

Criteria for Observational Equivalence in Applied Π -calculus

Eike Ritter

University of Birmingham



Need sometimes symbolic way of deciding observational equivalence in applied Π -calculus

Reasons:

- Don't have always bi-processes
- Need logical conditions for static equivalences to hold

\Rightarrow Need to have good criteria to decide observational equivalence

Key problem: Quantification over *all* evaluation contexts

Proofs usually work in two steps:

- Reduce observational equivalence to set of static equivalences
- Prove static equivalences

Have a couple of useful lemmata for first step:

Lemma 1 *If $\nu\vec{n}.\{M/x\}|P|P' \approx \nu\vec{n}\{N/x\}|Q|Q'$, then $\nu\vec{n}.\bar{c}\langle M \rangle.P|P' \approx \nu\vec{n}.\bar{c}\langle N \rangle.Q|Q'$*

Lemma 2 $\nu\vec{n}, c.\bar{c}\langle M \rangle.P|c(x).Q \approx \nu\vec{n}, c.P|Q\{M/x\}$.

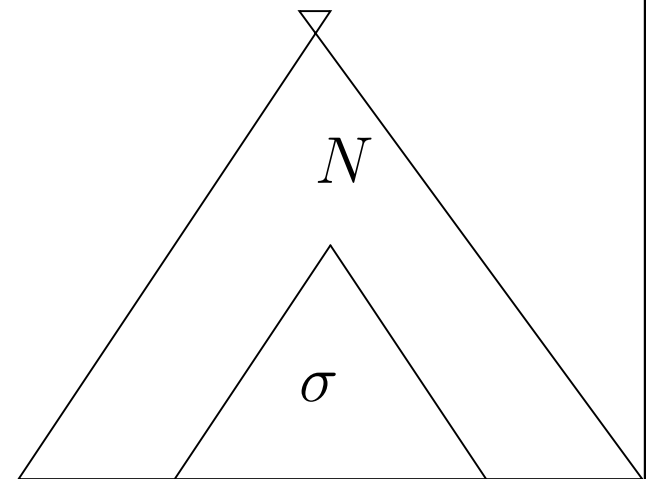
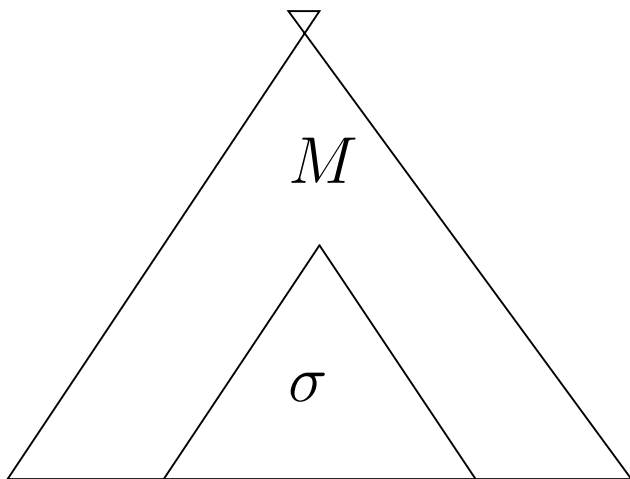
More complicated for input: need indeterminates

Proving static equivalences

First, simple case: Assume equational theory given by strongly normalising and confluent rewrite system

Moreover, ask for frame $\nu\vec{n}.\sigma$ to be *compatible with reduction*:

Let M be a term with no names in \vec{n} . Any rewrite of $M\sigma$ looks like



where $M \rightsquigarrow N$.

Can restrict ourselves to case when $M\sigma$ is an instance of a LHS of a reduction rule.

For frame $\nu\vec{n}.\sigma$ and term M with names possibly in \vec{n} define $\text{BNS}(M, \phi)$ to be the set of terms N with names not in \vec{n} such that $N\sigma = M$.



