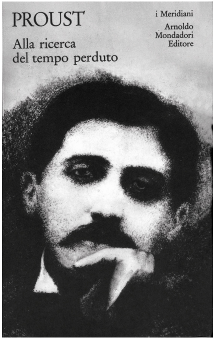
The equational logic of concurrent processes

Results and proof techniques

Luca Aceto
ICE-TCS, Dept. of Computer Science, Reykjavik University
Gran Sasso Science Institute, L'Aquila

EWSCS 2026, Viinistu, 2–5 March 2026

Why this short course?



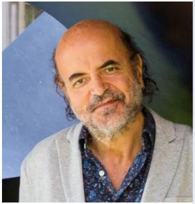
"Mathematicians, like Proust and everyone else, are at their best when writing about their first love." (Gian-Carlo Rota, Discrete Thoughts, p. 3)

Why this short course?

The moral of this story

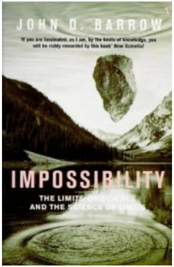
Take-home message (and side remarks)

- The life of a process algebraist is (equationally) hard ☹.
- Negative results abound.
- Call for new proof techniques.
- "Standard" proof technique $\neq$ Easy/shallow result.

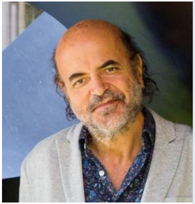


Christos Papadimitriou's viewpoint

Negative results are the only possible self-contained theoretical results in Computer Science. Successful exploratory theoretical research is bound to produce predominantly negative results. (From "Database metatheory: Asking the big queries")

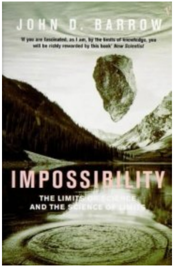


Why you might want to care



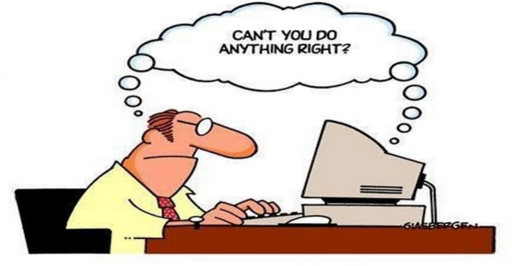
Christos Papadimitriou's viewpoint

Negative results are the only possible self-contained theoretical results in Computer Science. Successful exploratory theoretical research is bound to produce predominantly negative results. (From "Database metatheory: Asking the big queries")



There is still much to be done in the equational logic of processes!

Context: The Role of Equalities Between Programs



Fact of CS life

We use formal languages to communicate with machines and describe expected properties of computations.

Fact of CS life

We use formal languages to communicate with machines and describe expected properties of computations.

A key question When do two expressions describe the "same thing"?

- Abstract data types/algebraic specifications.
- Optimisation in compilers.
- Program analysis/partial evaluation.
- Correctness: Is SPECification equivalent to IMPlementation?

Context: The Role of Equalities Between Programs

A key question When do two expressions describe the "same thing"?

- Abstract data types/algebraic specifications.
- Optimisation in compilers.
- Program analysis/partial evaluation.
- Correctness: Is SPECification equivalent to IMPlementation?

Tenet

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

(Finite) Complete Axiomatisations

The Challenge

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

Is there a (finite) set $\mathcal{E}$ of Σ-equations $t_1 \approx t_2$ such that

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

for all (closed) Σ-terms t, u?

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

Why is this an interesting game?

Answer

An equational axiomatisation

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.

Equational characterizations also find practical use in verification, e.g., in normalization. Yet, they are most useful in illustrating the essential difference between process semantics, and thus form a guide in choosing the right one for an application. (Rob van Glabbeek)

Why is this a hard game?

Source: https://www.allformarathon.com/are-there-any-real-benefits-of-cold-shower-for-runners/

Cold shower

The life of a concurrency theorist is equationally hard ☹.
In many situations and even for very simple languages, non-finite axiomatisability lurks.

Examples?

What's next?

- Algebras and equational logic.
- Introduction to positive and negative results for some "simple" algebras.
- First proof techniques.
- First bridge to process algebras.

Signatures and terms: Syntax

- V, a countably infinite set of variables $(x, y, w, z \in V)$.
- A signature Σ is a set of operation symbols each with its arity. (Assumption: $\Sigma \cap V = \emptyset$.)

Terms

The set $\mathrm{T}(\Sigma, V)$ of terms over Σ is the least set such that

- $V \subseteq \mathrm{T}(\Sigma, V)$.
- If f is an n-ary operation symbol and $t_1, \ldots, t_n \in \mathrm{T}(\Sigma, V)$, then $f(t_1, \ldots, t_n) \in \mathrm{T}(\Sigma, V)$.

A term t is closed (aka ground) if it doesn't contain variables. $\mathrm{T}(\Sigma)$ is the set of all closed terms.

Reading material: A., Fokkink, Ingólfsdóttir and Luttik. Finite Equational Bases in Process Algebra: Results and Open Questions.

Signatures and terms: Syntax

Terms

The set $T(\Sigma, V)$ of terms over Σ is the least set such that

- $V \subseteq T(\Sigma, V)$.
- If f is an n-ary operation symbol and $t_1, \ldots, t_n \in T(\Sigma, V)$, then $f(t_1, \ldots, t_n) \in T(\Sigma, V)$.

A term t is closed (aka ground) if it doesn't contain variables.
$T(\Sigma)$ is the set of all closed terms.

Example: Natural numbers with $\max$

Two signatures for natural numbers with $\max$:

- $\Sigma_1 = \{0, S, \vee\}$ and
- $\Sigma_2 = \{0, +, \vee\}$,

where 0 is a constant symbol, S is unary, and $\vee$ and $+$ are binary.

Signatures and terms: Syntax

Terms

The set $\mathrm{T}(\Sigma, V)$ of terms over Σ is the least set such that

- $V \subseteq \mathrm{T}(\Sigma, V)$.
- If f is an n-ary operation symbol and $t_1, \ldots, t_n \in \mathrm{T}(\Sigma, V)$, then $f(t_1, \ldots, t_n) \in \mathrm{T}(\Sigma, V)$.

A term t is closed (aka ground) if it doesn't contain variables. $\mathrm{T}(\Sigma)$ is the set of all closed terms.

Example: A core process algebra

Signature for BCCSP:

- a constant $\mathbf{0}$,
- a binary operator $+$, and
- unary prefix operators a, where a ranges over a nonempty set A of actions.

Terms

The set $T(\Sigma, V)$ of terms over Σ is the least set such that

- $V \subseteq T(\Sigma, V)$.
- If f is an n-ary operation symbol and $t_1, \ldots, t_n \in T(\Sigma, V)$, then $f(t_1, \ldots, t_n) \in T(\Sigma, V)$.

A term t is closed (aka ground) if it doesn't contain variables. $T(\Sigma)$ is the set of all closed terms.

Congruences

A congruence over $T(\Sigma, V)$ is an equivalence relation $\sim$ such that, for each $f \in \Sigma$,

$$\text{if } t_i \sim u_i \ (1 \leq i \leq n) \text{ then } f(t_1, \ldots, t_n) \sim f(u_1, \ldots, u_n).$$

Σ-algebras: Semantics

Σ-algebras

$$\mathcal{A} = (\mathbf{A}, \{f^{\mathcal{A}} \mid f \in \Sigma\}),$$

where:

- $\mathbf{A} \neq \emptyset$ is a set (the carrier of the algebra), and
- $f^{\mathcal{A}} : \mathbf{A}^n \longrightarrow \mathbf{A}$, for each n-ary $f \in \Sigma$.

Examples?

Fact

T(Σ) is the initial Σ-algebra.

