Rooted Divergence-Preserving Branching Bisimilarity is a Congruence for Weakly Guarded CCS

Quán Sūn[NUAA] David N. Jansen[ISCAS] Xīnxīn Liǔ[ISCAS, SWU] Wēi Zhāng[SWU]

Nanjing University of Aeronautics and Astronautics, China
Institute of Software, Chinese Academy of Sciences, Beijing, China
Southwest University, Chongqing, China

Dies diem docet

CCS

calculus of communicating systems

- Process algebra to describe behaviour of a computer system
(behaviour := what actions can the system do? in which order?
what choices can it make?
what communication/synchronisation is possible?)

- Action names $\mathcal{A} = \{a, b, c, ...\}$ and co-names $\bar{\mathcal{A}} = \{\bar{a}, \bar{b}, \bar{c}, ...\}$.

  Labels $\mathcal{L} := \mathcal{A} \cup \bar{\mathcal{A}}$. $\ell \in \mathcal{L}$.

  Actions $Act = \mathcal{L} \cup \{\tau\}$. ($\tau$ is the internal or invisible action.) $\alpha, \beta, ... \in Act$.

- Variables $\mathcal{V} = \{X, Y, ...\}$.

CCS Processes

- Inaction: $\mathbf{0} \not\rightarrow$
- Action Prefix: $\alpha.E \xrightarrow{\alpha} E$
- Choice: $E + F$
  If $E \xrightarrow{\alpha} E'$, then $E + F \xrightarrow{\alpha} E'$
  If $F \xrightarrow{\alpha} F'$, then $E + F \xrightarrow{\alpha} F'$
- Variable: X
  Recursion: $\mu X.E$
  If $E[\mu X.E/X] \xrightarrow{\alpha} E'$,
  then $\mu X.E \xrightarrow{\alpha} E'$

Normally we will assume that recursions are (weakly) guarded, i.e. every occurrence of X in E is within some expression of the form $\alpha.F$.

CCS Processes

- Inaction: $\mathbf{0} \not\rightarrow$

- Action Prefix: $\alpha.E \xrightarrow{\alpha} E$

- Choice: $E + F$
  If $E \xrightarrow{\alpha} E'$, then $E + F \xrightarrow{\alpha} E'$
  If $F \xrightarrow{\alpha} F'$, then $E + F \xrightarrow{\alpha} F'$

- Variable: X
  Recursion: $\mu X.E$
  If $E[\mu X.E/X] \xrightarrow{\alpha} E'$,
  then $\mu X.E \xrightarrow{\alpha} E'$

- Parallelism: $E \mid F$
  If $E \xrightarrow{\alpha} E'$, then $E \mid F \xrightarrow{\alpha} E' \mid F$
  If $F \xrightarrow{\alpha} F'$, then $E \mid F \xrightarrow{\alpha} E \mid F'$
  If $E \xrightarrow{\ell} E'$ and $F \xrightarrow{\bar{\ell}} F'$, then $E \mid F \xrightarrow{\tau} E' \mid F'$

- Relabelling: $E[f]$ $\quad (f : \mathcal{L} \rightarrow \mathcal{L}$ with $f(\bar{a}) = \overline{f(a)})$
  If $E \xrightarrow{\alpha} E'$, then $E[f] \xrightarrow{f(\alpha)} E'[f]$

- Restriction: $E \backslash L$ $\quad (L \subseteq \mathcal{L})$
  If $E \xrightarrow{\alpha} E'$ and $\alpha, \bar{\alpha} \notin L$,
  then $E \backslash L \xrightarrow{\alpha} E' \backslash L$

Example: CCS counter

- Goal: model a counter for nonnegative numbers.
  Possible actions: *inc*, *dec*

- Idea: if the counter has value n, it has n processes that can do *dec*.

