UNIVERSITY OF TWENTE.

Model-based testing

NATO Summer School
Marktoberdorf, August, 2010

Ed Brinksma
University of Twente

CONTENTS

- Introduction control-oriented testing
- Input-output conformance testing
- Real-time conformance testing
- Test coverage measures

CONTENTS

PRACTICAL PROBLEMS OF TESTING

Testing is:

- important
- much practiced
- 30% - 50% of project effort
- expensive
- time critical
- not constructive
  (but sadistic?)

But also:

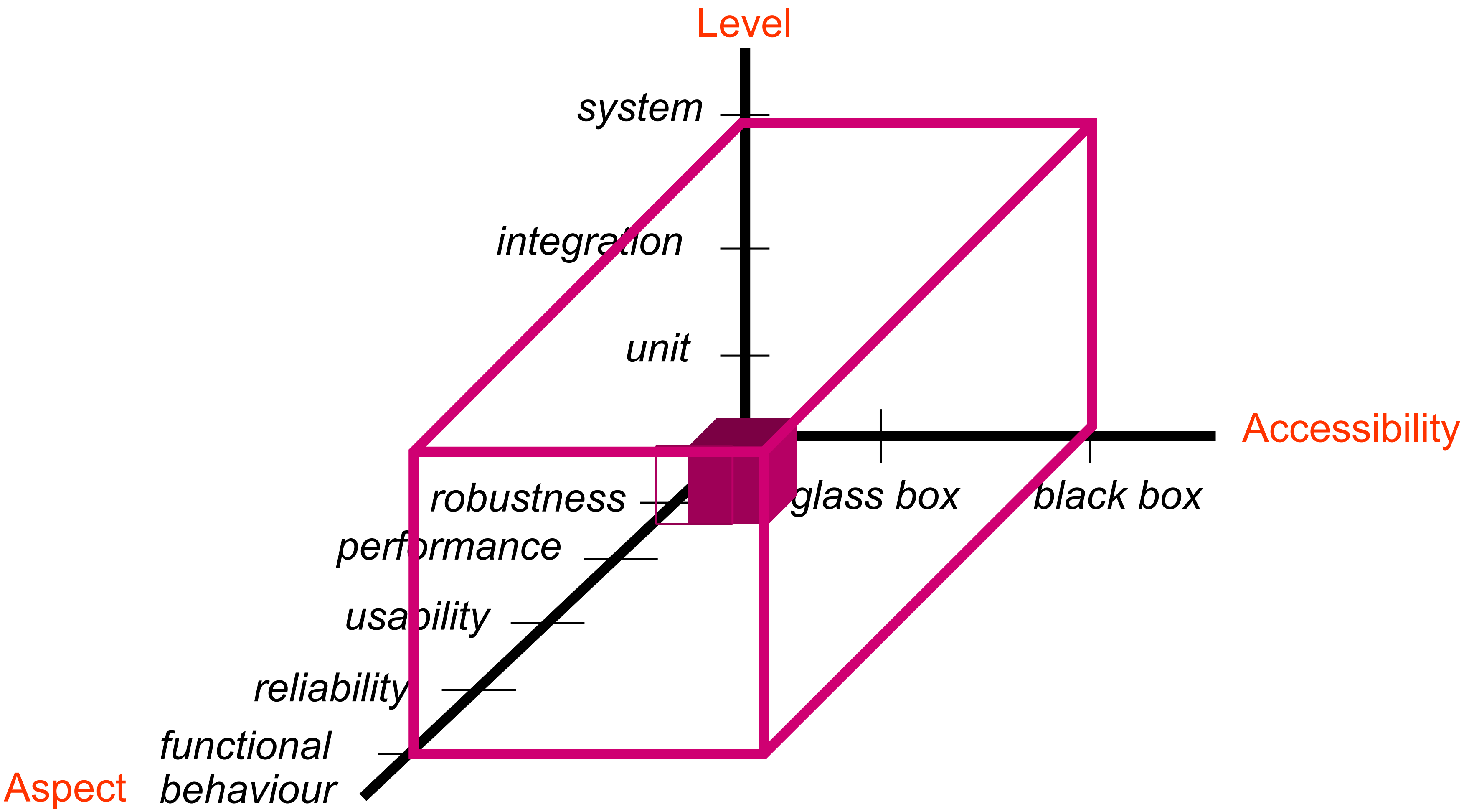
- ad-hoc, manual, error-prone
- limited theory / research
- little attention in curricula
- not *cool* :
  "if you're a bad programmer
  you might be a tester"

Attitude is changing:

- more awareness
- more professional

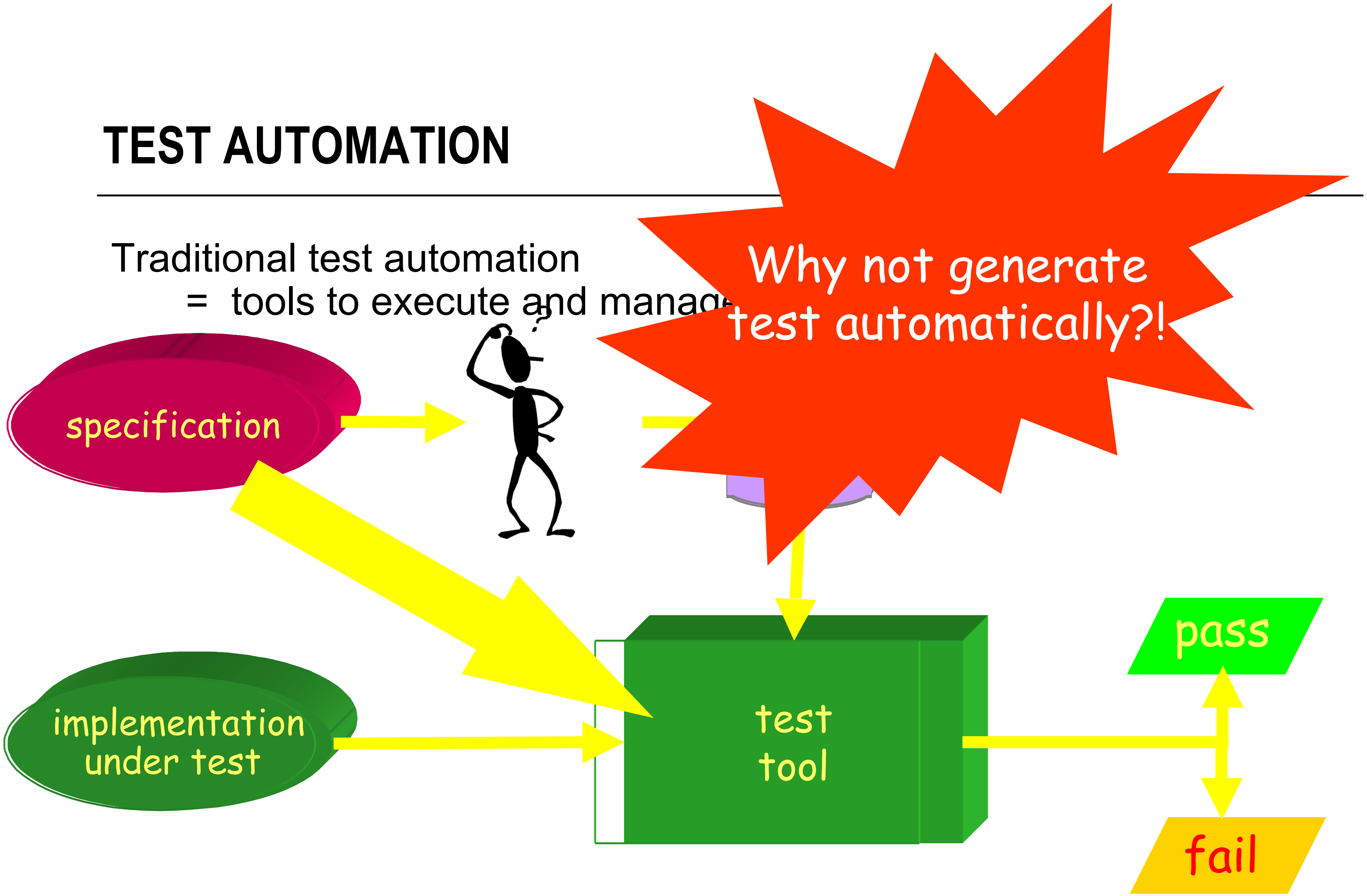
Improvements possible with formal methods ! ?

TYPES OF TESTING



TEST AUTOMATION

Traditional test automation
= tools to execute and manage



VERIFICATION AND TESTING

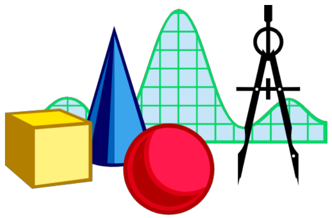
Verification :

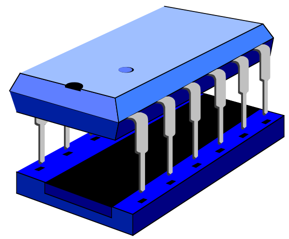
- formal manipulation
- prove properties
- performed on model

Testing :

- experimentation
- show error
- concrete system

formal world





concrete world

Verification is only as good as the validity of the model on which it is based

Testing can only show the presence of errors, not their absence

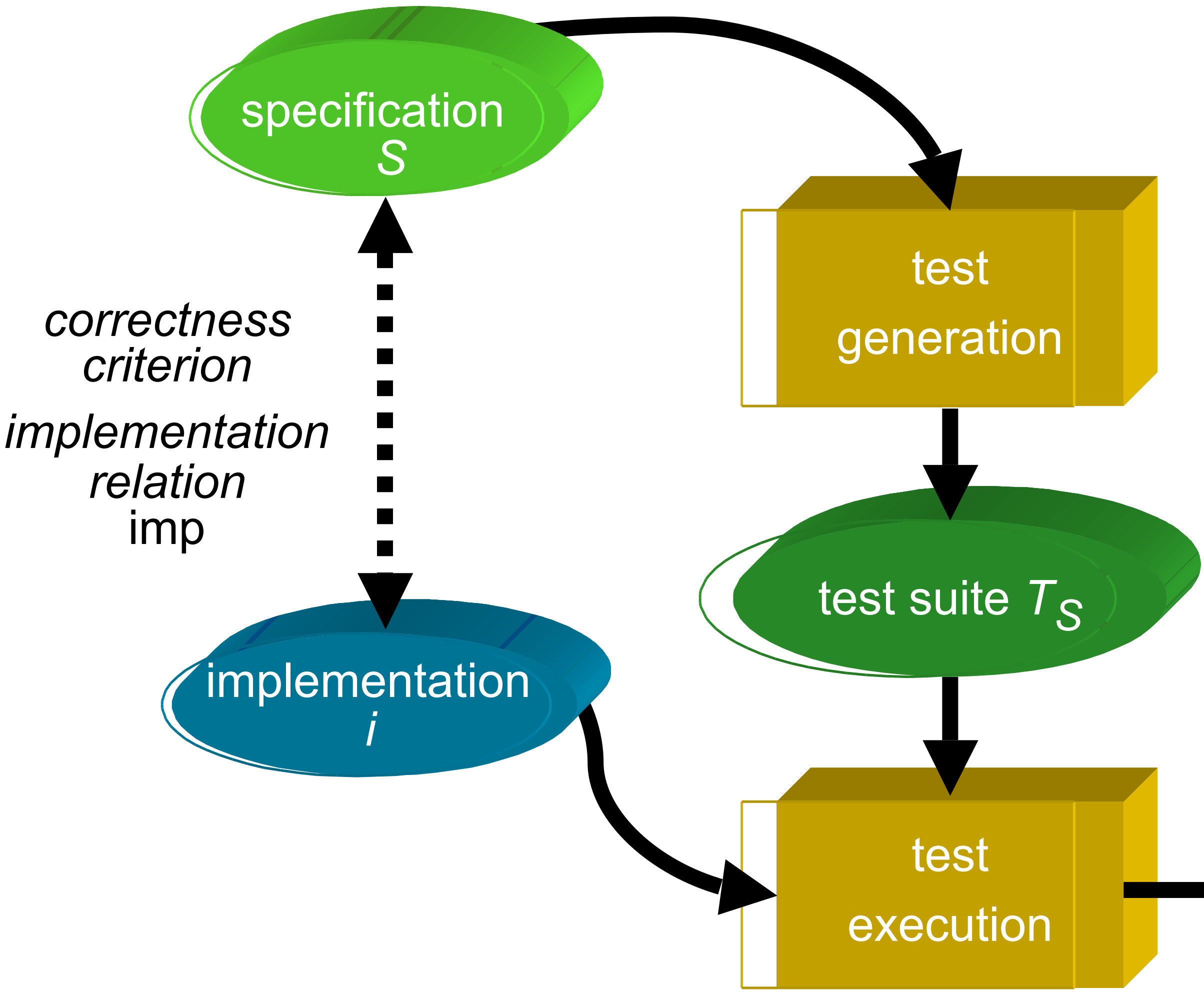
TESTING WITH FORMAL METHODS

- Testing with respect to a formal specification
- Precise, formal definition of correctness :
  good and unambiguous basis for testing
- Formal validation of tests
- Algorithmic derivation of tests :
  tools for automatic test generation
- Allows to define measures expressing coverage
  and quality of testing

CHALLENGES OF TESTING THEORY

- Infinity of testing:
  - too many possible input combinations: infinite breadth
  - too many possible input sequences: infinite depth
  - too many invalid and unexpected inputs
- Exhaustive testing never possible:
  - when to stop testing ?
  - how to invent effective and efficient test cases with high probability of detecting errors ?
- Optimization problem of testing yield vs. effort
  - usually stop when time is over ......

FORMAL TESTING

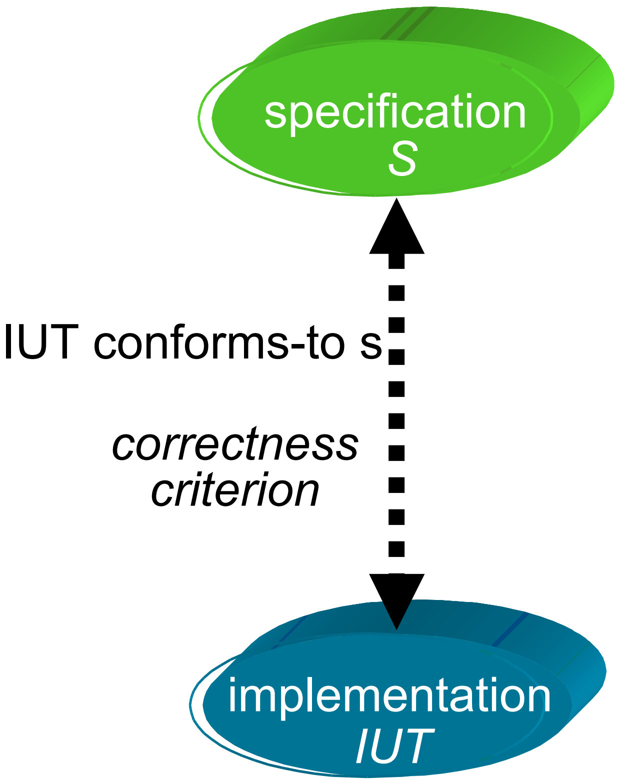


i imp s

exhaustive ⇑ ⇓ *sound*

i passes T_s

FORMAL TESTING : CONFORMANCE



$s \in SPECS$	specification
IUT	implementation under test

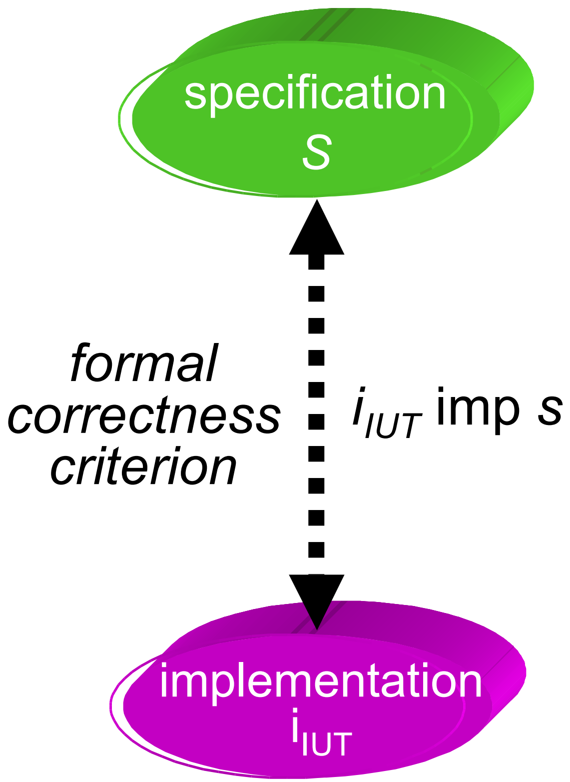
IUT is concrete, physical object

Model the physical world

But *IUT* is black box ! ?

Assume that model i_{IUT} exists

FORMAL TESTING : CONFORMANCE



$s \in SPECS$ Specification

$i_{IUT} \in MODS$ model of *IUT*

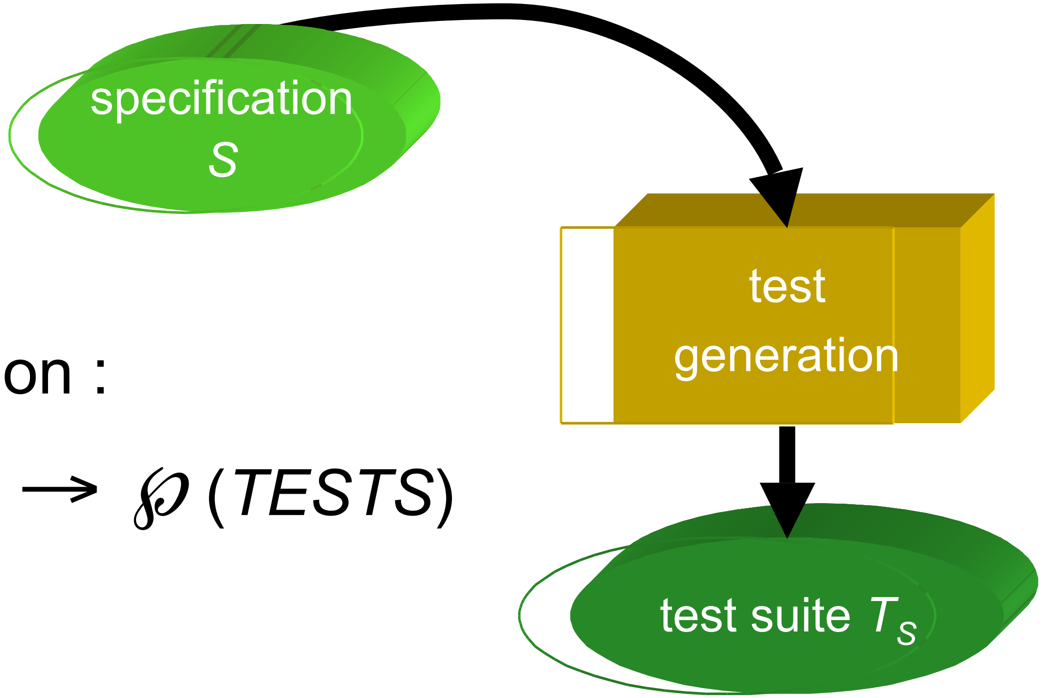
Test assumption :

each concrete *IUT* can be modelled by some $i_{IUT} \in MODS$

Conformance : i_{IUT} *imp* s

i_{IUT} is not known ;
testing to learn about i_{IUT}

FORMAL TESTING : TEST DERIVATION



Test generation :

$der : SPECS \longrightarrow \wp(TESTS)$

Test suite - set of test cases : $T \subseteq TESTS$

Test case : $t \in TESTS$

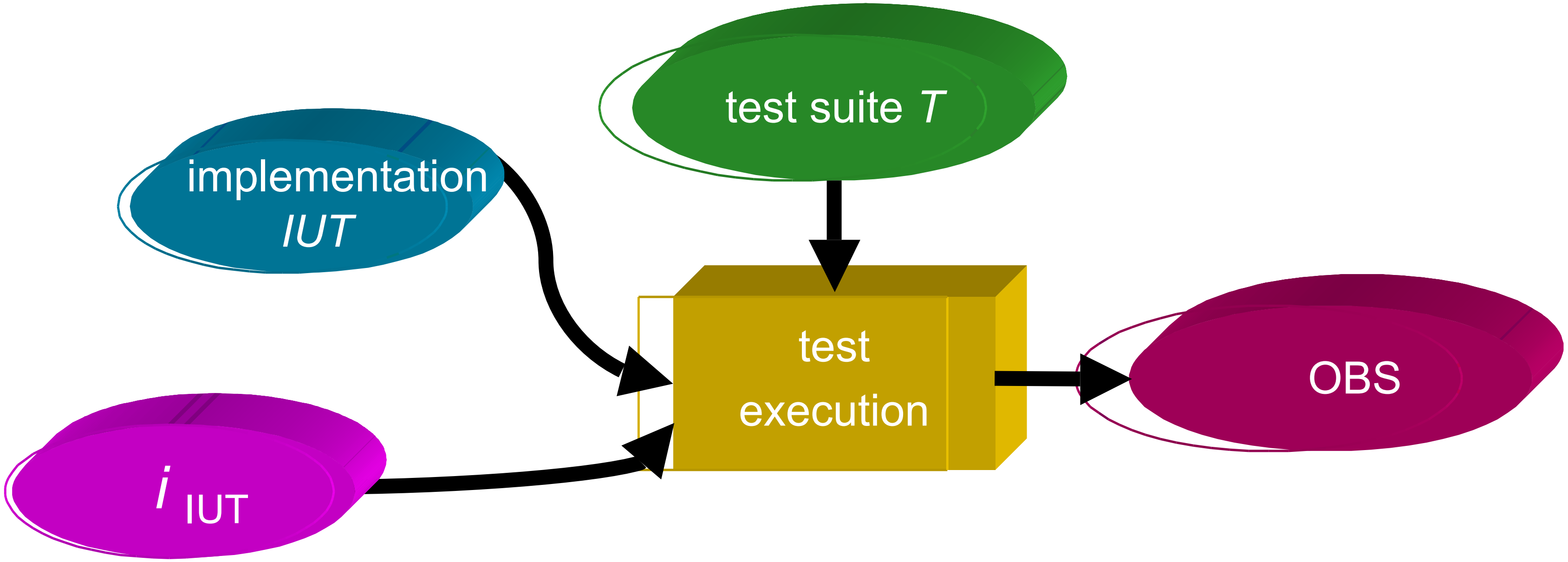
FORMAL TESTING : TEST EXECUTION

Test execution leads to a set of observations :

$$exec : TESTS \times IMPS \longrightarrow \wp(OBS)$$

Model of test execution :

$$obs : TESTS \times MODS \longrightarrow \wp(OBS)$$

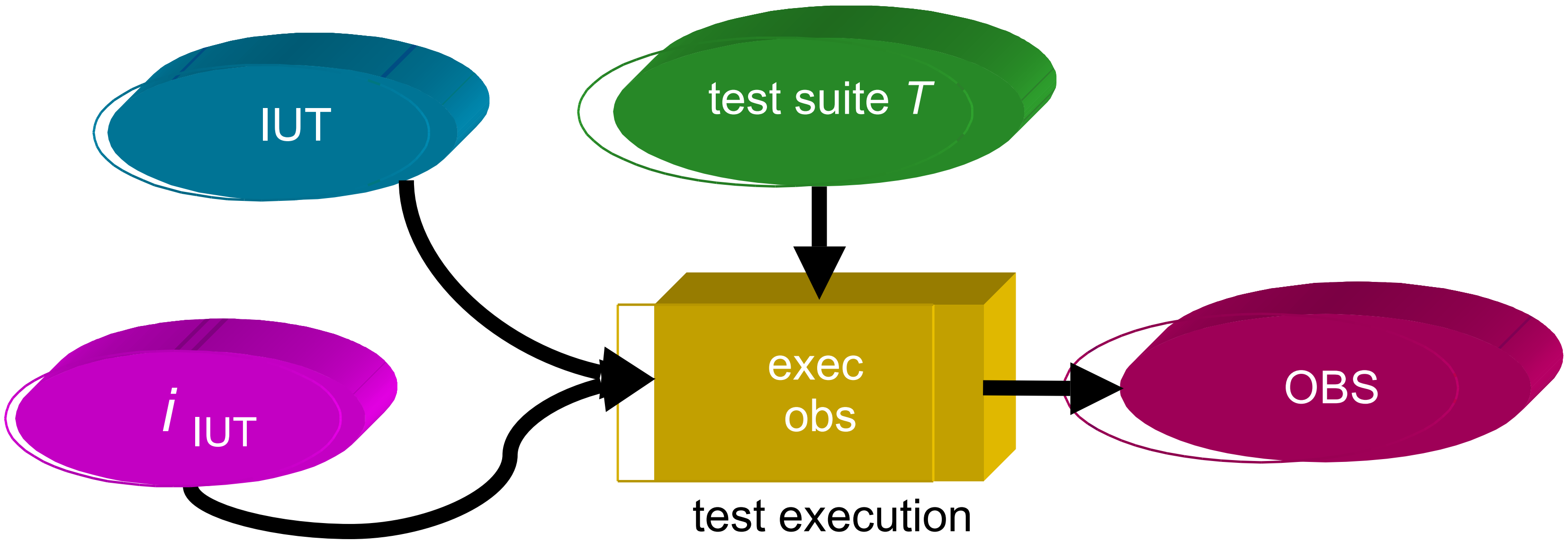


TEST HYPOTHESIS

Observational framework : *TESTS*, *OBS*, *exec*, *obs*

Test hypothesis : for all *IUT* in *IMPS* . $\exists\, i_{IUT} \in MODS$.

