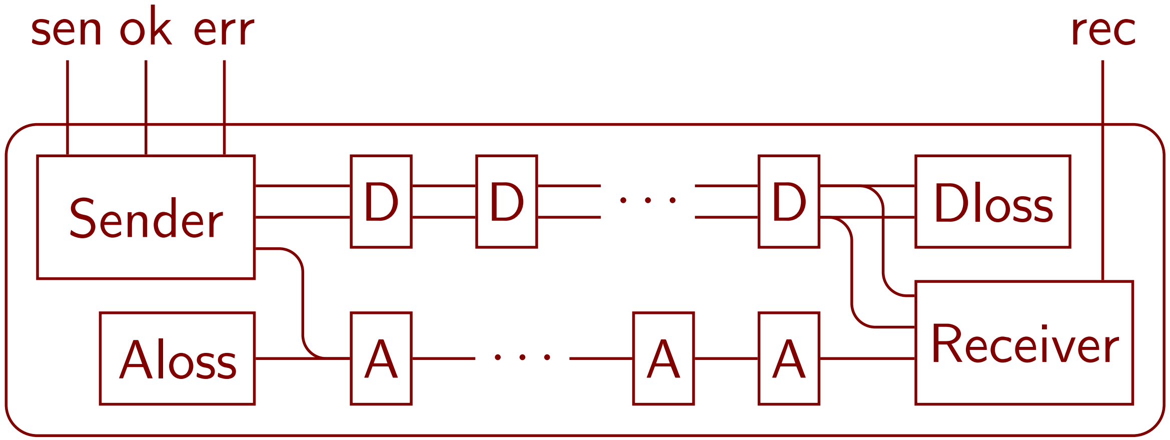
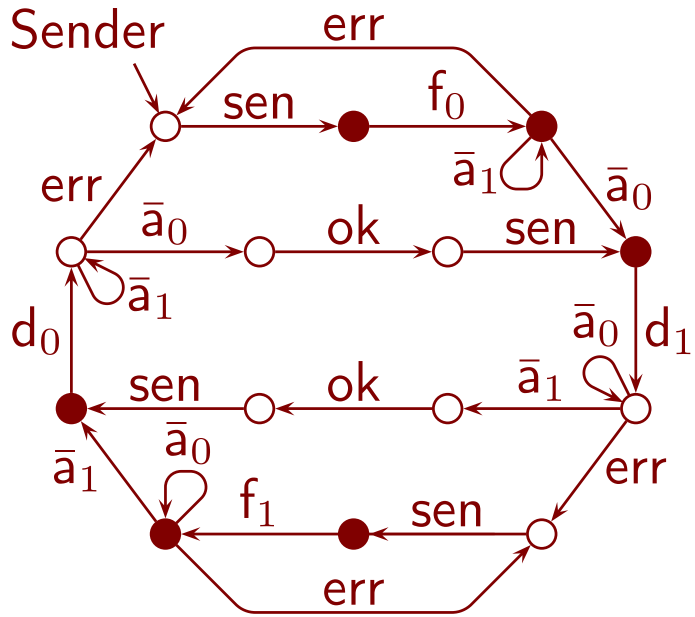
The Congruences Below Fair Testing with Initial Stability

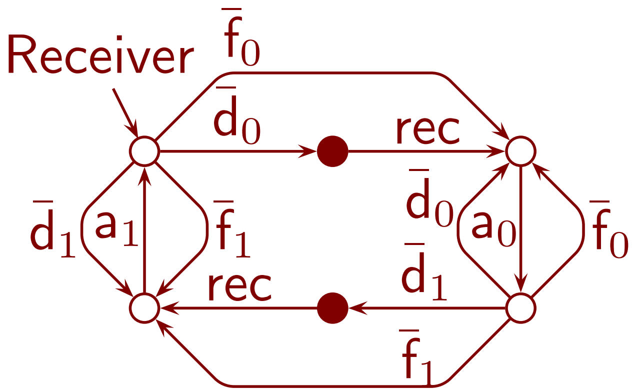
Antti Valmari

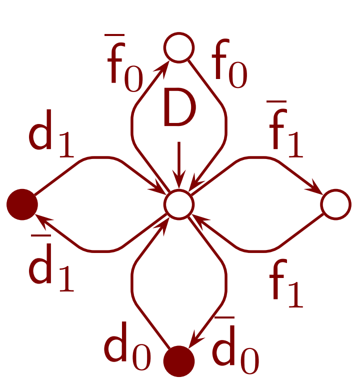
Tampere University of Technology
Department of Mathematics

