) \setminus \alpha \simeq \mu.(p \setminus \alpha) \quad \text{if } \mu \notin \{\alpha, \overline{\alpha}\} \]
\[ (p + q) \setminus \alpha \simeq (p \setminus \alpha) + (q \setminus \alpha) \]
\[ p \setminus \alpha \alpha \simeq p \setminus \alpha \]
\[ p \setminus \alpha \beta \simeq p \setminus \beta \alpha \]

\[ \text{nil}[\phi] \simeq \text{nil} \]
\[ (\mu.p)[\phi] \simeq \phi(\mu).(p[\phi]) \]
\[ (p + q)[\phi] \simeq (p[\phi]) + (q[\phi]) \]
\[ p[\phi][\eta] \simeq p[\eta \circ \phi] \]