Criterion for Static Equivalence

Theorem 3 Assume $\phi \stackrel{\text{def}}{=} \nu \vec{n}.\sigma$ and $\psi \stackrel{\text{def}}{=} \nu \vec{n}.\tau$ are compatible with reduction. Then ϕ and ψ are statically equivalent iff

- (i) if $x\sigma$ contains no bound names, so does $x\tau$, and $x\sigma = x\tau$;
- (ii) For every variable x , if $x\sigma$ contains bound names,
 $\text{BNS}(x\sigma, \sigma) \subseteq \text{BNS}(x\tau, \tau)$.

and symmetric conditions hold.

Proof:

Assume $M\sigma = N\sigma$, with M and N not containing any bound names.

Interesting case: $M = x$, and $x\sigma$ contains bound names. Hence

$N \in \text{BNS}(M, \sigma) = \text{BNS}(x\sigma, \sigma)$. But $\text{BNS}(x\sigma, \sigma) = \text{BNS}(x\tau, \tau)$, hence

$x\tau = N\tau$.

Other direction:

If $x\sigma$ does not contain any bound names, consider equation $x = x\sigma$.

If $x\sigma$ contains bound names, consider element M of $\text{BNS}(x\sigma, \sigma)$. Have

$M\sigma = x\sigma \Rightarrow M\tau = x\tau \Rightarrow M \in \text{BNS}(x\tau, \tau)$.

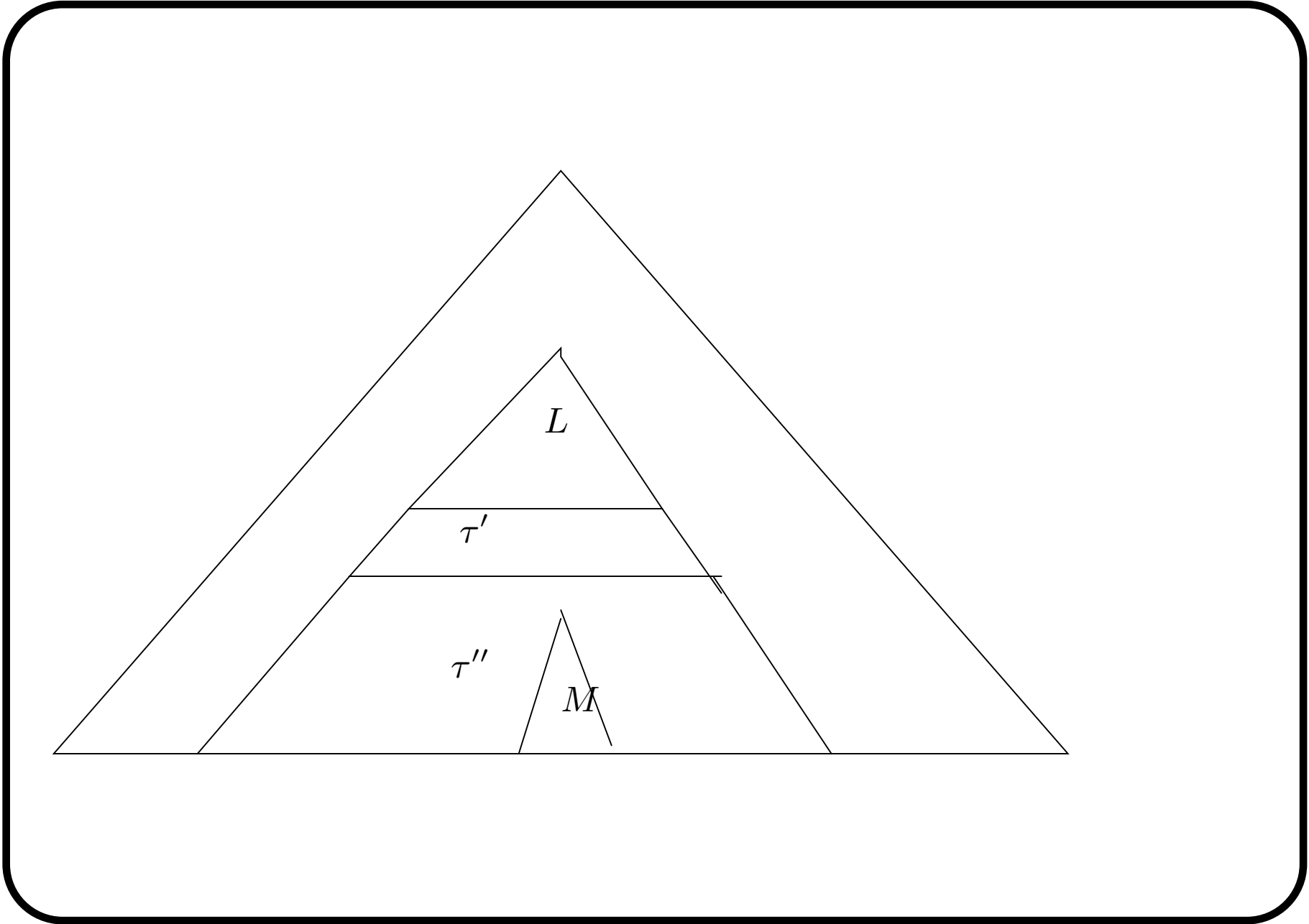
This reduces static equivalence to checks of occurrence.

