Syntactic Criteria for Language-Based Noninterference

Andrei Popescu, Johannes Hölzl, Tobias Nipkow

Fakultät für Informatik
Technische Universität München

Goal of This Talk

Exhibit a uniform pattern behind syntactic criteria for noninterference in a programming language

High points

- both nondeterministic and probabilistic variants
- uniform representation of several literature results
- fully verified in Isabelle

Low points

- only toy language
- no flexible scheduler—only the uniform one
- no fancy thread synchronization primitives

Setting for Noninterference

- Program runs operate on (memory) states
- Assume attacker view of the state
  modeled as an equivalence relation $\sim$ on states
- Example
  - **state** = **var** → **value**
  - **var** separated into low and high variables
  - low means attacker-observable
  - $s \sim s_1$ iff s and s_1 coincide on the low variables
  - this means attacker can only see the low variables

End-to-End Noninterference

Program runs: $s \overset{c}{\dashrightarrow} s'$

Attacker sees: $s/\!\sim\; \overset{c}{\dashrightarrow} s'/\!\sim$

Noninterference:

attacker cannot infer anything about s beyond $s/\!\sim$

Nuances of noninterference:

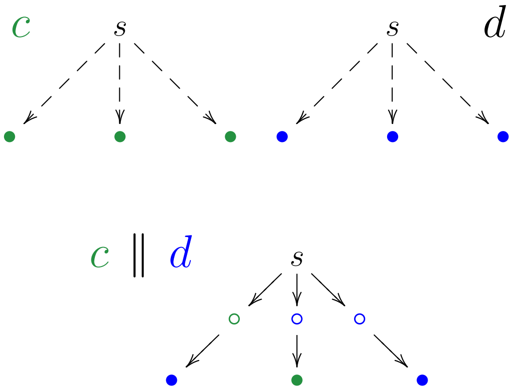
- What does it mean to see $\overset{c}{\dashrightarrow}$?
  - only see/know the program c?
  - also detect potential nontermination?
  - also see the number of steps (running time)?
- What does it mean to see $s'/\!\sim$?
  - only see the actual outcome of one computation?
  - or run c multiple times and gather statistical information about $s'/\!\sim$?

Bisimulation Noninterference

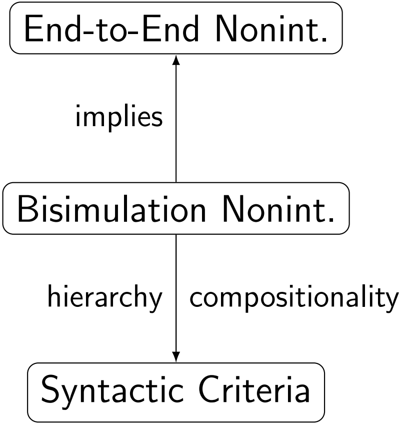
- Attacker may observe not only the final state, but also intermediate states
- Modeled as a bisimulation relation on configurations (c, s) or on programs c
- Why?
  - Handle interactive programs
  - Compositional reasoning
  - Syntactic criteria (a.k.a. security type systems)
- Typically: a bisim. nonint. is a sufficient criterion for an end-to-end nonint.

Compositional Reasoning

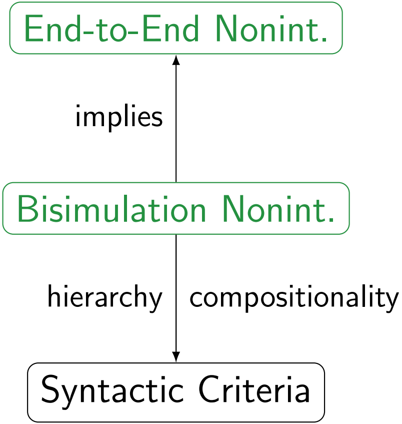
- Wish: $c \parallel d$ nonint. if c nonint. and d nonint.
- Impossible if nonint. ignores the intermediate states



Overview

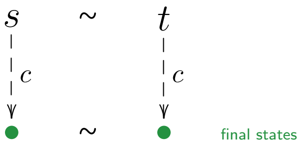

End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

Overview


End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

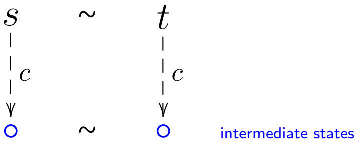
From End-to-End to Bisimulation Noninterference