- $C = \mathit{dec}.\mathit{inc}.C + \mathit{inc}.(C \mid C)$ $\qquad Z = \mathit{inc}.C$

- $C = \mu X.(\mathit{dec}.\mathit{inc}.X + \mathit{inc}.(X \mid X))$ $\qquad Z = \mathit{inc}.\mu X.(\mathit{dec}.\mathit{inc}.X + \mathit{inc}.(X \mid X))$

Expressions and Processes

- Using CCS grammar, one can define (arbitrary) expressions that may contain free variables (variable X outside subexpression $\mu X.E$)
- Process := expression without free variables
- $\mathcal{E}$ = set of all CCS expressions
  $\mathcal{P}$ = set of all CCS processes
- For now, restrict attention to processes

Compare processes

- specification and implementation process:
  the implementation process satisfies the specification
  if the two processes are equivalent

- depending on property: several notions of equivalence

Bisimulations

- defined through operators on relations.
  Let $R \subseteq \mathcal{P} \times \mathcal{P}$ be a symmetric relation.

- If $R \subseteq \mathcal{S}(R)$, then R is a strong bisimulation.

  $P\ \mathcal{S}(R)\ Q$ iff $P \xrightarrow{\alpha} P'$ implies $Q \xrightarrow{\alpha} Q'$ and $P'\ R\ Q'$.

- If $R \subseteq \mathcal{B}(R)$, then R is a branching bisimulation.

  $P\ \mathcal{B}(R)\ Q$ iff $P \xrightarrow{\alpha} P'$ implies $Q \Longrightarrow Q' \xrightarrow{(\alpha)} Q''$ and $P\ R\ Q'$ and $P'\ R\ Q''$.

- If $R \subseteq \mathcal{D}(R)$, then R is divergence-preserving.

  $P\ \mathcal{D}(R)\ Q$ iff $P \equiv P_0 \xrightarrow{\tau} P_1 \xrightarrow{\tau} P_2 \xrightarrow{\tau} \ldots$ implies $Q \xrightarrow{\tau} Q'$ and $P_i\ R\ Q'$ for some i.

Bisimilarity

- Strong bisimilarity, $\sim$
  is the union of all strong bisimulations.
  (It is a strong bisimulation itself.)

- Divergence-preserving branching bisimilarity, $\approx_b^\Delta$
  is the union of all d.-p. branching bisimulations.
  (It is a d.-p. branching bisimulation itself.)

Compare processes in context

- Compositional reasoning:
  check simple processes separately and combine them later

- Requires that equivalence relation is a congruence,
  i.e. if $E \asymp F$ then $C[E] \asymp C[F]$ in all contexts $C[\ ]$.

- (Divergence-preserving) branching bisimilarity is not a congruence:
  $a.\mathbf{0} \approx_b^\Delta \tau.a.\mathbf{0}$,
  but in context $C[\ ] := [\ ] + b.\mathbf{0}$ we have $C[a.\mathbf{0}] \not\approx_b^\Delta C[\tau.a.\mathbf{0}]$

Rooted (d.-p.) branching bisimularity

- Root condition:
  first action of a process must be matched as in strong bisimilarity,
  later actions as in (d.-p.) branching bisimilarity
- Root condition works for weak bisimilarity and branching bisimilarity.
- Does it work for divergence-preserving branching bisimilarity?
  - van Glabbeek/Luttik/Spanink 2020: Yes, for finite-state CCS
  - This presentation: Yes, for weakly guarded CCS
  - Our future collaboration: for full CCS?

Rooted (d.-p.) branching bisimularity

- Root condition:
  first action of a process must be matched as in strong bisimilarity,
  later actions as in (d.-p.) branching bisimilarity

- Rooted d.-p. branching bisimilarity is $=_b^\Delta := \mathcal{S}(\approx_b^\Delta) \cap \mathcal{S}(\approx_b^\Delta)^{-1}$

- Proof goal: $=_b^\Delta$ is a congruence

- For processes without recursion $\mu X.E$: the proof is simple

Bisimulation up to $\approx_b^\Delta$

- If $R \subseteq \mathcal{P} \times \mathcal{P}$ is symmetric, $R \subseteq \mathcal{B}(R{\approx_b^\Delta})$ and $R \subseteq \mathcal{D}({\approx_b^\Delta}R)$, then R is a divergence-preserving bisimulation up to $\approx_b^\Delta$.