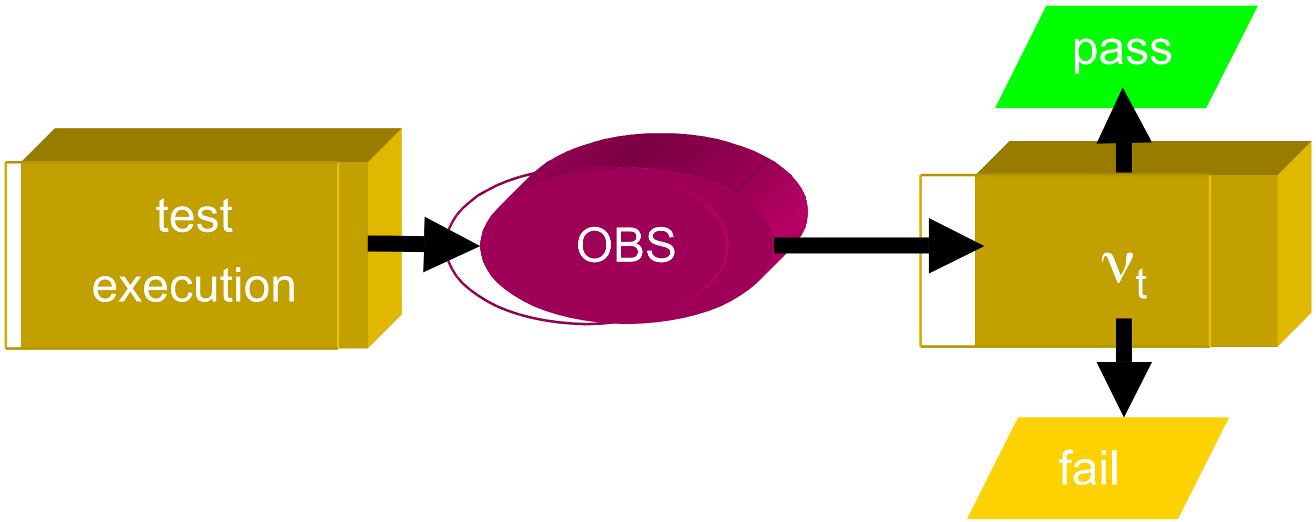
$$\forall t \in TESTS \,.\; exec\,(t, IUT) = obs\,(t, i_{IUT})$$



FORMAL TESTING : VERDICTS

Observations are interpreted :

$$\nu_t : \wp(OBS) \longrightarrow \{\, fail,\ pass \}$$



TESTING FOR CONFORMANCE

IUT *passes* $T_s \overset{?}{\Leftrightarrow}$ *i conforms-to s*

IUT passes $\boldsymbol{T_s}$

$\Leftrightarrow \quad \forall\, t \in T_s \,.\; IUT$ ***passes t***

$\Leftrightarrow \quad \forall\, t \in T_s \,.\; v_t\,(\, exec\,(\, t, IUT\,)\,) = pass$

$\Leftrightarrow \quad \forall\, t \in T_s \,.\; v_t\,(\, obs\,(\, t, i_{IUT}\,)\,) = pass$

$\Leftrightarrow \quad i_{IUT}$ ***imp s***

$\Leftrightarrow \quad$ **IUT conforms-to s**

IUT *passes* $T_s \Leftrightarrow_{def} \forall\, t \in T_s \,.\; IUT$ *passes t*

IUT *passes t* $\Leftrightarrow_{def} v_t\,(\, exec\,(\, t, IUT\,)\,) = pass$

Test hypothesis :

Proof obligation :

$\forall\, i \in MODS$

$(\; \forall\, t \in T_s \,.\; v_t\,(\, obs\,(\, t, i\,)\,) = pass\,) \Leftrightarrow i\ imp\ s$

Definition : *i conforms-to s*

TESTING FOR CONFORMANCE

Proof obligation :

$\forall\ i \in MODS\ .$

$(\ \forall\ t \in T_s\ .\ \nu_t\ (\ obs\ (\ t, i\ )\ )\ =\ pass\ )\ \Leftrightarrow\ \ i\ imp\ s$

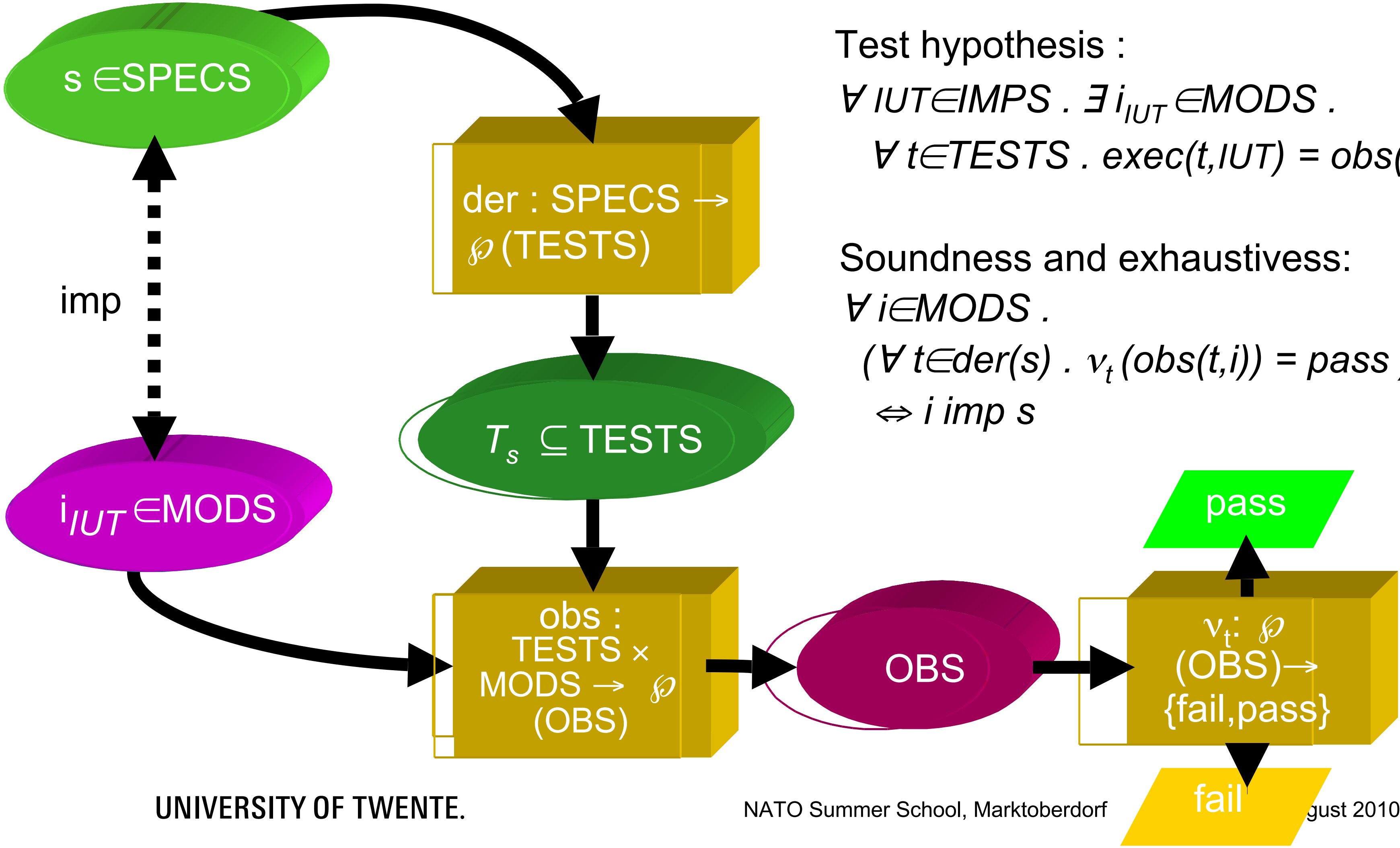
Proof of completeness on model leads to completeness for tested systems :

exhaustive

IUT *passes* T_s $\Rightarrow$ / $\Leftarrow$ *i conforms-to s*

sound

FORMAL TESTING



Test hypothesis :

$\forall\, IUT \in IMPS\ .\ \exists\, i_{IUT} \in MODS\ .$

$\quad \forall\, t \in TESTS\ .\ exec(t, IUT) = obs(t, i_{IUT})$

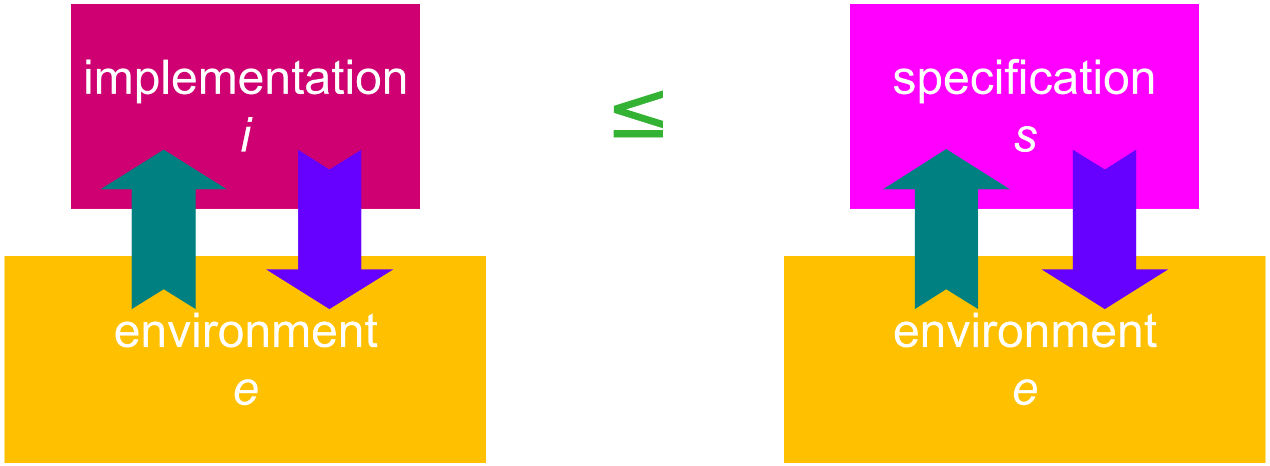
Soundness and exhaustivess:

$\forall\, i \in MODS\ .$

$\quad (\forall\, t \in der(s)\ .\ \nu_t\,(obs(t,i)) = pass\ )$

$\quad \Leftrightarrow\ i\ imp\ s$

TESTING PREORDERS



For all environments *e*
all observations of an implementation *i* in *e*
should be explained by
observations of the specification *s* in *e*.

$$i \leq s \quad \Leftrightarrow \quad \forall\, e \in \mathit{Env} : \quad \mathit{obs}\,(\, e, i\,) \subseteq \mathit{obs}\,(e, s\,)$$

? ? ?

LABELLED TRANSITION SYSTEMS

An LTS is a tuple $A = \langle S, S^0, L, \rightarrow \rangle$ with

- S a set of states
- $S^0 \subseteq S$ a nonempty set of initial states
- L a set of labels; $L_\tau = L \cup \{\tau\}$ with τ the invisible action
- $\rightarrow \subseteq S \times L_\tau \times S$ the transition relation;

We write :

- $s \xrightarrow{a} s'$ for $(s,a,s') \in \rightarrow$
- $s \xrightarrow{\sigma} s'$ for $\sigma = a_1 \ldots a_n$ and $s = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \ldots \xrightarrow{a_n} s_n$
- $s \xRightarrow{\sigma} s'$ for $\sigma = a_1 \ldots a_n$ and $s = s_0 \xrightarrow{\tau^{k_1}} \xrightarrow{a_1} \xrightarrow{\tau^{m_1}} s_1 \xrightarrow{\tau^{k_2}} \xrightarrow{a_2} \xrightarrow{\tau^{m_2}} \ldots \xrightarrow{\tau^{k_n}} \xrightarrow{a_n} \xrightarrow{\tau^{m_n}} s_n$
- $CTraces = \{ \sigma \mid \exists s_0 \in S_0 . s_0 \xRightarrow{\sigma} s \wedge s \not\xRightarrow{a} \ for\ any\ a \in L \}$

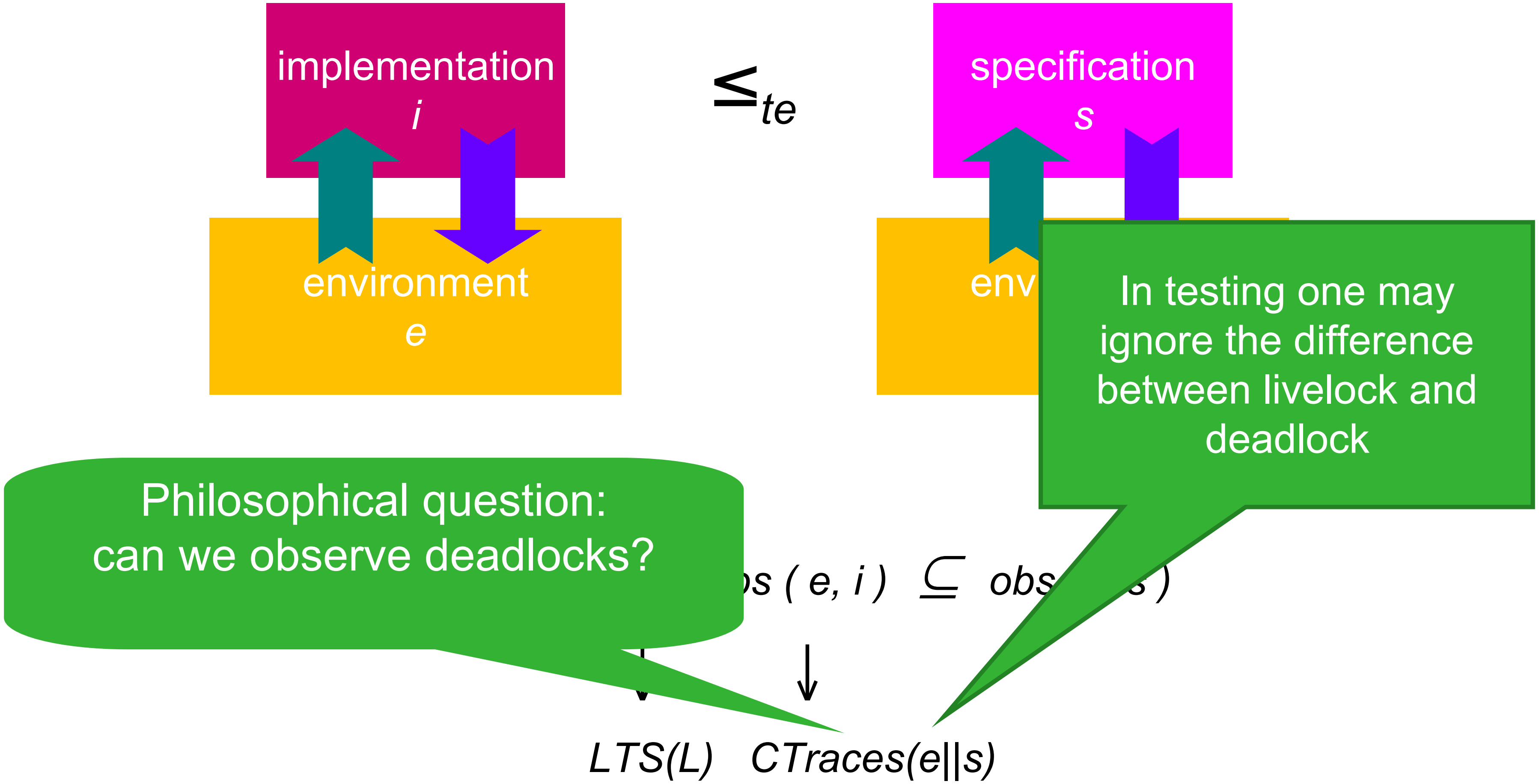
PARALLEL COMPOSITION

Let $A =$ and $B = \left\langle S_2 , S_2^0, L_2, \rightarrow_2 \right\rangle$ be two LTSs.

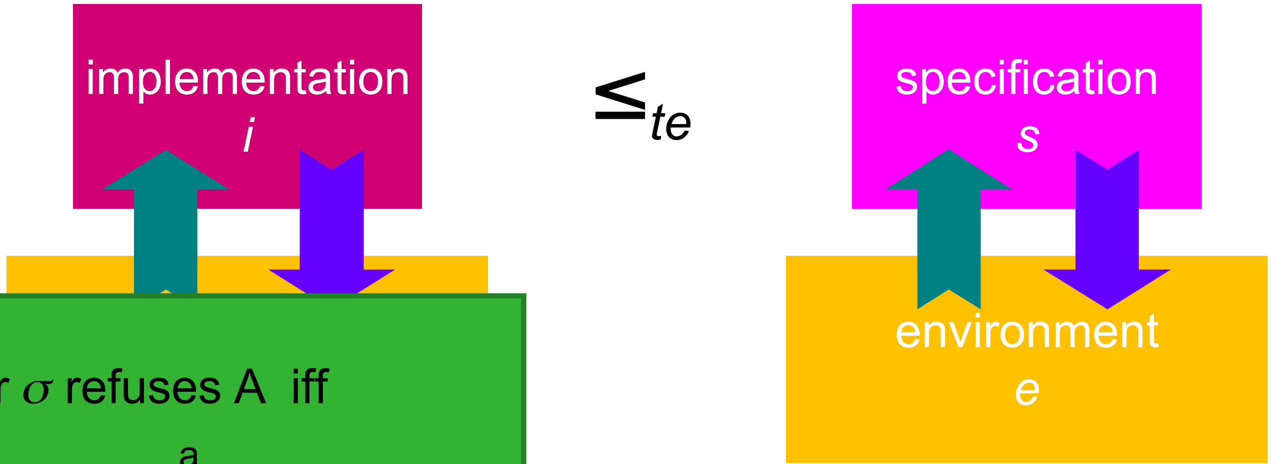
Then $A \| B = \left\langle S_1 \times S_2, \left(S_1^0, S_2^0\right), L_1 \cup L_2, \rightarrow \right\rangle$ with

$$\rightarrow = \{ ((s,t), a, (s',t')) \mid (s,a,s') \in \rightarrow_1, (t,a,t') \in \rightarrow_2, a \neq \tau \}$$
$$\cup \{ ((s,t), a, (s',t)) \mid \mid (s,a,s') \in \rightarrow_1, t \in S_2, a \in (L_1 \setminus L_2) \cup \{\tau\} \}$$
$$\cup \{ ((s,t), a, (s,t')) \mid \mid (t,a,t') \in \rightarrow_2, s \in S_1, a \in (L_2 \setminus L_1) \cup \{\tau\} \}$$

CLASSICAL TESTING PREORDER



TESTING PREORDER



p after σ refuses A iff

$p \stackrel{\sigma}{\Rightarrow} p'$ and $p' \stackrel{a}{\not\Rightarrow}$ for all $a \in A$

$i \leq_{te} s$ … $\sigma \in L^*$,

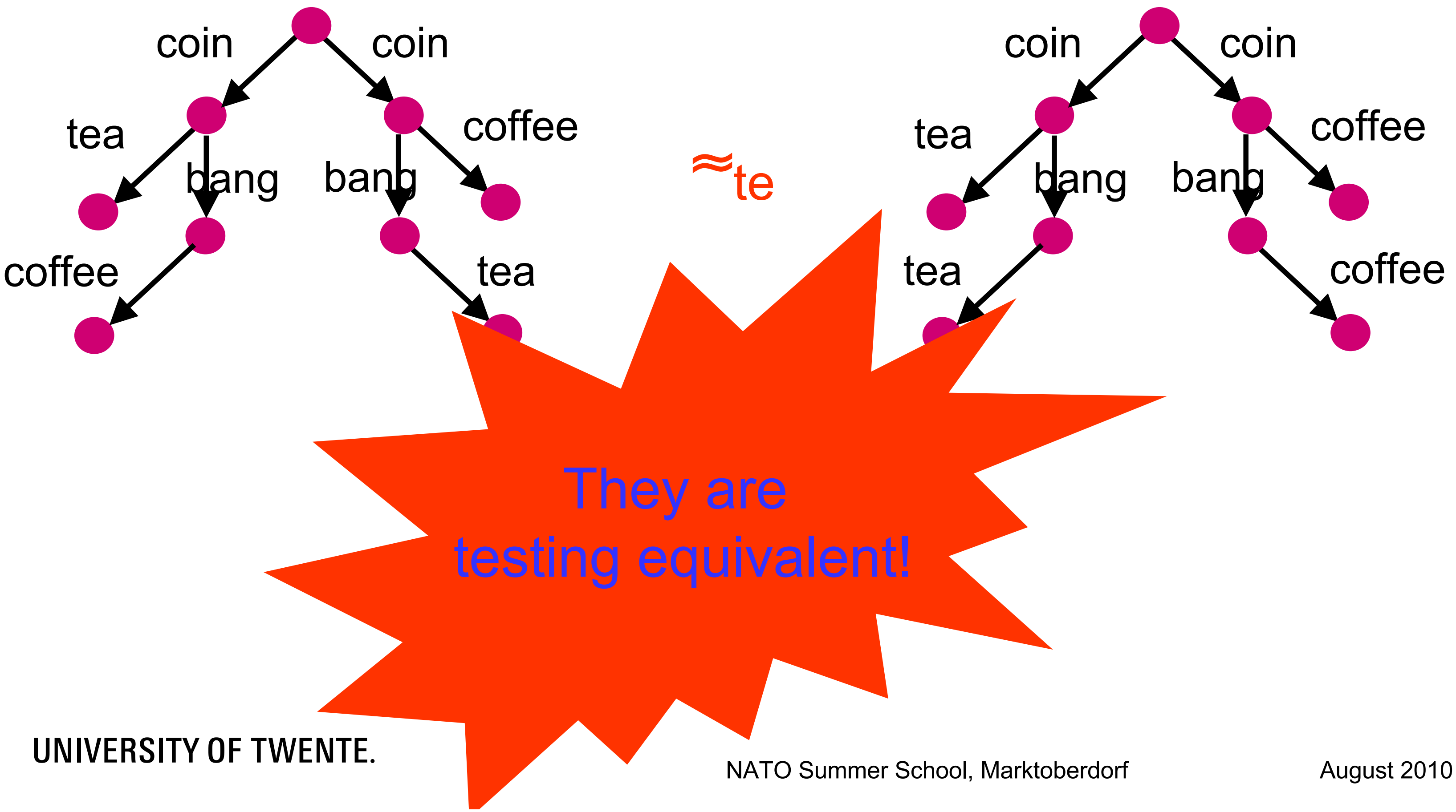
{ e||i deadlocks after σ } $\subseteq$ { e||s deadlocks after σ }

$\Leftrightarrow \quad FP(i) \subseteq FP(s)$

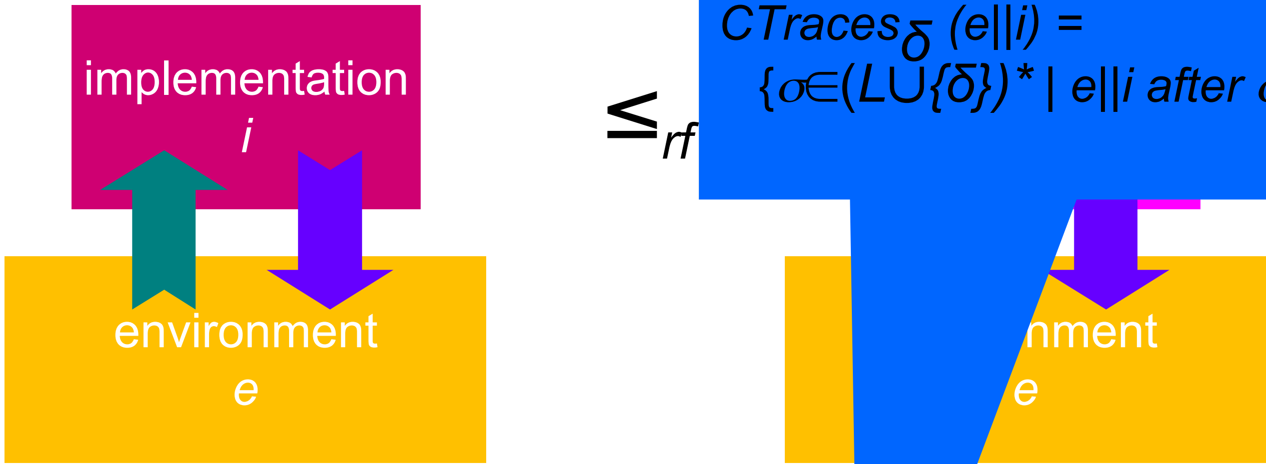
$FP(p) = \{ \langle \sigma, A \rangle \mid p \text{ after } \sigma \text{ refuses } A \}$

Can we distinguish between these machines?