End-to-end noninterference of c:



From End-to-End to Bisimulation Noninterference

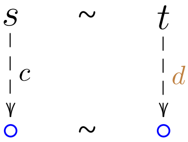
Bisimulation noninterference c:



In addition, what remains to be executed from (c, s) should be further bisimilar to what remains to be executed from (c, t)

From End-to-End to Bisimulation Noninterference

Bisimilarity between c and d:

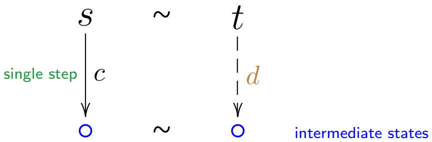


In addition, what remains to be executed from (c, s) should be further bisimilar to what remains to be executed from (d, t)

Bisimilarity = binary generalization of bisimulation nonint.:
"c versus d" instead of "c versus itself"

From End-to-End to Bisimulation Noninterference

Bisimilarity between c and d:



In addition, what remains to be executed from (c, s) should be further bisimilar to what remains to be executed from (c, t)

Bisimilarity = binary generalization of bisimulation nonint.: "c versus d" instead of "c versus itself"

Suffices to focus on single steps of c

Bisimilarity: Summary

$$c \approx d$$

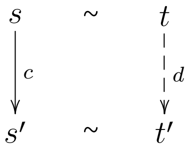
iff

$$\forall \ \exists$$

$$\begin{array}{ccc} s & \sim & t \\ \big\downarrow c & & \big\downarrow d \\ s' & \sim & t' \end{array}$$

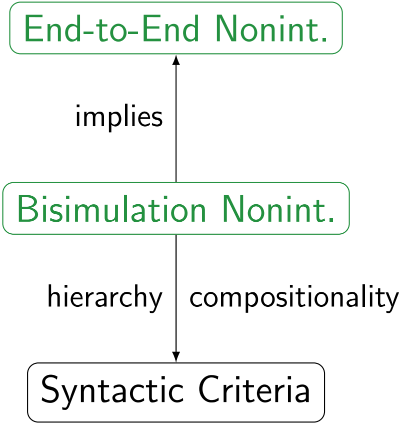
$$c' \approx d'$$

Variants of Bisimulation Nonint.

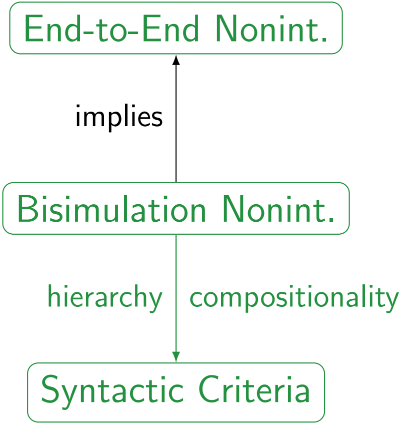


- Discreetness discr: never change the indis. class of state
- Self-isomorphism siso: 1 versus 1, identity on commands
- Strong bisimilarity $\approx_{\mathsf{S}}$: 1 versus 1
- 01-bisimilarity $\approx_{01}$: 1 versus 0 or 1
- Weak bisimilarity $\approx_{\mathsf{W}}$: 1 versus 0 or more
- Termination-sensitive: s' final iff t' final $\approx_{01\mathsf{T}}$, $\approx_{\mathsf{WT}}$

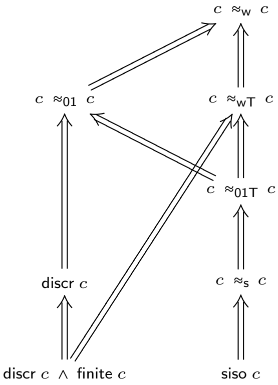
Overview


End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

Overview


End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

Hierarchy



$c \approx_{\mathsf{w}} c$
$c \approx_{01} c$
$c \approx_{\mathsf{wT}} c$
$c \approx_{01\mathsf{T}} c$
discr c
$c \approx_{\mathsf{s}} c$
discr c $\wedge$ finite c
siso c