Σ-algebras: Semantics

Σ-algebras

$$\mathcal{A} = (\mathbf{A}, \{f^{\mathcal{A}} \mid f \in \Sigma\}),$$

where:

- $\mathbf{A} \neq \emptyset$ is a set (the carrier of the algebra), and
- $f^{\mathcal{A}} : \mathbf{A}^n \longrightarrow \mathbf{A}$, for each n-ary $f \in \Sigma$.

The meaning of terms: $\mathrm{T}(\Sigma, V)$ is the free algebra

Each environment $\rho : V \longrightarrow \mathbf{A}$ can be extended to terms homomorphically in a unique way thus:

$$\rho(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\rho(t_1), \ldots, \rho(t_n)).$$

Σ-algebras

$$\mathcal{A} = (\mathbf{A}, \{f^{\mathcal{A}} \mid f \in \Sigma\}),$$

where:

- $\mathbf{A} \neq \emptyset$ is a set (the carrier of the algebra), and
- $f^{\mathcal{A}} : \mathbf{A}^n \to \mathbf{A}$, for each n-ary $f \in \Sigma$.

The meaning of terms: $\mathrm{T}(\Sigma, V)$ is the free algebra

Each environment $\rho : V \to \mathbf{A}$ can be extended to terms homomorphically in a unique way thus:

$$\rho(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\rho(t_1), \ldots, \rho(t_n)).$$

When t is closed we write $t^{\mathcal{A}}$ for its interpretation in $\mathcal{A}$. We say that $a \in \mathbf{A}$ is denotable if $a = t^{\mathcal{A}}$ for some t. Examples?

Σ-algebras: Semantics

The meaning of terms: $T(\Sigma, V)$ is the free algebra

Each environment $\rho : V \to \mathbf{A}$ can be extended to terms homomorphically in a unique way thus:

$$\rho(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\rho(t_1), \ldots, \rho(t_n)).$$

Interpretations $\leadsto$ congruences

Let $t, u \in T(\Sigma, V)$ and $\mathcal{A}$ be a Σ-algebra. Then,

$$t =_{\mathcal{A}} u \text{ iff } \rho(t) = \rho(u), \text{for each environment } \rho.$$

Examples?

Interpretations $\rightsquigarrow$ congruences

Let $t, u \in \mathrm{T}(\Sigma, V)$ and $\mathcal{A}$ be a Σ-algebra. Then,

$$t =_{\mathcal{A}} u \text{ iff } \rho(t) = \rho(u), \text{ for each environment } \rho.$$

Examples?

Our main question

Can one give a syntactic characterisation of the congruence $=_{\mathcal{A}}$ over (closed) terms in $\mathrm{T}(\Sigma, V)$?

Equational logic

An axiom system is a set $\mathcal{E}$ of equations (aka axioms) $t \approx u$, where $t, u \in \mathrm{T}(\Sigma, V)$.
A substitution is a function $\sigma : V \to \mathrm{T}(\Sigma, V)$. A closed substitution has codomain $\mathrm{T}(\Sigma)$.

Provability in equational logic: $\mathcal{E} \vdash t \approx u$

$$\frac{}{t \approx t} \qquad \frac{u \approx t}{t \approx u} \qquad \frac{t \approx u \quad u \approx v}{t \approx v} \qquad \frac{}{t \approx u}\ (t \approx u) \in \mathcal{E}$$

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)} \qquad \frac{t_1 \approx u_1, \ldots, t_n \approx u_n}{f(t_1, \ldots, t_n) \approx f(u_1, \ldots, u_n)}$$

Examples?

Suggested reading for the keenest: Walter Taylor. Equational logic. Houston Journal of Mathematics, survey 1979, iii+83 pp.

Equational logic

Provability in equational logic: $\mathcal{E} \vdash t \approx u$

$$\frac{}{t \approx t} \qquad \frac{u \approx t}{t \approx u} \qquad \frac{t \approx u \quad u \approx v}{t \approx v} \qquad \frac{}{t \approx u}\ (t \approx u) \in \mathcal{E}$$

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)} \qquad \frac{t_1 \approx u_1, \ldots, t_n \approx u_n}{f(t_1, \ldots, t_n) \approx f(u_1, \ldots, u_n)}$$

Variants

- Substitution only for axioms in $\mathcal{E}$:

$$\frac{}{\sigma(t) \approx \sigma(u)}\ (t \approx u) \in \mathcal{E}$$

- If $\mathcal{E}$ is closed under symmetry, there is no need for

$$\frac{u \approx t}{t \approx u}$$

Equational logic

Provability in equational logic: $\mathcal{E} \vdash t \approx u$

$$\frac{}{t \approx t} \quad \frac{u \approx t}{t \approx u} \quad \frac{t \approx u \quad u \approx v}{t \approx v} \quad \frac{}{t \approx u}\ (t \approx u) \in \mathcal{E}$$

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)} \quad \frac{t_1 \approx u_1, \ldots, t_n \approx u_n}{f(t_1, \ldots, t_n) \approx f(u_1, \ldots, u_n)}$$

Variant: Inequational logic

Omit the symmetry rule

$$\frac{u \approx t}{t \approx u}$$

Inequation: $t \preceq u$.

Equational logic

Provability in equational logic: $\mathcal{E} \vdash t \approx u$

$$\frac{}{t \approx t} \qquad \frac{u \approx t}{t \approx u} \qquad \frac{t \approx u \quad u \approx v}{t \approx v} \qquad \frac{}{t \approx u}\ (t \approx u) \in \mathcal{E}$$

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)} \qquad \frac{t_1 \approx u_1, \ldots, t_n \approx u_n}{f(t_1, \ldots, t_n) \approx f(u_1, \ldots, u_n)}$$

Exercise

Assume that σ and σ' are substitutions such that $\mathcal{E} \vdash \sigma(x) \approx \sigma'(x)$ for each $x \in V$. Prove that, for every term t,

$$\mathcal{E} \vdash \sigma(t) \approx \sigma'(t).$$

Provability vs validity

Let $\mathcal{A}$ be a Σ-algebra.

Soundness

An axiom system $\mathcal{E}$ is sound with respect to $=_{\mathcal{A}}$ iff for all t, u, if $\mathcal{E} \vdash t \approx u$ then $t =_{\mathcal{A}} u$. In this case, we say that $\mathcal{A}$ is a model of $\mathcal{E}$.

Birkhoff's completeness theorem (1935)

$\mathcal{E} \vdash t \approx u$ iff $t =_{\mathcal{A}} u$ in all models $\mathcal{A}$ of $\mathcal{E}$.

See Section 2.2 of George F. McNulty's notes on equational logic for a proof.

Provability vs validity

Let $\mathcal{A}$ be a Σ-algebra.

Soundness

An axiom system $\mathcal{E}$ is sound with respect to $=_\mathcal{A}$ iff for all t, u, if $\mathcal{E} \vdash t \approx u$ then $t =_\mathcal{A} u$. In this case, we say that $\mathcal{A}$ is a model of $\mathcal{E}$.

Shades of completeness

- An axiom system $\mathcal{E}$ is (ground) complete with respect to $=_\mathcal{A}$ iff for all (closed) t, u, if $t =_\mathcal{A} u$ then $\mathcal{E} \vdash t \approx u$.
- An axiom system $\mathcal{E}$ is ω-complete iff for all t, u,

$$\mathcal{E} \vdash t \approx u \text{ iff } \mathcal{E} \vdash \sigma(t) \approx \sigma(u), \text{ for all closed substitutions } \sigma.$$

Provability vs validity

Let $\mathcal{A}$ be a Σ-algebra.

