Some of my Favourite Open Problems in the Equational Logic of Processes

Luca Aceto
ICE-TCS, School of Computer Science, Reykjavik University
Open Problems in Concurrency Theory
Bertinoro, 20 June 2014

Why This Talk at OPCT and in 2014?

Why This Talk at OPCT and in 2014?

Goal (Hope?)

- To rekindle interest in some questions that I hope will be solved before I sign off.
- To issue a call to arms (and to myself).

Why This Talk at OPCT and in 2014?

Goal (Hope?)

- To rekindle interest in some questions that I hope will be solved before I sign off.
- To issue a call to arms (and to myself).

What questions?

The Role of Equational Logic in Process Algebra

Motto: In process algebra, we use formal languages to describe reactive systems and specifications of their expected behaviour.

Fact of Life: We often need to know when two syntactically different descriptions are describing the "same thing".

> *Correctness: Is SPECification equivalent to IMPlementation?*

Tenet: Equational logic can be used to capture "valid" equivalences. In process algebra, the equational characterization of parallel composition is key.

Finite, Complete Axiomatizations

The Challenge

Given some algebraic signature Σ, and some congruence $\sim$ over (closed) terms

Is there a finite set $\mathcal{E}$ of Σ-equations $s = t$ such that

$$t \sim u \quad \Leftrightarrow \quad \mathcal{E} \vdash t = u$$

for all (closed) Σ-terms t, u?

$\mathcal{E}$ is called a sound and (ground-)complete axiomatization.

Why is This an Interesting Game?

Why is This an Interesting Game?

A non-answer

I have always liked it!

Why is This an Interesting Game?

A non-answer

I have always liked it!

The official answer

An equational axiomatization

1. tells ye all ye need to know about your notion of program equivalence;
2. allows you to relate it to other types of program equivalence by simply looking at laws;
3. may form the basis for program verification tools based on theorem proving technology. (See J.F. Groote's talk later today.)

The Cold Shower

Empirically proven fact

The life of a concurrency theorist is equationally hard.

In many situations, the collection of valid equivalences cannot be "captured" by means of a finite collection of equations. This holds true even for very simple languages!

There are still (natural) open problems in this area.

The Cold Shower

Empirically proven fact

The life of a concurrency theorist is equationally hard.

In many situations, the collection of valid equivalences cannot be "captured" by means of a finite collection of equations. This holds true even for very simple languages!

There are still (natural) open problems in this area.

Rest of the Talk

- Examples of problems I'd like to see solved.
- A suggestion.

A Core Language: CCS

The Language

CCS nil $\mathbf{0}$ prefixing at variables x
choice $t + u$ parallel $t \| u$

where a is an action drawn from a non-empty, finite set A. We assume A includes τ and complementary actions.

A Core Language: CCS

The Language

CCS nil $\mathbf{0}$ prefixing at variables x
choice $t + u$ parallel $t \| u$

where a is an action drawn from a non-empty, finite set A. We assume A includes τ and complementary actions.

Its (Operational) Semantics (Sample Rules)

Given by transitions between terms of the form $t \xrightarrow{a} u$. These associate a loop-free finite automaton with each term. How?

$$\frac{}{ax \xrightarrow{a} x} \qquad \frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'} \qquad \frac{x \xrightarrow{a} x'}{x \| y \xrightarrow{a} x' \| y} \qquad \frac{x \xrightarrow{a} x',\ y \xrightarrow{\bar{a}} y'}{x \| y \xrightarrow{\tau} x' \| y'}$$

Axiomatizing strong bisimilarity

Consider strong bisimilarity $\underline{\leftrightarrow}$.

Fact: Strong bisimilarity is a congruence over CCS and all of its "reasonable extensions".

Axiomatizing strong bisimilarity

Consider strong bisimilarity $\underline{\leftrightarrow}$.

Fact: Strong bisimilarity is a congruence over CCS and all of its "reasonable extensions".

Motivating Question

Is there a (finite) collection of equations (valid with respect to $\underline{\leftrightarrow}$) that allows us to prove all the valid (ground) equivalences modulo $\underline{\leftrightarrow}$ over CCS?