Language

While language augmented with parallel composition

$$c ::= \textit{atm} \mid c_1 \,;c_2 \mid \text{If } \textit{tst } c_1 \; c_2 \mid \text{While } \textit{tst } c \mid c_1 \parallel c_2$$

Imperative state-based semantics
Atoms (atomic commands) interpreted as state transf.
Tests interpreted as state predicates
Interleaving semantics for $\parallel$

Compositionality

c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$

$\varphi \in \{\mathsf{siso}, \approx_{\mathsf{s}}, \approx_{01\mathsf{T}}, \approx_{\mathsf{wT}}\}$ $\quad \psi \in \{\approx_{01}, \approx_{\mathsf{w}}\}$ $\quad \psi_{\mathsf{T}}$ = termination-sensitive version of ψ

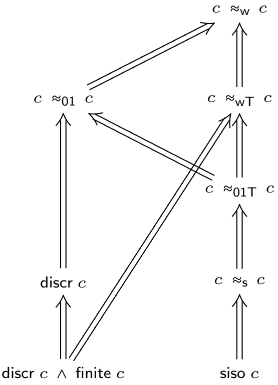
Compositionality

c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_\mathsf{T}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \|\|\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$

$\varphi \in \{\mathsf{siso}, \approx_\mathsf{s}, \approx_{01\mathsf{T}}, \approx_{\mathsf{wT}}\}$ $\psi \in \{\approx_{01}, \approx_\mathsf{w}\}$ ψ_T = termination-sensitive version of ψ

From Compositionality and Hierarchy to Syntactic Criteria

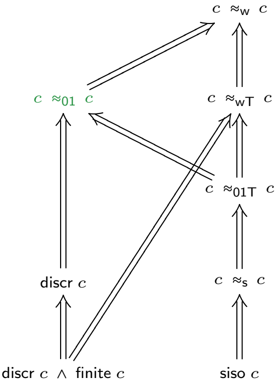
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_\mathsf{T}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

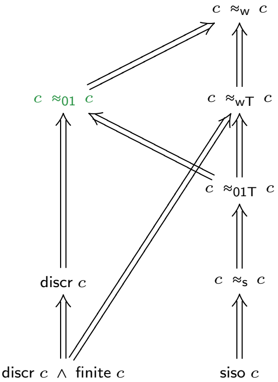
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

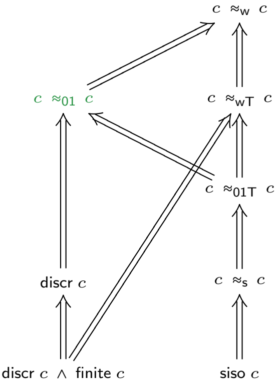
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

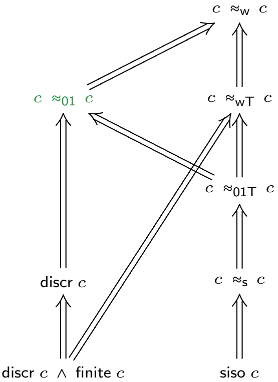
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_T\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

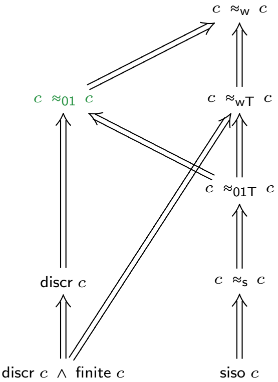
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

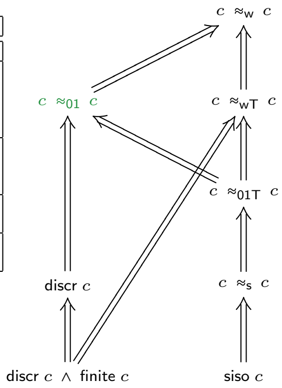
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1 ; c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ — $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1 \parallel c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$\text{if } h = 0 \text{ then } \{h := 1 ; h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

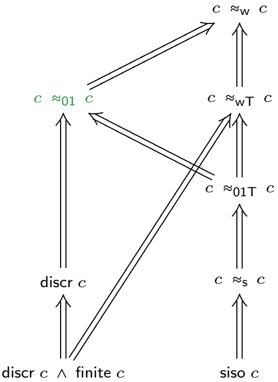
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$\text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