Shades of completeness

- An axiom system $\mathcal{E}$ is (ground) complete with respect to $=_{\mathcal{A}}$ iff for all (closed) t, u, if $t =_{\mathcal{A}} u$ then $\mathcal{E} \vdash t \approx u$.
- An axiom system $\mathcal{E}$ is ω-complete iff for all t, u,

$$\mathcal{E} \vdash t \approx u \text{ iff } \mathcal{E} \vdash \sigma(t) \approx \sigma(u), \text{ for all closed substitutions } \sigma.$$

Theorem

Let $\mathcal{A}$ be a Σ-algebra whose elements are all denotable. Assume that $\mathcal{E}$ is sound and complete for $=_{\mathcal{A}}$. Then, $\mathcal{E}$ is also ω-complete.

Sound and ground complete, but not complete

$$0 \vee x \approx x \quad x \vee 0 \approx x \quad S(x) \vee S(y) \approx S(x \vee y).$$

The equation $x \vee x \approx x$ cannot be derived! Why?

Complete and ω-complete

$$x \vee 0 \approx x \quad S(x) \vee S(y) \approx S(x \vee y) \quad S(x) \vee x \approx S(x)$$

$$x \vee x \approx x \quad x \vee y \approx y \vee x \quad x \vee (y \vee z) \approx (x \vee y) \vee z.$$

Axiom systems for $\Sigma_1 = \{0, S, \vee\}$ over $\mathbb{N}$

Sound and ground complete, but not complete

$$0 \vee x \approx x \quad x \vee 0 \approx x \quad S(x) \vee S(y) \approx S(x \vee y).$$

The equation $x \vee x \approx x$ cannot be derived! Why?

Complete and ω-complete

$$x \vee 0 \approx x \quad S(x) \vee S(y) \approx S(x \vee y) \quad S(x) \vee x \approx S(x)$$

$$x \vee x \approx x \quad x \vee y \approx y \vee x \quad x \vee (y \vee z) \approx (x \vee y) \vee z.$$

How can one prove these claims?

Proof technique for positive results No. 1: Normal forms

Goal

Prove that $\mathcal{E}$ is a sound and (ground) complete axiomatisation of $=_{\mathcal{A}}$ (aka, of $\mathcal{A}$).

A three-step proof strategy

1. Identify normal forms.
2. Show that each (closed) term can be proved equal to a normal form using $\mathcal{E}$.
3. Prove that two normal forms are related by $=_{\mathcal{A}}$ iff they are "identical".

Let's do it!

Axiom systems for $\Sigma_2 = \{0, +, \bigvee\}$ over $\mathbb{N}$

Some sound equations

$$x \vee 0 \approx x \quad x \vee y \approx y \vee x \quad x \vee (y \vee z) \approx (x \vee y) \vee z$$

$$x + 0 \approx x \quad x + y \approx y + x \quad x + (y + z) \approx (x + y) + z$$

$$(x \vee y) + z \approx (x + z) \vee (y + z).$$

- The equations

$$(x + y) \vee x \approx x + y \qquad x \vee x \approx x$$

  can be derived!
- The above equations can prove all the valid equations in at most one variable.

Axiom systems for $\Sigma_2 = \{0, +, \vee\}$ over $\mathbb{N}$

The first cold shower (A., Ésik and Ingólfsdóttir)

The max-plus algebra of the natural numbers has no finite equational axiomatisation!

1. There is no finite set of sound equations that can prove all the valid equations in two variables. (See STACS 2000.)
2. For each $n \geq 1$, the set of valid equations in n variables is not complete. (See TCS 2003.)
3. These negative results extend to tropical semirings—see TCS 2003.

Axiom systems for $\Sigma_2 = \{0, +, \vee\}$ over $\mathbb{N}$

The first cold shower (A., Ésik and Ingólfsdóttir)

The max-plus algebra of the natural numbers has no finite equational axiomatisation!

1. There is no finite set of sound equations that can prove all the valid equations in two variables. (See STACS 2000.)
2. For each $n \geq 1$, the set of valid equations in n variables is not complete. (See TCS 2003.)
3. These negative results extend to tropical semirings—see TCS 2003.

How can one prove these claims?

Proof technique for negative results No. 1: Model-theoretic approach

The approach in one pill

For each sound axiomatisation $\mathcal{E}$ with some property, find a model for $\mathcal{E}$ and a sound equation that fails in this model.

Proof technique for negative results No. 1: Model-theoretic approach

The approach in one pill

For each sound axiomatisation $\mathcal{E}$ with some property, find a model for $\mathcal{E}$ and a sound equation that fails in this model.

$$nx \vee ny \approx n(x \vee y) \quad (n \geq 0)$$
$$p_n \vee q_n \approx q_n \quad (n \geq 2)$$

Example from the second family

$$p_3 = x_1 + x_2 + x_3$$
$$q_3 = (2x_1 + x_3) \vee (x_1 + 2x_2) \vee (x_2 + 2x_3)$$

Proof technique for negative results No. 1: Model-theoretic approach

The approach in one pill

For each sound axiomatisation $\mathcal{E}$ with some property, find a model for $\mathcal{E}$ and a sound equation that fails in this model.

Another 'nasty' family of equations, $n \geq 1$:

$$nx_1 \bigvee \cdots \bigvee nx_n \approx nx_1 \bigvee \cdots \bigvee nx_n \bigvee x_1 + \cdots + x_n$$

Proof technique for negative results No. 1: Model-theoretic approach

The approach in one pill

For each sound axiomatisation $\mathcal{E}$ with some property, find a model for $\mathcal{E}$ and a sound equation that fails in this model.

Another 'nasty' family of equations, $n \geq 1$:

$$nx_1 \vee \cdots \vee nx_n \approx nx_1 \vee \cdots \vee nx_n \vee x_1 + \cdots + x_n$$

What does this have to do with process algebra?

A first bridge to process algebra

The Language

BPA action a variables x
choice $t + u$ sequencing $t \cdot u$

Semantics

The set $T(t)$ of traces of a closed BPA term is defined thus:

$$
\begin{aligned}
T(a) &= \{\varepsilon, a\} \\
T(t+u) &= T(t) \cup T(u) \\
T(t \cdot u) &= T(t) \cup \{a^k w \mid a^k \text{ longest in } T(t) \text{ and } w \in T(u)\}.
\end{aligned}
$$

Two closed terms t, u are trace equivalent, written $t \simeq_T u$, iff $T(t) = T(u)$.

A first bridge to process algebra

Semantics

The set $T(t)$ of traces of a closed BPA term is defined thus:

$$T(a) = \{\varepsilon, a\}$$
$$T(t + u) = T(t) \cup T(u)$$
$$T(t \cdot u) = T(t) \cup \{a^k w \mid a^k \text{ longest in } T(t) \text{ and } w \in T(u)\}.$$

Two closed terms t, u are trace equivalent, written $t \simeq_T u$, iff $T(t) = T(u)$.

Theorem (A., Ésik and Ingólfsdóttir)

1. The relation $\simeq_T$ is a congruence.
2. The algebra of closed BPA terms modulo $\simeq_T$ has no finite equational axiomatisation.

Why?

What's next in our story?

- Some core process algebras (focus on CCS).
- Positive and negative results for some "simple" process algebras.
- Proof techniques.
- Open problems.

Notation

I will often write equations as $t = u$.

A Core Language for Parallel Processes: Milner's 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 for Parallel Processes: Milner's 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?

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

A yardstick notion: strong bisimilarity $\underline{\leftrightarrow}$ (Milner 1980, Park 1981).

Definition

A binary relation $\mathcal{R}$ over closed CCS terms is a bisimulation iff

- it is symmetric and
- if $t \mathrel{\mathcal{R}} u$ and $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$.

$t \underline{\leftrightarrow} u$ iff $t \mathrel{\mathcal{R}} u$ for some bisimulation $\mathcal{R}$.

Theorem

Strong bisimilarity is the largest bisimulation and is a congruence over CCS and all of its extensions considered in this course.

A yardstick notion: strong bisimilarity $\leftrightarrow$ (Milner 1980, Park 1981).

Definition

A binary relation $\mathcal{R}$ over closed CCS terms is a bisimulation iff

- it is symmetric and
- if $t \mathrel{\mathcal{R}} u$ and $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$.

