Teoria współbieżności

Piotr Hofman

Theoretical aspects of concurrency

Bisimulation - why is it interesting?

How we can use bisimulation?

The system minimisation (Pre-processing)

Take a quotient of a system along to the bisimilarity relation. States of the obtained system are bisimilar to the states in the corresponding equivalence classes of the bisimilarity relation.

How we can use bisimulation?

The system minimisation (Pre-processing)

Take a quotient of a system along to the bisimilarity relation. States of the obtained system are bisimilar to the states in the corresponding equivalence classes of the bisimilarity relation.

The system specification.

Suppose you have a system specified in an abstract language and you have its concrete implementation, how to prove that the implementation corresponds to the specification?

A bisimulation perspective.

Suppose you want to prove some properties of the system. Why do you think you can see its states? Actually, often you observe some signals emitted by the system.

A bisimulation perspective.

Suppose you want to prove some properties of the system. Why do you think you can see its states? Actually, often you observe some signals emitted by the system.

Definition LTS-labelled transition system

A labelled transition system is 5-tuple $A = (Q, \Sigma, I, T, L)$ where:

1. Q is the set of states,
2. Σ is the finite alphabet of signals (actions),
3. I is the set of initial states, $I \subseteq S$,
4. T is the transition relation $T \subseteq Q \times Q$,
5. L is the labelling (or interpretation) function $L : T \to \Sigma$.

Lemma

There is a strict correspondence between LTS and Kripke structures. (LTS are introduced to change the perspective).

A bisimulation one more time

Bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma$ and t such that $s \xrightarrow{a} t$ there is t' such that $s' \xrightarrow{a} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma$ ant t' such that $s' \xrightarrow{a} t'$ there is t such that $s \xrightarrow{a} t$ and $(t, t') \in B$,

A bisimulation one more time

Bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma$ and t such that $s \xrightarrow{a} t$ there is t' such that $s' \xrightarrow{a} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma$ ant t' such that $s' \xrightarrow{a} t'$ there is t such that $s \xrightarrow{a} t$ and $(t, t') \in B$,

Approximants

- Let B_0 be a set of all pairs of configurations.
- $(s, s') \in B_{i+1}$ if and only if:
  1. For any $a \in \Sigma$ and all t such that $s \xrightarrow{a} t$ there is a $s' \xrightarrow{a} t'$ where $(t, t') \in B_i$.
  2. For any $a \in \Sigma$ and all t' such that $s' \xrightarrow{a} t'$ there is a $s \xrightarrow{a} t$ where $(t, t') \in B_i$.

Game characterisation of Bisimilarity for LTS

Definition

A bisimulation game is played in rounds between two players Spoiler and Duplicator. Arena is a set of pairs of states of the LTS. Suppose that current pair of configurations is (s, s').
Rules of a round are as follows:

- First Spoiler chooses one of states s or s'. Without lost of generality we may assume that it is s.
- Next he chooses a state t such that $s \xrightarrow{a} t$.
- Next Duplicator chooses a state t' such that $s' \xrightarrow{a} t'$ where s' is a configuration no chosen by Spoiler.
- The next round of the game will be plaid from (t, t').

Winning conditions:

- If any player can not make his part of the move then he looses.
- Infinite plays are won by Duplicator.

Inclusion ?

LTL	CTL
Language equivalence	Bisimulation
Language containment	???

Simulation for LTS

We say that S is a relation of simulation on a set of states if

1. for every $(s, s') \in S$ and any $a \in \Sigma$ if $s \xrightarrow{a} t$ there is t' such that $s' \xrightarrow{a} t'$ and $(t, t') \in S$,

We say that s is simulated by s'.

Lemma

Union of simulations is a simulation so there is a biggest simulation (similarity).

Inclusion ?