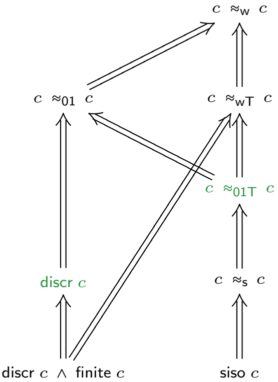
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_\mathsf{T}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$\text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

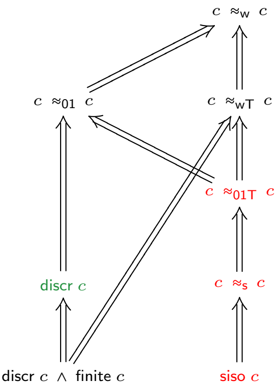
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$\text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

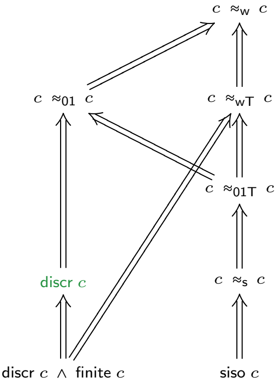
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



if $h = 0$ then $\{h := 1\ ;\ h := 2\}$ else $h := 3$

From Compositionality and Hierarchy to Syntactic Criteria

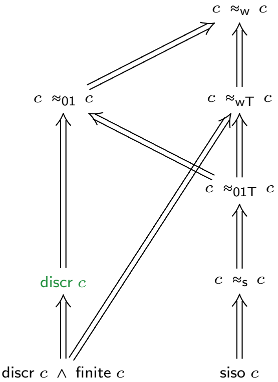
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$$\text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3$$

From Compositionality and Hierarchy to Syntactic Criteria

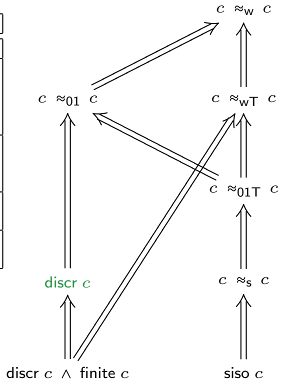
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_{\mathsf{T}}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$h := 1\ ;\ h := 2$ $\qquad$ $h := 3$

From Compositionality and Hierarchy to Syntactic Criteria

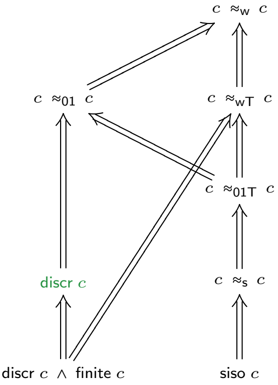
c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
c_1 ; c_2	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_T\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* c_1 c_2	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1 \parallel c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



$h := 1$ $h := 2$ $h := 3$

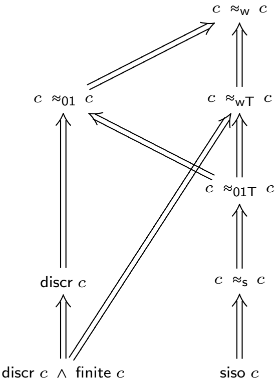
From Compositionality and Hierarchy to Syntactic Criteria

c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
$c_1\ ;\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_\mathsf{T}\ c_1$ $\psi\ c_2$ ——— $\psi\ c_1$ discr c_2
If *tst* $c_1\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$



From Compositionality and Hierarchy to Syntactic Criteria

c	finite c	discr c	$\varphi\ c$	$\psi\ c$
atm	True	pres *atm*	compat *atm*	compat *atm*
c_1 ; c_2	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi_\mathsf{T}\ c_1$ $\psi\ c_2$ ――― $\psi\ c_1$ discr c_2
If *tst* c_1 c_2	finite c_1 finite c_2	discr c_1 discr c_2	compat *tst* $\varphi\ c_1$ $\varphi\ c_2$	compat *tst* $\psi\ c_1$ $\psi\ c_2$
While *tst* d	False	discr d	compat *tst* $\varphi\ d$	False
$c_1\ \parallel\ c_2$	finite c_1 finite c_2	discr c_1 discr c_2	$\varphi\ c_1$ $\varphi\ c_2$	$\psi\ c_1$ $\psi\ c_2$