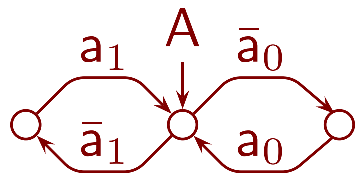
1 Introduction

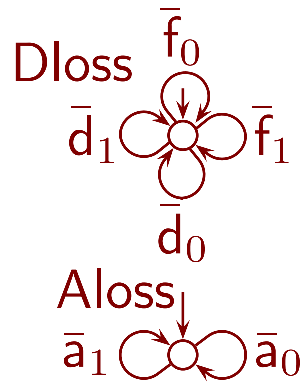












Labelled transition system $(S, \Sigma, \Delta, \hat{s})$

- $\tau \notin \Sigma, \quad \hat{s} \in S, \quad \Delta \subseteq S \times (\Sigma \cup \{\tau\}) \times S$
- both technical and "philosophical" reasons for Σ instead of a common global alphabet

Important operators for the present study

- *parallel composition* $L_1 \,||\, L_2$
  - L_1 and L_2 perform a synchronously if and only if $a \in \Sigma_1 \cap \Sigma_2$
- *hiding* $L \setminus A$
- *functional renaming* $\phi(L)$
- these suffice for representing architecture drawings

Additional discussed operators

- *relational renaming* $L\Phi$
  - may map a visible action to many visible actions, allows building $||_A$, ...
- *action prefix* $\tau.L$, $a.L$
- *choice* $L_1 + L_2$
- . and $+$ are widely used

Congruence

- an equivalence "$\cong$" such that for every LTS expression f only built from given operators and every L_1, ..., L_n, L'_1, ..., L'_n,

$$L_1 \cong L'_1 \wedge \cdots \wedge L_n \cong L'_n \;\Rightarrow\; f(L_1, \ldots, L_n) \cong f(L'_1, \ldots, L'_n)$$

- depends on the chosen operators
- facilitates multi-layer compositional analysis and LTS reduction of systems

2 The Fair Testing Congruence

An equivalence *preserves property* prop if and only if for every L_1 and L_2

$$L_1 \cong L_2 \ \Rightarrow\ \mathsf{prop}(L_1) = \mathsf{prop}(L_2)$$

- e.g., both or neither of L_1 and L_2 deadlock
- e.g., both or neither of Protocol1 and Protocol2 may deliver twice a message that has been only sent once

The weakest congruence that preserves prop is optimal for compositional analysis of prop

- widest collection of algorithms
  - reduction algorithms for stronger equivalences are valid

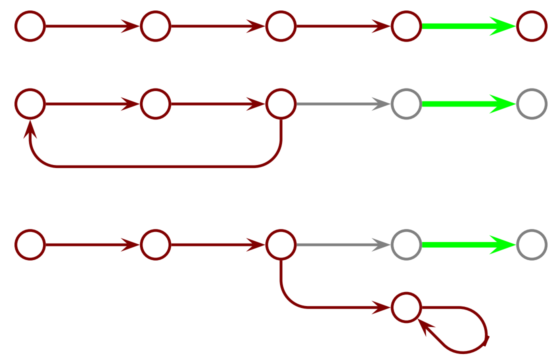
$\Rightarrow$ (potentially) best reduction results

Mainstream approach to verifying liveness uses *fairness assumptions*

- e.g., if infinitely many messages are sent, at least one gets through
- problematic regarding compositionality
- burden for modellers
- with protocols with connection phase and data transfer phase, may be ..., then at least once a message and one of the next three messages get through

Three kinds of possible futures

- the desired action eventually occurs
- the desired action does not occur but stays possible
- the desired action does not occur and eventually becomes impossible



Fair testing

- mainstream liveness treats "not occurs but stays possible" as not live
- fair testing treats it as live

$\Rightarrow$ fair testing guarantees liveness in a strictly weaker sense

- the sense is sometimes fully satisfactory and often better than nothing
- no fairness assumptions needed
- compositionality is obtained

The fair testing congruence

- [Brinksma, Rensink, Vogler 1995], [Rensink, Vogler 2007]
- the weakest congruence that preserves AG EF a
- a stubborn set method that preserves it exists [Valmari, Vogler SPIN 2016]
- difficult definition $\rightsquigarrow$ next slide