- Theorem: If R is a d.-p. bisimulation up to $\approx_b^\Delta$, then $R \subseteq {\approx_b^\Delta}$.

Bisimulations of expressions $\in \mathcal{E}$

- Expressions are bisimilar if all processes derived from them are bisimilar.

- If $fv(E) \cup fv(F) = \{ X_1, X_2, \ldots, X_n \}$, then

  $E \sim F$ iff $E[P_1/X_1, \ldots, P_n/X_n] \sim F[P_1/X_1, \ldots, P_n/X_n]$ for all $P_1, \ldots, P_n \in \mathcal{P}$

  $E \approx_b^\Delta F$ iff $E[P_1/X_1, \ldots, P_n/X_n] \approx_b^\Delta F[P_1/X_1, \ldots, P_n/X_n]$ for all $P_1, \ldots, P_n \in \mathcal{P}$

  $E =_b^\Delta F$ iff $E[P_1/X_1, \ldots, P_n/X_n] =_b^\Delta F[P_1/X_1, \ldots, P_n/X_n]$ for all $P_1, \ldots, P_n \in \mathcal{P}$

Key lemma for μX.*E*

Lemma. Let E, $F \in \mathcal{E}$ be expressions that contain (at most) X as free variable, and X be weakly guarded in E, F. If $E =_b^\Delta F$, then $\mu X.E =_b^\Delta \mu X.F$.

Proof. We define the relation:

$$R = \{\ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\}\ \}$$

This relation satisfies:

(1) $R \subseteq \mathcal{S}(R{\approx_b^\Delta})$

(2) $R^{-1} \subseteq \mathcal{S}(R^{-1}{\approx_b^\Delta})$

(3) $R \subseteq \mathcal{S}({\approx_b^\Delta}R)$

(4) $R^{-1} \subseteq \mathcal{S}({\approx_b^\Delta}R^{-1})$

(5) $R \cup R^{-1}$ is a d.-p. branching bisimulation up to $\approx_b^\Delta$, so $R \subseteq \approx_b^\Delta$.

Key lemma for μX.E

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$ (1) $R \subseteq \mathcal{S}(R{\approx}_b^{\Delta})$

We prove: If $G[\mu X.E/X] \xrightarrow{a} P'$,

then there exists Q' such that $G[\mu X.F/X] \xrightarrow{a} Q'$ and $P' \; R{\approx}_b^{\Delta} \; Q'$.

Proof by transition induction
(i.e. induction over the derivation of the transition $G[\mu X.E/X] \xrightarrow{a} P'$):
Assume that it holds for all $\tilde{G}[\mu X.E/X] \xrightarrow{\tilde{a}} \tilde{P}'$ with a shorter derivation,
then we prove the statement for $G[\mu X.E/X] \xrightarrow{a} P'$.

Within the transition induction: case distinction on the form of G.

Key lemma for μX.E

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$ (1) $R \subseteq \mathcal{S}(R{\approx}_b^\Delta)$

We prove: If $G[\mu X.E/X] \xrightarrow{a} P'$,

then there exists Q' such that $G[\mu X.F/X] \xrightarrow{a} Q'$ and $P' \; R{\approx}_b^\Delta \; Q'$.

Assume that $G \equiv X$, i.e. $G[\mu X.E/X] \equiv \mu X.E$.

If $\mu X.E \xrightarrow{a} P'$, this is the case because $E[\mu X.E/X] \xrightarrow{a} P'$ by a shorter inference.

So, by induction hypothesis, there is Q'' s.t. $E[\mu X.F/X] \xrightarrow{a} Q''$ and $P' \; R{\approx}_b^\Delta \; Q''$.