LTL	CTL
Language equivalence	Bisimulation
Language containment	Simulation

Simulation for LTS

We say that S is a relation of simulation on a set of states if

1. for every $(s, s') \in S$ and any $a \in \Sigma$ if $s \xrightarrow{a} t$ there is t' such that $s' \xrightarrow{a} t'$ and $(t, t') \in S$,

We say that s is simulated by s'.

Lemma

Union of simulations is a simulation so there is a biggest simulation (similarity).

Simulation

Specification

1. Our system should be simulated by an LTS that models all acceptable behaviours (safety).
2. Our system should simulate all desired scenarios.

Simulation

Specification

1. Our system should be simulated by an LTS that models all acceptable behaviours (safety).
2. Our system should simulate all desired scenarios.

Example:

Simulation

Specification

1. Our system should be simulated by an LTS that models all acceptable behaviours (safety).
2. Our system should simulate all desired scenarios.

Example:

Problem

How to represent internal steps of the system?

Weak Bisimulation.

Internal steps of the system.

What if system has internal steps?

We introduce τ transitions, which are not observable. (Like ϵ transitions in automata.)

Internal steps of the system.

What if system has internal steps?

We introduce τ transitions, which are not observable. (Like ϵ transitions in automata.)

Let $\stackrel{a}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}\xrightarrow{a}\xrightarrow{\tau} \dots \xrightarrow{\tau}$, and $\stackrel{\tau}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}$ (the sequence can be empty).

Internal steps of the system.

What if system has internal steps?

We introduce τ transitions, which are not observable. (Like ϵ transitions in automata.)

Let $\stackrel{a}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}\xrightarrow{a}\xrightarrow{\tau} \dots \xrightarrow{\tau}$, and $\stackrel{\tau}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}$ (the sequence can be empty).

Weak bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \xrightarrow{a} t$ there is t' such that $s' \stackrel{a}{\Rightarrow} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t' such that $s' \xrightarrow{a} t'$ there is t such that $s \stackrel{a}{\Rightarrow} t$ and $(t, t') \in B$,

Internal steps of the system.

What if system has internal steps?

We introduce τ transitions, which are not observable. (Like ϵ transitions in automata.)

Let $\stackrel{a}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}\xrightarrow{a}\xrightarrow{\tau} \dots \xrightarrow{\tau}$, and $\stackrel{\tau}{\Rightarrow}$ denotes a sequence of transitions $\xrightarrow{\tau} \dots \xrightarrow{\tau}$ (the sequence can be empty).

Weak bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \xrightarrow{a} t$ there is t' such that $s' \stackrel{a}{\Rightarrow} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t' such that $s' \xrightarrow{a} t'$ there is t such that $s \stackrel{a}{\Rightarrow} t$ and $(t, t') \in B$,

Weak simulation can be defined in a similar way.

Weak bisimulation via game

Definition

A weak bisimulation game is played in rounds between two players Spoiler and Duplicator. Arena is a set of pairs of configurations of the LTS. Suppose that current pair of configurations is (s, s').
Rules of a round are as follows:

- First Spoiler chooses one of configurations s or s'. Without lost of generality we may assume that it is s.
- Next he chooses $a \in \Sigma \cup \{\tau\}$ and a configuration t such that $s \xrightarrow{a} t$.
- Next Duplicator chooses a configuration t' such that $s' \stackrel{a}{\Rightarrow} t'$ where s' is the configuration not chosen by Spoiler.
- The next round of the game will be plaid from (t, t').

Winning conditions:

- If a player can not make his move then his opponent wins.
- Infinite plays are winning for Duplicator.

Is it a good definition?

Weak bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \xrightarrow{a} t$ there is t' such that $s' \xRightarrow{a} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ ant t' such that $s' \xrightarrow{a} t$ there is t such that $s \xRightarrow{a} t$ and $(t, t') \in B$,

Question

What if Spoiler can play long moves $s \xRightarrow{a} s'$?

Is it a good definition?