$t \leftrightarrow u$ iff $t \mathrel{\mathcal{R}} u$ for some bisimulation $\mathcal{R}$.

Theorem

Strong bisimilarity is the largest bisimulation and is a congruence over CCS and all of its extensions considered in this course.

Motivating Question

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

Axiomatisation of Bisimilarity: The Saga

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

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

Let $x = \sum_{i \in I} a_i x_i$ and $y = \sum_{j \in J} b_j y_j$. Then,

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

Theorem (Hennessy and Milner, circa 1980, JACM 1985)

$t \underline{\leftrightarrow} u \iff \mathcal{E} \vdash t = u$, for all closed CCS terms t, u. However, $\mathcal{E}$ is neither complete nor ω-complete.

Proof technique: Elimination of $\parallel$ from closed terms and normal forms.

Groovy! But, can one obtain a finite axiomatisation?

Bergstra and Klop's Auxiliary Operators

ID Card

Symbols: $\llfloor$ (left merge), $|$ (communication merge).
Origin: Together for the first time in "Process Algebra for Synchronous Communication", Information & Control 60:109–137, 1984.
Operational Rules:

$$\frac{x \xrightarrow{a} x'}{x \llfloor y \xrightarrow{a} x' \| y} \qquad \frac{x \xrightarrow{a} x', \; y \xrightarrow{\bar{a}} y'}{x \mid y \xrightarrow{\tau} x' \| y'}$$

Relationship with $\|$:

$$x \| y = (x \llfloor y) + (y \llfloor x) + (x \mid y)$$

Why Are $\parallel$ and $\mid$ Good?

Theorem (Bergstra and Klop 1984, yours truly et al. ToCL 2009)

Bisimilarity affords a finite complete axiomatisation over CCS with left and communication merge!

Key to the above result:

$$
\begin{aligned}
(x+y) \mathbin{\|\!\!\_} z &= (x \mathbin{\|\!\!\_} z) + (y \mathbin{\|\!\!\_} z) \\
(x+y) \mid z &= (x \mid z) + (y \mid z)
\end{aligned}
$$

Completeness proof for open terms is tricky and uses equations such as

$$
\begin{aligned}
(x \mathbin{\|\!\!\_} y) \mathbin{\|\!\!\_} z &= x \mathbin{\|\!\!\_} (y \| z) \\
(x \mathbin{\|\!\!\_} y) \mid z &= (x \mid z) \mathbin{\|\!\!\_} y
\end{aligned}
$$

Why Are $\|\!\!\lfloor$ and $|$ Good?

Theorem (Bergstra and Klop 1984, yours truly et al. ToCL 2009)

Bisimilarity affords a finite complete axiomatisation over CCS with left and communication merge!

Question

Can auxiliary operators be synthesised automatically?

Why Are $\|$ and $|$ Good?

Question

Can auxiliary operators be synthesised automatically?

Theorem (A., Bloom and Vaandrager 1994)

Yes, for each language whose semantics is given by rules in GSOS format!

Key ideas

- Smooth and distinctive operations $\leadsto$ distributivity, action and inaction laws.
- Smooth but not distinctive operation = a sum of smooth and distinctive ones.
- Non-smooth operation = smooth operation, but possibly with (many) more arguments.

Concrete examples?

Theorem (Bergstra and Klop 1984, yours truly et al. ToCL 2009)

Bisimilarity affords a finite complete axiomatisation over CCS with left and communication merge!

Cool! But, are auxiliary operators necessary?

Auxiliary Operators Are Necessary!

Theorem (Moller, PhD thesis 1989 and LICS 1990)

No "reasonable" congruence affords a finite equational axiomatisation over closed CCS terms. Bisimilarity is "reasonable".

Auxiliary Operators Are Necessary!

Theorem (Moller, PhD thesis 1989 and LICS 1990)

No "reasonable" congruence affords a finite equational axiomatisation over closed CCS terms. Bisimilarity is "reasonable".

- Proof idea (for bisimilarity): No finite, sound axiom system $\mathcal{E}$ over CCS is powerful enough to "simulate" the expansion laws.
- Implementation: $\mathcal{E}$ cannot prove the sound equation

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

Technical Problem

How can one prove negative results like Moller's one?

Technical Problem

How can one prove negative results like Moller's one?

1. Model-theoretic approach: For each finite sound axiomatisation $\mathcal{E}$, find a model for $\mathcal{E}$, and a sound equation that fails in this model.

Technical Problem

How can one prove negative results like Moller's one?

1. Model-theoretic approach: For each finite sound axiomatisation $\mathcal{E}$, find a model for $\mathcal{E}$, and a sound equation that fails in this model.
2. Compactness theorem: Find an (infinite) sound and complete axiomatisation for which no finite subset is complete.

Intermezzo: Techniques for Proving Negative Results

Technical Problem

How can one prove negative results like Moller's one?

1. Model-theoretic approach: For each finite sound axiomatisation $\mathcal{E}$, find a model for $\mathcal{E}$, and a sound equation that fails in this model.
2. Compactness theorem: Find an (infinite) sound and complete axiomatisation for which no finite subset is complete.

A classic example

Proving that the equational theory of regular expressions is not finitely based (V.N. Redko 1964, J.H. Conway 1971).
Redko's infinite complete axiomatisation includes:

$$(S_k) \qquad a^* = (a^k)^*(1 + a + \cdots + a^{k-1}) \qquad (k \geq 1).$$

For each prime p, it isn't complete if one removes S_k with $k \geq p$.

Intermezzo: Techniques for Proving Negative Results

Technical Problem

How can one prove negative results like Moller's one?

1. Model-theoretic approach: For each finite sound axiomatisation $\mathcal{E}$, find a model for $\mathcal{E}$, and a sound equation that fails in this model.
2. Compactness theorem: Find an (infinite) sound and complete axiomatisation for which no finite subset is complete.
3. Proof-theoretic approach: For each finite sound axiomatisation $\mathcal{E}$, find a property of equations that
   (A) is satisfied by all instantiations of axioms in $\mathcal{E}$,
   (B) is preserved by the rules of equational logic, and
   (C) fails for some sound equation.

Proof-theoretic Approach: Another Example

The Language

$\mathbf{BCCS}_\Omega$	nil $\mathbf{0}$	prefixing at	variables x
	choice $t + u$	divergence Ω	

where a is an action drawn from a non-empty, finite set A.

Operational semantics

- $t \xrightarrow{a} t'$ as before;
- Ω has no transitions;
- $t \downarrow$ ("Ω isn't a summand of t").

Proof-theoretic Approach: Another Example

Prebisimilarity

A binary relation $\mathcal{R}$ over closed BCCS_Ω terms is a prebisimulation iff for all $t \mathrel{\mathcal{R}} u$,

- if $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$;
- if $t\downarrow$ then
  - $u\downarrow$ and
  - if $u \xrightarrow{a} u'$, then $t \xrightarrow{a} t'$ for some t' such that $t' \mathrel{\mathcal{R}} u'$.

$t \preceq_\Omega u$ iff $t \mathrel{\mathcal{R}} u$ for some prebisimulation $\mathcal{R}$.