But $E =_b^\Delta F$, so $E[\mu X.F/X] =_b^\Delta F[\mu X.F/X]$, so there is Q' s.t. $F[\mu X.F/X] \xrightarrow{a} Q'$ and $Q'' \approx_b^\Delta Q'$.

So $P' \; R{\approx}_b^\Delta{\approx}_b^\Delta \; Q'$. As $\approx_b^\Delta$ is transitive, we have $P' \; R{\approx}_b^\Delta \; Q'$.

Key lemma for μX.*E*

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$ (2) $R^{-1} \subseteq \mathcal{S}(R^{-1}\approx_b^\Delta)$

Proof exactly analogous to (1).

Key lemma for μX.*E*

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$ (3) $R \subseteq \mathcal{S}(\approx_b^\Delta R)$

We prove: If $G[\mu X.E/X] \xrightarrow{a} P'$,

then there exists Q' such that $G[\mu X.F/X] \xrightarrow{a} Q'$ and $P' \approx_b^\Delta R\ Q'$.

Proof by transition induction
(i.e. induction over the derivation of the transition $G[\mu X.E/X] \xrightarrow{a} P'$):
Assume that it holds for all $\tilde{G}[\mu X.E/X] \xrightarrow{\tilde{a}} \tilde{P}'$ with a shorter derivation,
then we prove the statement for $G[\mu X.E/X] \xrightarrow{a} P'$.

Within the transition induction: case distinction on the form of *G*.

Key lemma for μX.*E*

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$ (3) $R \subseteq \mathcal{S}(\approx_b^\Delta R)$

We prove: If $G[\mu X.E/X] \xrightarrow{\alpha} P'$,

then there exists Q' such that $G[\mu X.F/X] \xrightarrow{\alpha} Q'$ and $P' \approx_b^\Delta R\ Q'$.

Assume that $G \equiv X$, i.e. $G[\mu X.E/X] \equiv \mu X.E$.
If $\mu X.E \xrightarrow{\alpha} P'$, this is the case because $E[\mu X.E/X] \xrightarrow{\alpha} P'$.
As $E =_b^\Delta F$, so $E[\mu X.E/X] =_b^\Delta F[\mu X.E/X]$, so there is P'' s.t. $F[\mu X.E/X] \xrightarrow{\alpha} P''$ and $P' \approx_b^\Delta P''$.
Now, as X is weakly guarded in F, there is F' s.t. $F \xrightarrow{\alpha} F'$ and $P'' \equiv F'[\mu X.E/X]$.
Also, $F[\mu X.F/X] \xrightarrow{\alpha} F'[\mu X.F/X]$, so $\mu X.F \xrightarrow{\alpha} F'[\mu X.F/X] \equiv: Q'$. Then $P' \approx_b^\Delta R\ Q'$.

Key lemma for $\mu X.E$

$R = \{\, (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \,\}$

(4) $R^{-1} \subseteq \mathcal{S}(\approx_b^\Delta R^{-1})$

Proof exactly analogous to (3).

Key lemma for $\mu X.E$

$R = \{ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\} \}$

(5) $R \cup R^{-1}$ is a d.-p. branching bisimulation up to $\approx_b^\Delta$, so $R \subseteq \approx_b^\Delta$.

		(1) and (2)		$\mathcal{S}\subseteq\mathcal{B}$		monotonicity of $\mathcal{B}$	
R	$\subseteq$	$\mathcal{S}(R\approx_b^\Delta)$	$\subseteq$	$\mathcal{B}(R\approx_b^\Delta)$	$\subseteq$	$\mathcal{B}((R \cup R^{-1})\approx_b^\Delta)$	
R^{-1}	$\subseteq$	$\mathcal{S}(R^{-1}\approx_b^\Delta)$	$\subseteq$	$\mathcal{B}(R^{-1}\approx_b^\Delta)$	$\subseteq$	$\mathcal{B}((R \cup R^{-1})\approx_b^\Delta)$	