QUIRKY COFFEE MACHINE [Langerak]



REFUSAL PREORDER



CTraces$_\delta$ *(e||i)* =
$\{\sigma \in (L \cup \{\delta\})^* \mid e||i \text{ after } \sigma \text{ refuses } L\}$

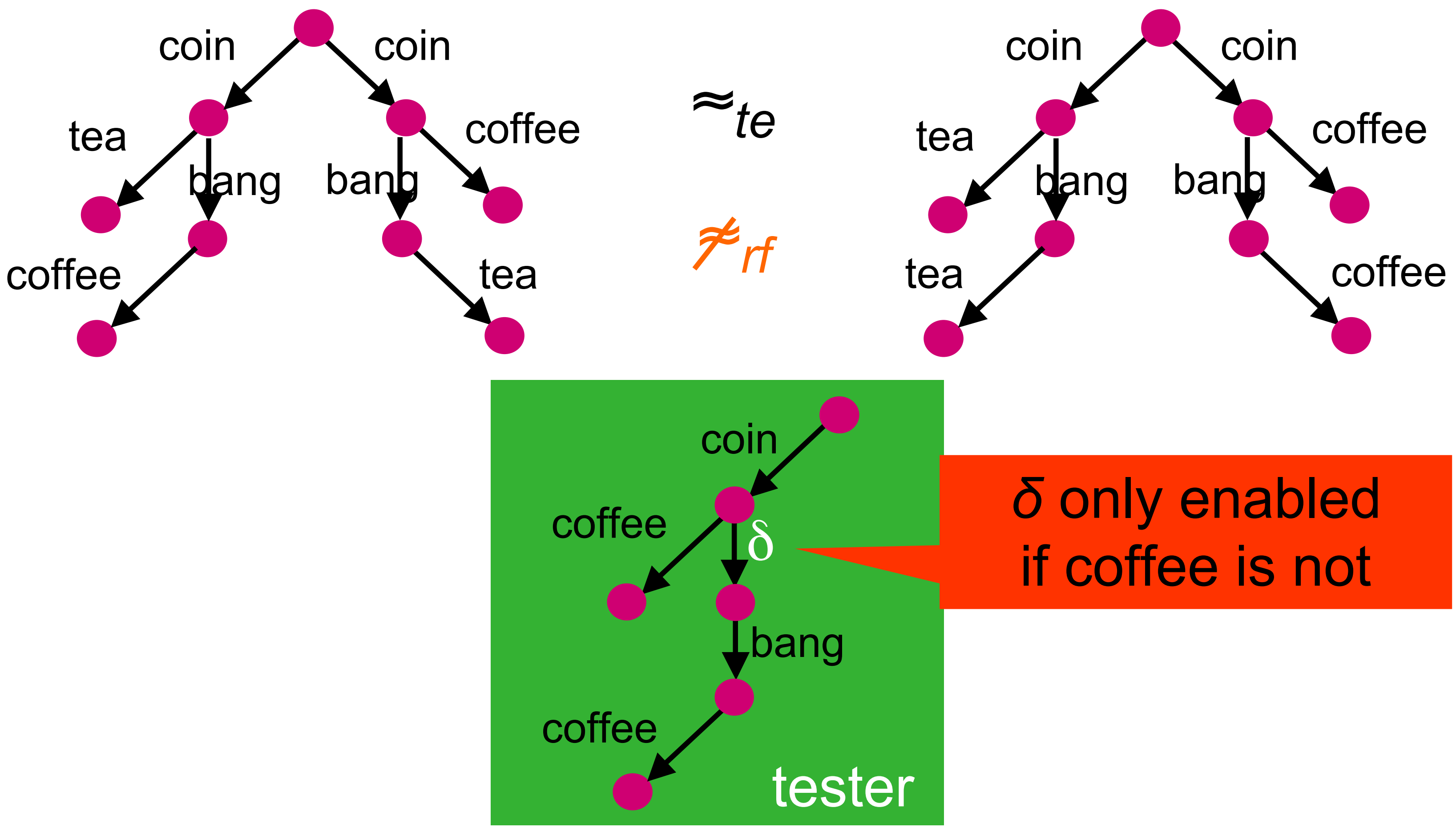
$i \leq_{rf} s \quad \Leftrightarrow \quad \forall\, e \in E \,.\; obs\,(e, i) \subseteq obs\,(e, s)$

↓ ↓

$LTS(L \cup \{\delta\})$ $\quad CTraces_\delta(e||i)$

e observes with δ deadlock on all alternative actions

QUIRKY COFFEE MACHINE REVISITED



CONTENTS

- Introduction control-oriented testing
- Input-output conformance testing
- Real-time conformance testing
- Test coverage measures

CONTENTS

I/O TRANSITION SYSTEMS

- testing actions are usually directed, i.e. there are inputs and outputs

  $L = L_{in} \cup L_{out}$ with $L_{in} \cap L_{out} = \emptyset$

- systems can always accept all inputs: *input enabledness*

  for all states s, for all $a \in L_{in}$ $s \stackrel{a}{\Rightarrow}$

- testers are I/O systems
  - output (stimulus) is input for the SUT
  - input (response) is output of the SUT

QUIESCENCE

- Because of input enabledness $S||T$ deadlocks iff T produces no stimuli and S no responses. This is known as *quiescence*
- Observing quiescence leads to two implementation relations for I/O systems I and S :

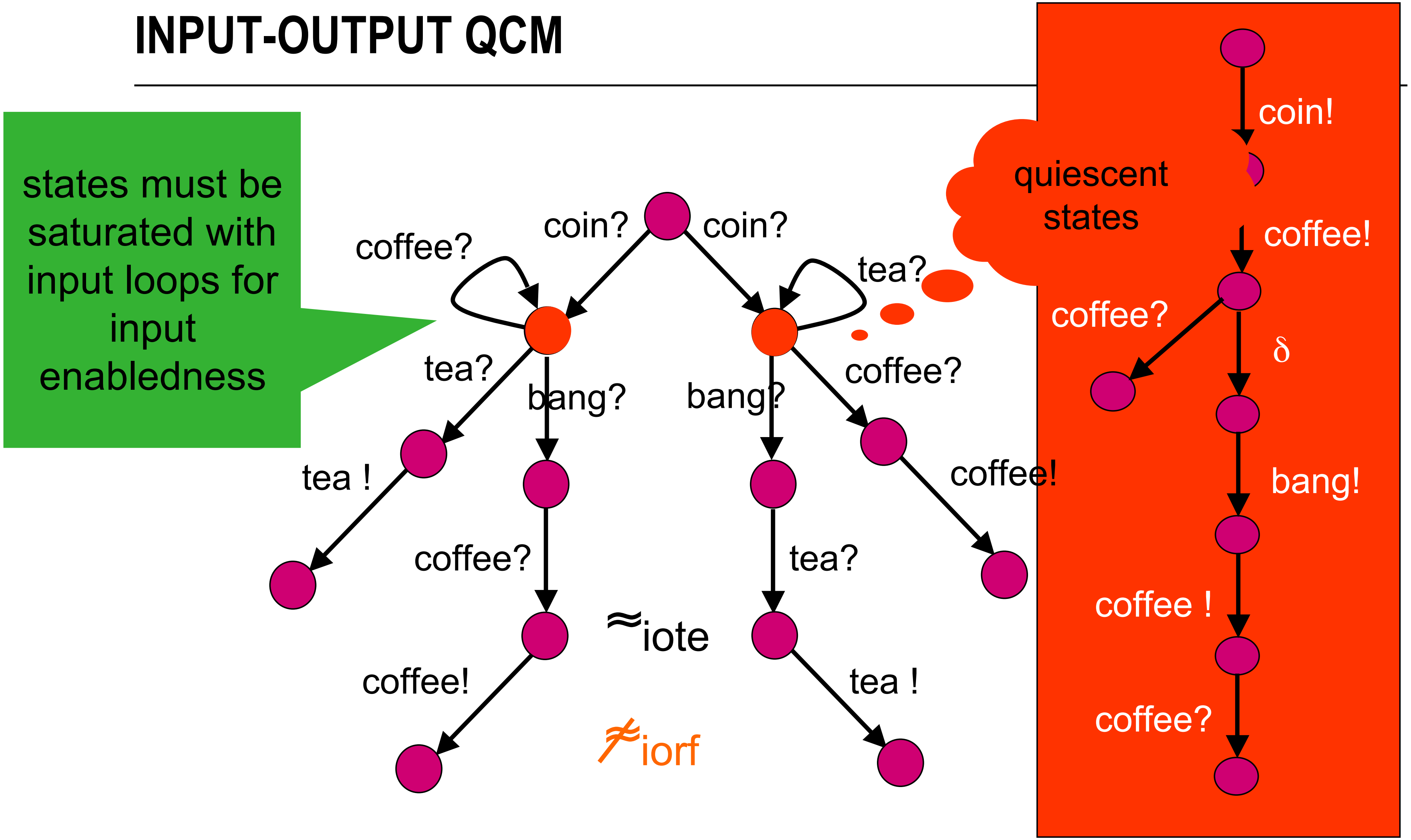
  ✍ $I \leq_{iote} S$ iff for all I/O testers T :

  $CTraces(I||T) \subseteq CTraces(S||T)$ *(quiescence)*

  2. $I \leq_{iorf} S$ iff for all I/O testers T :

  $CTraces_{\delta}(I||T) \subseteq Ctraces_{\delta}(S||T)$ *(repetitive quiescence)*

INPUT-OUTPUT QCM



QUIESCENT LABELLED TRANSITION SYSTEMS

A QLTS is an LTS $A = \langle S, S^0, L_1 \cup L_O^\delta, \rightarrow \rangle$

with special (output) label δ

such that if $s \xrightarrow{\delta} s'$ then $s' \xrightarrow{\delta} s'$ and s' is quiescent.

This definition is closed under determinisation.

Let $A = \langle S, S^0, L, \rightarrow \rangle$ be an LTS with $L = L_I \cup L_O$ and $\delta \notin L$,

then its underlying QLTS $\delta(A)$ is the QLTS

$\langle S, S^0, L \cup \{\delta\}, \rightarrow' \rangle$ with

$\rightarrow' = \rightarrow \cup \{(s, \delta, s) \mid s \in S, s$ is quiescent$\}$

Moreover, $traces_{\delta(A)} = traces_A \setminus \{\delta\}$

IMPLEMENTATION RELATION IOCO

Let i and s be be QTLSs
(possibly after applying $\delta(.)$)
over $L = L_I \cup L_O^\delta$, then we define

$$i \subseteq_{iorf} s \quad \text{iff} \quad \forall \sigma \in L^* \; out_i(\sigma) \subseteq out_s(\sigma)$$

For implementations we will require input-enabledness,

But not for specifications.

In this setting it makes sense to restrict testing

to the traces of the implementation:

$$i \subseteq_{ioco} s \quad \text{iff} \quad \forall \sigma \in traces_s \; out_i(\sigma) \subseteq out_s(\sigma)$$

INTUITION BEHIND *IOCO*

$$i \subseteq_{ioco} s \quad \text{iff} \quad \forall \sigma \in traces_s \; out_i(\sigma) \subseteq out_s(\sigma)$$

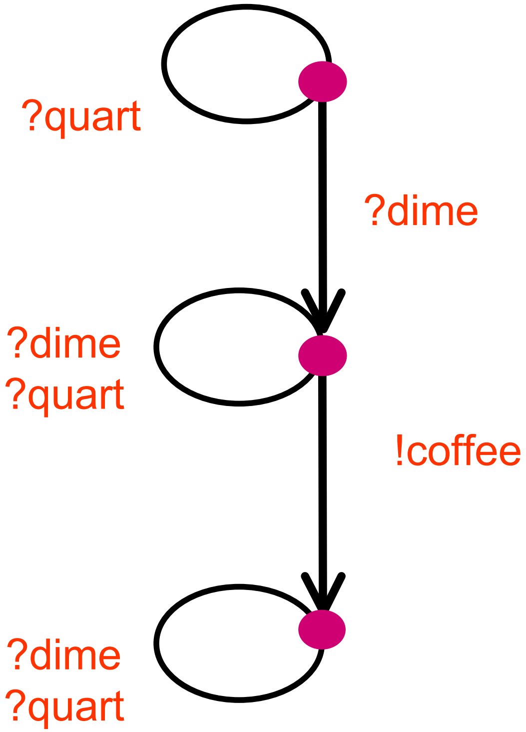
Intuition:

i ioco-conforms to *s*, iff

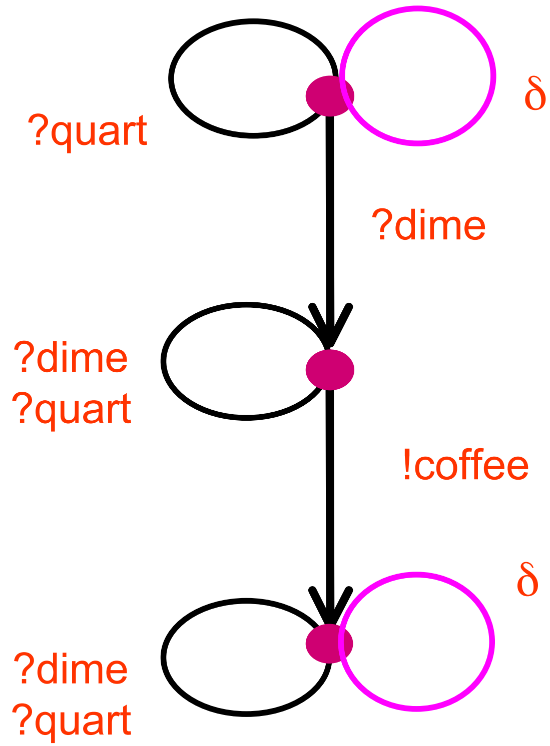
1. if *i* produces output *x* after a specified trace σ,
   then *s* can produce *x* after σ
2. if *i* cannot produce any output after a specified trace σ,
   then *s* cannot produce any output after σ (*quiescence* δ)

ADDING QUIESCENCE

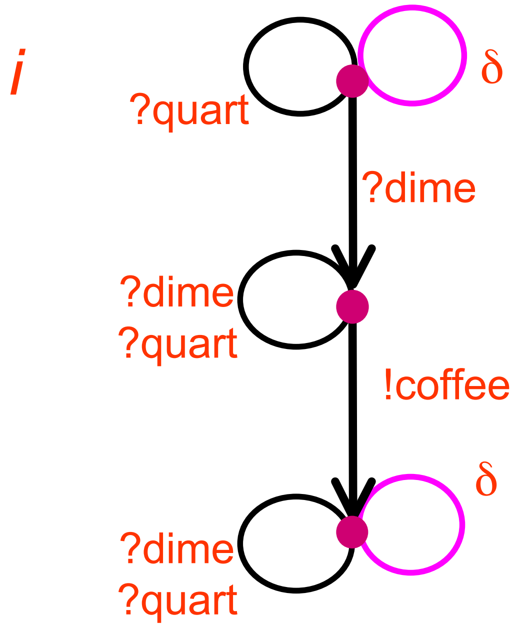
i



δ(i)



CALCULATING *OUT*



$out_i(\varepsilon)$ = { δ }

out_i(?dime) = { !coffee }

out_i(?dime.?dime = { !coffee }

out_i(?dime.!coffee) = { δ }

out_i(?quart) = { δ }

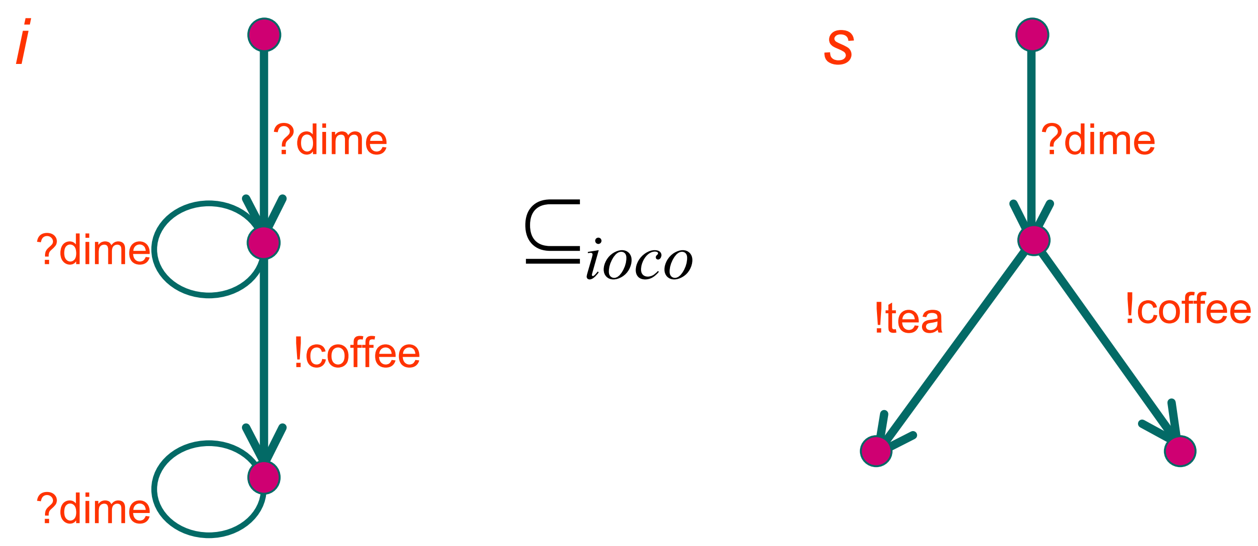
out_i(!coffee) = ∅

out_i(?dime.!tea) = ∅

$out_i(\delta)$ = {δ }

IMPLEMENTATION RELATION *IOCO*

$$i \subseteq_{ioco} s \quad \text{iff} \quad \forall \sigma \in traces_s \; out_i(\sigma) \subseteq out_s(\sigma)$$

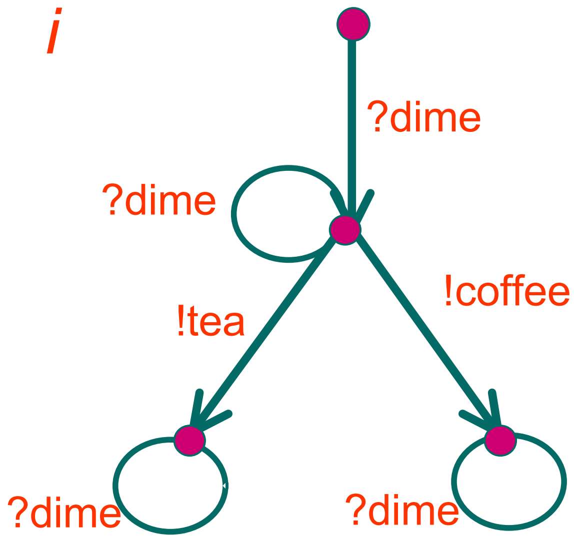


out_i(?dime) = { !coffee }

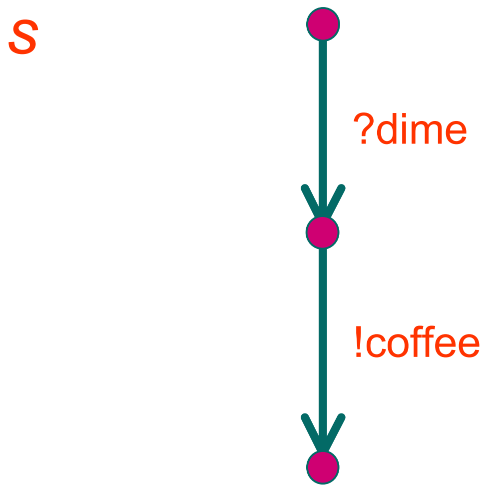
out_s(?dime) = { !coffee, !tea }

IMPLEMENTATION RELATION *IOCO*

$$i \subseteq_{ioco} s \quad \text{iff} \quad \forall \sigma \in traces_s \; out_i(\sigma) \subseteq out_s(\sigma)$$



$$\not\subseteq_{ioco}$$

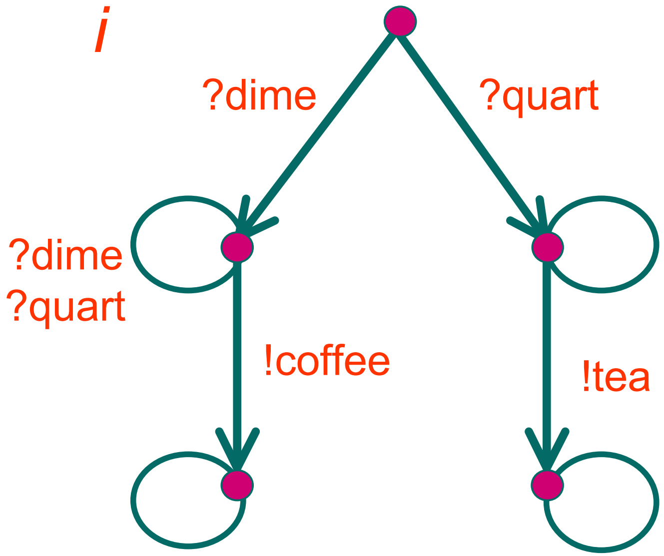


out_i(?dime) = { !coffee, !tea } $\not\subset$ out_s(?dime) = { !coffee}

IMPLEMENTATION RELATION *IOCO*

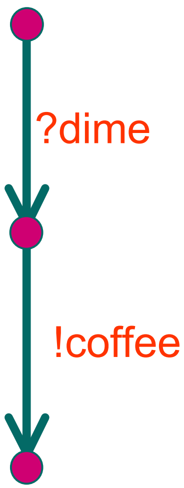
$i \sqsubseteq_{ioco} s$ iff $\forall \sigma \in traces_s \; out_i(\sigma) \subseteq out_s(\sigma)$

i



$\sqsubseteq_{ioco}$

s



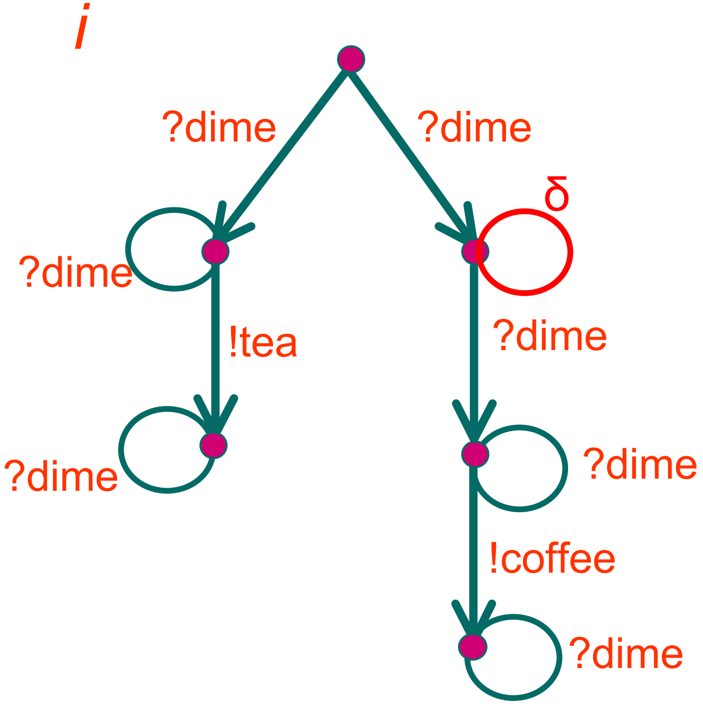
out_i (?dime) = { !coffee }
out_i (?quart) = { !tea }

out_s (?dime) = { !coffee }
out_s (?quart) = $\emptyset$

But ?quart $\notin Traces_\delta(s)$

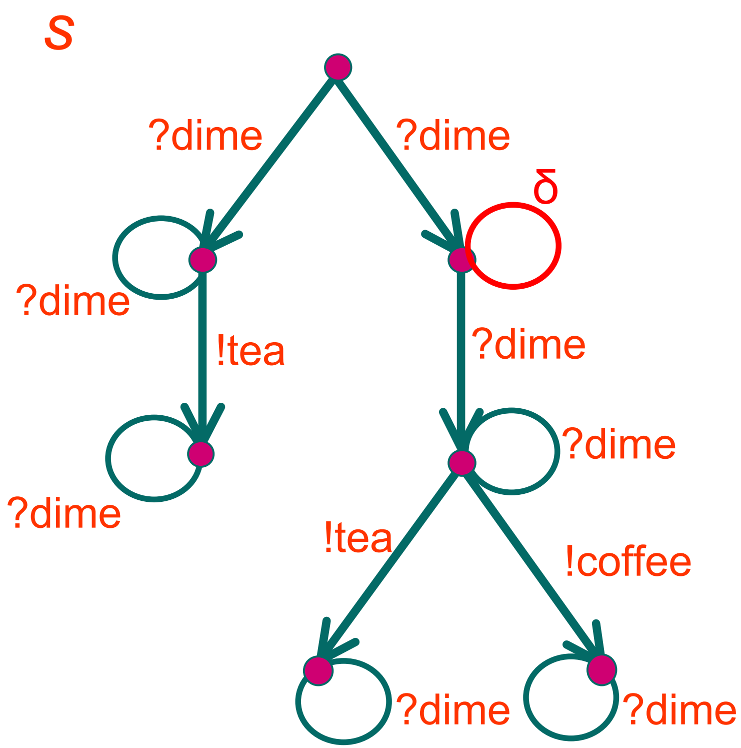
IMPLEMENTATION RELATION *IOCO*

$i \subseteq_{ioco} s$ iff $\forall \sigma \in traces_s\ out_i(\sigma) \subseteq out_s(\sigma)$



$i \subseteq_{ioco} s$

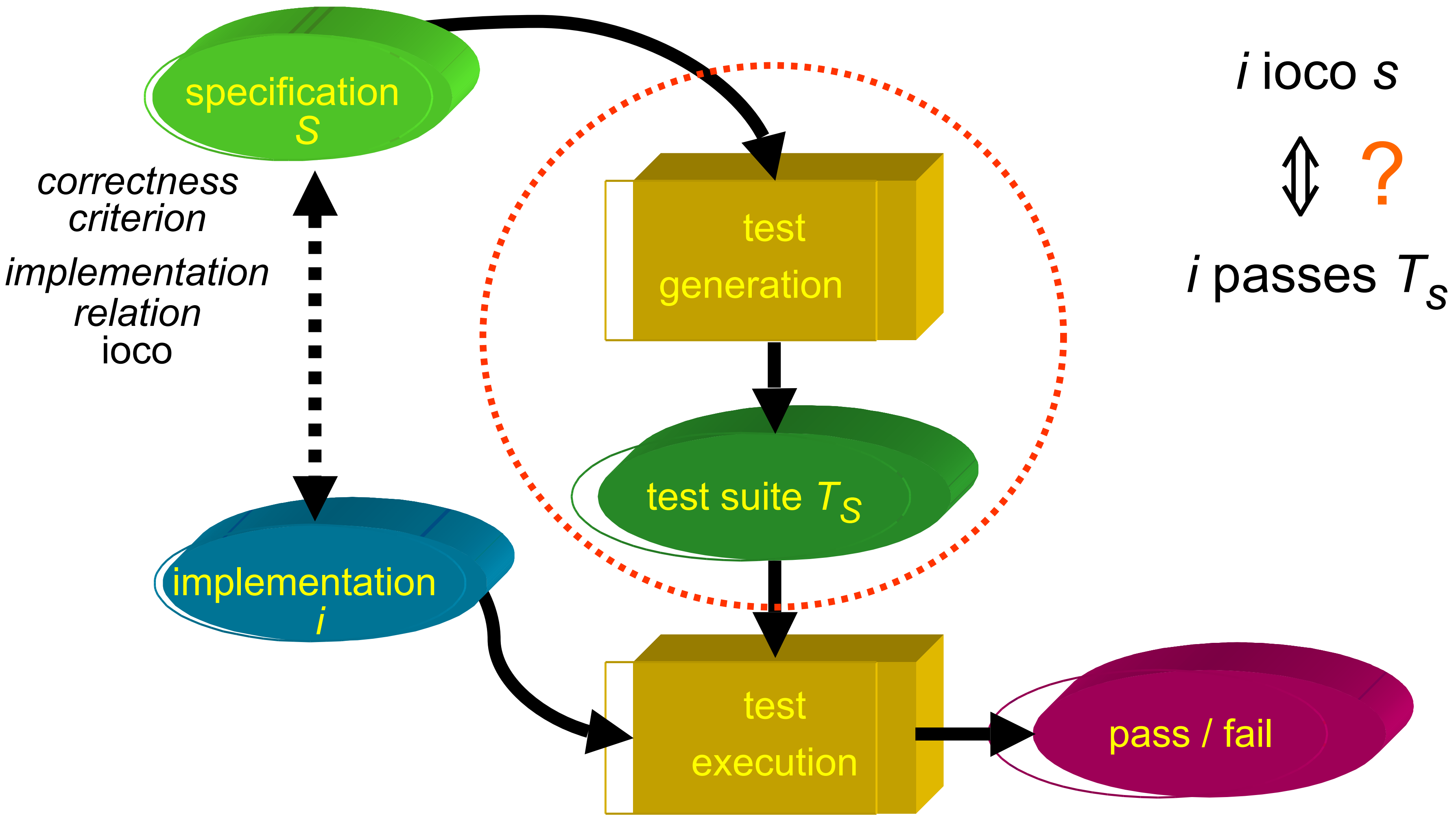
$s \not\subseteq_{ioco} i$



out_i (?dime.? dime) = out_s (? dime.? dime) = { !tea, !coffee }

out_i (? dime.δ.? dime) = { !coffee } ≠ out_s (? dime.δ.? dime) = { !tea, !coffee }