Examples

$$
\begin{array}{rcl}
\Omega & \preceq_\Omega & x \\
a^n(x + a\Omega) + \Omega & \preceq_\Omega & a^n x + a^{n+1}\mathbf{0} \quad (n \geq 0, \text{ when } A = \{a\}).
\end{array}
$$

Proof-theoretic Approach: Another Example

Examples

$$\begin{array}{rcl} \Omega & \preceq_\Omega & x \\ a^n(x + a\Omega) + \Omega & \preceq_\Omega & a^n x + a^{n+1}\mathbf{0} \quad (n \geq 0, \text{ when } A = \{a\}). \end{array}$$

Theorem (A. Capobianco, Ingólfsdóttir and Luttik 2008)

Assume that $A = \{a\}$. Then, no finite set of inequations that are sound modulo $\preceq_\Omega$ can prove all of the inequations

$$a^n(x + a\Omega) + \Omega \preceq_\Omega a^n x + a^{n+1}\mathbf{0} \quad (n \geq 0).$$

Proof-theoretic Approach: Another Example

Theorem (A. Capobianco, Ingólfsdóttir and Luttik 2008)

Assume that $A = \{a\}$. Then, no finite set of inequations that are sound modulo $\preceq_\Omega$ can prove all of the inequations

$$a^n(x + a\Omega) + \Omega \preceq_\Omega a^n x + a^{n+1}\mathbf{0} \quad (n \geq 0).$$

The Invariant

Assume that $\mathcal{E}$ is a finite set of inequations that are sound modulo $\preceq_\Omega$. Let n be larger than the "depth" of $\mathcal{E}$. Furthermore, let t and u be terms such that $\mathcal{E} \vdash t \preceq u$ and

$$t + \Omega \preceq_\Omega u + \Omega \preceq_\Omega a^n x + a^{n+1}\mathbf{0}.$$

Assume that there is some t' such that $t \xrightarrow{a^n} t'$ and $x + a\Omega \preceq_\Omega t' \preceq_\Omega x + a\mathbf{0}$. Then there is some u' such that $u \xrightarrow{a^n} u'$ and $x + a\Omega \preceq_\Omega u' \preceq_\Omega x + a\mathbf{0}$.

Proof-theoretic Approach: Another Example

The Invariant

Assume that $\mathcal{E}$ is a finite set of inequations that are sound modulo $\precsim_\Omega$. Let n be larger than the "depth" of $\mathcal{E}$. Furthermore, let t and u be terms such that $\mathcal{E} \vdash t \precsim u$ and

$$t + \Omega \precsim_\Omega u + \Omega \precsim_\Omega a^n x + a^{n+1}\mathbf{0}.$$

Assume that there is some t' such that $t \stackrel{a^n}{\rightarrow} t'$ and $x + a\Omega \precsim_\Omega t' \precsim_\Omega x + a\mathbf{0}$. Then there is some u' such that $u \stackrel{a^n}{\rightarrow} u'$ and $x + a\Omega \precsim_\Omega u' \precsim_\Omega x + a\mathbf{0}$.

The Bitter Truth

Simple language and standard proof technique don't mean "the proof is easy". ☹

Back to the Saga: The Positive Message in the Negative Result

What we have learnt so far, in one pill

1. Thou shalt add auxiliary operators to CCS!
2. The left and communication merge do the job.

Question

Is there any alternative to Bergstra and Klop?

Back to the Saga: The Positive Message in the Negative Result

Question

Is there any alternative to Bergstra and Klop?

Hennessy's Merge (ID card)

Symbol: $|^{\!/}$

Origin: "On the Relationship Between Time and Interleaving", CMA Preprint, 1981. (Journal version, 1988!)

Operational Rules:

$$\frac{x \xrightarrow{a} x'}{x \,|^{\!/}\, y \xrightarrow{a} x' \| y} \qquad \frac{x \xrightarrow{a} x', \; y \xrightarrow{\bar{a}} y'}{x \,|^{\!/}\, y \xrightarrow{\tau} x' \| y'}$$

Relationship with $\|$: $x \| y = (x \,|^{\!/}\, y) + (y \,|^{\!/}\, x)$

Does Hennessy's merge help?

Question and an old conjecture

Does bisimilarity afford a finite equational axiomatisation over CCS with $|\!\!/$?

> *It seems that $|\!\!/$ does not have a finite equational axiomatization. (Bergstra and Klop, 1984, p. 118)*

Does Hennessy's merge help?

Question and an old conjecture

Does bisimilarity afford a finite equational axiomatisation over CCS with $|\!/$?

> *It seems that $|\!/$ does not have a finite equational axiomatization. (Bergstra and Klop, 1984, p. 118)*

Theorem (Fokkink, Ingólfsdóttir, Luttik and yours truly, 2005)

Bergstra and Klop were right! Bisimilarity affords no finite equational axiomatisation over CCS with $|\!/$.

The pudding is in the proof!

The Proof

Proof idea: No finite, sound axiom system $\mathcal{E}$ over CCS with $|\!/$ is powerful enough to "expand" the initial synchronisation behaviour of a term of the form $a \,|\!/\, p$ when p has large branching degree.

Implementation: We show that $\mathcal{E}$ cannot prove the sound equation

$$a \,|\!/\, \sum_{i=0}^{n} \bar{a}a^i = a(\sum_{i=0}^{n} \bar{a}a^i) + \sum_{i=0}^{n} \tau a^i \qquad (n > \text{size}(\mathcal{E})) \enspace .$$

Message (anthropomorphically):

Hennessy cannot replace Bergstra and Klop!

A natural question

Question to the community, yours truly, BEATCS 2003

Is there a single binary operator that can be added to CCS to finitely axiomatise bisimilarity?

A natural question

Question to the community, yours truly, BEATCS 2003

Is there a single binary operator that can be added to CCS to finitely axiomatise bisimilarity?

How does one prove anything like that?

. . . under some, IMHO reasonable, assumptions.

Some handles

Assumptions on the binary operator $f(x, y)$

1. The operator f is specified using "CCS-like operational rules" (de Simone rules for the cognoscenti).
2. Parallel composition can be expressed using f "à la Bergstra and Klop".
3. A mild one that plays a role in the proof of one technical lemma.

Some handles

Assumptions on the binary operator $f(x, y)$

1. The operator f is specified using "CCS-like operational rules" (de Simone rules for the cognoscenti).
2. Parallel composition can be expressed using f "à la Bergstra and Klop".
3. A mild one that plays a role in the proof of one technical lemma.

Theorem (A., Castiglioni, Fokkink, Ingófsdóttir, Luttik, CSL 2021 and ToCL 2022)

Under the above assumptions, bisimilarity has no finite equational axiomatisation over CCS augmented with f.

High-level proof idea

The slow-cooker recipe (for five); timing $\approx$ 2003–2020

1. Use our assumptions to map out the universe of "meaningful operators f".
2. Prove the negative result for all "meaningful f" that distribute over $+$ in one argument (such as Hennessy's merge).
3. Do the same for all "meaningful f" that distribute over $+$ in neither argument (such as variations on $\|$).

High-level proof idea

The slow-cooker recipe (for five); timing ≈ 2003–2020

1. Use our assumptions to map out the universe of "meaningful operators f".
2. Prove the negative result for all "meaningful f" that distribute over $+$ in one argument (such as Hennessy's merge).
3. Do the same for all "meaningful f" that distribute over $+$ in neither argument (such as variations on $\|$).

Friday, April 30, 2021

PolyConc: Online collaboration to improve on a result on the equational theory of CCS modulo bisimilarity

The aim of this post is to try and start an online collaboration to improve the solution to a problem in the equational logic of processes that I posed in a survey paper in 2003, namely

> Can one obtain a finite axiomatisation of the parallel composition operator in bisimulation semantics by adding only one binary operator to the signature of (recursion, restriction, and relabelling free) CCS?

https://processalgebra.blogspot.com/2021/04/polyconc-online-collaboration-to.html

Definition

A closed term t is (parallel) prime if $t \not\leftrightarrow \mathbf{0}$, and $t \underline{\leftrightarrow} u \| v$ implies $u \underline{\leftrightarrow} \mathbf{0}$ or $v \underline{\leftrightarrow} \mathbf{0}$.

A parallel decomposition of t is a finite multiset $[t_1, \ldots, t_n]$ of primes such that

$$t \underline{\leftrightarrow} t_1 \| \cdots \| t_n.$$

Examples?