		(3) and (4)		$\mathcal{S}\subseteq\mathcal{D}$		monotonicity of $\mathcal{D}$	
R	$\subseteq$	$\mathcal{S}(\approx_b^\Delta R)$	$\subseteq$	$\mathcal{D}(\approx_b^\Delta R)$	$\subseteq$	$\mathcal{D}(\approx_b^\Delta(R \cup R^{-1}))$	
R^{-1}	$\subseteq$	$\mathcal{S}(\approx_b^\Delta R^{-1})$	$\subseteq$	$\mathcal{D}(\approx_b^\Delta R^{-1})$	$\subseteq$	$\mathcal{D}(\approx_b^\Delta(R \cup R^{-1}))$	

X

Key lemma for μ$X.E$

$R = \{\ (G[\mu X.E/X], G[\mu X.F/X]) \mid G \in \mathcal{E}, fv(G) \subseteq \{X\}\ \}$

(5) $R \cup R^{-1}$ is a d.-p. branching bisimulation up to $\approx_b^\Delta$, so $R \subseteq \approx_b^\Delta$.

Consequence of (5): $R{\approx_b^\Delta} \subseteq {\approx_b^\Delta}{\approx_b^\Delta} \subseteq {\approx_b^\Delta}$.

So, $R \subseteq \mathcal{S}(R{\approx_b^\Delta}) \subseteq \mathcal{S}(\approx_b^\Delta)$. Similarly, $R^{-1} \subseteq \mathcal{S}(R^{-1}{\approx_b^\Delta}) \subseteq \mathcal{S}(\approx_b^\Delta)$, so $R \subseteq \mathcal{S}(\approx_b^\Delta)^{-1}$.

So, $R \subseteq \mathcal{S}(\approx_b^\Delta) \cap \mathcal{S}(\approx_b^\Delta)^{-1} \subseteq =_b^\Delta$.

Finally $\mu X.E \equiv X[\mu X.E/X]\ R\ X[\mu X.F/X] \equiv \mu X.F$, so $\mu X.E =_b^\Delta \mu X.F$.

Lemma. Let $E, F \in \mathcal{E}$ be expressions that contain (at most) X as free variable.
and X be weakly guarded in E, F. If $E =_b^\Delta F$, then $\mu X.E =_b^\Delta \mu X.F$.

Congruence for all expressions

Theorem. Let $E, F \in \mathcal{E}$ be expressions with $E =_b^\Delta F$.

Then $\quad \alpha.E =_b^\Delta \alpha.F,$

$$E + D =_b^\Delta F + D, \quad D + E =_b^\Delta D + F,$$

$$E \mid D =_b^\Delta F \mid D, \quad D \mid E =_b^\Delta D \mid F,$$

$$E \backslash L =_b^\Delta F \backslash L,$$

$$E[f] =_b^\Delta F[f], \text{ and}$$

$$\mu X.E =_b^\Delta \mu X.F \text{ if } X \text{ is weakly guarded in } E \text{ and } F.$$

Proof: substitutions are transparent, e.g. $\alpha.(E[P/X, \ldots]) \equiv (\alpha.E)[P/X, \ldots]$.

Consequences

- Weak guardedness is the only restriction of the result.
  In practice, it does not make sense to have unguarded variables,
  as they do not lead to any behaviours.
  ➥ **Rooted divergence-preserving branching bisimilarity
  is a congruence for all practically relevant CCS processes.**

- Simple general components (e.g. counters) may require infinite state space
  ➥ **Component library can be filled with usable components;
  they can be combined without changing the specified behaviour.**

Still Open...

- Still, the proof requires that recursions be weakly guarded.
- While unguarded variables do not add any behaviours,
  there may be situations where eliminating them is complex.

  May also need to restrict contexts to those avoiding unguarded variables.
- Problem: In step (3) of the key lemma,
  we cannot use the full power of transition induction.