FORMAL TESTING



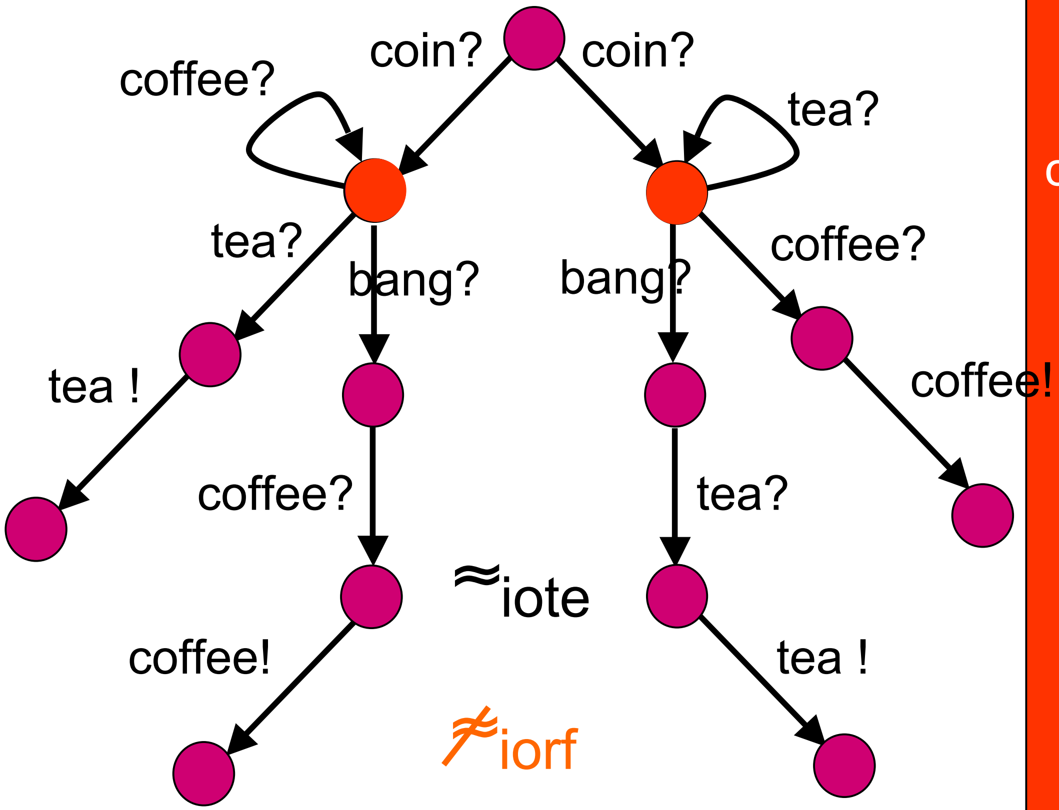
TEST CASES

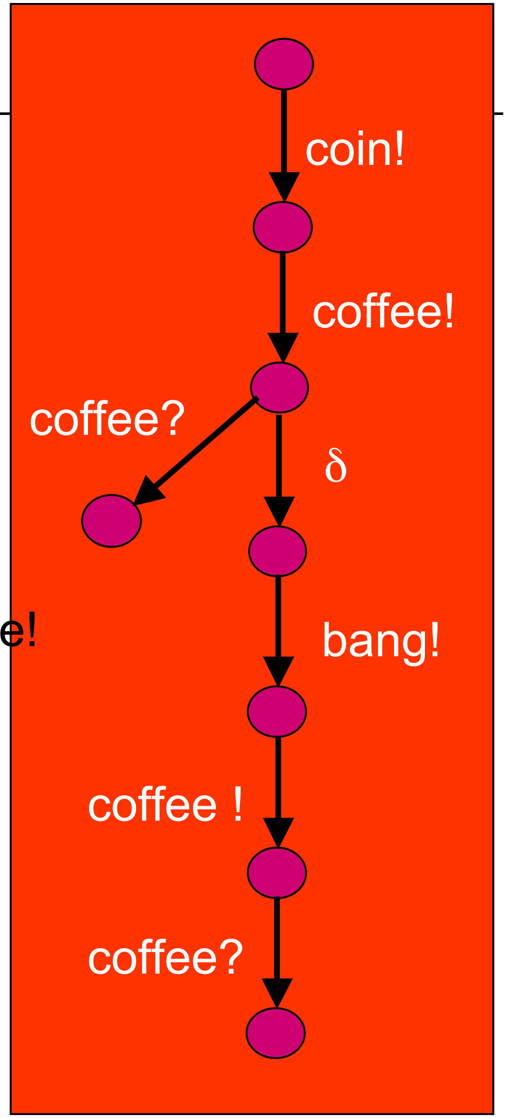
A test (case) t over $L=L_I \cup L^{\delta}_O$ is an LTS with

- t is deterministic
- t does not contain an infinite
- t is acyclic and connected
- for all states s of t we have
  - $after(s)= \emptyset$, or (termination)
  - $after(s)= L^{\delta}_O$, or (response observation)
  - $after(s)= \{a?\} \cup L_O$ (stimulus)

Alternatively, a test case can be characterised by the prefix-closed set of its traces

INPUT-OUTPUT QCM AGAIN





TEST ANNOTATIONS

Let *t* be a test case:

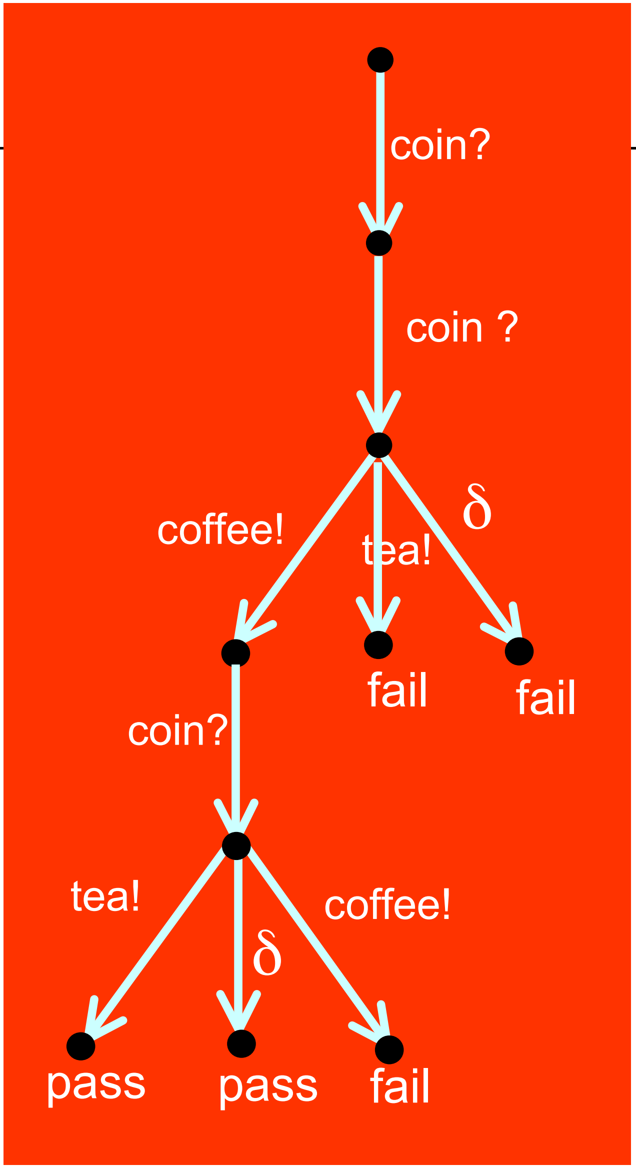
- an annotation of *t* is a function

  a: $Ctraces_t \rightarrow \{ pass, fail \}$
- the pair $\dot{t} = (t,a)$ is an annotated test case

When *a* is clear from the context, or irrelevant, we use *t* for both test case and its annotation.

ANNOTATED TEST CASES VS TTCN

test case t	
!coin	
!coin ; Start timer1	
?tea	fail
?timer1	fail
?coffee	
!coin ; Start timer2	
?tea	pass
?timer2	pass
?coffee	fail



EXECUTION AND EVALUATION

Let *A* be a QLTS over *L* and *t* a test over *L.*

The executions of *t* with *A* are defined as

- $exec_t(A) = Ctraces(t||A)$
- in fact, $exec_t(A) = Ctraces(t) \cap traces($

This can be lifted in the obvious way to sets of tests, i.e. test suites.

Let $\dot{t} = (t,a)$ be an annotated test case.

The verdict of $\dot{t}$ is the function

$v_{\dot{t}}$:QLTS(*L*) → {*pass*,*fail*} with

$$v_{\dot{t}}(A) = \begin{cases} pass & \text{if for all } \sigma \in exec_t(A)\ \ a(\sigma) = pass \\ fail & \text{otherwise} \end{cases}$$

A SOUND AND COMPLETE TEST SUITE

Given a specification *s* we define the annotation

$a_s^{ioco}(\sigma)$ = *fail* if $\exists \sigma_1 \in traces_s$, …
and $\sigma_1 a \notin tr$…
pass otherwise

Tests(*s*) contains all tests over the same label set *L* as *s*

Given *s* and any $t \in Tests(s)$, its annotated version (t, a_s^{ioco}) is *sound* w.r.t. *s* under $\sqsubseteq_{ioco}$.

The test suite $T = \{(t, a_s^{ioco}) \mid t \in Tests(s)\}$ is *sound* and *complete* w.r.t. *s* under $\sqsubseteq_{ioco}$.

DESIRABLE TEST CASE PROPERTIES

Let *s* be specification over a label set *L*, then

- a test *t* is *fail-fast* w.r.t. *s* if
  $\sigma \notin traces_s$ implies that $\forall a \in L\ \sigma a \notin t$

- a test *t* is *input-minimal* w.r.t. *s* if
  for all $\sigma a? \in t$ with $a? \in L_I$ it holds that
  $\sigma \in traces_s$ implies $\sigma a? \in traces_s$

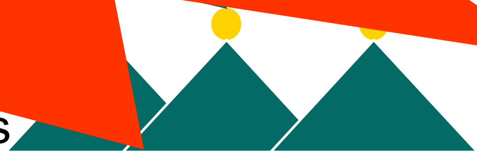
ANNOTATED TEST GENERATION AL... THM

To g... erate a test case ... ystem
speci... ith *S* s ... *S*)

Apply t...

fail-fast, input-minimal,
ioco-sound &
(in the limit) ioco-complete

...d outputs *o*!



... outputs

t(*S after o*!)

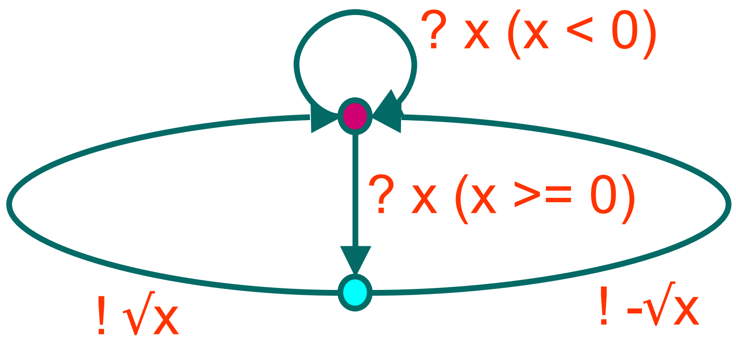
...ve ou... (no δ)

t(*S after i*?)

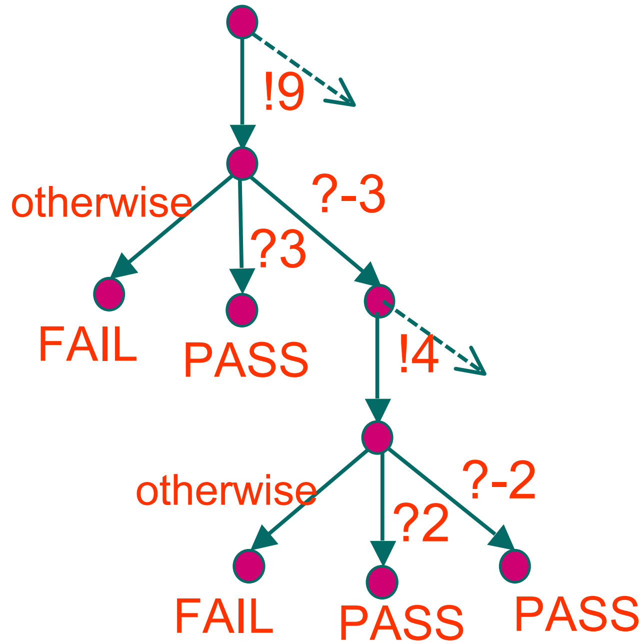
TEST GENERATION EXAMPLE

Equation solver for $y^2=x$

specification

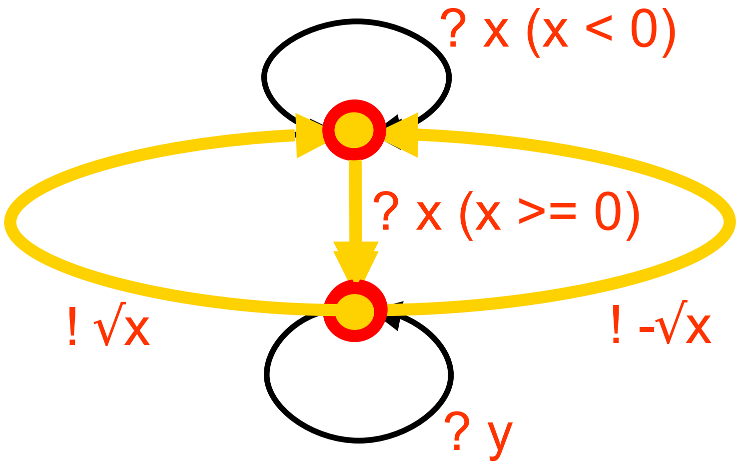


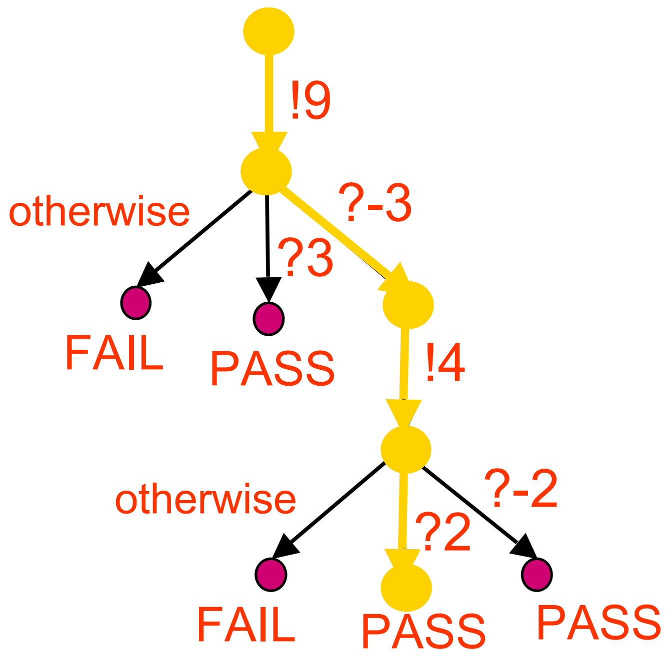
test



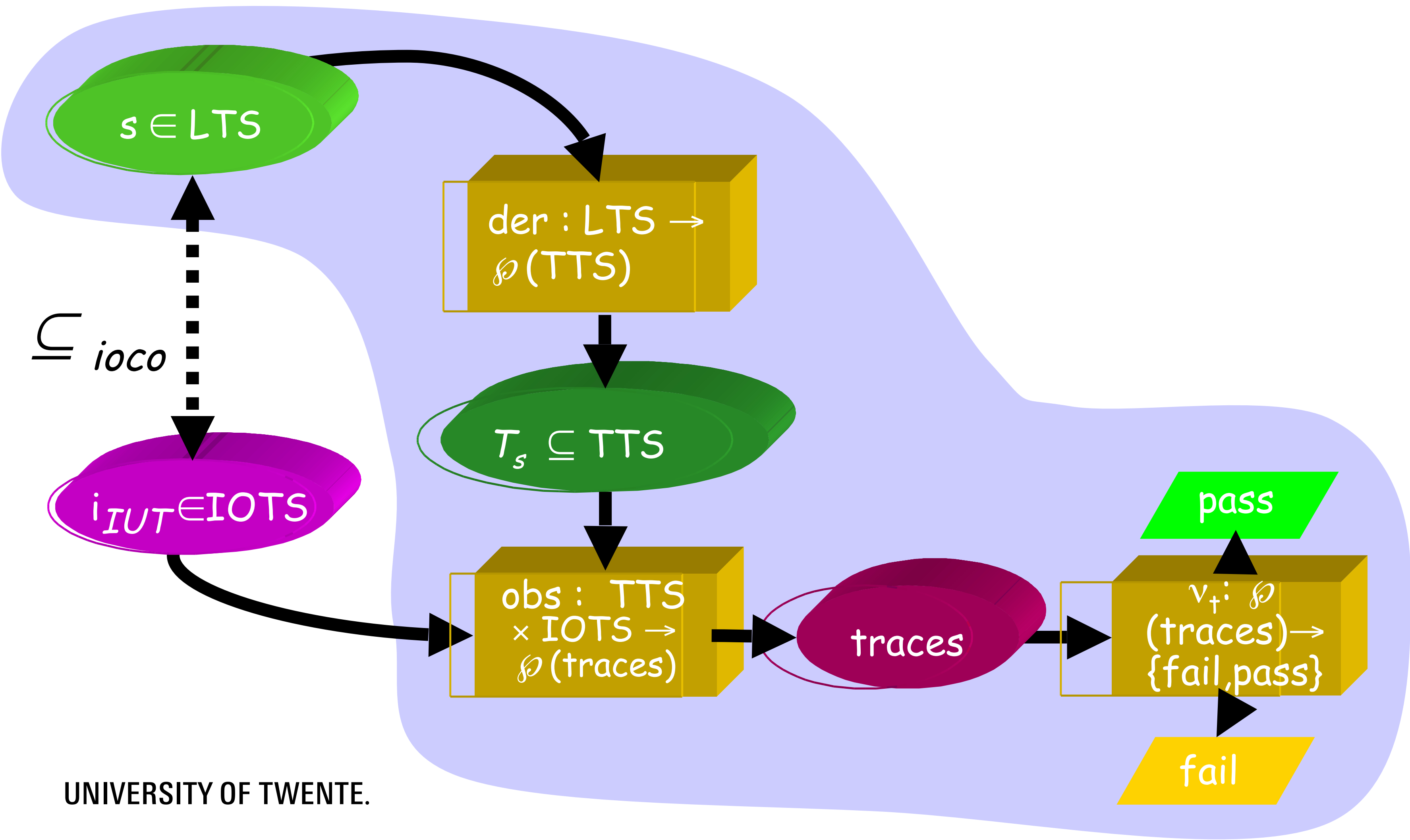
TEST EXECUTION EXAMPLE

implementation || test





FORMAL TESTING WITH TRANSITION SYSTEMS

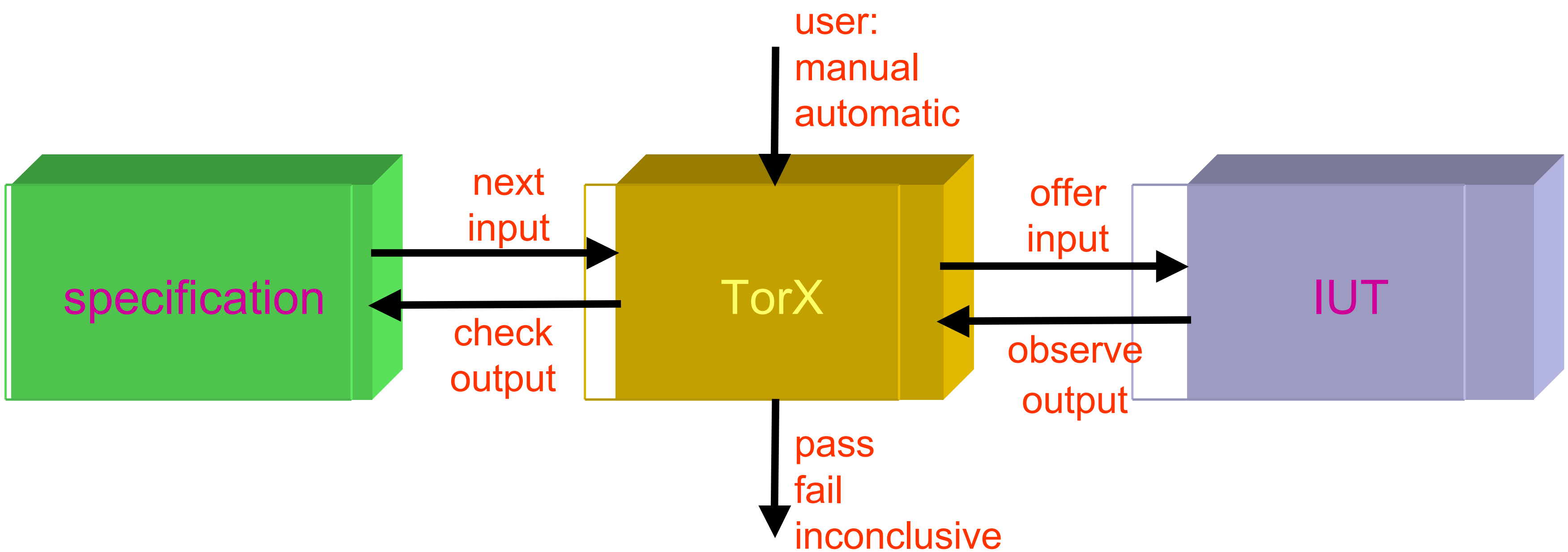


SOME TEST GENERATION TOOLS FOR *IOCO*

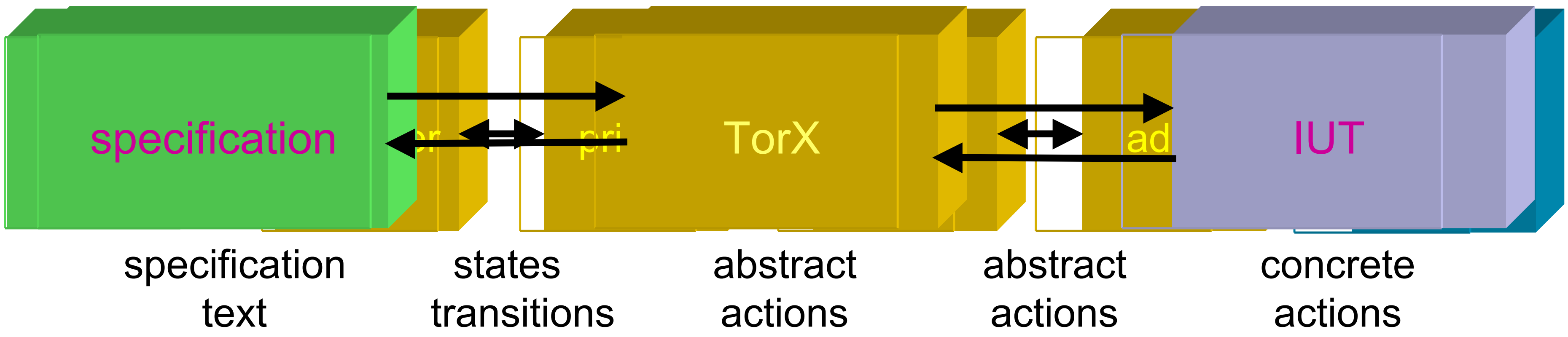
- TVEDA (CNET - France Telecom)
  - derives TTCN tests from single process SDL specification
  - developed from practical experiences
  - implementation relation R1 $\approx$ ioco
- TGV (IRISA - Rennes)
  - derives tests in TTCN from LOTOS or SDL
  - uses test purposes to guide test derivation
  - implementation relation: unfair extension of ioco
- TestComposer (Verilog)
  - Combination of TVEDA and TGV in ObjectGeode
- TestGen (Stirling)
  - Test generation for hardware validation
- TorX (University of Twente, ESI)