Weak bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \stackrel{a}{\Rightarrow} t$ there is t' such that $s' \stackrel{a}{\Rightarrow} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ ant t' such that $s' \stackrel{a}{\Rightarrow} t'$ there is t such that $s \stackrel{a}{\Rightarrow} t$ and $(t, t') \in B$,

Question

What if Spoiler can play long moves $s \stackrel{a}{\Rightarrow} s'$?

Is it a good definition?

Weak bisimulation for LTS

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \stackrel{a}{\Rightarrow} t$ there is t' such that $s' \stackrel{a}{\Rightarrow} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ ant t' such that $s' \stackrel{a}{\Rightarrow} t'$ there is t such that $s \stackrel{a}{\Rightarrow} t$ and $(t, t') \in B$,

Question

What if Spoiler can play long moves $s \stackrel{a}{\Rightarrow} s'$?

Lemma

Both definitions of the weak bisimulation describes the same relations.

Is it a good definition 2?

Weak bisimulation for LTS, another proposal

Bisimulation B is any relation on a set of configurations (states) that satisfies following conditions

1. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ and t such that $s \stackrel{a}{\Rightarrow} t$ there is t' such that $s' \stackrel{a}{\Rightarrow} t'$ and $(t, t') \in B$,
2. if $(s, s') \in B$ then for every $a \in \Sigma \cup \{\tau\}$ ant t' such that $s' \stackrel{a}{\Rightarrow} t'$ there is t such that $s \stackrel{a}{\Rightarrow} t$ and $(t, t') \in B$,

Question

Why $a \in \Sigma \cup \{\tau\}$ and not simply $a \in \Sigma$?.

Properties of weak bisimulation

Lemma

Properties of weak bisimulation

Lemma

- *Union of weak bisimulation relations is a weak bisimulation relation.*

Properties of weak bisimulation

Lemma

- *Union of weak bisimulation relations is a weak bisimulation relation.*
- *There is a biggest weak bisimulation relation called a weak bisimilarity.*

Properties of weak bisimulation

Lemma

- *Union of weak bisimulation relations is a weak bisimulation relation.*
- *There is a biggest weak bisimulation relation called a weak bisimilarity.*
- *The week bisimilarity is an equivalence relation.*

Properties of weak bisimulation

Lemma

- *Union of weak bisimulation relations is a weak bisimulation relation.*
- *There is a biggest weak bisimulation relation called a weak bisimilarity.*
- *The week bisimilarity is an equivalence relation.*

Lemma

Let L' be a labelled transition system obtained from a system L by a adding a labelled shortcuts for sequences of transition of a form $\tau^* a \tau^*$ adding τ self loop to every node. Two nodes (configurations) s and s' are weakly bisimilar in L if and only if s and s' are bisimilar in L'.

How to compute the weak bisimilarity relation?

Idea 1.

Use the lemma from previous slide, change it to question about the strong bisimilarity, and use Page and Tarjan's algorithm.

Complexity? $\rightarrow$ Number of edges may grow from $O(n)$ to $O(n^2)$, so $O(|\Sigma| \cdot |V|^2 \cdot log(|V|))$.

Idea 1.

Use the lemma from previous slide, change it to question about the strong bisimilarity, and use Page and Tarjan's algorithm.

Complexity? $\rightarrow$ Number of edges may grow from $O(n)$ to $O(n^2)$, so $O(|\Sigma| \cdot |V|^2 \cdot log(|V|))$.

Approximants

- Let B_0 be a set of all pairs of configurations.
- $(s, s') \in B_{i+1}$ if and only if:
  1. For all $\alpha \in \Sigma \cup \{\tau\}$ and t such that $s \xrightarrow{\alpha} t$ there is a $s' \overset{\alpha}{\Rightarrow} t'$ where $(t, t') \in B_i$.
  2. For all $\alpha \in \Sigma \cup \{\tau\}$ and t' such that $s' \xrightarrow{\alpha} t'$ there is a $s \overset{\alpha}{\Rightarrow} t$ where $(t, t') \in B_i$.