Intermezzo: Unique Parallel Decompositions

Definition

A closed term t is (parallel) prime if $t \not\underline{\leftrightarrow}\ \mathbf{0}$, and $t \underline{\leftrightarrow} u \| v$ implies $u \underline{\leftrightarrow} \mathbf{0}$ or $v \underline{\leftrightarrow} \mathbf{0}$.

A parallel decomposition of t is a finite multiset $[t_1, \ldots, t_n]$ of primes such that

$$t \underline{\leftrightarrow} t_1 \| \cdots \| t_n.$$

Theorem (Milner and Moller 1993)

Every closed t in CCS has a unique parallel decomposition.

See also a vast generalisation by Luttik and van Oostrom in TCS 2005.

Intermezzo: Unique Parallel Decompositions

Definition

A closed term t is (parallel) prime if $t \not\underline{\leftrightarrow} \mathbf{0}$, and $t \underline{\leftrightarrow} u \| v$ implies $u \underline{\leftrightarrow} \mathbf{0}$ or $v \underline{\leftrightarrow} \mathbf{0}$.
A parallel decomposition of t is a finite multiset $[t_1, \ldots, t_n]$ of primes such that

$$t \underline{\leftrightarrow} t_1 \| \cdots \| t_n.$$

Theorem (Milner and Moller 1993)

Every closed t in CCS has a unique parallel decomposition.

See also a vast generalisation by Luttik and van Oostrom in TCS 2005.

Cancellation

If $t \| v \underline{\leftrightarrow} u \| v$ then $t \underline{\leftrightarrow} u$.

Other Parallel Composition Operators

The Language

$\mathbf{BCCSP}_B^p$ nil $\mathbf{0}$ prefixing at variables x
choice $t + u$ CSP parallel $t \parallel_B u$

where a is an action drawn from a non-empty, finite set A and $B \subseteq A$.

Other Parallel Composition Operators

The Language

$\mathbf{BCCSP}_B^p$ nil $\mathbf{0}$ choice $t + u$ prefixing at CSP parallel $t \parallel_B u$ variables x

where a is an action drawn from a non-empty, finite set A and $B \subseteq A$.

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?

$$\frac{x \xrightarrow{a} x'}{x \parallel_B y \xrightarrow{a} x' \parallel_B y} \quad a \notin B \qquad \frac{y \xrightarrow{a} y'}{x \parallel_B y \xrightarrow{a} x \parallel_B y'} \quad a \notin B$$

$$\frac{x \xrightarrow{a} x', \; y \xrightarrow{a} y'}{x \parallel_B y \xrightarrow{a} x' \parallel_B y'} \quad a \in B$$

Theorem (A., Anastasiadi, Castiglioni and Ingólfsdóttir 2022)

Let $B \subset A$. Then, BCCSP_B^p does not have a finite, ground-complete axiomatisation modulo bisimilarity.

Is Bisimilarity Finitely Axiomatisable over $BCCSP_B^p$?

Proof technique: Reduction mappings (A., Fokkink, Ingólfsdóttir, Mousavi).

Key ideas:

- L_{new} and L_{bad} two languages modulo $\underline{\leftrightarrow}$.
- $\mathcal{H}$ is hard family of sound equations over L_{bad} that no finite set of sound equations over L_{bad} can prove.
- There is a function from L_{new} and L_{bad} that preserves soundness and provability, and reflects the equations in $\mathcal{H}$. Then, L_{new} is not finitely axiomatisable modulo $\underline{\leftrightarrow}$.

Is Bisimilarity Finitely Axiomatisable over BCCSP_B^p?

Proof technique: Reduction mappings (A., Fokkink, Ingólfsdóttir, Mousavi).

Key ideas:

- L_{new} and L_{bad} two languages modulo $\underline{\leftrightarrow}$.
- $\mathcal{H}$ is hard family of sound equations over L_{bad} that no finite set of sound equations over L_{bad} can prove.
- There is a function from L_{new} and L_{bad} that preserves soundness and provability, and reflects the equations in $\mathcal{H}$. Then, L_{new} is not finitely axiomatisable modulo $\underline{\leftrightarrow}$.

Note: "Structural mappings" preserve provability.

Structural = identity over variables + no new variables + compositionality.

Is Bisimilarity Finitely Axiomatisable over BCCSP_B^p?

Consider the operator $\|_A$ with rules

$$\frac{x \xrightarrow{a} x', \; y \xrightarrow{a} y'}{x \|_A y \xrightarrow{a} x' \|_A y'} \quad a \in A$$

Theorem (A., Anastasiadi, Castiglioni and Ingólfsdóttir 2022)

BCCSP_A^p has a finite, ground-complete axiomatisation modulo bisimilarity.

Proof technique: Elimination of $\|_A$ and normal forms.

Question for you

Which equations would you use to remove all occurrences of $\|_A$ from closed terms?

Limitations of the Reduction-based Technique

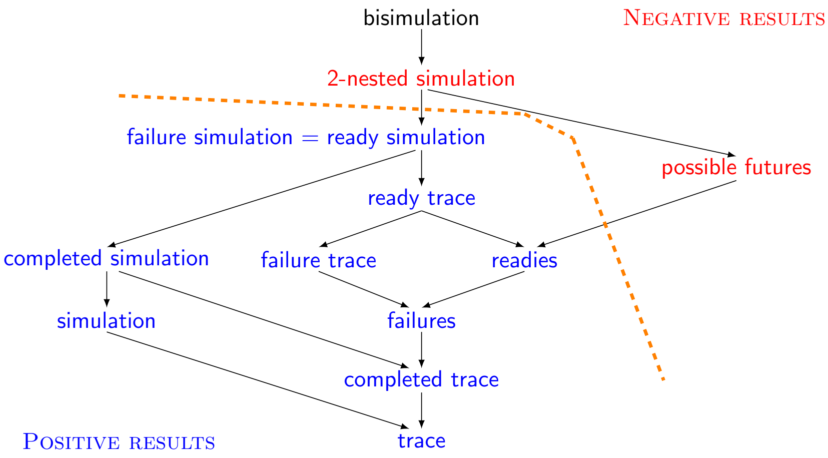
Let BCCSP^p be the language that includes the BCCSP constructs and all the $\|_B$, with $B \subseteq A$.

Theorem (A., Anastasiadi, Castiglioni and Ingólfsdóttir 2022)

There is no structural reduction from BCCSP^p to CCS that reflects the hard family of equations used in the proof of Moller's negative results.

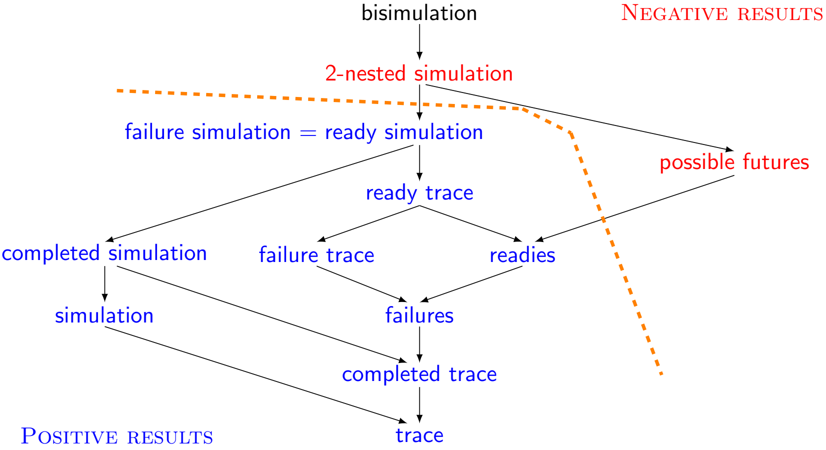
Source: https://www.allformarathon.com/are-there-any-real-benefits-of-cold-shower-for-runners/

A Journey in van Glabbeek's Spectrum (CONCUR 2020 and LMCS 2022)