A TEST TOOL : TORX

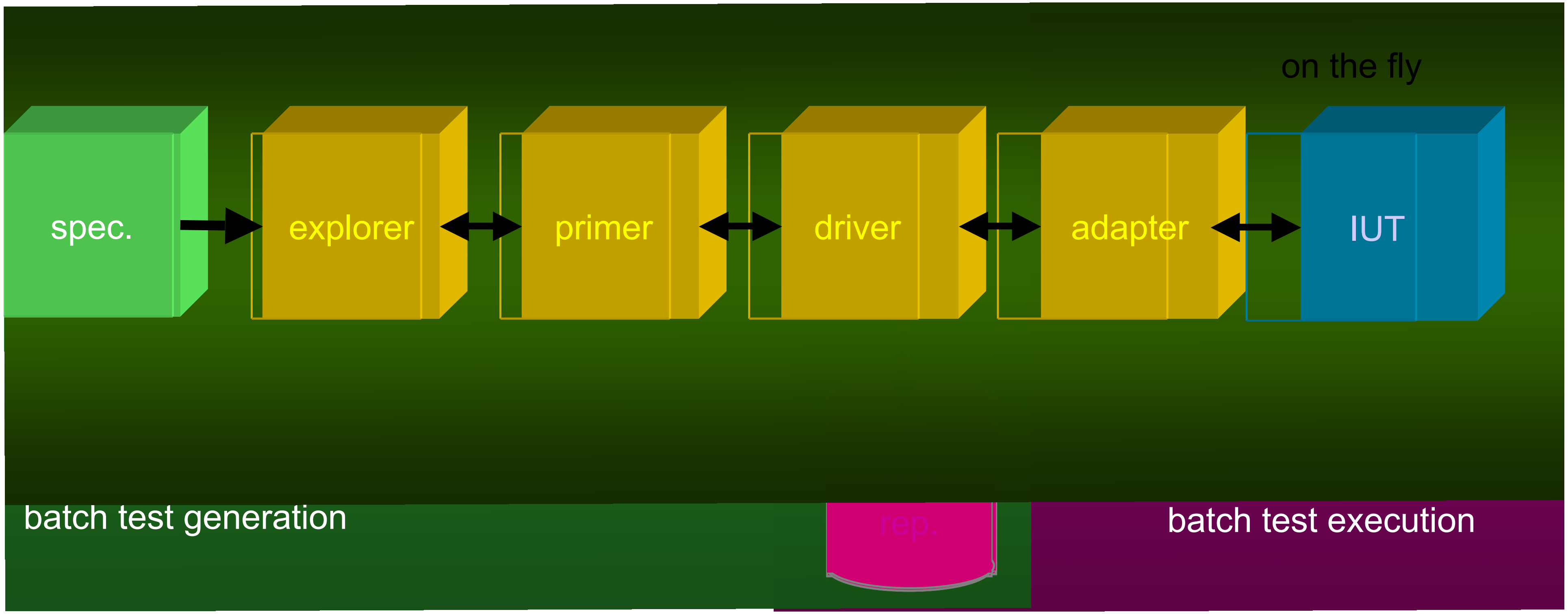
- On-the-fly test generation and test execution
- Implementation relation: *ioco*
- Specification languages: LOTOS, Promela, FSP, Automata



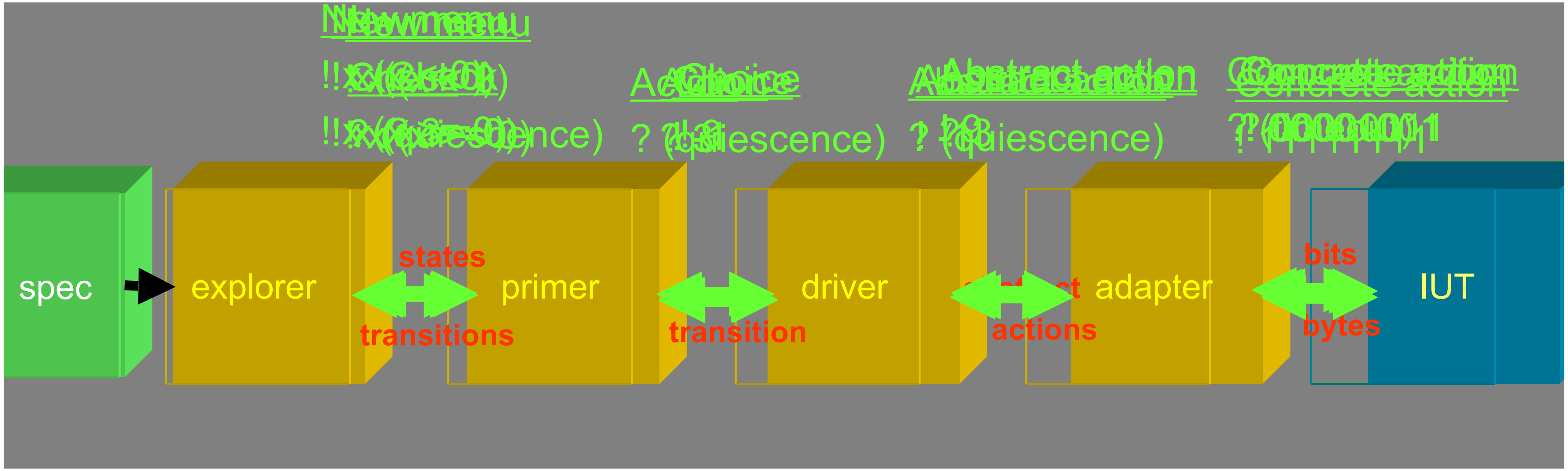
TORX TOOL ARCHITECTURE



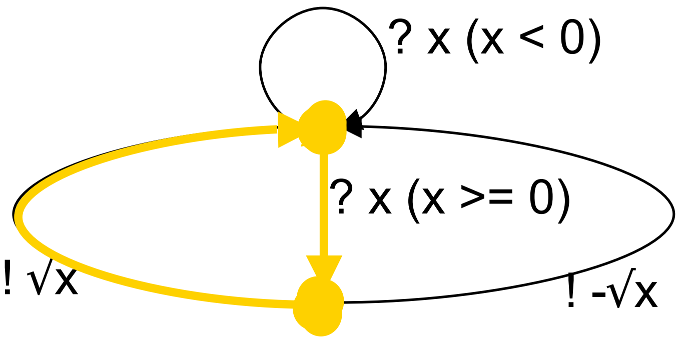
ON-THE-FLY ↔ BATCH TESTING



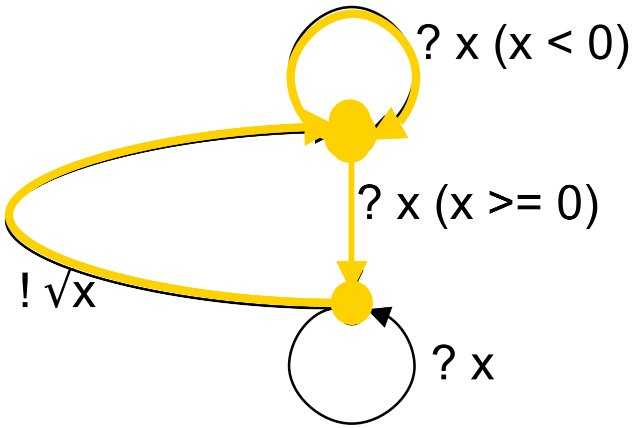
ON-THE-FLY TESTING



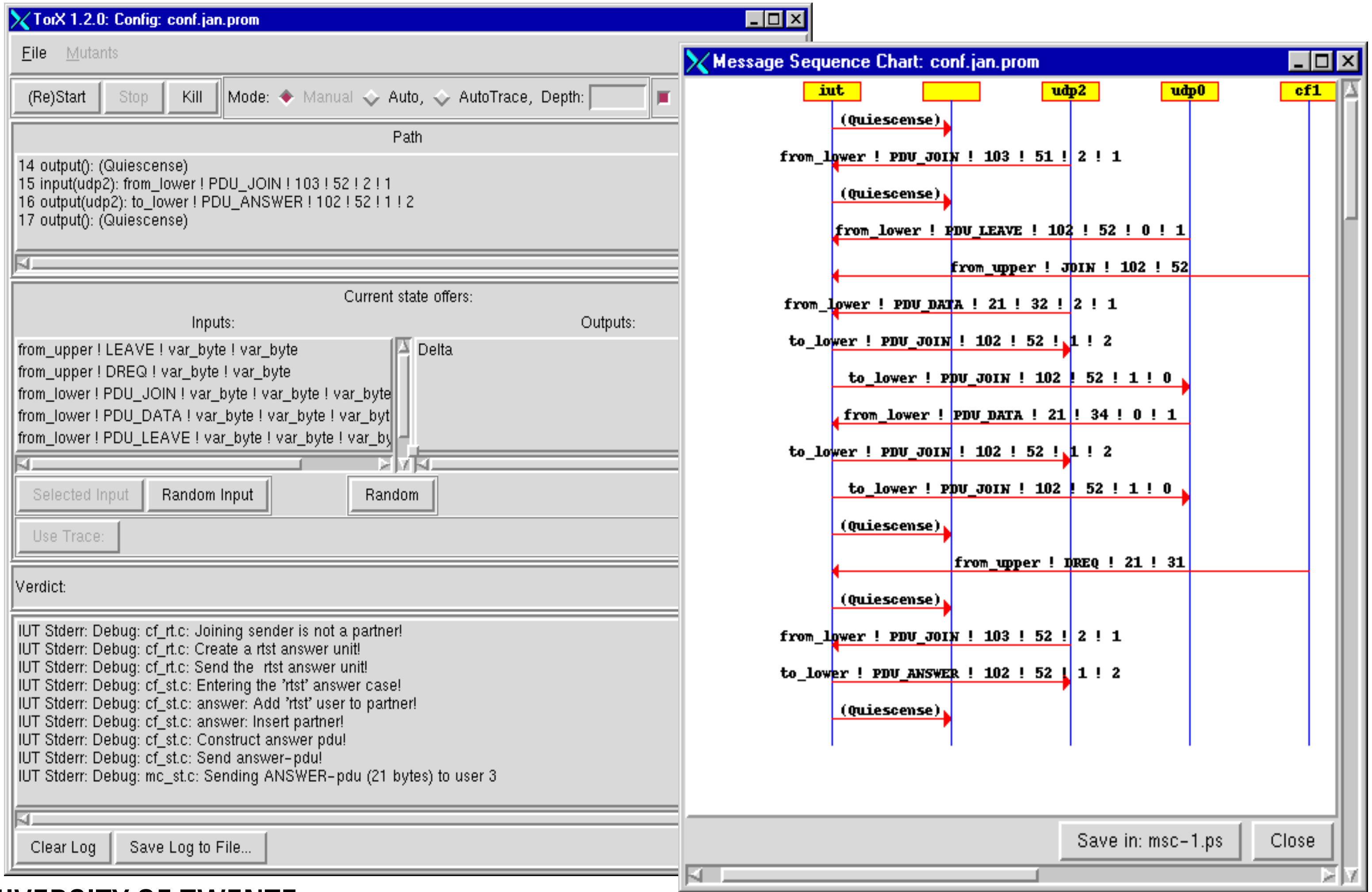
specification



implementation



TORX


TorX 1.2.0: Config: conf.jan.prom
File
Mutants
(Re)Start
Stop
Kill
Mode:
Manual
Auto,
AutoTrace,
Depth:
Path
14 output(): (Quiescense)
15 input(udp2): from_lower ! PDU_JOIN ! 103 ! 52 ! 2 ! 1
16 output(udp2): to_lower ! PDU_ANSWER ! 102 ! 52 ! 1 ! 2
17 output(): (Quiescense)
Current state offers:
Inputs:
Outputs:
from_upper ! LEAVE ! var_byte ! var_byte
from_upper ! DREQ ! var_byte ! var_byte
from_lower ! PDU_JOIN ! var_byte ! var_byte ! var_byte
from_lower ! PDU_DATA ! var_byte ! var_byte ! var_byt
from_lower ! PDU_LEAVE ! var_byte ! var_byte ! var_by
Delta
Selected Input
Random Input
Random
Use Trace:
Verdict:
IUT Stderr: Debug: cf_rt.c: Joining sender is not a partner!
IUT Stderr: Debug: cf_rt.c: Create a rtst answer unit!
IUT Stderr: Debug: cf_rt.c: Send the rtst answer unit!
IUT Stderr: Debug: cf_st.c: Entering the 'rtst' answer case!
IUT Stderr: Debug: cf_st.c: answer: Add 'rtst' user to partner!
IUT Stderr: Debug: cf_st.c: answer: Insert partner!
IUT Stderr: Debug: cf_st.c: Construct answer pdu!
IUT Stderr: Debug: cf_st.c: Send answer-pdu!
IUT Stderr: Debug: mc_st.c: Sending ANSWER-pdu (21 bytes) to user 3
Clear Log
Save Log to File...
Message Sequence Chart: conf.jan.prom
iut
udp2
udp0
cf1
(Quiescense)
from_lower ! PDU_JOIN ! 103 ! 51 ! 2 ! 1
(Quiescense)
from_lower ! PDU_LEAVE ! 102 ! 52 ! 0 ! 1
from_upper ! JOIN ! 102 ! 52
from_lower ! PDU_DATA ! 21 ! 32 ! 2 ! 1
to_lower ! PDU_JOIN ! 102 ! 52 ! 1 ! 2
to_lower ! PDU_JOIN ! 102 ! 52 ! 1 ! 0
from_lower ! PDU_DATA ! 21 ! 34 ! 0 ! 1
to_lower ! PDU_JOIN ! 102 ! 52 ! 1 ! 2
to_lower ! PDU_JOIN ! 102 ! 52 ! 1 ! 0
(Quiescense)
from_upper ! DREQ ! 21 ! 31
(Quiescense)
from_lower ! PDU_JOIN ! 103 ! 52 ! 2 ! 1
to_lower ! PDU_ANSWER ! 102 ! 52 ! 1 ! 2
(Quiescense)
Save in: msc-1.ps
Close

TORX CASE STUDIES

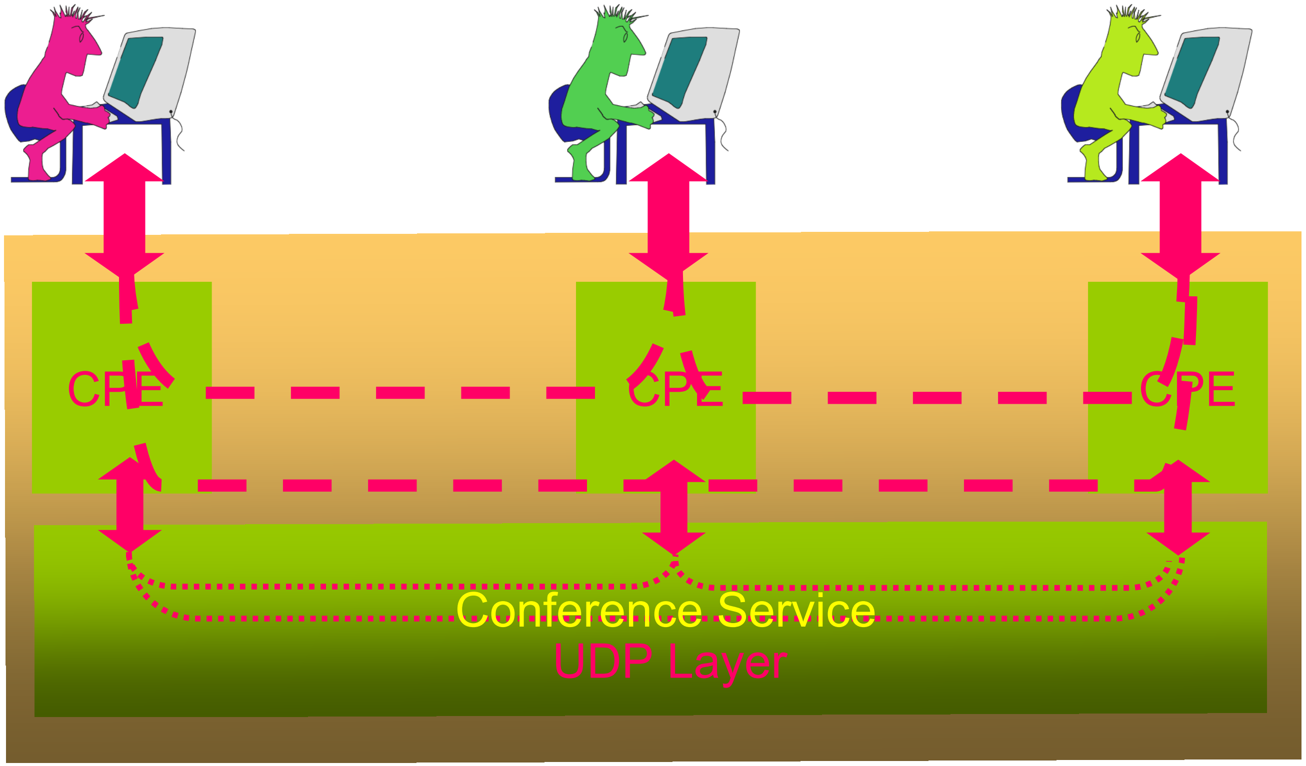
▪ Conference Protocol	academic
▪ EasyLink TV-VCR protocol	Philips
▪ Cell Broadcast Centre component	CMG
▪ Road Toll Payment Box protocol	Interpay
▪ V5.1 Access Network protocol	Lucent
▪ Easy Mail Notification	CMG
▪ FTP Client	academic
▪ “Oosterschelde” storm surge barrier-control	CMG
▪ TANGRAM: testing VLSI lithography machine	ASML

THE CONFERENCE PROTOCOL EXPERIMENT

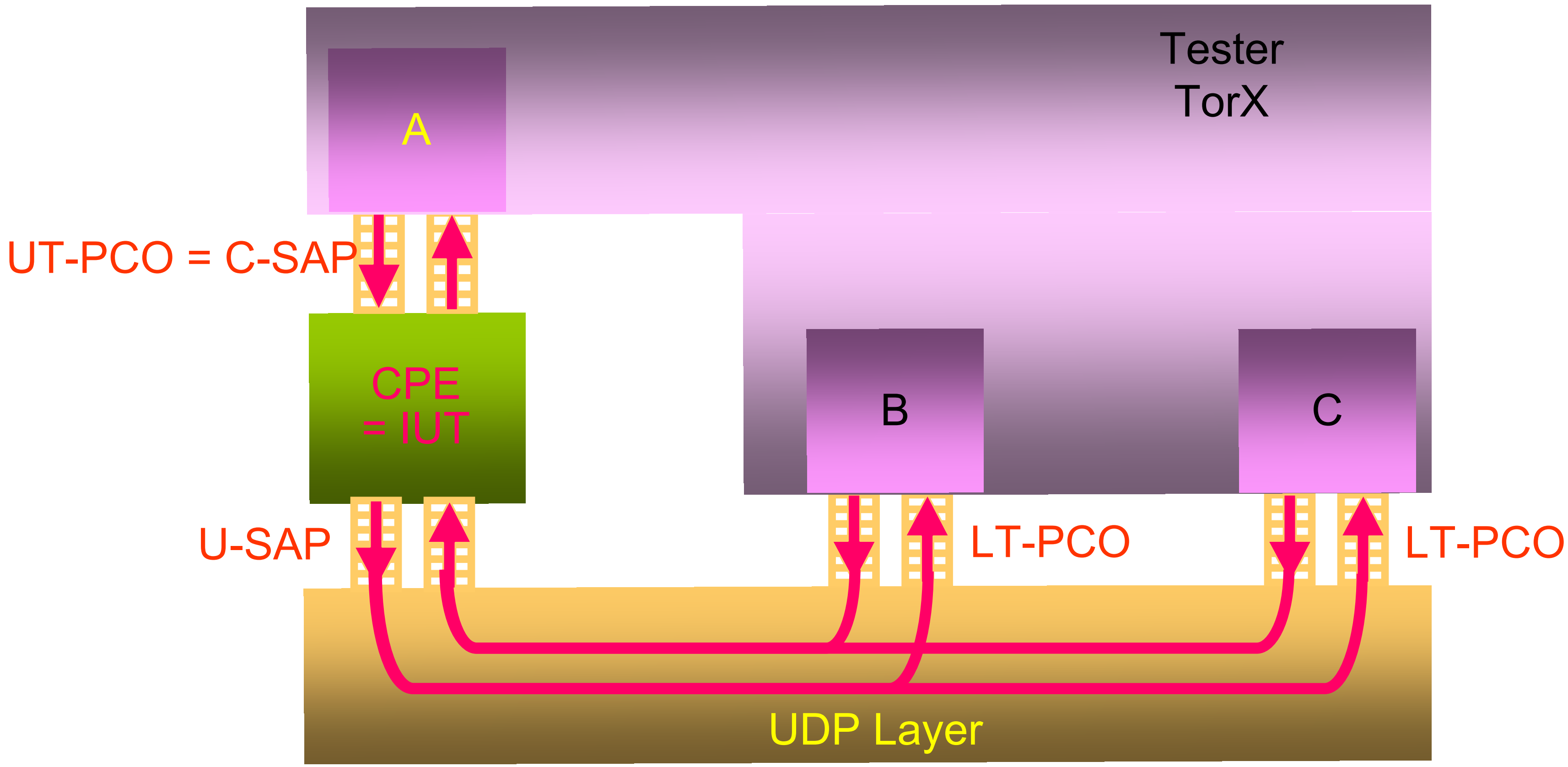
- Academic benchmarking experiment,
  initiated for test tool evaluation and comparison
- Based on really testing different implementations
- Simple, yet realistic protocol (chatbox service)
- Specifications in LOTOS, Promela, SDL, EFSM
- 28 different implementations in C
  - one of them (assumed-to-be) correct
  - others manually derived mutants
- http://fmt.cs.utwente.nl/ConfCase

THE CONFERENCE PROTOCOL

join
leave
send
receive



CONFERENCE PROTOCOL TEST ARCHITECTURE



THE CONFERENCE PROTOCOL EXPERIMENTS

- TorX - LOTOS, Promela : on-the-fly ioco testing

  Axel Belinfante et al.,
  Formal Test Automation: A Simple Experiment
  IWTCS 12, Budapest, 1999.

- Tau Autolink - SDL : semi-automatic batch testing
- TGV - LOTOS : automatic batch testing with test purposes

  Lydie Du Bousquet et al.,
  Formal Test Automation: The Conference Protocol with TGV/TorX
  TestCom 2000, Ottawa.

- PHACT/Conformance KIT - EFSM : automatic batch testing

  Lex Heerink et al.,
  Formal Test Automation: The Conference Protocol with PHACT
  TestCom 2000, Ottawa.

CONFERENCE PROTOCOL RESULTS

Results:	TorX LOTOS	TorX Promela	PHACT EFSM	TGV LOTOS random	TGV LOTOS purposes
fail	25	25	21	25	24
pass	3	3	6	3	4
core dump	0	0	1	0	0
pass	000 444 666	000 444 666	000 444 666 289 293 398	000 444 666	000 444 666 332

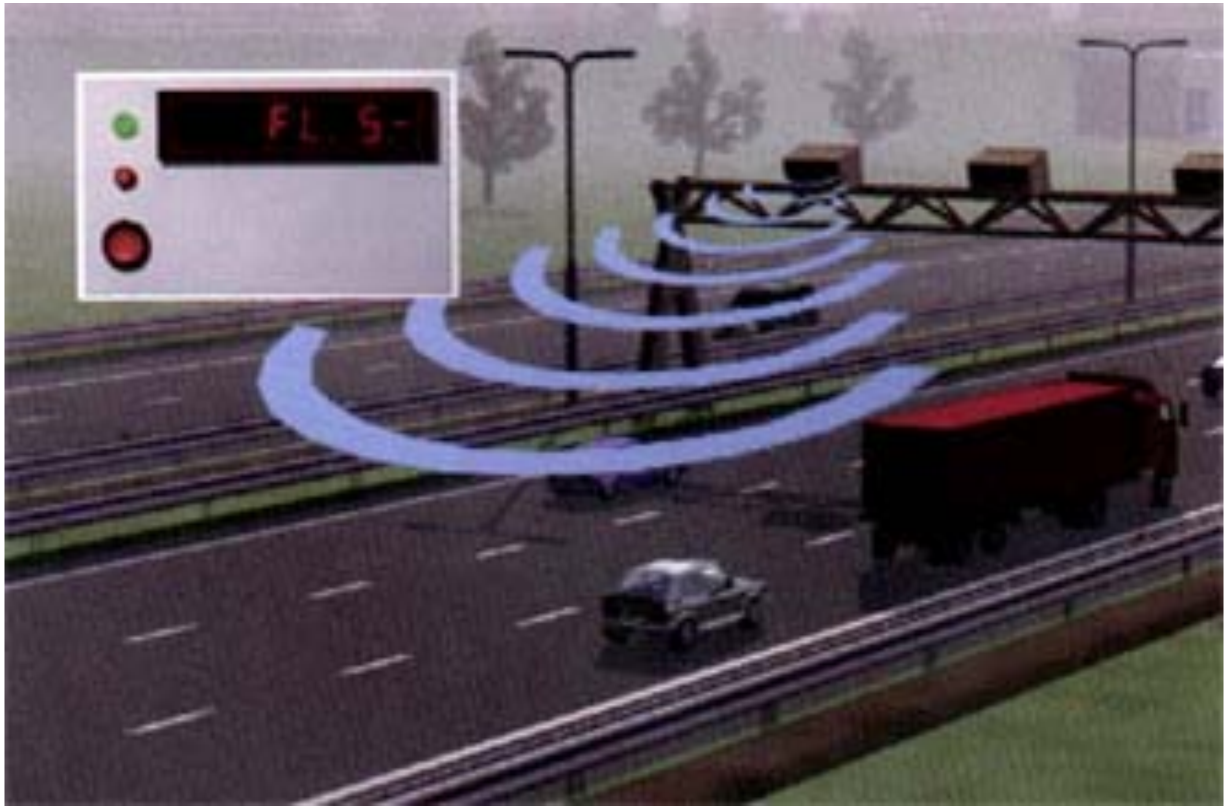
CONFERENCE PROTOCOL ANALYSIS

- Mutants 444 and 666 react to PDU’s from non-existent partners:
  - no explicit reaction is specified for such PDU’s,
    so *ioco*-correct, and TorX does not test such behaviour
- So, for LOTOS/Promela with TGV/TorX:
  All *ioco*-erroneous implementations detected
- EFSM:
  - two “additional-state” errors not detected
  - one implicit-transition error not detected

CONFERENCE PROTOCOL ANALYSIS

- TorX statistics
  - all errors found after 2 - 498 test events
  - maximum length of tests : > 500,000 test events
- EFSM statistics
  - 82 test cases with “partitioned tour method” (= UIO)
  - length per test case : < 16 test events
- TGV with manual test purposes
  - ~ 20 test cases of various length
- TGV with random test purposes
  - ~ 200 test cases of 200 test events

