Environmental Bisimulations and Its Open Questions

Eijiro Sumii

(Tohoku University)

Executive Summary

- Environmental bisimulations:
  A proof method for contextual equivalence
  - Syntactic/operational/"elementary"
  - Applicable to rich languages: Polymorphic/untyped λ-calculi with recursive functions/types and general references/encryption, higher-order π-calculi with locations/encryption, etc. [Sumii, Pierce, et al. POPL’04, POPL’05, ESOP’09, CSL’09, APLAS'09, LICS’12, etc.]
  - Complete (but undecidable)
- Open questions: No context closures? Semantic interpretation? Generic framework? Parameterizing negative recursion?

Talk Outline

- Background
  - Contextual equivalence
  - (Non-environmental) bisimulations
  - Problems of non-environmental bisimulations
- Environmental bisimulations
- Up-to techniques
- Open questions

Contextual Equivalence [Morris 73]

Two programs M, N are <u>contextually equivalent</u>

$$M \equiv N$$

if they "behave the same" under any context

E.g., in pure lambda-calculi, $M \equiv N$ if

$$\forall C.\ \ C[M] \Rightarrow \mathit{true} \ \text{ iff } \ C[N] \Rightarrow \mathit{true}$$

- Direct proof is hard because of "$\forall C$"

$\Rightarrow$ Proof technique is desired

(Non-Environmental) Bisimulations

Two programs M, N are <u>bisimilar</u>

$$M \sim N$$

if they can simulate
each other's input/output behavior

- Soundness: Bisimilar programs are contextually equivalent
- Completeness: Vice versa

$\Rightarrow$ Gives a proof technique for contextual equivalence

Problems of Non-Environmental Bisimulations (1/2)

$M \sim N$ if:

1. If M outputs M_1 and becomes M', then N outputs N_1 and becomes N' with $M' \sim N'$

What condition is needed for M_1 and N_1?

- "$M_1 \sim N_1$" is too strong, because M_1 and M' (N_1 and N') may share a "secret"

  $\Rightarrow$ Incomplete in impure languages

Problems of Non-Environmental Bisimulations (2/2)

$M \sim N$ if:

2. If M becomes M' for input M_2, then N becomes N' for input N_2 with $M' \sim N'$

What condition is needed for M_2 and N_2?

- "$M_2 \sim N_2$" is ill-formed, because it appears in a negative position

  $\Rightarrow$ Bisimilarity ($\sim$) may not exist

Talk Outline

- Background
- Environmental bisimulations
  - Key idea
  - General "definition"
  - Specific definitions
- Up-to techniques
- Open questions

Environmental Bisimulations

Key idea: Use relation-indexed relation $\sim_R$ to represent the "changing world" or the "knowledge of the context"

- R is called an environment
- Accounts for the generativity of
  - Locations (in λ-calculus with store),
  - Channels (in higher-order π-calculus), etc.

- Complete also in impure languages
- Monotone (union-closed) and well-defined

General "Definifion" (1/3)

X is an environmental simulation
if $M\ X_R\ N$ implies:

1. If $M \rightarrow M'$, then $N \Rightarrow N'$ and $M'\ X_R\ N'$
2. If M outputs M_1 and becomes M', then N outputs N_1 and becomes N' with $M'\ X_{R \cup \{(M1,\ N1)\}}\ N'$

General "Definifion" (2/3)

X is an environmental simulation
if $M \; X_R \; N$ implies:

3. For all $M_1 \; R^* \; N_1$,
if M becomes M' for input M_1,
then N becomes N' for input N_1
with $M' \; X_R \; N'$
   - R^* is the <u>context closure</u> of R

     $\{ (C[M_1,\ldots,M_n], C[N_1,\ldots,N_n]) \mid \forall i.\; M_i \; R \; N_i \}$
   - Represents "synthesis of knowledge" by the context

General "Definition" (3/3)

- X is an environmental <u>bi</u>simulation if both X and X^{-1} are environmental simulations
  - X^{-1} is defined by $(X^{-1})_R = (X_R)^{-1}$
- Environmental bisimilarity (**~**) is the largest environmental bismulation

Instance 1: Env. Bisim. for Higher-Order π-Calculus (Simplified)

X is an environmental simulation
 if $P \; X_R \; Q$ implies:

1. If $P \to P'$, then $Q \Rightarrow Q'$ and $P' \; X_R \; Q'$
2. If $P = c!M.P'$, then $Q \Rightarrow c!N.Q'$ and $P' \; X_{R \cup \{(M, N)\}} \; Q'$
3. If $P = c?x.P'$, then $Q \Rightarrow c?x.Q'$ and $P'\{P_1/x\} \; X_R \; Q'\{Q_1/x\}$ for all $P_1 \; R^* \; Q_1$
4. $P \mid P_1 \; X_R \; Q \mid Q_1$ for all $P_1 \; R \; Q_1$