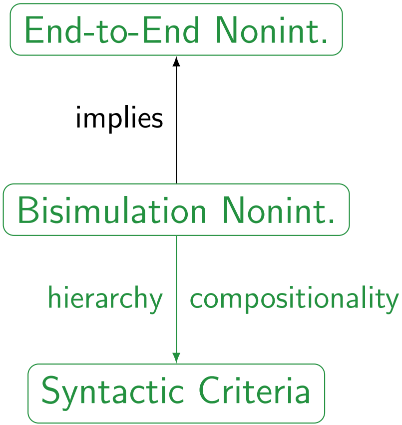


$$l := 4\ ;\ \text{if } h = 0 \text{ then } \{h := 1\ ;\ h := 2\} \text{ else } h := 3 \quad \checkmark$$

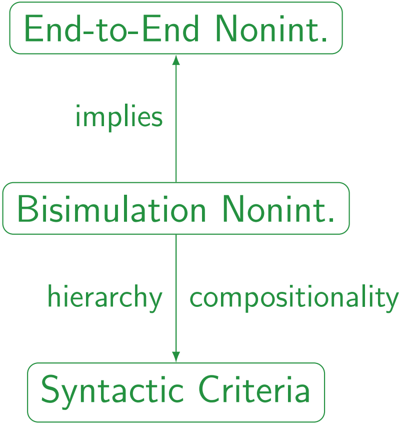
Syntactic Criteria

- Table-and-graph method produces, for each notion of nonint. $\approx$, a recursive function $\overline{\approx}$ on the syntax of programs
- These correspond to ad hoc criteria proposed in the literature, eg:
  - $\overline{\approx_{wT}}$: Smith and Volpano, POPL 1998
  - $\overline{\approx_{01}}$: Boudol and Castellani, TCS 2002
  - $\overline{\approx_{w}}$: Boudol, ICTAC 2005
- This method is a uniform proof for the soundness of all these criteria

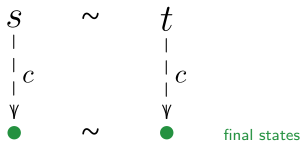
Overview


End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

Overview


End-to-End Nonint.
implies
Bisimulation Nonint.
hierarchy
compositionality
Syntactic Criteria

From Bisimulation Noninterference Back to End-to-End Noninterference



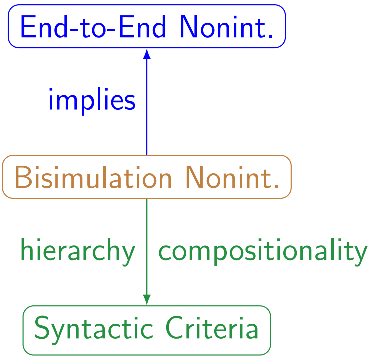
$\overline{\approx_{\mathsf{s}}}$: $\exists$ execution of equal length
$\overline{\approx_{\mathsf{01T}}}$: $\exists$ execution of smaller or equal length
$\overline{\approx_{\mathsf{wT}}}$: $\exists$ execution

For the termination-insensitive notions:
the same results, but conditioned by overall termination

Extension to a Probabilistic Language?

Define notions of bisimulation noninterference that

- are compositional and well-placed in “the hierarchy”
- imply reasonable end-to-end probabilistic noninterference



Probabilistic Language

$$c \ ::= \ \textit{atm} \mid c_1 \,;\, c_2 \mid \mathsf{Ch}\ \textit{ch}\ c_1\ c_2 \mid \mathsf{While}\ \textit{tst}\ c \mid$$
$$\mathsf{Par}\ [c_1, \ldots, c_n] \mid \mathsf{ParT}\ [c_1, \ldots, c_n]$$

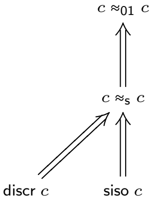
Factor in probabilistic behavior

- probabilistic choice in threads
  - Choices *ch* interpreted as state functions **state** $\to [0, 1]$
  - if image is $\{0, 1\}$, obtain If tests
  - if function is constant, obtain standard choice
- uniform probabilistic scheduler
  - parallel composition now takes lists of threads