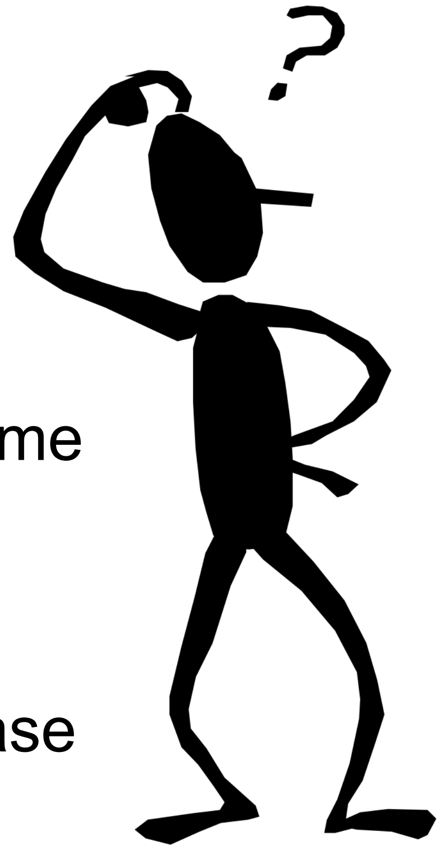
INTERPAY HIGHWAY TOLLING SYSTEM



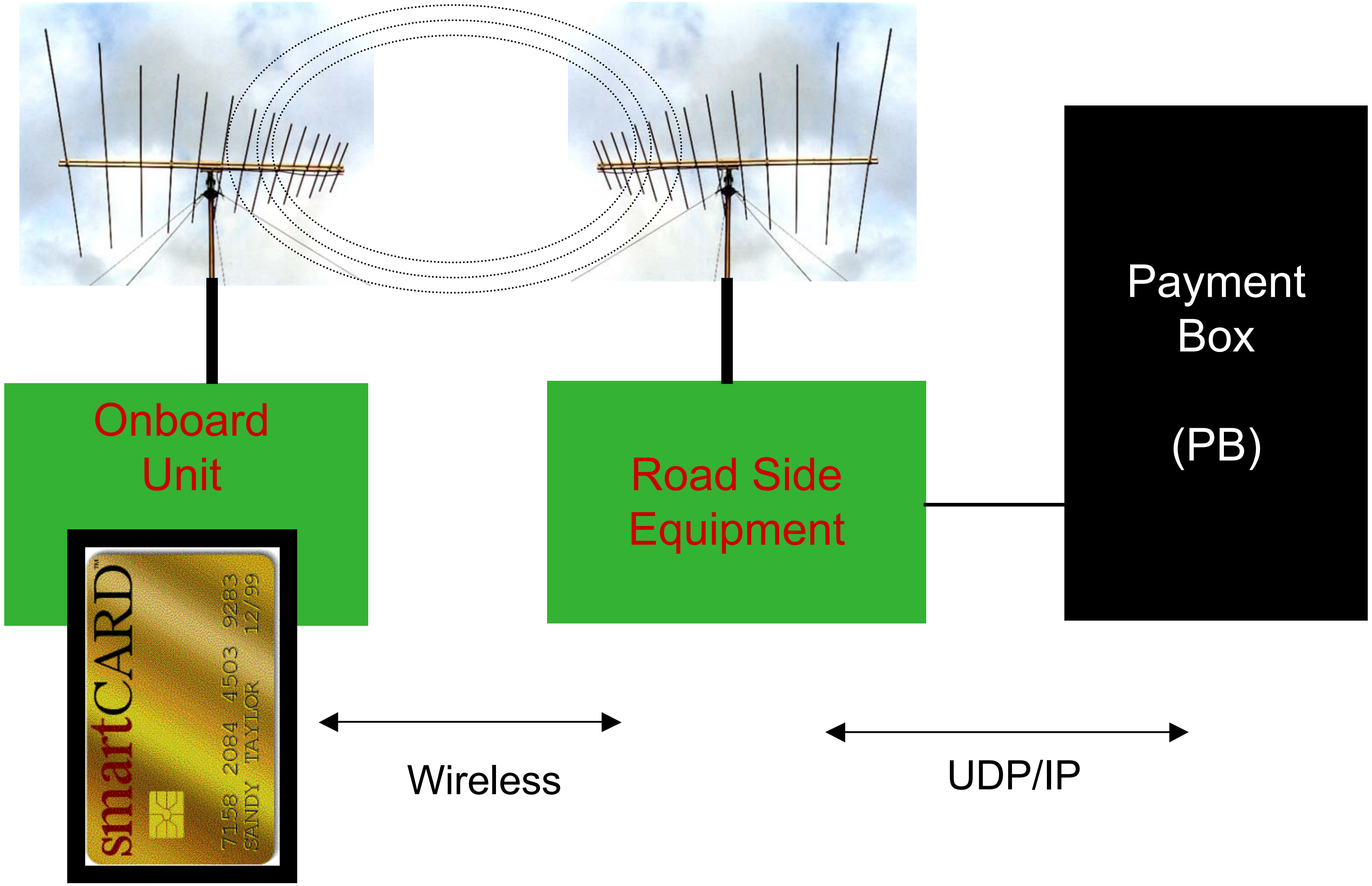
HIGHWAY TOLLING PROTOCOL

Characteristics :

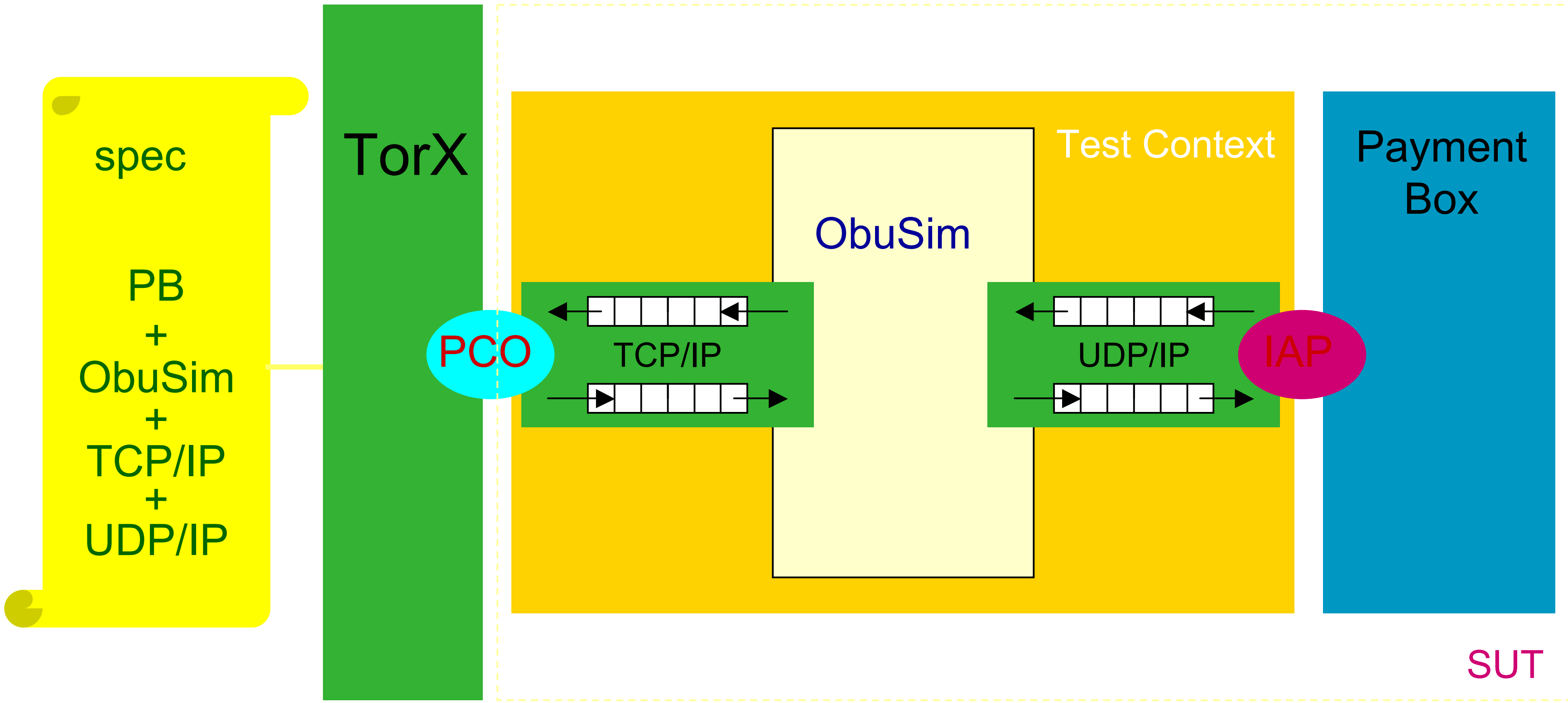
- simple protocol
- parallelism: many cars at the same time
- encryption
- system passed traditional testing phase



HIGHWAY TOLLING SYSTEM



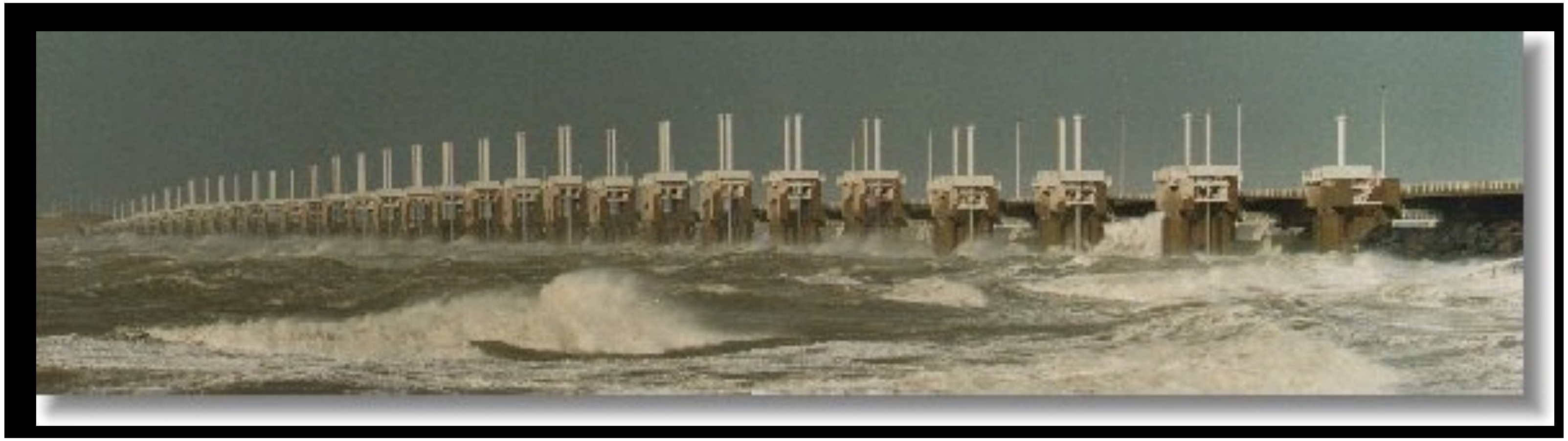
HIGHWAY TOLLING: TEST ARCHITECTURE



HIGHWAY TOLLING: RESULTS

- Test results :
  - 1 error during validation   (design error)
  - 1 error during testing   (coding error)
- Automated testing :
  - beneficial: high volume and reliability
  - many and long tests executed   (> 50,000 test events)
  - very flexible: adaptation and many configurations
- Real-time :
  - interference computation time on-the-fly testing
  - interference quiescence and time-outs

STORM SURGE BARRIER CONTROL



Oosterschelde Stormvloedkering (OSVK)

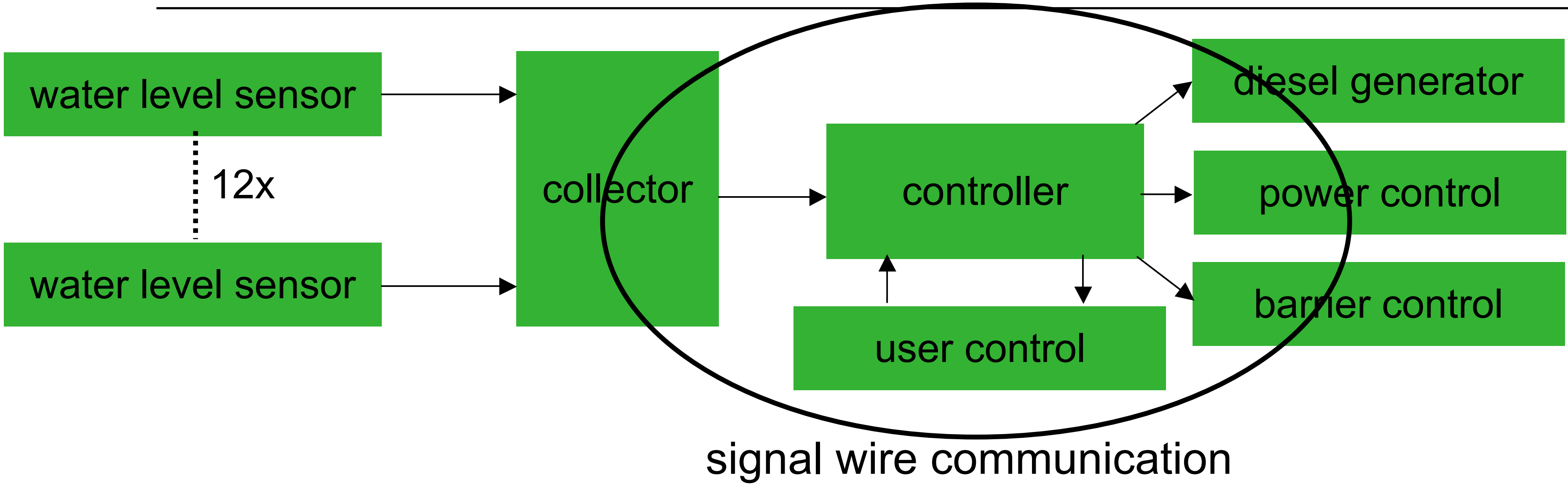
SVKO EMERGENCY CLOSING SYSTEM

- Collect water level sensor readings (12x, 10Hz)
- Calculate mean outer-water level and mean inner-water level
- Determine closing conditions

```
if (closing_condition)
{notify officials
 start diesel engines
 block manual control
 control local computers}
```

- Failure rate: 10^{-4}/closing event

TESTING SVKO



- test controller (Unix port)
- many timed observations
  - shortest timed delay: 2 seconds
  - longest timed delay: 85 minutes

RESULTS

- real-time control systems can be tested with TorX-technology
  - addition of discrete real time
  - time stamped actions
- quiescence action is not used
  - time spectrum of 3 orders of magnitude
  - deterministic system
- adhoc implementation relation

RT TORX HACKS: APPROACH 1

Ignore RT functionality:

- test pure functional behaviour
- analyse timing requirements using TorX log files & assumed frequency of wire polling actions

RT TORX HACKS: APPROACH 2

Add timestamps to observations

- adapter adds timestamps to observations when they are made and passed on to the driver
- timestamps are used to analyse TorX log files

TIMING ERROR LOGGING

```
int time,newtime;
...
input?value,time            // input: stimulus
...                         // variable time is set here
output!param,&newtime       // output: observation
         // & is extension to promela:
if         // variable newtime is set here
:: (newtime==time+60)       // expected delay of 60 is
    print(“OK”,...)         // checked & logged
:: (newtime!=time+60)
    print(“NOK”,...)
fi;
```

RT TORX HACKS: APPROACH 3

Add timestamps to stimuli & observations

- adapter add timestamps to observations when they are made and passed on to the driver
- adapter adds timestamps to stimuli when they are applied and returned to the driver
- analysis:
  - timing error logging: observed errors are written to TorX log file
  - timing error failure: observed errors cause fail verdict of test case

TIMING ERROR FAILURE

```
int time;
...          // input: stimulus
input?value,time     // variable time is set here
...
if              // output: observation
:: output!param,(time+59)    // wait 60 (-1)
:: output!param,(time+60)     // wait 60
:: output!param,(time+61)     // wait 60 (+1)
fi            // if observation is not made
                                 // after approx. 60 units,
              // quiescence will be
            // observed
```

CONTENTS

- Introduction control-oriented testing
- Input-output conformance testing
- Real-time conformance testing
- Test coverage measures

CONTENTS

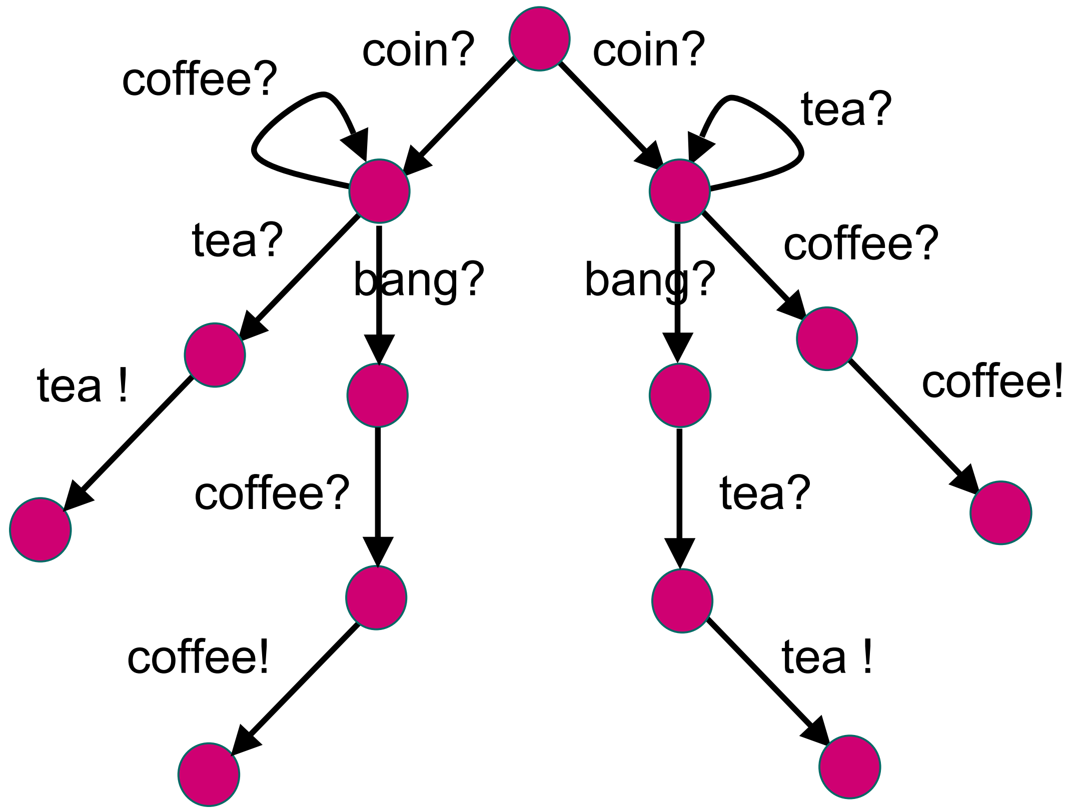
REAL-TIME TESTING AND I/O SYSTEMS

- can the notion of repetitive quiescence be combined with real-time testing?
- is there a well-defined and useful conformance relation that allows sound and (relative) complete test derivation?
- can the TorX test tool be adapted to support Real-timed conformance testing?

WITH REAL-TIME DO WE STILL NEED QUIESCENCE?

Yes!

the example processes should also be distinct in a real-time context



REAL-TIME AND QUIESCENCE

- s is *quiescent* iff:

  for no output action a and delay d: $s \overset{a(d)}{\Rightarrow}$

- special transitions:

  $s \overset{\delta}{\rightarrow} s$ for every quiescent system state s

- testers observing quiescence take time:

  $Test_M$: set of test processes having only $\delta_{(M)}$-actions to observe quiescence

- assume that implementations are M-quiescent:

  for all reachable states s and s':

  if $s \overset{\varepsilon(M)}{\Rightarrow} s'$ then s' is quiescent

REAL-TIME AND QUIESCENCE

$$i \leq^{M}_{tiorf} s \;\Leftrightarrow\; \forall T \in Test_M :$$

$$Deadlocks_\delta(i||T) \subseteq Deadlocks_\delta(s||T)$$

$$\Leftrightarrow\; \forall \sigma \in (L \cup \{\delta(M)\})^* :$$

$$out_M\,(\,i\ after\ \sigma) \subseteq out_M\,(\,s\ after\ \sigma)$$

$$i\ tioco_M\ s \;\Leftrightarrow\; \forall \sigma \in Traces_{\delta(M)}(\,s\,) :$$

$$out_M\,(\,i\ after\ \sigma) \subseteq out_M\,(\,s\ after\ \sigma)$$

PROPERTIES

- for all $M_1 \leq M_2$:

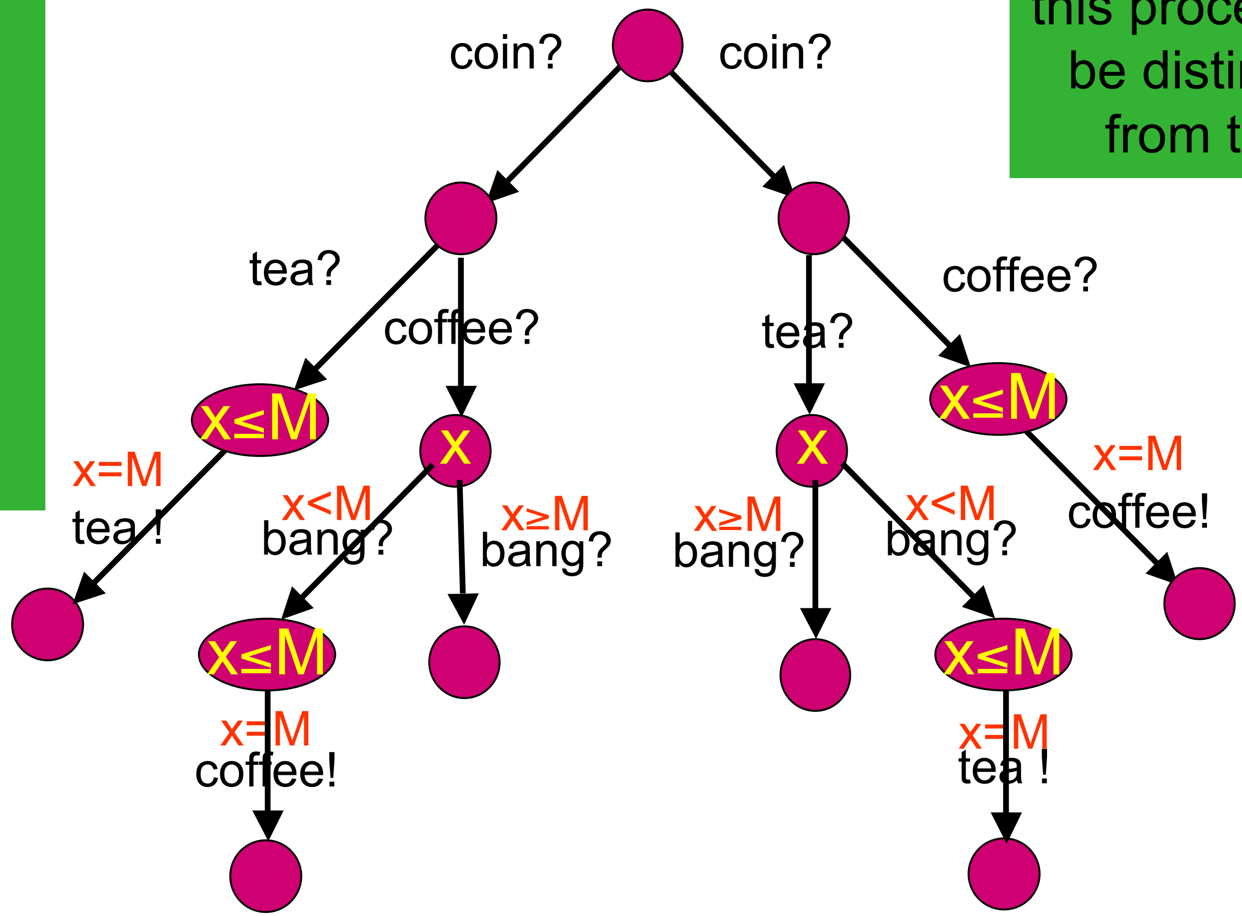
  $i \leq_{tiorf}^{M_1} s$ implies $i \leq_{tiorf}^{M_2} s$

- for all time-independent i,s and $M_1,M_2>0$

  $i \leq_{tiorf}^{M_1} s$ *iff* $i \leq_{tiorf} s$ *iff* $i \leq_{iorf}^{M_2} s$

A LIMITATION

states are saturated with input loops that reset the clocks



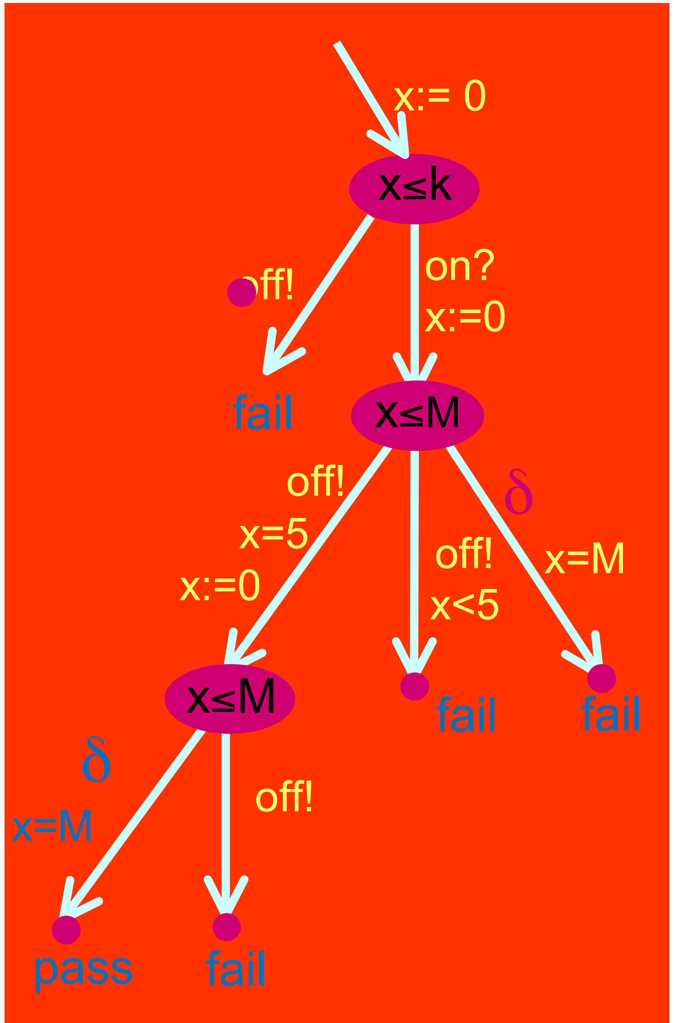
this process cannot be distinguished from the next