Independence results:

Theorem 4 *Assume $\phi = \nu \vec{n}, \vec{m}. \{\sigma, M/x\}$ is a closed frame such that all names in \vec{m} are free names of M but not of σ such that*

- (i) There exists no terms N and N' with no names in \vec{n} nor \vec{m} such that $N\sigma \rightsquigarrow^* N'$; and M is a subterm of N' ;*
- (ii) Let N be any term which contains no names in \vec{n} nor \vec{m} . If $N\sigma \rightsquigarrow^* N'$ and $L\tau$ is a subterm of $N'\{M/x\}$ for some reduction rule $L \rightsquigarrow R$ and some substitution τ , then there exist substitutions τ' and τ'' such that $L\tau'\tau'' = L\tau$ and $L\tau'$ is a subterm of N' .*

Then ϕ is statically equivalent to $\nu \vec{n}, m. \{\sigma, m/x\}$, where m is a fresh name.



Simplified version:

Theorem 5 *Assume $\phi = \nu \vec{n}, \vec{m}. \{\sigma, M/x\}$ is a closed frame which is compatible with reduction such that all names in \vec{m} are free names of M but not of σ such that $\text{BNS}(y\sigma, \phi)$ does not contain x for all variables $y \neq x$. Then ϕ is statically equivalent to $\nu \vec{n}, m. \{\sigma, m/x\}$, where m is a fresh name.*



This covers important cases of cryptographic protocols:

Symmetric encryption:

Have equations like

$$\text{dec}(\text{enc}(x, y), y) \rightsquigarrow x$$

and frames like

$$\phi \stackrel{\text{def}}{=} \nu \vec{n}, k. \{ \sigma, \text{enc}(M, k) / x \}$$

If key k is secret (either does not occur in σ or only in terms enc), ϕ is compatible with reduction if $\nu \vec{n}, k. \sigma$ is.

If in addition, $y\sigma \neq \text{enc}(M, k)$ for all variables y in σ , then ϕ is statically equivalent to $\nu \vec{n}, m. \{ \sigma, m / x \}$.

Proverif shows all concrete instances of these theorems

Abadi and Cortier give general criterion for rewrite systems

Assumption: firstly, rewriting does not increase term size too much
secondly, terms obtained by re-writing frames don't expose additional
bound names

⇒ for each frame ϕ , obtain finite set of equations which characterise
static equivalence

In general, this set is a superset of the equations considered in the
theorem.

Further work

Give a criterion for static equivalence also in the case where frames are non-compatible with reduction
 \Rightarrow obtain stronger version of theorem 4.