Instance 2: Env. Bisim. for Pure Call-by-Name λ-Calculus

X is an environmental simulation if $M\ X_R\ N$ implies:

1. If $M \to M'$, then $N \Rightarrow N'$ and $M'\ X_R\ N'$
2. If $M = \lambda x.M'$, then $N \Rightarrow \lambda x.N'$ and $\lambda x.M'\ X_{R \cup \{(\lambda x.M',\ \lambda x.N')\}}\ \lambda x.N'$
   - Moreover, $M'\{M_1/x\}\ X_R\ N'\{N_1/x\}$ for all $M_1\ R^*\ N_1$

Simple Example (for Pedagogy)

$$M = \lambda x.(\lambda y.y)x \text{ and } N = \lambda x.x$$

- Consider $X_0 = \{ (R, M, N) \}$ where $R = \{(M, N)\}$
- For any $M_1 \; R^* \; N_1$,

  $M \; M_1 \rightarrow (\lambda y.y)M_1 \rightarrow M_1$

  $N \; N_1 \rightarrow N_1$
- Extend X_0 to $X =$

  $\{ (R^*, (\lambda y.y)M_1, N_1), (R^*, M_1, N_1) \mid M_1 \; R^* \; N_1 \}$
- X is an environmental bisimulation

Talk Outline

- Background
- Environmental bisimulation
- Up-to techniques
  - Big-step environmental bisimulation up to reduction and context
- Open questions

Big-Step Env. Bisim. up to Reduction and Context

X is a <u>big-step environmental simulation up to reduction and context</u> if $M\ X_R\ N$ impilies:

- If $M \Rightarrow \lambda x.M'$, then $N \Rightarrow \lambda x.N'$ and for all $M_1\ R^*\ N_1$, $M'\{M_1/x\} \Rightarrow (X_{R \cup \{(\lambda x.M',\ \lambda x.N')\}})^* \Leftarrow N'\{N_1/x\}$
  - Recall R* is the context closure of R

The Example Revisited

$$M = \lambda x.(\lambda y.y)x \text{ and } N = \lambda x.x$$

- Take $X = \{ (R, M, N) \}$ where $R = \{(M, N)\}$
- For any $M_1\ R^*\ N_1$,

  $M\ M_1 \Rightarrow M_1$

  $R\ R^* \qquad R^* = (X_R)^*$

  $N\ N_1 \Rightarrow N_1$
- X is a big-step environmental bisimulation up to reduction and context
  - The proof is now as easy as it should be!

Talk Outline

- Background
- Environmental bisimulation
- Up-to techniques
- Open questions
  - No context closures?
  - Semantic interpretation?
  - Generic framework?
  - Parameterizing negative recursion?

Open Question 1: No Context Closures?

X is a big-step env. bisim. up to reduction and context if $M \; X_R \; N$ impilies:

- If $M \Rightarrow \lambda x.M'$, then $N \Rightarrow \lambda x.N'$ and

  for all $M_1 \; R^* \; N_1$,

  $M'\{M_1/x\} \Rightarrow \left(X_{R \cup \{(\lambda x.M', \lambda x.N')\}}\right)^* \Leftarrow N'\{N_1/x\}$

$R^* = \{ (C[M_1,\ldots,M_n], C[N_1,\ldots,N_n]) \mid \forall i.\; M_i \; R \; N_i \}$

Syntactically identical C (not C and C')

⇒ Cannot relate "bisimilar contexts"

Open Question 2:
Semantic Interpretation?

Relation-indexed relation $\sim_R$

to represent the "changing world"

or the "knowledge of the context"

What is it, denotationally?

Open Question 3: Generic Framework?

- "Applicable to rich languages"
- "General definition"

How to <u>formalize</u>?

Generic operational semantics and generic env. bisim.?

Open Question 4: Parameterizing Negative Recursion?

- "$\lambda x.M \sim \lambda y.N$ iff for any $M' \sim N'$ we have $M\{M'/x\} \sim N\{N'/x\}$" is not a valid (co)inductive definition
  - Cf. type t = Abs of (t → t) (* HOAS *)
    ⇒ type 'a t = Abs of ('a → t) (* PHOAS *)
- By analogy, "$\lambda x.M \sim_R \lambda y.N$ iff for any $M'\ R\ N'$ we have $M\{M'/x\} \sim_R N\{N'/x\}$"?
  - Cf. [Hur, Dreyer, et al. POPL'12] is incomplete because of "uncivilized" R's (disrespect equivalence)