REAL-TIME TEST CASES

Test case $t \in TTA$

TTA – Test Timed Automata :

- labels in $L \cup \{\delta\}$, $G(d)$
- tree-structured
- finite, deterministic
- final states pass and fail
- from each state ≠ pass, fail
  - choose an input *i?* and a time *k* and wait for the time *k* accepting all outputs *o!* and after *k* time units provide input *i?*
  - or wait for time *M* accepting all outputs *o!* and δ



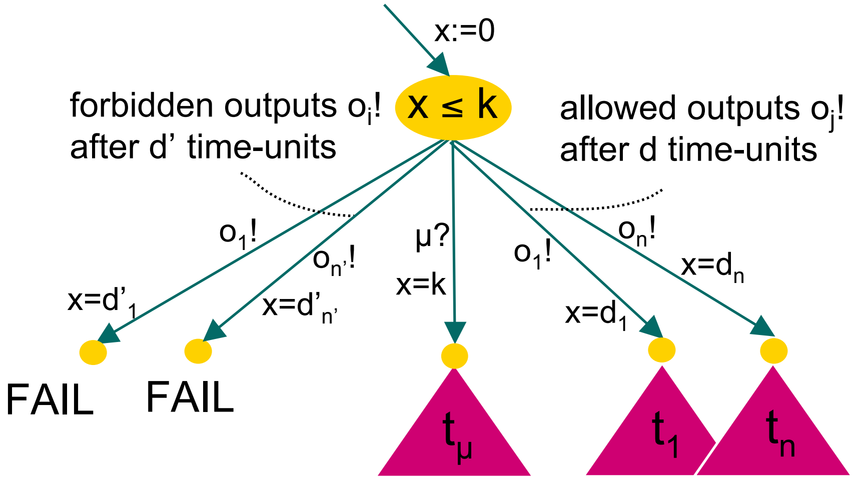
TIMED TEST GENERATION PROTO-ALGORITHM

To generate a test case t(S) from a timed transition system specification with S set of states (initially $S = \{s_0\}$)

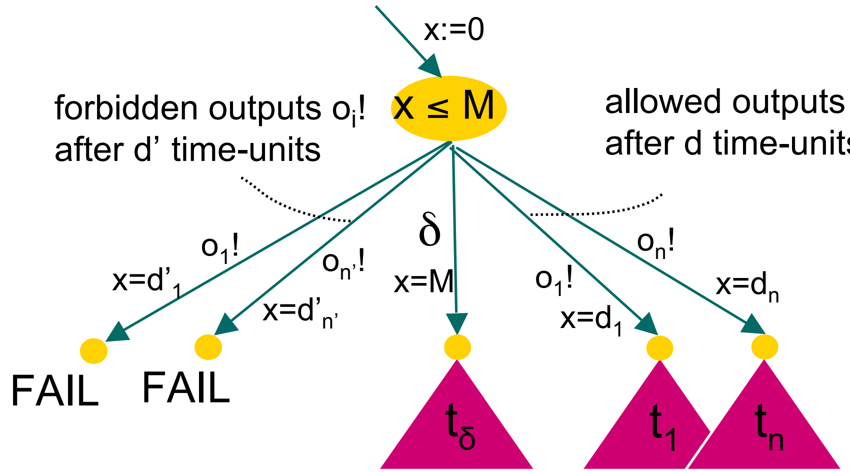
Apply the following steps recursively, non-deterministically

1. end test case — PASS

2. choose $k \in (0, M)$ and input μ



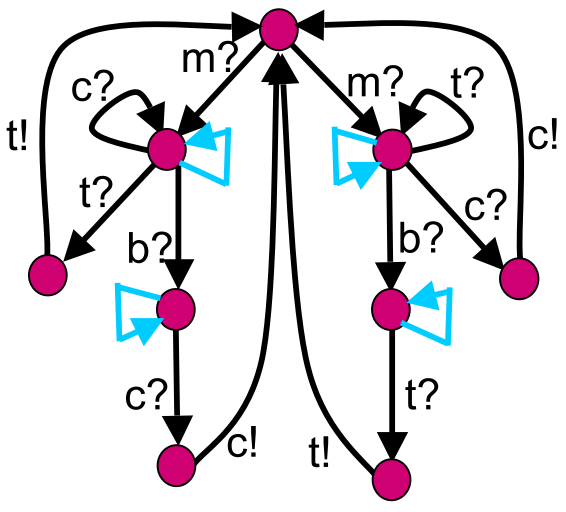
3. wait for observing possible output



Example

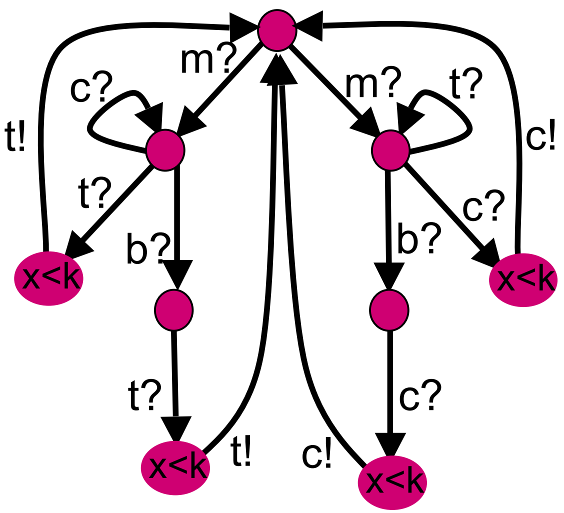
spec:

δ

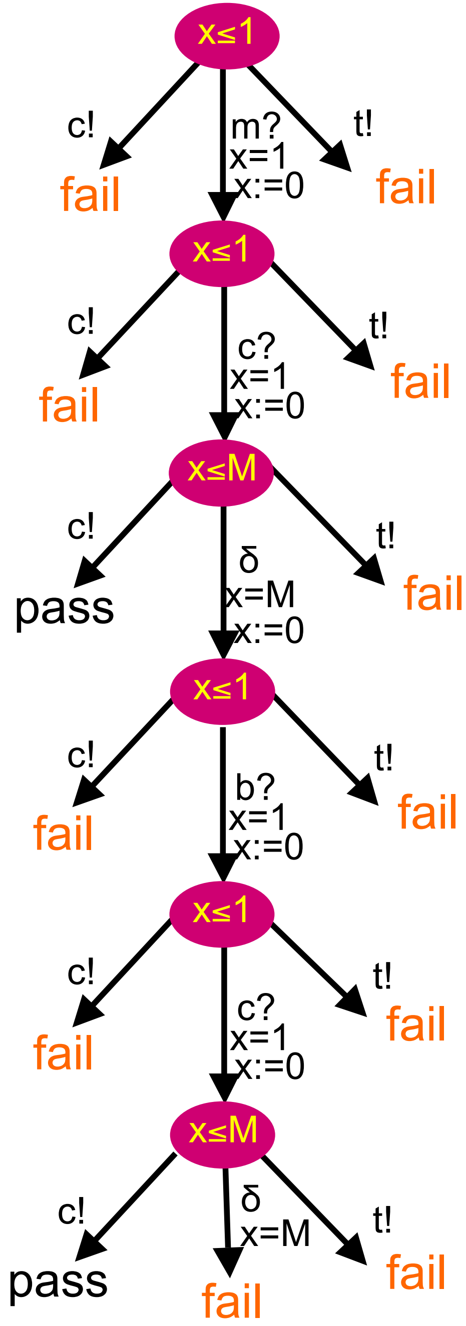


impl:

M=k



test:



SOUNDNESS & COMPLETENESS

- the non-timed generation algorithm can be s
  only sound real-time test cases
- test generation is complete

  for every erroneous trace it can generate a

  test that exposes it
- test generation is not limit complete

  because of continuous time there are uncountably many timed error traces and only countably many test are generated by repeated runs
- test generation is almost limit complete

  repeated test geration runs will eventually generate a test case that will expose one of the non-spurious errors of a non-conforming implementation

non-spurious errors
=
errors with a positive probability of occurring

CONTENTS

- Introduction control-oriented testing
- Input-output conformance testing
- Real-time conformance testing
- Test coverage measures

CONTENTS

COVERAGE: MOTIVATION

- Testing is inherently incomplete
  - Test selection is crucial

- Coverage metrics
  - Quantitative evaluation of test suite
  - Count how much of specification/implementation has been examined

- Examples:
  - White box (implementation coverage):
  - Statement, path, condition coverage
  - Black box (specification coverage)
  - State, transition coverage

TRADITIONAL COVERAGE MEASURES

Traditional measures are:

- based on syntactic model features
  - states, transitions, statements, tests
- uniform
  - all system parts treated as bequally important

Disadvantages:

- replacing the spec by an equivalent one yields different coverage
  - we need a *semantic* approach
- some bugs are more important than others;
  - test crucial behaviour first and better

OUR APPROACH

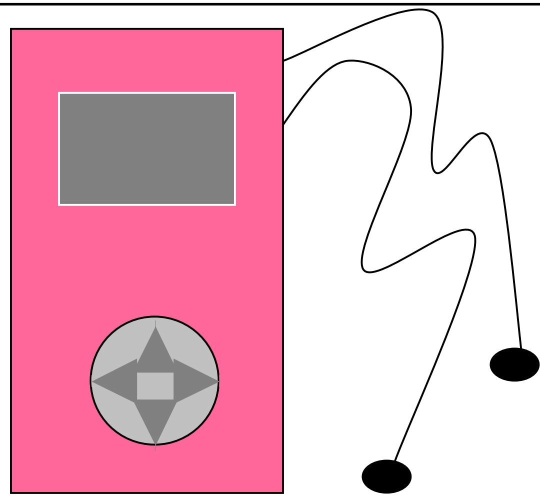
- Considers black box coverage
  - similar ideas could apply to white box coverage
- Is semantic
  - Semantically equivalent specs yield same coverage
- Is risk-based
  - more important bugs/system parts

  → higher contribution to coverage
- Allows for optimization
  - Cheapest test suite with 90% coverage
  - Maximal coverage within cost budget

FAULT MODELS

- f: *Observation* → $R^{\geq 0}$
  - f(σ) = 0 : correct behaviour
  - f(σ) > 0 : incorrect behaviour

    : f(σ) severity
  - $0 < \Sigma_\sigma f(\sigma) < \infty$
- Observations are traces
  - *Observations* = L^*
  - $L = (L_I, L_U)$
- How to obtain f?
  - E.g. via fault automaton



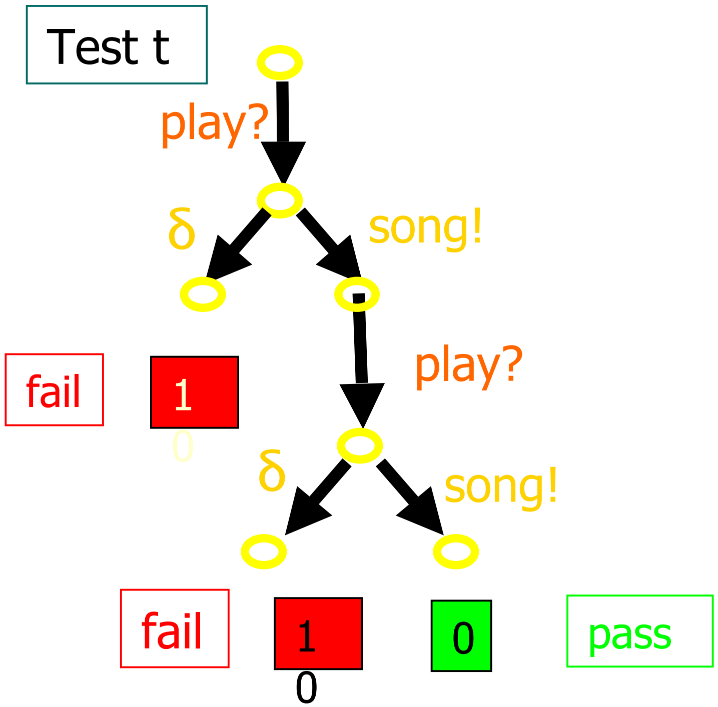
f: L* → $R^{\geq 0}$

f(play? song!) = 0 correct

f(play? silence!) = 10 incorrect

f(song!) = 3 incorrect

EXAMPLE TEST CASE

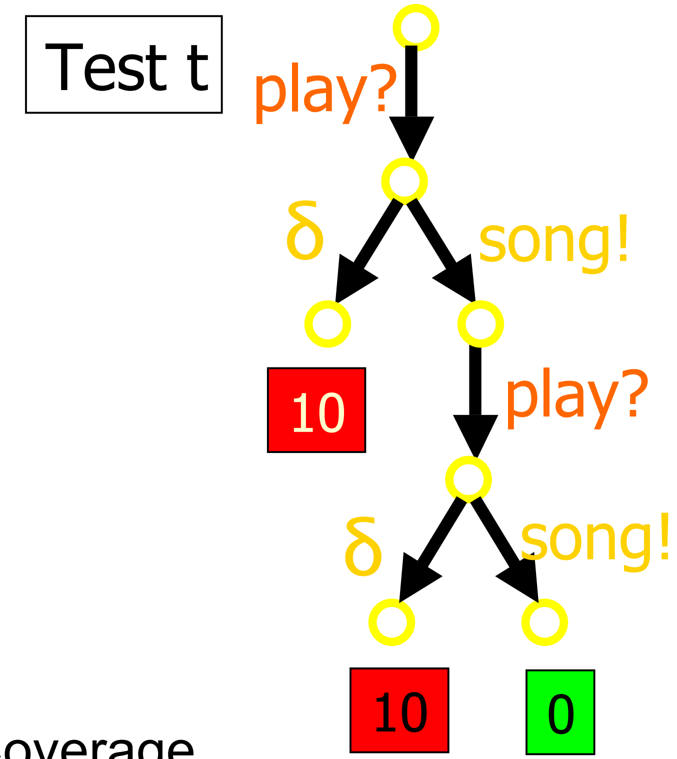


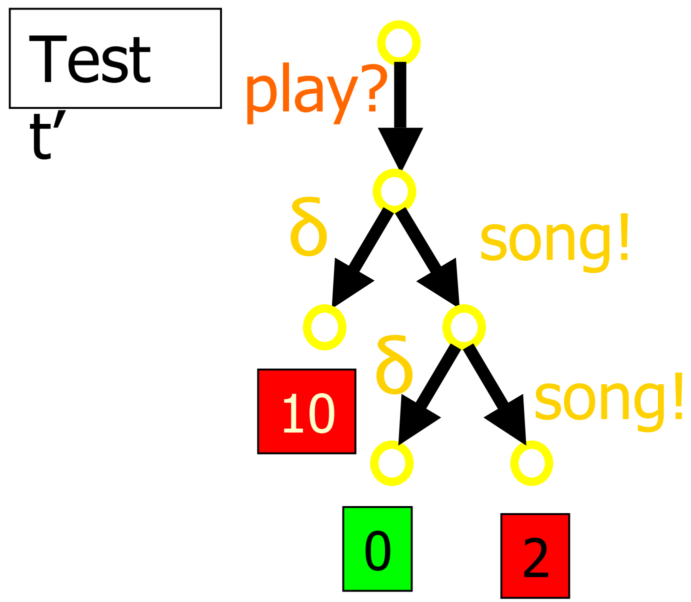
- f: L* → R
  - f(play? song!) = 0
  - f(play? δ) = 10
  - f(play? song! play? δ) = 10
  - f(song!) = 3
- Σ_{σ} f(σ) = 100 (assumption)
- Absolute Coverage abscov(f,t)
  - sum the error weights
  - 10 + 10 + 0 = 20
- Relative Coverage

$$\frac{abscov(f,t)}{totcov(f)} = \frac{20}{100}$$

should be ≠ 0, ≠∞

EXAMPLE TEST SUITE





Absolute Coverage

- count each trace once !
- 10 + 10 + 0 + 0 + 2 = 22

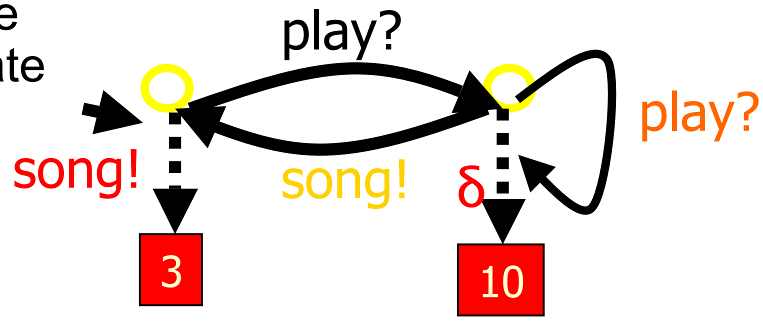
Relative Coverage

$$\frac{\text{abscov}(f,t)}{\text{totcov}(f)} = \frac{22}{100} = 22\%$$

FAULT SPECIFICATIONS

fault model

- $f(\sigma) = 0$ if σ trace of automaton
- $f(\sigma) = 3 \cdot \alpha^{|\sigma|-1}$ if σ ends in 3-state
- $f(\sigma) = 10 \cdot \alpha^{|\sigma|-1}$ if σ ends in 10-state



infinite total coverage !!

- $\Sigma_{\sigma} f(\sigma) = 3 + 10 + 3 + 10 + \ldots = \infty$

Solution 1: restrict to traces of lenght k

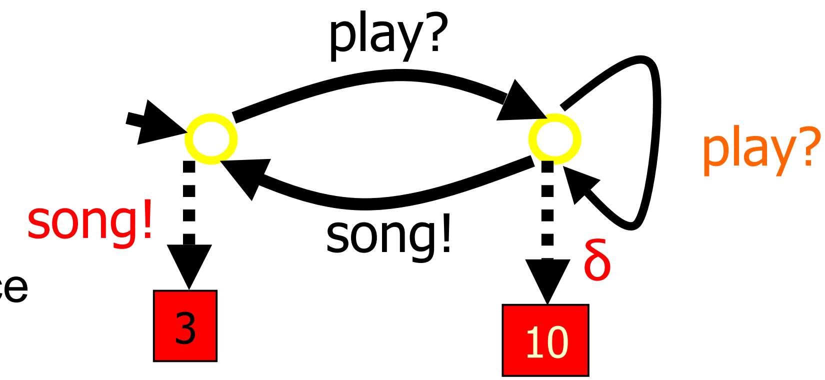
- Omit here, works as solution 2, less efficient, more boring

Solution 2: discounting

- errors in short traces are worse
- Lower the weight proportional to length

Use your favorite Formalism, e.g. UML state charts, LOTOS, etc

FAULT SPECIFICATIONS



fault model

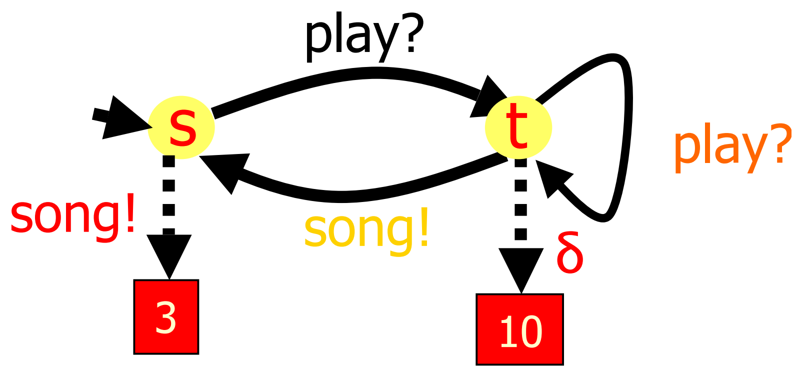
- $f(\sigma) = 0$ if σ automaton trace
- $f(\sigma) = 3 \cdot \alpha^{|\sigma|-1}$ if σ end in 3-state
- $f(\sigma) = 10 \cdot \alpha^{|\sigma|-1}$ if σ ends in 10-state

Example

- f(play?) = 0
- f(play? δ) = $10 \cdot \alpha$
- f(play? song! song!) = $3 \cdot \alpha^2$
- ....

- $\alpha < 1/out(spec) = 1/2$
- α can vary per transition
- tune α

FAULT SPECIFICATIONS



Total coverage becomes fcomputable:

$tc(s) = 3 + \alpha\, tc(t)$

$tc(t) = 10 + \alpha\, tc(t) + \alpha\, tc(s)$

$tc(x) = wgt(x) + \alpha \sum_{y:\, succ(x)} tc(y)$

Solve linear equations

$tc = wgt\, (I - \alpha A)^{-1}$

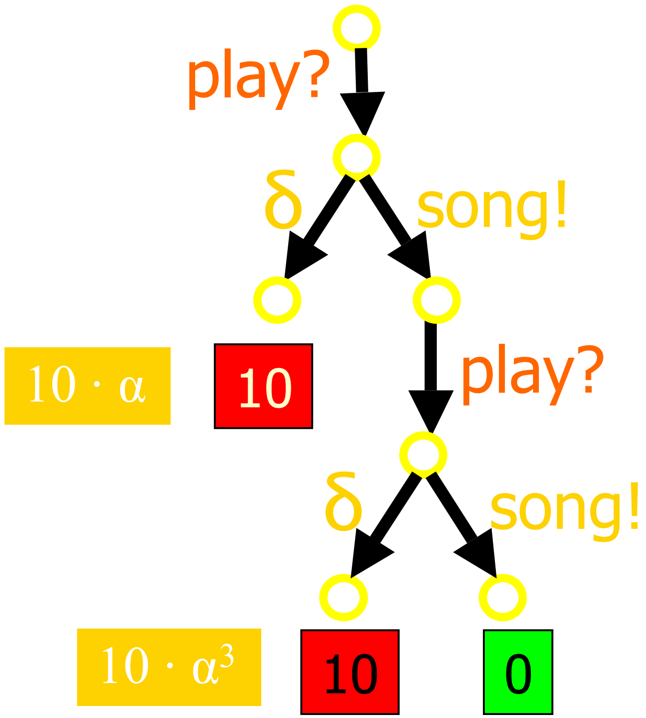
with A adjacency matrix

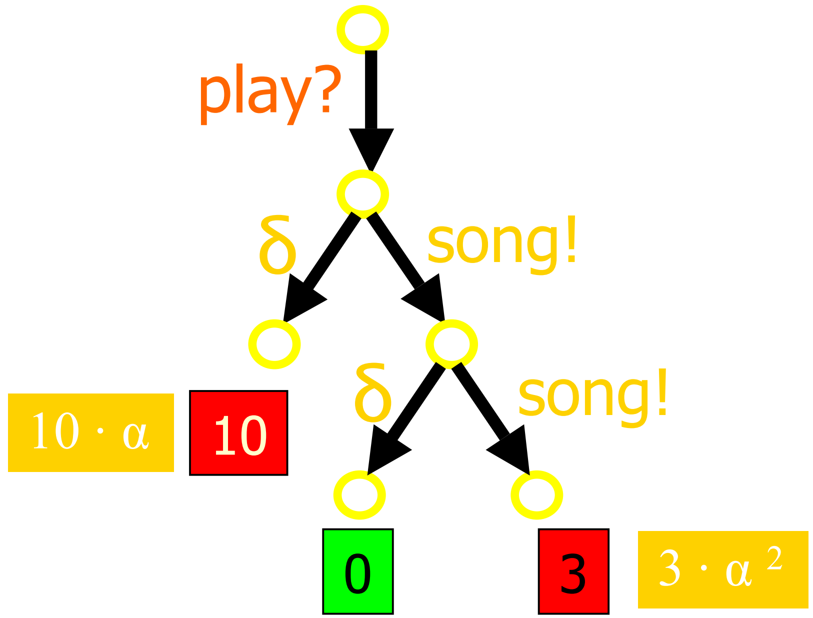
$$tc(s) = \frac{10 + 7\alpha}{1 - \alpha - \alpha^2}$$

Relative Coverage

$$\frac{abscov(f,t)}{totcov(f)}$$

TEST SUITE COVERAGE





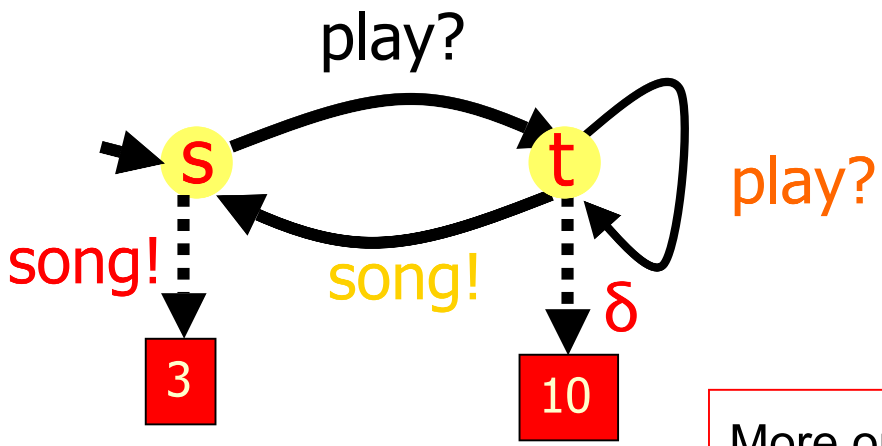
Absolute test suite coverage

- count each trace once!
- merge test cases first

Relative test suite coverage

$$\frac{\text{abscov}(f,t)}{\text{totcov}(f)} = \frac{10\alpha + 3\alpha^2 + 10\alpha^3}{\dfrac{10 + 7\alpha}{1 - \alpha - \alpha^2}}$$

OPTIMIZATION



Find best test case of lenght *n*

$$v_1(s) = 3$$
$$v_1(t) = 10$$
$$v_{k+1}(s) = \max(3, \alpha\ v_k(t))$$
$$v_{k+1}(t) = \max(10 + \alpha\ v_k(s), \alpha\ v_k(t))$$

Complexity: O(*n* #transitions in spec)

More optimizations:

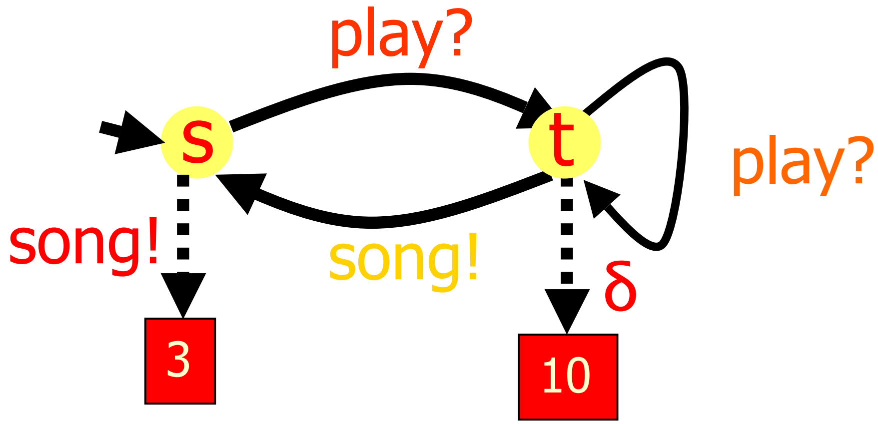
- Test suite of k tests & lenght n;
- Best test case in budget;
- Add costs
- ....