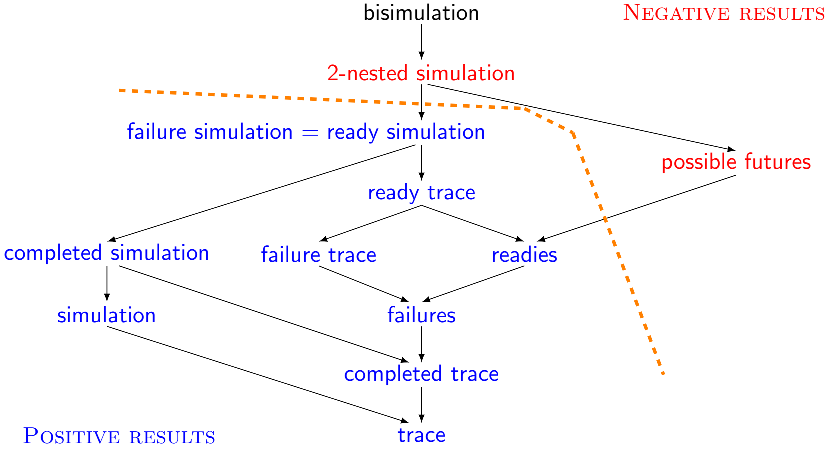
Results for ground-complete axiomatisations over CCS.

A Journey in van Glabbeek's Spectrum (CONCUR 2020 and LMCS 2022)



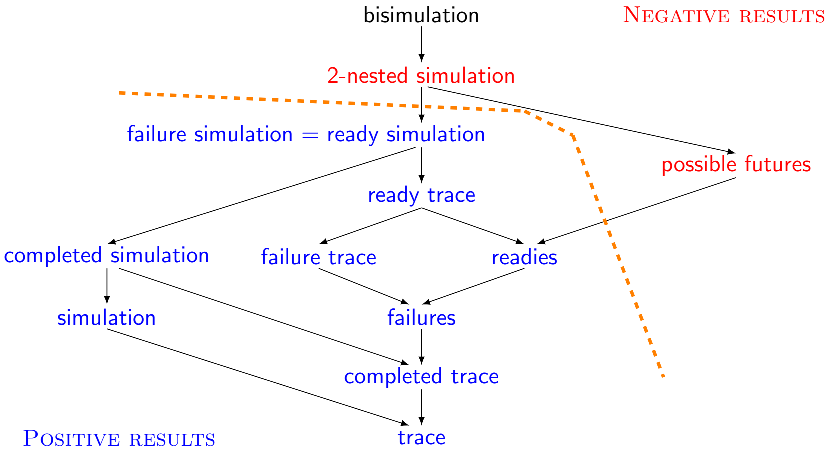
Question 1: How are these semantics defined?

A Journey in van Glabbeek's Spectrum (CONCUR 2020 and LMCS 2022)



Question 2: Are the inclusion relations in the above lattice strict?

A Journey in van Glabbeek's Spectrum (CONCUR 2020 and LMCS 2022)



Question 3: Are those relations congruences over CCS?

A Journey in the Spectrum: Ready Simulation

Definition

A binary relation $\mathcal{R}$ over closed CCS terms is a simulation iff

- if $t \mathrel{\mathcal{R}} u$ and $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$.

$t \preceq_S u$ iff $t \mathrel{\mathcal{R}} u$ for some simulation $\mathcal{R}$.

Definition

A binary relation $\mathcal{R}$ over closed CCS terms is a ready simulation iff it is a simulation and

- if $t \mathrel{\mathcal{R}} u$ and $u \xrightarrow{a}$, then $t \xrightarrow{a}$.

$t \preceq_{RS} u$ iff $t \mathrel{\mathcal{R}} u$ for some ready simulation $\mathcal{R}$.

Theorem

The relations $\preceq_S$ and $\preceq_{RS}$ are precongruences over CCS and are the largest simulation and ready simulation, respectively.

Some equations (modulo the kernel of $\preceq_{RS}$)

Simplifying assumption: No synchronisation!

$$(\mathrm{EL}_f) \quad \sum_{i\in I} a_i x_i \parallel \sum_{j\in J} b_j y_j \approx$$
$$\sum_{i\in I} a_i(x_i \parallel (\sum_{j\in J} b_j y_j)) + \sum_{j\in J} b_j((\sum_{i\in I} a_i x_i) \parallel y_j)$$

where the a_i's are all different and so are the b_j's.
There are finitely many such equations.

Some equations (modulo the kernel of $\preceq_{RS}$)

Simplifying assumption: No synchronisation!

$$(\text{RSP1}) \quad (ax + ay + u) \parallel (bz + bw + v) \approx$$
$$(ax + u) \parallel (bz + bw + v) + (ay + u) \parallel (bz + bw + v)$$
$$+ (ax + ay + u) \parallel (bz + v) + (ax + ay + u) \parallel (bw + v)$$

$$(\text{RSP2}) \quad \sum_{i \in I} a_i x_i \parallel (by + bz + w) \approx$$
$$\sum_{i \in I} a_i x_i \parallel (by + w) + \sum_{i \in I} a_i x_i \parallel (bz + w)$$
$$+ \sum_{i \in I} a_i (x_i \parallel (by + bz + w))$$

where the a_i's are all different.

A Journey in the Spectrum: Ready Simulation

The Elimination Theorem

Using (EL_f), (RSP1), (RSP2) and

$$\begin{aligned} x \parallel \mathbf{0} &\approx x \\ x \parallel y &\approx y \parallel x, \end{aligned}$$

one can eliminate $\parallel$ from all closed terms.

The Ground-Completeness Theorem

Using the above equations, classic axioms for $+$ and

$$a(bx + by + z) \approx a(bx + by + z) + a(bx + z),$$

one can prove all the sound equivalences between closed terms.

A Journey in the Spectrum: Simulation

Some equations (modulo the kernel of $\precsim_S$)

Simplifying assumption: No synchronisation!

$$(\mathrm{EL}_1) \quad ax \| by \quad \approx \quad a(x \| by) + b(ax \| y)$$

$$(\mathrm{SP1}) \quad (x+y) \| (z+w) \approx$$
$$x \| (z+w) + y \| (z+w) + (x+y) \| z + (x+y) \| w$$
$$(\mathrm{SP2}) \quad ax \| (y+z) \approx$$
$$a(x \| (y+z)) + ax \| y + ax \| z$$

The Elimination Theorem

Using (EL_1), (SP1), (SP2) and

$$\begin{aligned} x \parallel \mathbf{0} &\approx x \\ x \parallel y &\approx y \parallel x, \end{aligned}$$

one can eliminate $\parallel$ from all closed terms.

The Ground-Completeness Theorem

Using the above equations, classic axioms for $+$ and

$$a(x+y) \approx a(x+y) + ax,$$

one can prove all the sound equivalences between closed terms.

Definition

The set of traces of a closed term t is

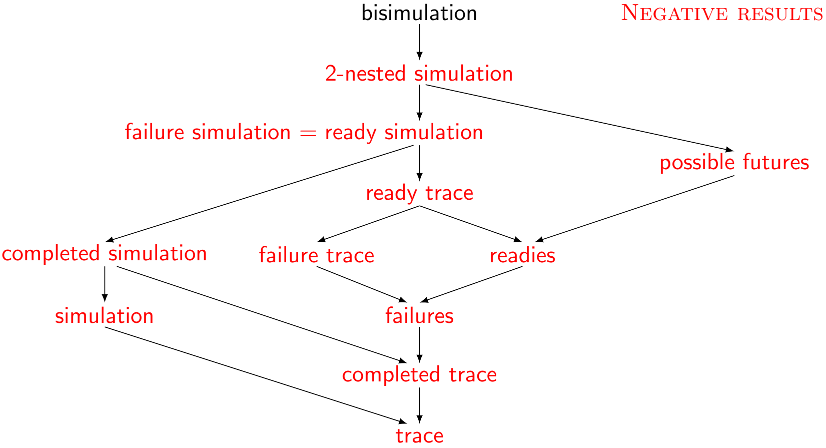
$$\text{Traces}(t) = \{s \mid s \in A^* \text{ and } t \xrightarrow{s} t', \text{ for some } t'\}.$$

$t \simeq_T u$ iff $\text{Traces}(t) = \text{Traces}(u)$.