Trace equivalence

$$L_1 \cong_{\mathsf{tr}} L_2 \text{ if and only if } \Sigma(L_1) = \Sigma(L_2) \text{ and } \mathsf{Tr}(L_1) = \mathsf{Tr}(L_2)$$

Tree failure

- (σ, K) where $\sigma \in \mathsf{Tr}(L)$ and $K \subseteq \Sigma^+$ such that
  there is s such that $\hat{s} =\sigma\Rightarrow s$ and $s =\rho\Rightarrow$ for **no** $\rho \in K$
- that is, a *language* is refused instead of a set of actions
- s need not be *stable*
  - that is, $s -\tau\rightarrow$ is allowed
- $\varepsilon \notin K$, because ε cannot be refused and this convention simplifies the math

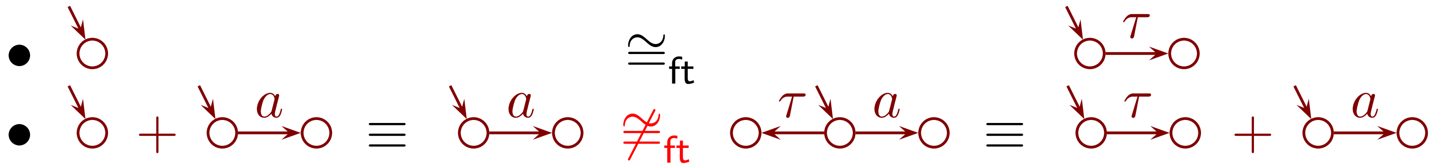
Fair testing equivalence

- $\pi^{-1}K \;=\; \{\rho \mid \pi\rho \in K\}$
- $L_1 \preceq L_2$ if and only if for every $(\sigma, K) \in \mathsf{Tf}(L_1)$
  - $(\sigma, K) \in \mathsf{Tf}(L_2)$, or
  - there is π such that $\pi^{-1}K \neq \emptyset$ and $(\sigma\pi, \pi^{-1}K) \in \mathsf{Tf}(L_2)$
- $L_1 \cong_{\mathsf{ft}} L_2$ if and only if $\Sigma_1 = \Sigma_2$, $L_1 \preceq L_2$, and $L_2 \preceq L_1$

$L_1 \cong_{\mathsf{ft}} L_2$ implies $L_1 \cong_{\mathsf{tr}} L_2$

3 Initial Stability

A congruence problem with $\cong_{\mathsf{ft}}$ and $+$



Widely used solution: *initial stability*

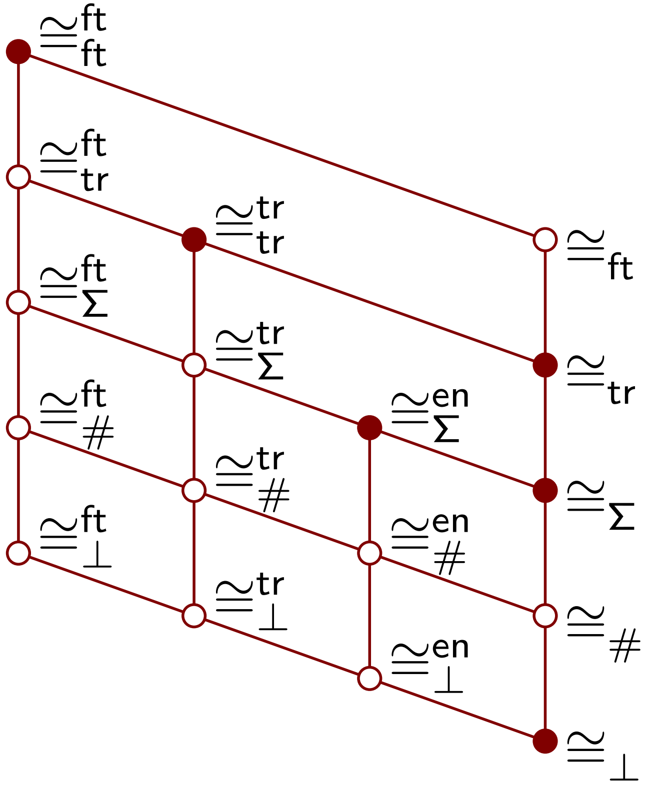
$$L_1 \cong L_2 \;\text{ if and only if } \;\ldots\; \text{and either none or both of } \hat{s}_1 \text{ and } \hat{s}_2 \text{ is stable}$$