PROPERTIES

Framework for black box coverage

- robustness
  - small changes in weight yield small changes in coverage
  - relcov(s) continuous
- tunable (calibration)
  - change α : get as much total coverage as desired

CALIBRATION



α small → present is important, future unimportant

→ few small test cases with high (>0.999) coverage

tune α → make tests with length >*k* important, i.e make $cov(T_k, f)$ as small as desired.

→ $\alpha(s) = 1/n(s) - \varepsilon$ n(s) =outinf(s)

→ $\lim_{\varepsilon \to 0} cov(T_k, f_\alpha) = 0$ for all k

CONCLUSIONS

CONCLUSIONS

- model-based testing offers theory and tools for (real-time) conformance testing, in particular:
  - test generation, execution & evaluation
  - coverage analysis
- ioco-theory, TorX and related tools have been evaluated against many industrial cases
  - on-the-fly application very productive
  - good coverage with random test execution
- current theory is control-oriented
  - OK for classical embedded applications
  - must be extended to cope with data-intensive systems

FUTURE WORK

- integration with data-oriented testing
  classical, symbolic
- stochastic systems
  continuous & discrete time Markov chains
- quality of service
  performance testing
- hybrid systems
  testing discrete vs polling continuous behaviour
- actual coverage measures
  actual coverage during test execution
- integration white/black box spectrum
  grey-box testing
- ...

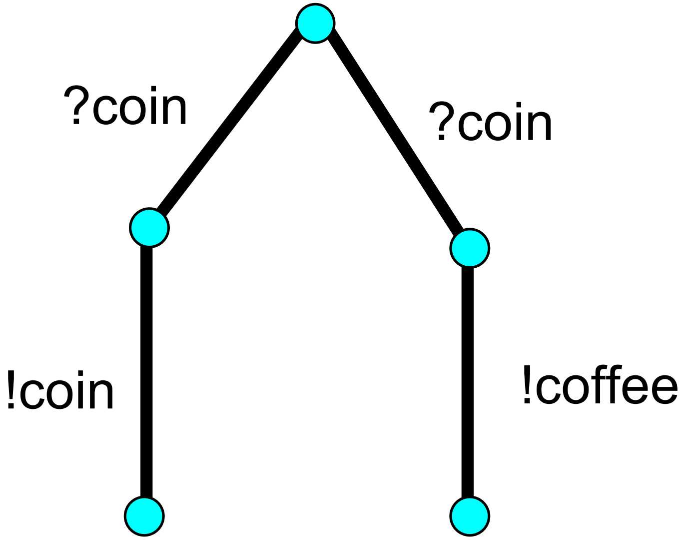
RESOURCES

- http://fmt.cs.utwente.nl/tools/torx/introduction.html
- http://www.testingworld.org/
- http://www.laquso.com/knowledge/toolstable.php
- http://www.irisa.fr/vertecs/
- http://www.cs.aau.dk/~marius/tuppaal/

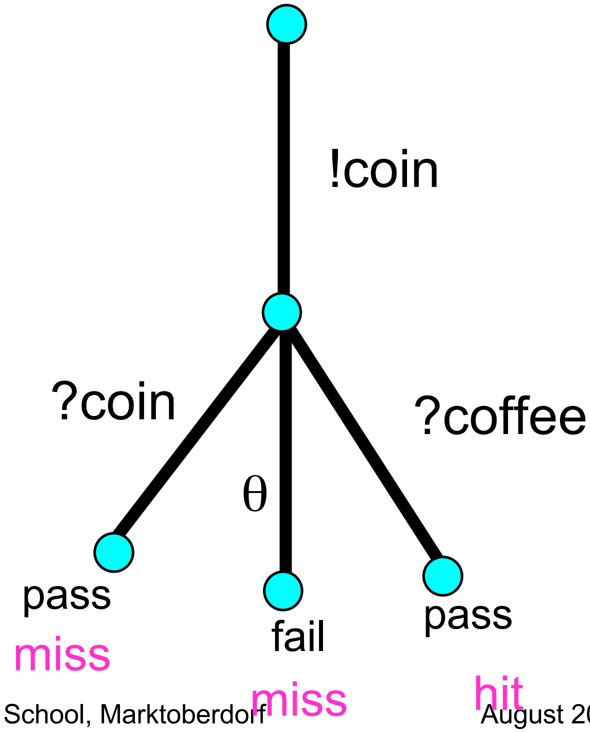
TEST SELECTION : TEST PURPOSES

- User specifies what (s)he wants to test :
  - very detailed behaviours
  - generic : criteria, strategies
- Questions :
  - Appropriate formalism for test purposes?
  - Relation between test purposes and test suites?
  - Interpretation of test results w.r.t. test purposes?
  - When is a test suite able to “challenge” the implementation to “satisfy” the test purpose?

TEST PURPOSE : EXAMPLE

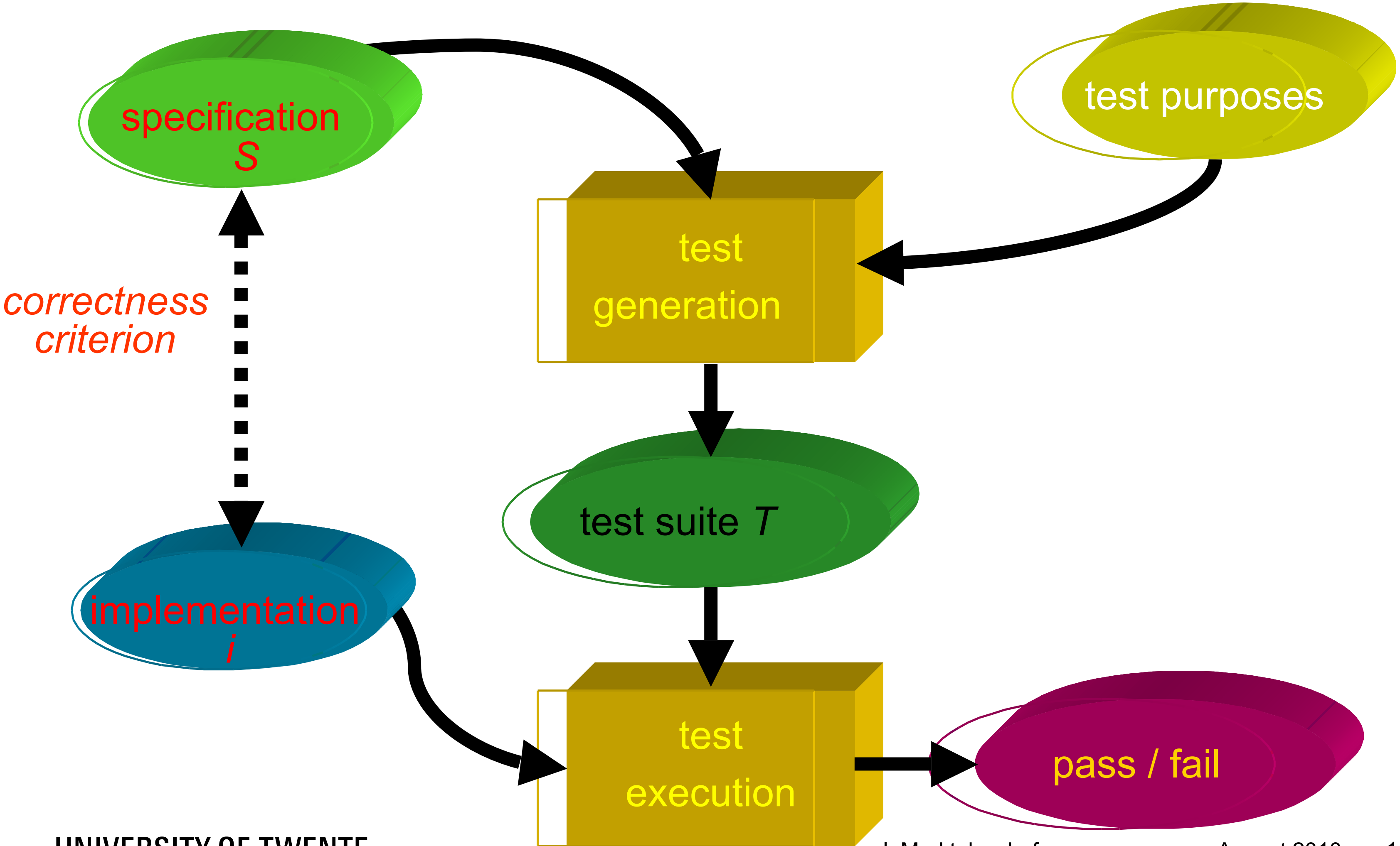


Test purpose:
can the machine deliver coffee?



Desired observation
= observation objective :
?coin . !coffee

TEST PURPOSES

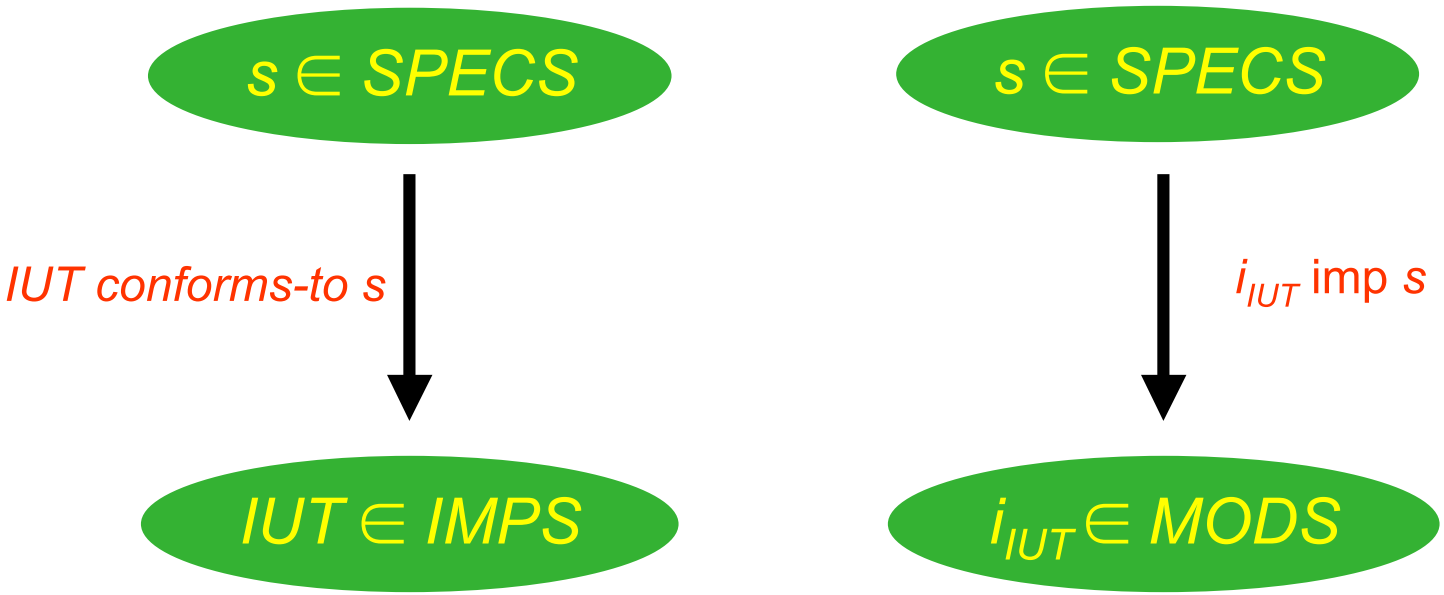


OBSERVATION OBJECTIVES

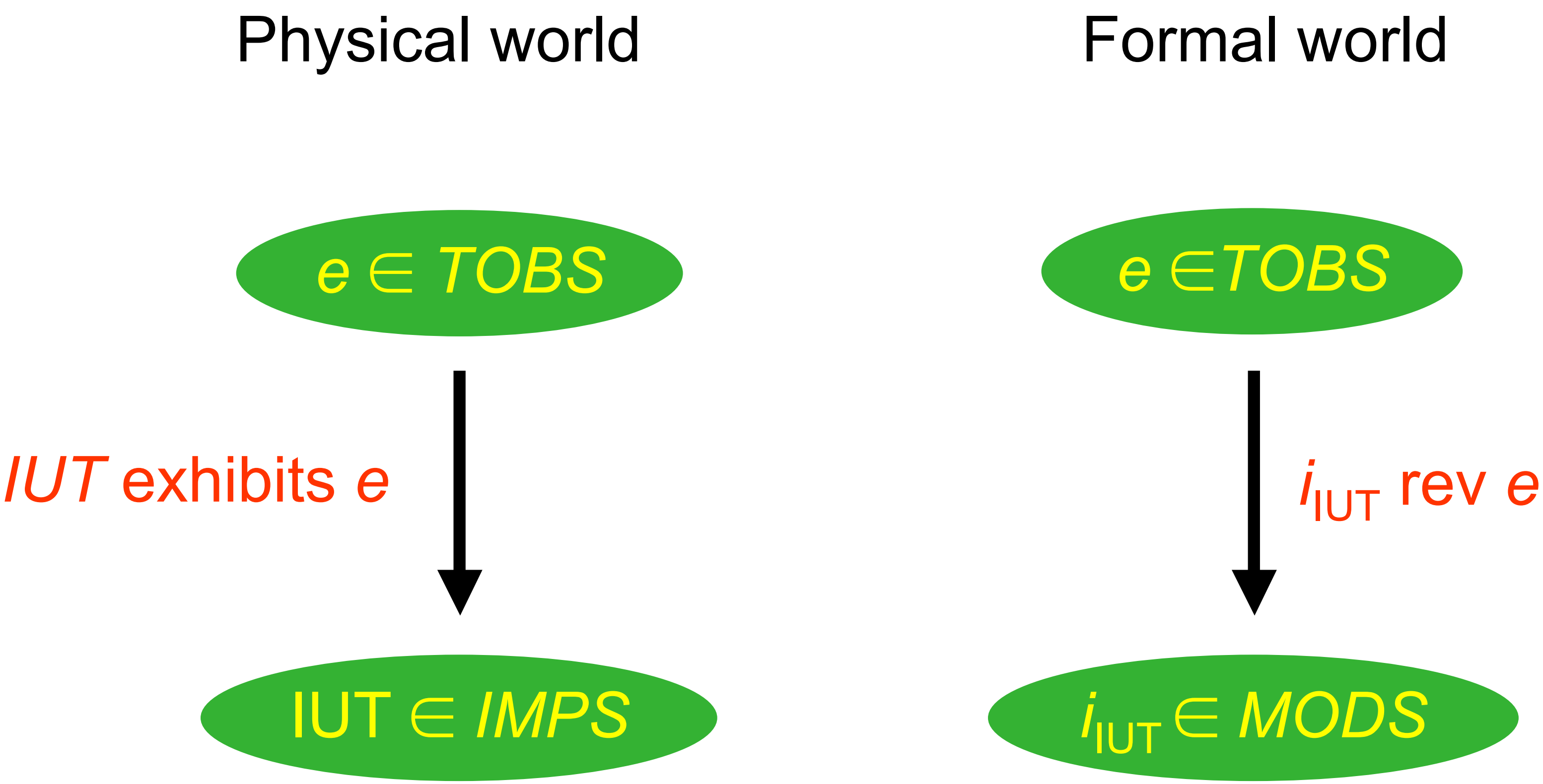
- Observation objective related to observations made during testing
- Steering the test in order to meet certain observations is *exhibition testing*
- Exhibition is orthogonal to conformance

TESTING FOR CONFORMANCE

Physical world | Formal world



TESTING FOR EXHIBITION



OBSERVATION & EXHIBITION

- hit-function :

  $H_e : P(OBS) \rightarrow \{ \text{hit}, \text{miss} \}$

- i hits e by t_e $=_{\text{df}}$ $H_e (EXEC (t_e, i)) = \text{hit}$

- i hits e by T_e $=_{\text{df}}$

  $H_e (\cup \{ EXEC (t_e, i) \mid t_\text{e} \in T_e \}) = \text{hit}$

TESTING FOR EXHIBITION

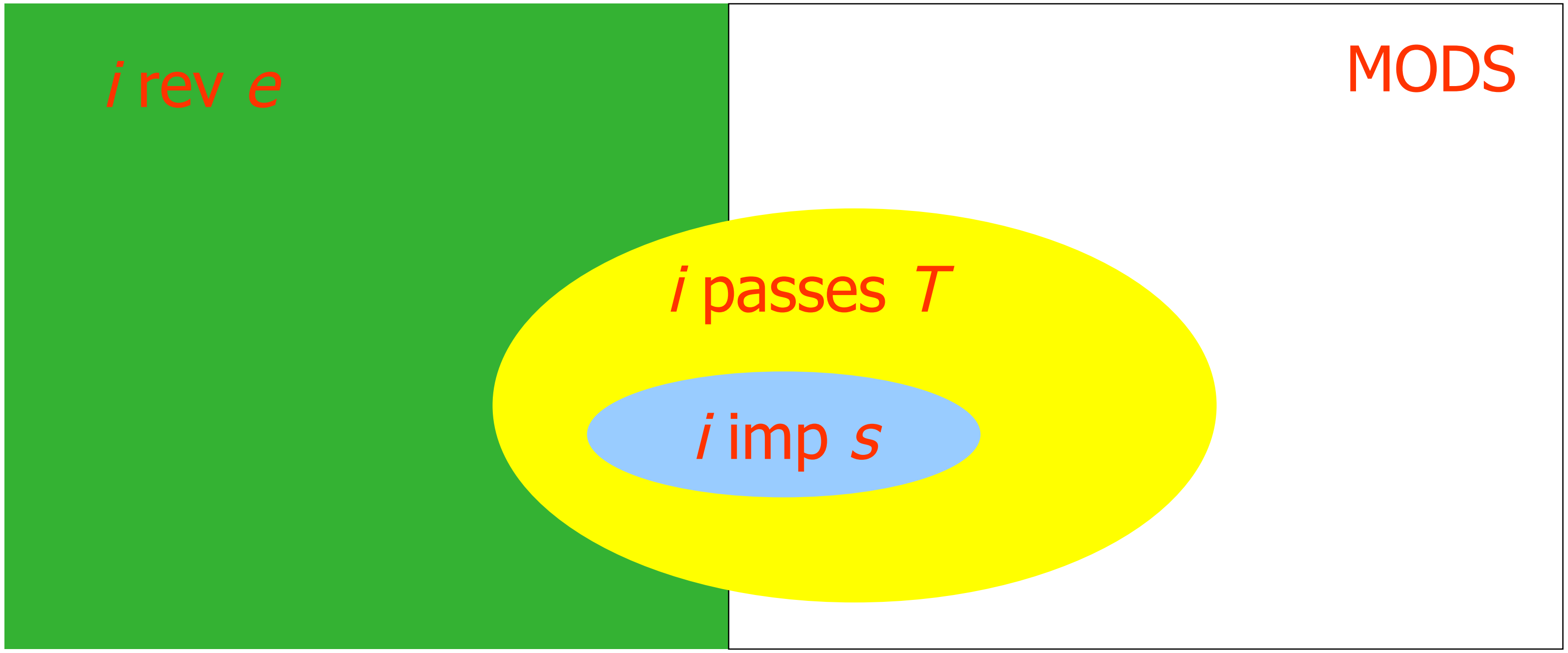
i hits e by T_e $\Leftrightarrow$ i rev e

e-sound : i rev e $\Leftarrow$ i hits e by T_e

e-exhaustive : i rev e $\Rightarrow$ i hits e by T_e

We want an e-sound and e-exhaustive test suite

COMBINING EXHIBITION AND CONFORMANCE



practical approach :

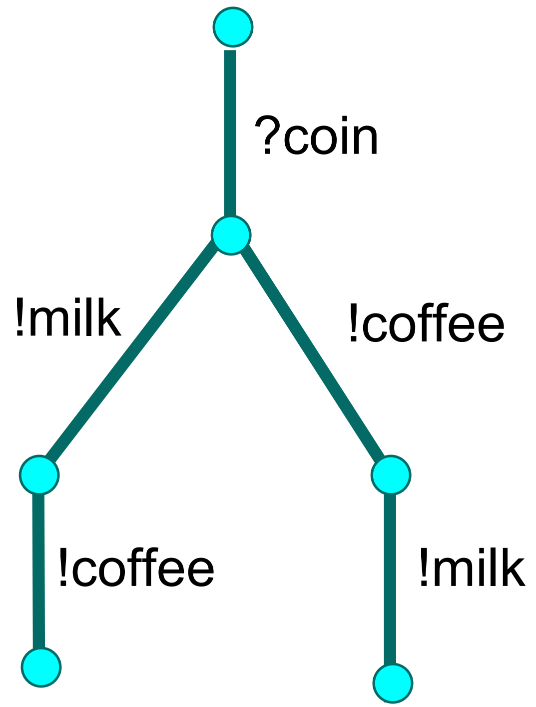
$\{ i \mid i \text{ hits } e \text{ by } T \} \cap \{ i \mid i \text{ imp } s \} \neq \emptyset$

IOTS : REVEAL RELATIONS

- $L_\delta = L_I \cup L_U \cup \{\delta\}$
- $TOBS = P((L_\delta)^*)$
- rev relation:

  i rios e $=_{df}$

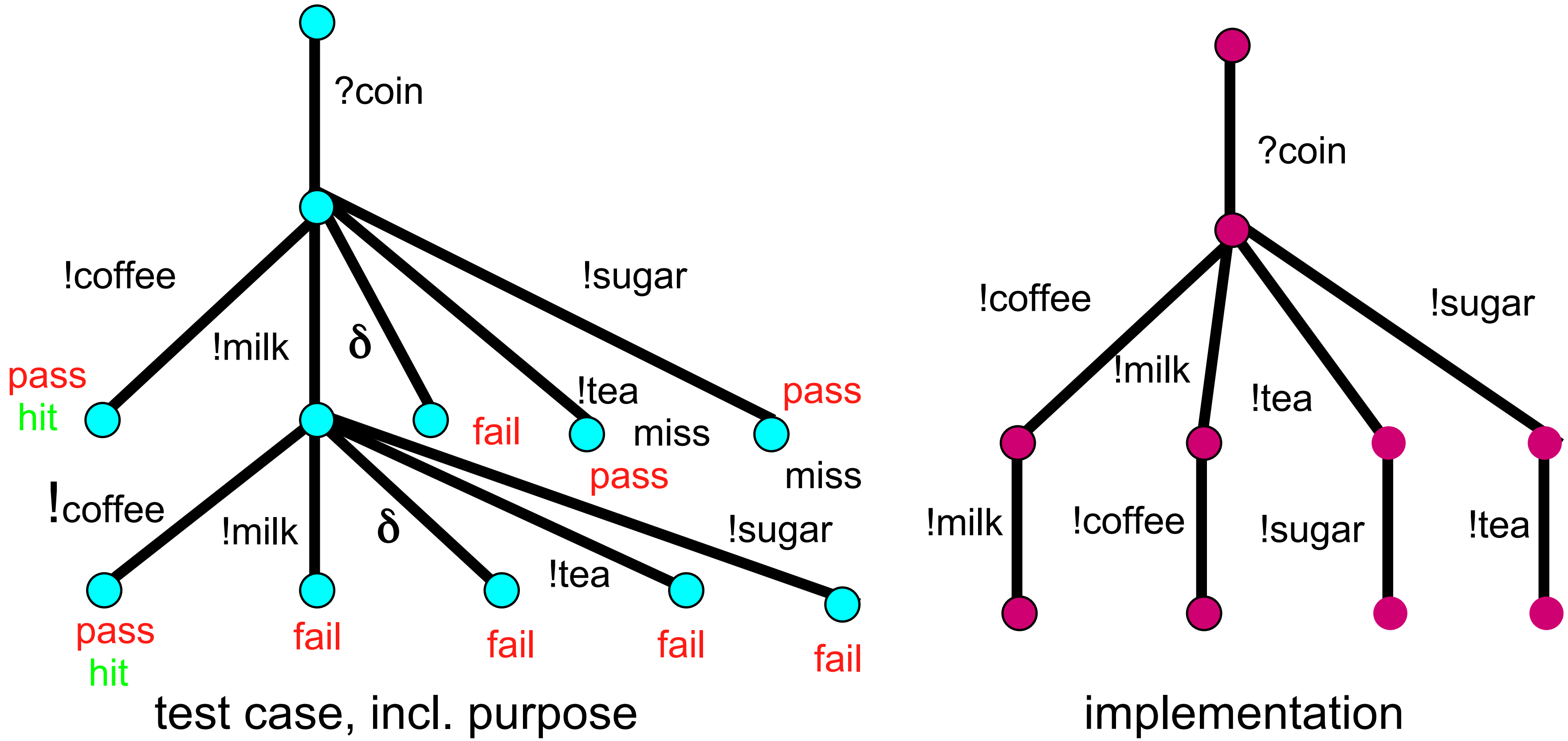
  $traces_\delta(i) \cap e \neq \emptyset$
- $H^{rios\text{-}e}(O) = hit \Leftrightarrow prefix(O) \cap e \neq \emptyset$



implementation

i rios { ?coin . !coffee, ?coin . !milk . !coffee}

TESTING FOR CONFORMANCE AND EXHIBITION



e = { ?coin . !coffee, ?coin . !milk . !coffee }

TORX : TEST PURPOSES, SELECTION, ……