An Axiom System $\mathcal{E}$ for Bisimilarity over CCS

$$\begin{aligned} x + y &= y + x \\ (x + y) + z &= x + (y + z) \\ x + x &= x \\ x + \mathbf{0} &= x \end{aligned}$$

$$\sum_{i \in I} a_i x_i \parallel \sum_{j \in J} b_j y_j =$$

$$\sum_{i \in I} a_i (x_i \parallel y) + \sum_{j \in J} b_j (x \parallel y_j) + \sum_{i \in I, j \in J, a_i = \overline{b_j}} \tau (x_i \parallel y_j)$$

Soundness & completeness (Hennessy and Milner, circa 1980):
$t \leftrightarrows u \Leftrightarrow \mathcal{E} \vdash t = u$, for all ground CCS terms t, u.

An Axiom System $\mathcal{E}$ for Bisimilarity over CCS

$$\begin{aligned} x + y &= y + x \\ (x + y) + z &= x + (y + z) \\ x + x &= x \\ x + \mathbf{0} &= x \end{aligned}$$

$$\sum_{i \in I} a_i x_i \parallel \sum_{j \in J} b_j y_j =$$

$$\sum_{i \in I} a_i (x_i \parallel y) + \sum_{j \in J} b_j (x \parallel y_j) + \sum_{i \in I, j \in J, a_i = \overline{b_j}} \tau (x_i \parallel y_j)$$

Soundness & completeness (Hennessy and Milner, circa 1980):

$t \leftrightarrows u \Leftrightarrow \mathcal{E} \vdash t = u$, for all ground CCS terms t, u.

Groovy! But, can one obtain a finite axiomatization?

Some classic results

Theorem (Bergstra and Klop 1984, yours truly et al. ICALP 2006)

Bisimilarity affords a finite complete axiomatization over CCS with left and communication merge.

Some classic results

Theorem (Bergstra and Klop 1984, yours truly et al. ICALP 2006)

Bisimilarity affords a finite complete axiomatization over CCS with left and communication merge.

Theorem (Moller)

No "reasonable" congruence affords a finite equational axiomatization over CCS (without auxiliary operators). Bisimilarity is "reasonable".

Some classic results

Theorem (Bergstra and Klop 1984, yours truly et al. ICALP 2006)

Bisimilarity affords a finite complete axiomatization over CCS with left and communication merge.

Theorem (Moller)

No "reasonable" congruence affords a finite equational axiomatization over CCS (without auxiliary operators). Bisimilarity is "reasonable".

Proof idea (for bisimilarity): No finite, sound axiom system $\mathcal{E}$ over CCS is powerful enough to prove the sound equation

$$a \| \sum_{i=1}^{n} a^i = a(\sum_{i=1}^{n} a^i) + \sum_{i=2}^{n+1} a^i \qquad (n > \mathrm{size}(\mathcal{E})) \ .$$

Axiomatizing $\underline{\leftrightarrow}$ over full recursion-free CCS

We have known for ages how to give a ground-complete axiomatization $\underline{\leftrightarrow}$ over full recursion-free CCS (with left-merge and synchronization merge), but...

Problem 1

1. Does bisimilarity afford a finite complete axiomatization over recursion-free CCS (with left and communication merge)?
2. Give a complete axiomatization of bisimilarity over recursion-free CCS (with left and communication merge).

Axiomatizing $\underline{\leftrightarrow}$ over full recursion-free CCS

We have known for ages how to give a ground-complete axiomatization $\underline{\leftrightarrow}$ over full recursion-free CCS (with left-merge and synchronization merge), but...

Problem 1

1. Does bisimilarity afford a finite complete axiomatization over recursion-free CCS (with left and communication merge)?
2. Give a complete axiomatization of bisimilarity over recursion-free CCS (with left and communication merge).

The following paper does not consider synchronization:
Luca Aceto, Anna Ingólfsdóttir, Bas Luttik and Paul van Tilburg. Finite Equational Bases for Fragments of CCS with Restriction and Relabelling. IFIP TCS 2008: 317–332.

Auxiliary operators

Bergstra and Klop taught us how to give a finite axiomatization of parallel composition, modulo $\underline{\leftrightarrow}$, using the left and communication merge operators.

Problem 2

Is there a single auxiliary binary operator f that can be used to axiomatize bisimilarity over CCS as presented earlier? Conjecture: No. Prove or disprove.

Auxiliary operators

Bergstra and Klop taught us how to give a finite axiomatization of parallel composition, modulo $\leftrightarrow$, using the left and communication merge operators.

Problem 2

Is there a single auxiliary binary operator f that can be used to axiomatize bisimilarity over CCS as presented earlier? Conjecture: No. Prove or disprove.