- $\hat{s}_1$ is stable $\;\Leftrightarrow\; \neg(\hat{s}_1 -\tau\rightarrow)$

4 The Result

Theorem Only considering countable LTSs, all congruences w.r.t. $||$, $\backslash$, and ϕ that are implied by initial stability -preserving fair testing are in the picture

- $\cong_\Sigma$ only compares the alphabets
- $\cong_\perp$ compares nothing
  (yieds always "true")
- $\cong_\#$ will be discussed soon
- $\cong^x_y$ compares stable LTSs with $\cong_x$
  and unstable LTSs with $\cong_y$
- $\cong^x_y$ does and $\cong_y$ does not
  preserve initial stability
- $\cong^{\mathsf{en}}_y$ compares of stable LTSs
  only the alphabets and first actions
- line from $\cong_1$ down(-right) to $\cong_2$
  denotes that $\cong_1$ implies $\cong_2$



Only three are really interesting: $\cong^{\mathsf{ft}}_{\mathsf{ft}}$, $\cong_{\mathsf{ft}}$, and $\cong_{\mathsf{tr}}$

If Φ, ., and $+$ are added, then only $\cong^{\mathsf{ft}}_{\mathsf{ft}}$, $\cong^{\mathsf{tr}}_{\mathsf{tr}}$, $\cong_{\mathsf{tr}}$, $\cong^{\mathsf{en}}_\Sigma$, $\cong_\Sigma$, and $\cong_\perp$ remain

If you want something towards fair testing, you must take fair testing.

$\cong^{\mathsf{en}}_{\Sigma}$ (or $\cong^{\mathsf{en}}_{\perp}$) is the weakest congruence that preserves initial stability

- may be of some interest

The $\cong^{x}_{y}$ with $x \neq y$ compare stable LTSs with a stronger equivalence than unstable LTSs

- . can yield a stable LTS from an unstable one $\quad \tau.L_1 \cong_y \quad \tau.L_2$

$\Rightarrow$ excluding $\cong^{\mathsf{en}}_{\Sigma}$ they go away, when . is present $\quad a.\tau.L_1 \not\cong_x a.\tau.L_2$

- $\cong^{\mathsf{en}}_{\Sigma}$ does not go away, because for any L, the first action of $a.L$ is a

$L_1 \cong_{\#} L_2 \;\Leftrightarrow\;$ the difference of Σ_1 and Σ_2 is finite

- Φ makes $\cong_{\#}$ go away, because it can convert a finite difference to infinite
- if uncountable alphabets are allowed, there probably are $\cong^{\mathsf{ft}}_{y}$, $\cong^{\mathsf{tr}}_{y}$, $\cong^{\mathsf{en}}_{y}$, and $\cong_{y}$ for each uncountable cardinality y

So no new interesting congruences found, but

- it is surprising that there are none, because
  - $\cong_{\mathsf{ft}}$ seems branching-time: preserves the stereotypical AG EF a
  - the definition of $\cong_{\mathsf{ft}}$ seems quite ad-hoc
- now we will not search in vain for one
- there are remarkable differences to an earlier result
  - next slide

5 An Earlier Result

The operators are $||$, $\backslash$, Φ, and .

Theorem $\cong_\perp$ is the only congruence that is implied by $\equiv$ and does not preserve Σ