Semantics: Markov chain on **command** $\times$ **state**

Compositionality and Hierarchy for Probabilistic Noninterference

c	discr c	siso c	$c \approx_{\mathsf{s}} c$	$c \approx_{01} c$
atm	pres *atm*	compat *atm*	compat *atm*	compat *atm*
$c_1 \, ; \, c_2$	discr c_1 discr c_2	siso c_1 siso c_2	siso c_1 $\dfrac{c_2 \approx_{\mathsf{s}} c_2}{c_1 \approx_{\mathsf{s}} c_1}$ discr c_2	siso c_1 $\dfrac{c_2 \approx_{01} c_2}{c_1 \approx_{01} c_1}$ discr c_2
Ch *ch* $c_1 \; c_2$	discr c_1 discr c_2	compat *ch* siso c_1 siso c_2	compat *ch* $c_1 \approx_{\mathsf{s}} c_1$ $c_2 \approx_{\mathsf{s}} c_2$	compat *ch* $c_1 \approx_{01} c_1$ $c_2 \approx_{01} c_2$
While *tst* d	discr d	compat *tst* siso d	False	False
Par $[c_0, \ldots, c_{n-1}]$	discr c_l $0 \leq l < n$	siso c_l $0 \leq l < n$	$c_l \approx_{\mathsf{s}} c_l$ $0 \leq l < n$	False
$\mathsf{Par}_{\mathsf{T}} \, [c_0, \ldots, c_{n-1}]$	discr c_l $0 \leq l < n$	False	False	$c_l \approx_{\mathsf{s}} c_l$ $0 \leq l < n$



- siso and discr: straightforward probabilistic adaptations of the nondeterministic notions
- $\approx_{\mathsf{s}}$: strong probabilistic bisimilarity (lumpability)
- $\approx_{01}$: relaxation allowing delays

Strong Probabilistic Bisimilarity

$$c \quad \approx_{\mathsf{s}} \quad d$$

iff $\forall$ $\exists$

$$s \quad \sim \quad t$$

$$s \xrightarrow{c} P_1, \ldots, P_n \qquad t \overset{d}{\dashrightarrow} Q_1, \ldots, Q_n$$

$$P_1, \ldots, P_n \quad \sim \quad Q_1, \ldots, Q_n$$

$\mathsf{prob}(c, s, P_i) = \mathsf{prob}(d, t, Q_i)$

$(c', s') \in P_i \ \wedge \ (d', t') \in Q_i \ \rightarrow \ c' \approx_{\mathsf{s}} d' \ \wedge \ s' \sim t'$

01 Probabilistic Bisimilarity

$$c \quad \approx_{01} \quad d$$

iff $\forall$ $\exists$

$$s \quad \sim \quad t$$

$$s \xrightarrow{c} P_0, P_1, \ldots, P_n \qquad t \overset{d}{\dashrightarrow} Q_0, Q_1, \ldots, Q_n$$

$$P_0, P_1, \ldots, P_n \quad \sim \quad Q_0, Q_1, \ldots, Q_n$$

$\mathsf{prob}(c, s, P_i) = \mathsf{prob}(d, t, Q_i)$ relative to P_0 and Q_0

$(c', s') \in P_i \;\wedge\; (d', t') \in Q_i \;\rightarrow\; c' \approx_{01} d' \;\wedge\; s' \sim t'$

$(c', s') \in P_0 \;\rightarrow\; c' \approx_{\mathsf{s}} c \;\wedge\; s' \sim t'$

End-to-End Probabilistic Noninterference

$$\begin{array}{ccc} c \approx_{01} c & \xRightarrow{\text{if c terminates almost everywhere}} & c \text{ is end-secure} \\ \Uparrow & & \Uparrow \\ c \approx_{\mathsf{S}} c & \Longrightarrow & c \text{ is any-moment secure} \end{array}$$

Any-moment security: for any two executions starting in indistinguishable states and any given time, the probability of being at that time in any given indistinguishability class is the same

End security: for any two executions starting in indistinguishable states, the probability of ending up in any given indistinguishability class is the same

Comparison

Probabilistic noninterference

- Less compositional
- Termination-sensitive notions lacking
- Relationship with end-to-end noninterference nontrivial

Conclusion

Hierarchy + Compositionality $\Longrightarrow$ Security Type Systems