# Axiomatising Verdict Equivalence over Regular monitors

Elli Anastasiadi

Reykjavik University

HÁSKÓLINN Í REYKJAVÍK
REYKJAVIK UNIVERSITY


12th Panhellenic Logic Symposium
June 26-30, Anogeia, Greece

# The field

Processes and Concurrency, Modeling (Mathematical), Monitors, Formal Verifications, Equational Logic

# The field

Processes and Concurrency, Modeling (Mathematical), Monitors, Formal Verifications, Equational Logic

Why?

# The field

Processes and Concurrency, Modeling (Mathematical), Monitors, Formal Verifications, Equational Logic

Why?

- To describe actual systems (make models) - LTS, process description language CCS
- To write desirable (or not) behaviors about our models - HML, system terms
- Final purpose is to (almost)-automatically analyze and manipulate these descriptions - both the models and their properties

# How to define and check properties

One way to go about it: Monitors!

# How to define and check properties

One way to go about it: Monitors!

Little gadgets that are build to read and categorize traces which are produced by processes. Monitors are to processes, ***almost*** what automata are to formal languages.

# How to define and check properties

One way to go about it: Monitors!

Little gadgets that are build to read and categorize traces which are produced by processes. Monitors are to processes, ***almost*** what automata are to formal languages.

- They have their own syntax and correspond to different sets of processes accordingly.

# How to define and check properties

One way to go about it: Monitors!

Little gadgets that are build to read and categorize traces which are produced by processes. Monitors are to processes, ***almost*** what automata are to formal languages.

- They have their own syntax and correspond to different sets of processes accordingly.

The ones we study in this work (Regular):

$$m, n ::= \quad v \quad | \quad a.m \quad | \quad m + n \quad | \quad x$$

$$v ::= end \quad | \quad yes \quad | \quad no,$$

where $a \in Act$ and $x \in Var$.

The terms "*end*", "*yes*" and "*no*" are called *verdicts*.

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

Not particularly useful

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

Not particularly useful

**Comments**

- Dual verdicts are allowed for the same trace

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

Not particularly useful

**Comments**

- Dual verdicts are allowed for the same trace
- Verdicts are irrevocable

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

Not particularly useful

**Comments**

- Dual verdicts are allowed for the same trace
- Verdicts are irrevocable
- Looks like a very restricted automaton.

# Example Monitor

$$m = a.a.a.a.yes + a.b.no + a.a.a \ldots .end$$

Not particularly useful

**Comments**

- Dual verdicts are allowed for the same trace
- Verdicts are irrevocable
- Looks like a very restricted automaton.

We start so restricted because the complexity for model checking can get very easily out of hand.

# Equivalences

For all monitors $m$ we can define the following sets of traces:

$L_a(m) = \{s \in Act^* \mid m \stackrel{s}{\Rightarrow} yes\}$ and $L_r(m) = \{s \in Act^* \mid m \stackrel{s}{\Rightarrow} no\}$.

## Notions of Equivalence

- Verdict equivalence: $L_a(m) = L_a(n)$ and $L_r(m) = L_r(n)$
- $\omega$-Verdict Equivalence: $L_a(m) \cdot Act^\omega = L_a(n) \cdot Act^\omega$ and $L_r(m) \cdot Act^\omega = L_r(n) \cdot Act^\omega$

# Our goal

Find a sound and complete axiomatixation for each of the above notions of equivalence.

# Our goal

Find a sound and complete axiomatixation for each of the above notions of equivalence.

- A finite set of equations $t \approx u$ over the syntax of our monitors that are sound and can prove all other valid equalities.

# Our goal

Find a sound and complete axiomatixation for each of the above notions of equivalence.

- A finite set of equations $t \approx u$ over the syntax of our monitors that are sound and can prove all other valid equalities.

**Equational Logic**

An equation $t \simeq u$ is derivable from an axiom system $\mathcal{E}$ (notation $\mathcal{E} \vdash u = t$) if it can be proven from the axioms in $\mathcal{E}$ using the rules of equational logic (reflexivity, symmetry, transitivity, substitution and closure under our the monitor context)

# Our goal

Find a sound and complete axiomatixation for each of the above notions of equivalence.

- A finite set of equations $t \approx u$ over the syntax of our monitors that are sound and can prove all other valid equalities.

**Equational Logic**

An equation $t \simeq u$ is derivable from an axiom system $\mathcal{E}$ (notation $\mathcal{E} \vdash u = t$) if it can be proven from the axioms in $\mathcal{E}$ using the rules of equational logic (reflexivity, symmetry, transitivity, substitution and closure under our the monitor context)

Some times such a thing does not exist.

## Candidate Axioms

- $A1$: $x + y = y + x$
- $A2$: $x + (y + z) = (x + y) + z$
- $A3$: $x + x = x$
- $A4$: $x + end = x$
- $E1_a$: $a.end = end$
- $Y_a$: $yes = yes + a.yes$
- $N_a$: $no = no + a.no$
- $D1$: $a.(x + y) = a.x + a.y$

## Candidate Axioms

- $A1$: $x + y = y + x$
- $A2$: $x + (y + z) = (x + y) + z$
- $A3$: $x + x = x$
- $A4$: $x + end = x$
- $E1_a$: $a.end = end$
- $Y_a$: $yes = yes + a.yes$
- $N_a$: $no = no + a.no$
- $D1$: $a.(x + y) = a.x + a.y$

Notes:

- Variables are used to represent any monitor term.