Theorem

If $B_i = B_{i+1}$ then B_i is the weak bisimilarity relation.

Induced labelled transition systems

Question?

How to define bisimulation for programs in C?

Induced LTS

1. States - configurations of the system.
2. Transitions - steps between configurations determined by the semantics of the machine/formalism.
3. The initial states - the initial configuration.
4. Labels - we decorate edges of the control automaton with alphabet and label transitions in LTS accordingly.

Induced labelled transition systems

Question?

How to define bisimulation for turing machines?

Induced LTS

1. States - configurations of the system.
2. Transitions - steps between configurations determined by the semantics of the machine/formalism.
3. The initial states - the initial configuration.
4. Labels - we decorate edges of the control automaton with alphabet and label transitions in LTS accordingly.

The Turing machine can be exchanged by, a pushdown automaton, a timed automaton, a register automaton, a Petri net, a process algebra definition, and many more.

Infinite LTS - Strategies in the game

Spoiler strategy is a tree.

1. Each branch is finite.
2. Branching is finite.

Infinite LTS - Strategies in the game

Spoiler strategy is a tree.

1. Each branch is finite.
2. Branching is finite.

Lemma

For every initial pair of configurations the Spoiler strategy tree is finite.

Question.

Can we put a bound on depths of Spoiler's strategy trees for different initial configurations.

Infinite LTS - Strategies in the game

Spoiler strategy is a tree.

1. Each branch is finite.
2. Branching is finite.

Lemma

For every initial pair of configurations the Spoiler strategy tree is finite.

Question.

Can we put a bound on depths of Spoiler's strategy trees for different initial configurations.

$\sim = \bigcap_{i \in \mathbb{N}} \mathit{Approximant}_i$

Infinite LTS - *tau*-steps - Strategies in the game

Spoiler strategy is a tree.

1. Each branch is finite.
2. Branching is not-finite.

Lemma

For some initial pairs of configurations the Spoiler strategy tree is infinite.

Question.

How to redefine approximants?

Apprximants one more time

Approximants

- Let B_0 be a set of all pairs of configurations.
- $(s, s') \in B_i$ if and only if:
  1. For all $j < i$, $\alpha \in \Sigma \cup \{\tau\}$, and t such that $s \xrightarrow{\alpha} t$ there is a $s' \stackrel{\alpha}{\Rightarrow} t'$ where $(t, t') \in B_j$.
  2. For all $j < i$, $\alpha \in \Sigma \cup \{\tau\}$, and t' such that $s' \xrightarrow{\alpha} t'$ there is a $s \stackrel{\alpha}{\Rightarrow} t$ where $(t, t') \in B_j$.

Theorem

If $B_i = B_{i+1}$ then B_i is a weak bisimilarity relation.

Faster approximants

Approximants

- Let B_0 be a set of all pairs of configurations.
- $(s, s') \in B_i$ if and only if:
  1. For all $j < i$, $\alpha \in \Sigma \cup \{\tau\}$, and t such that $s \stackrel{\alpha}{\Rightarrow} t$ there is a $s' \stackrel{\alpha}{\Rightarrow} t'$ where $(t, t') \in B_j$.
  2. For all $j < i$, $\alpha \in \Sigma \cup \{\tau\}$, and t' such that $s' \stackrel{\alpha}{\Rightarrow} t'$ there is a $s \stackrel{\alpha}{\Rightarrow} t$ where $(t, t') \in B_j$.

Theorem

If $B_i = B_{i+1}$ then B_i is a weak bisimilarity relation.

Exercise

1. Propose a PDA in which “faster” approximants converge faster.
2. Propose a type of approximants which will converge even faster.
3. Define $Approximant_i$ Game in which Duplicator wins form (s, s') if and only if the pair of the configurations is in the relation $Approximant_i$ where i can be any ordinal number.