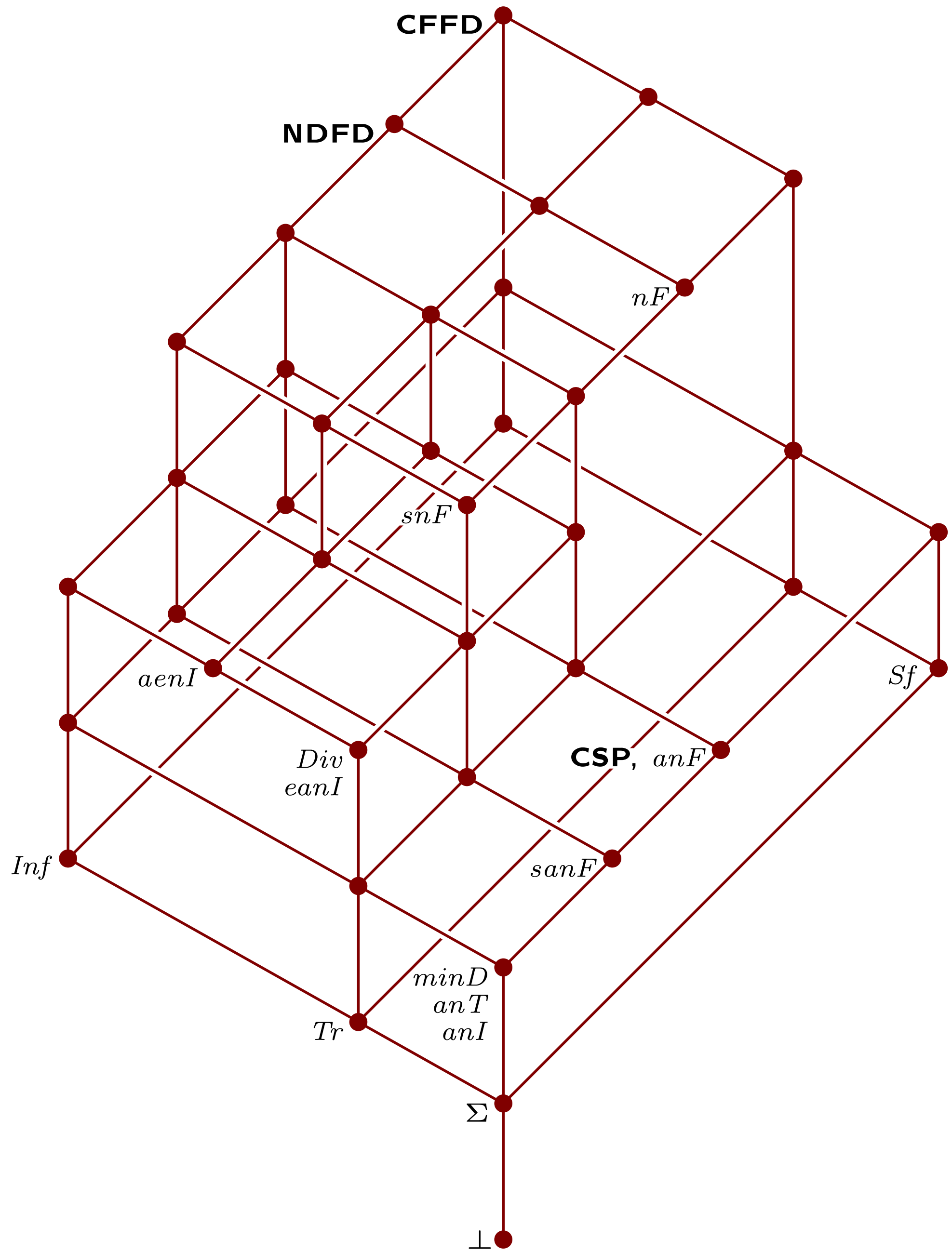
Theorem All congruences that are implied by $\cong_{\mathsf{CFFD}}$ are in the picture

- $L_1 \cong_{\mathsf{CFFD}} L_2$ if and only if
  - $\Sigma_1 = \Sigma_2$
  - $\mathsf{Sf}(L_1) = \mathsf{Sf}(L_2)$
  - $\mathsf{Div}(L_1) = \mathsf{Div}(L_2)$
  - $\mathsf{Inf}(L_1) = \mathsf{Inf}(L_2)$
- CSP-equivalence is there
- initial stability would at least add $\cong^{\mathsf{en}}_{\Sigma}$ and duplicate most congruences

The new results

- require significantly fewer operators
- yield significantly fewer new congruences

$\Rightarrow$ $\cong_{\mathsf{ft}}$ induces much fewer congruences than $\cong_{\mathsf{CFFD}}$



6 Discussion

A fairly large region of low-end congruences has now been fully covered

- for completeness, the region below "$\cong_{\mathrm{CFFD}}$" $\cap$ "$\cong_{\mathrm{ft}}^{\mathrm{ft}}$" should be studied
  - it would probably be hard and uninteresting
- of course, a lot is still uncovered
  - e.g., traces with failures in the middle and at the end
  - there are infinitely many weak bisimilarity -like congruences

Despite being branching-time and seemingly ad-hoc, $\cong_{\mathrm{ft}}$ has surprisingly simple behaviour

Sorry for telling nothing about the proofs ...

- a long series of lemmas develops technicalities that facilitate the main proof
- everything is in the paper
- the reviewers checked most or all of it
  - thanks for pointing out a small bug and for other good comments!

Thank you for attention!
Questions?