Simplifying assumptions from a 50-page draft from 2003

- The behaviour of f is described by rules in de Simone format.
- For some $J \subseteq \{x, y\}^2$,

$$x \parallel y \leftrightarrow \sum \{f(z_1, z_2) \mid (z_1, z_2) \in J\}.$$

Optimizing "Turning SOS rules into equations"

In 1992, Bloom, Vaandrager and I gave an algorithm for generating ground-complete axiomatizations of $\underline{\leftrightarrow}$ from GSOS languages.

Problem 3

1. Optimize algorithms for the generation of ground-complete axiomatizations from SOS specifications so that they generate axiom systems close to hand-crafted ones.
2. How about generating complete axiomatizations for some classes of languages?

Luca Aceto, Eugen-Ioan Goriac, Anna Ingólfsdóttir, Mohammad Reza Mousavi, Michel A. Reniers. Exploiting Algebraic Laws to Improve Mechanized Axiomatizations. CALCO 2013: 36–50

Extending Moller's result to τ-abstracting congruences

Problem 4

1. Do the congruences induced by weak bisimilarity and branching bisimilarity afford a finite complete axiomatization over the fragment of CCS considered earlier?
2. Are there general techniques for lifting negative results from strong to weak congruences? (See W. Fokkink's talk later.)

Extending Moller's result to τ-abstracting congruences

Problem 4

1. Do the congruences induced by weak bisimilarity and branching bisimilarity afford a finite complete axiomatization over the fragment of CCS considered earlier?
2. Are there general techniques for lifting negative results from strong to weak congruences? (See W. Fokkink's talk later.)

Luca Aceto, Wan Fokkink, Anna Ingólfsdóttir, Mohammad Reza Mousavi. Lifting non-finite axiomatizability results to extensions of process algebras. Acta Inf. 47(3):147–177 (2010)

What if we change the language slightly?

Problem 5

Are there general techniques for transferring negative results from one language to another? Concretely: How can one lift a negative result proved for (an extension of) BCCSP, say, to (an extension of) BPA? Or from strong to weak semantics?

Consider, for instance,
Luca Aceto, Taolue Chen, Anna Ingolfsdottir, Bas Luttik and Jaco van de Pol. On the Axiomatizability of Priority II. Theoretical Computer Science 412(28):3035–3044, 2011.

Some other (more or less) wild thoughts

- Non-existence of a finite equational axiomatization for BPA with Kleene star and the empty process (Corradini's conjecture).
- Find general sufficient conditions ensuring finite axiomatizability of bisimilarity over process algebras.
- What about results for other semantic equivalences in the linear-time/branching-time spectrum?
- Add you own favourite problems!

A proposal

I believe that we should solve some of the problems mentioned earlier. How?

A proposal

I believe that we should solve some of the problems mentioned earlier. How?

Polyconc project?

- Could we follow the lead of the Polymath Projects and begin an on-line collaboration among interested concurrency theorists devoted to solving some of the above-mentioned problems?
- Proposal: Problems 2 or 4 could be the topic for Polyconc 1.

A proposal

I believe that we should solve some of the problems mentioned earlier. How?

Polyconc project?

- Could we follow the lead of the Polymath Projects and begin an on-line collaboration among interested concurrency theorists devoted to solving some of the above-mentioned problems?
- Proposal: Problems 2 or 4 could be the topic for Polyconc 1.

On authorship

No D.H.J. POLYCONC. In the spirit of the annual workshops in Probability, Combinatorics and Geometry (Barbados), everyone who feels they offered a sufficient contribution would be an author of any resulting paper.

Conclusion

Drop me a line, if you are interested in Polyconc or any of the specific problems mentioned in this talk.

A Pearl of Wisdom from Giorgio Parisi

The attraction of a scientific field depends a lot on fashion and on the story-telling ability of its expositors. In reality, each field has its own interesting and difficult problems, which are an intellectual challenge that may stimulate the interest of curious observers. (From *La Chiave, La Luce e L'Ubriaco*, p. 10, Di Renzo Editore)

Conclusion

Drop me a line, if you are interested in Polyconc or any of the specific problems mentioned in this talk.

A Pearl of Wisdom from Giorgio Parisi

The attraction of a scientific field depends a lot on fashion and on the story-telling ability of its expositors. In reality, each field has its own interesting and difficult problems, which are an intellectual challenge that may stimulate the interest of curious observers. (From *La Chiave, La Luce e L'Ubriaco*, p. 10, Di Renzo Editore)

Thank You!

Any Questions?

Subliminal message

Join the EATCS!

The more, the merrier!