## Candidate Axioms

- $A1$: $x + y = y + x$
- $A2$: $x + (y + z) = (x + y) + z$
- $A3$: $x + x = x$
- $A4$: $x + end = x$
- $E1_a$: $a.end = end$
- $Y_a$: $yes = yes + a.yes$
- $N_a$: $no = no + a.no$
- $D1$: $a.(x + y) = a.x + a.y$

Notes:

- Variables are used to represent any monitor term.
- Axioms $E1_a$, $Y_a$ and $N_a$ depend on the number of actions in our systems. There is a version of those for each action.

# Proofs

- Soundness is proved via mutual inclusion of the accepting and rejecting sets of each equation's side.

# Proofs

- Soundness is proved via mutual inclusion of the accepting and rejecting sets of each equation's side.
- Completeness?

# Proofs

- Soundness is proved via mutual inclusion of the accepting and rejecting sets of each equation's side.
- Completeness?
  1. Prove that each monitor has a specific form (called normal).

# Proofs

- Soundness is proved via mutual inclusion of the accepting and rejecting sets of each equation's side.
- Completeness?
  1. Prove that each monitor has a specific form (called normal).
  2. Prove properties of each normal form.

# Proofs

- Soundness is proved via mutual inclusion of the accepting and rejecting sets of each equation's side.
- Completeness?
  1. Prove that each monitor has a specific form (called normal).
  2. Prove properties of each normal form.
  3. Structural Induction : Assume an arbitrary valid equation and prove the relevant normal forms are identical.

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

## Properties

- The only normal form that does not contain occurrences of "*yes*" and "*no*" is "*end*".

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

## Properties

- The only normal form that does not contain occurrences of "$yes$" and "$no$" is "$end$".
- For each action $a$, if $m$ is a "$no$"-free term then $yes + a.m = yes$.

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

## Properties

- The only normal form that does not contain occurrences of "$yes$" and "$no$" is "$end$".
- For each action $a$, if $m$ is a "$no$"-free term then $yes + a.m = yes$. Symmetrically for "$no$".

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

## Properties

- The only normal form that does not contain occurrences of "$yes$" and "$no$" is "$end$".
- For each action $a$, if $m$ is a "$no$"-free term then $yes + a.m = yes$. Symmetrically for "$no$".
- If $m$ contains occurrences of "$no$" then $yes + a.m = yes + a.n$ for some"$yes$"-free monitor n.

# A monitor in normal form

$$m = \sum_{a \in A} a.m_a \ [+yes] \ [+no],$$

## Properties

- The only normal form that does not contain occurrences of "$yes$" and "$no$" is "$end$".
- For each action $a$, if $m$ is a "$no$"-free term then $yes + a.m = yes$. Symmetrically for "$no$".
- If $m$ contains occurrences of "$no$" then $yes + a.m = yes + a.n$ for some"$yes$"-free monitor n. Symmetrically for "$yes$"

Conveniently this far: No variables!

Conveniently this far: No variables!

- These axioms are not complete for open terms

Conveniently this far: No variables!

- These axioms are not complete for open terms
- There are some equations that are valid and these axioms cannot prove (Ex. $yes + no = yes + no + x$)

Conveniently this far: No variables!

- These axioms are not complete for open terms
- There are some equations that are valid and these axioms cannot prove (Ex. $yes + no = yes + no + x$)
- We expand the axiom system (usually by the equations we fail to prove)

Conveniently this far: No variables!

- These axioms are not complete for open terms
- There are some equations that are valid and these axioms cannot prove (Ex. $yes + no = yes + no + x$)
- We expand the axiom system (usually by the equations we fail to prove)

Lately we have stumbled upon various equations that are not provable when there are variables involved.

Conveniently this far: No variables!

- These axioms are not complete for open terms
- There are some equations that are valid and these axioms cannot prove (Ex. $yes + no = yes + no + x$)
- We expand the axiom system (usually by the equations we fail to prove)

Lately we have stumbled upon various equations that are not provable when there are variables involved.
There is always hope!
We also have a complete axiomatization of verdict and $\omega$-verdict equivalence for open terms when the set of actions is infinite. :)

Conveniently this far: No variables!

- These axioms are not complete for open terms
- There are some equations that are valid and these axioms cannot prove (Ex. $yes + no = yes + no + x$)
- We expand the axiom system (usually by the equations we fail to prove)

Lately we have stumbled upon various equations that are not provable when there are variables involved.
There is always hope!
We also have a complete axiomatization of verdict and $\omega$-verdict equivalence for open terms when the set of actions is infinite. :)

Hint: Design a substitution for the variables of a term that is one to one and reversible from open to closed monitors.

# Conclusion

Next steps:

- $\omega$-verdict equivalence for closed terms ($\surd$ )
- verdict equivalence for open terms and finite actions (almost $\surd$ )
- $\omega$-verdict equivalence for open terms and finite actions (almost $\surd$ but more work to be done)

# Conclusion

Next steps:

- $\omega$-verdict equivalence for closed terms ($\surd$ )
- verdict equivalence for open terms and finite actions (almost $\surd$ )
- $\omega$-verdict equivalence for open terms and finite actions (almost $\surd$ but more work to be done)

Interesting Questions:

- What separates regular monitors form other kinds that do not have finite axiomatizations.
- Other notions of equivalence and correlation with their axiomatizability results.

Thank you for your attention!

Questions?