Tasks for you, later today!

1. Prove that $\simeq_T$ is a congruence over CCS.
2. Prove that the equation $ax + ay \approx a(x + y)$ is sound $\simeq_T$.
3. Find some sound equations that allow one to eliminate $\|$ from closed terms.
4. Use the above results to obtain a ground-complete axiomatisation of $\simeq_T$.

A Journey in the Spectrum II (Versteeg, Castiglioni and Luttik, CONCUR 2025)



Results for complete axiomatisations ☹.

A Journey in the Spectrum II (Versteeg, Castiglioni and Luttik, CONCUR 2025): From RS to CT

Theorem (Precongruences)

No precongruence that includes $\precsim_{RS}$ and is included in $\precsim_{CT}$ is finitely axiomatisable over CCS.

Proof (using the proof-theoretic approach)

- Family of bad inequations:

$$x \precsim x + x^n \quad (n \geq 1,\ x^n = \underbrace{x \| \cdots \| x}_{n-\text{times}}).$$

- The proof invariant:

  Let $\mathcal{E}$ be a finite set of inequations that is sound modulo $\precsim_{CT}$. Let $n \geq 2$ be greater than the breadth of any term in $\mathcal{E}$. Assume that $\mathcal{E} \vdash t \precsim u$, $u \precsim_{CT} x + x^n$ and $t \simeq_{CT} x$. Then $u \simeq_{CT} x$.

A Journey in the Spectrum II (Versteeg, Castiglioni and Luttik, CONCUR 2025): From RS to CT

Theorem (Congruences)

No congruence that includes the kernel of $\preceq_{RS}$ and is included in the kernel of $\preceq_{CT}$ is finitely axiomatisable over CCS.

Proof (using the proof-theoretic approach)

Family of bad equations:

$$ax + a(x + x^n) \approx a(x + x^n) \quad (n \geq 1,\ x^n = \underbrace{x \| \cdots \| x}_{n-\text{times}}).$$

A Journey in the Spectrum II (Versteeg, Castiglioni and Luttik, CONCUR 2025): Simulation and Trace Semantics

Theorem (Congruences)

Assume that A is finite and non-empty. Then, no congruence that includes the kernel of $\preceq_S$ and is included in the kernel of $\preceq_T$ is finitely axiomatisable over CCS.

A Journey in the Spectrum II (Versteeg, Castiglioni and Luttik, CONCUR 2025): Simulation and Trace Semantics

Theorem (Congruences)

Assume that A is finite and non-empty. Then, no congruence that includes the kernel of $\preceq_S$ and is included in the kernel of $\preceq_T$ is finitely axiomatisable over CCS.

Proof for the case when A is a singleton (using the reduction approach)

- In this case, simulation $=$ trace. Why?
- Can you reduce this axiomatisation problem to one we saw earlier?
- What do the operations $+$ and $\|$ really do in trace semantics when A is a singleton?

Theorem (Congruences)

Assume that A is finite and non-empty. Then, no congruence that includes the kernel of $\preceq_S$ and is included in the kernel of $\preceq_T$ is finitely axiomatisable over CCS.

Proof for the case when $|A| \geq 2$ (using the proof-theoretic approach)

Family of bad equations when $A = \{a, b\}$:

$$\begin{aligned} ab^n x + t_n &\approx t_n, \text{ where } n \geq 1 \text{ and} \\ t_n &= ab^n\mathbf{0} + b^n x \parallel x + a(x \parallel x^n). \end{aligned}$$

A Menagerie of Nasty Operations

Question

Is parallel composition the only operator that spoils finite axiomatisability?

A Menagerie of Nasty Operations

Question

Is parallel composition the only operator that spoils finite axiomatisability?

No way!

The bestiary of "equationally nasty operations" includes

- interrupt (see A., Fokkink, Ingólfsdóttir, Nain 2006),
- priority (several combinations of my co-authors, MSCS 2008, TCS 2011, TCS 2020),
- Kleene star and finite-state recursion (Sewell; A., Fokkink, Ingólfsdóttir).

A Menagerie of Nasty Operations: Interrupt

The Language

$\mathbf{BPA}_{\triangleright}$ action a choice $t + u$ variables x sequencing $t \cdot u$ interrupt $t \triangleright u$

Semantics (of interrupt)

$$\frac{t \xrightarrow{a} \checkmark}{t \triangleright u \xrightarrow{a} \checkmark} \qquad \frac{t \xrightarrow{a} t'}{t \triangleright u \xrightarrow{a} t' \triangleright u} \qquad \frac{u \xrightarrow{a} \checkmark}{t \triangleright u \xrightarrow{a} t} \qquad \frac{u \xrightarrow{a} u'}{t \triangleright u \xrightarrow{a} u' \cdot t}$$

A Menagerie of Nasty Operations: Interrupt

Semantics (of interrupt)

$$\frac{t \xrightarrow{a} \surd}{t \rhd u \xrightarrow{a} \surd} \qquad \frac{t \xrightarrow{a} t'}{t \rhd u \xrightarrow{a} t' \rhd u} \qquad \frac{u \xrightarrow{a} \surd}{t \rhd u \xrightarrow{a} t} \qquad \frac{u \xrightarrow{a} u'}{t \rhd u \xrightarrow{a} u' \cdot t}$$

Exercise

Show that there is no term t in BPA such that $t \underline{\leftrightarrow} x \rhd y$.

Semantics (of interrupt)

$$\frac{t \xrightarrow{a} \surd}{t \rhd u \xrightarrow{a} \surd} \qquad \frac{t \xrightarrow{a} t'}{t \rhd u \xrightarrow{a} t' \rhd u} \qquad \frac{u \xrightarrow{a} \surd}{t \rhd u \xrightarrow{a} t} \qquad \frac{u \xrightarrow{a} u'}{t \rhd u \xrightarrow{a} u' \cdot t}$$

Theorem

Let $\mathcal{E}$ be a finite collection of equations over the language $\mathrm{BPA}_{\rhd}$ that are sound modulo $\underline{\leftrightarrow}$. Let $n > 3$ be larger than the size of each term in the equations in $\mathcal{E}$. Then $\mathcal{E}$ cannot prove

$$\Phi_n \rhd a \approx a + \sum_{i=2}^{n} a((a^{i-1} + a^3 + a) \rhd a) + a\Phi_n.$$

In the above family, $\Phi_n = \sum_{i=1}^{n} t_i$ where $t_1 = a$ and $t_i = a(a^{i-1} + a^3 + a)$ for $i > 1$.

A Menagerie of Nasty Operations: Interrupt

Theorem

Let $\mathcal{E}$ be a finite collection of equations over the language $\text{BPA}_{\triangleright}$ that are sound modulo $\underline{\leftrightarrow}$. Let $n > 3$ be larger than the size of each term in the equations in $\mathcal{E}$. Then $\mathcal{E}$ cannot prove

$$\Phi_n \triangleright a \approx a + \sum_{i=2}^{n} a((a^{i-1} + a^3 + a) \triangleright a) + a\Phi_n.$$

In the above family, $\Phi_n = \sum_{i=1}^{n} t_i$ where $t_1 = a$ and $t_i = a(a^{i-1} + a^3 + a)$ for $i > 1$.

The life of a concurrency theorist is equationally hard, indeed...

Assumption: τ steps are unobservable.

Two Variations on Bisimilarity

A symmetric binary relation $\mathcal{R}$ over closed CCS terms is a weak bisimulation iff for all $t \mathrel{\mathcal{R}} u$, if $t \xrightarrow{a} t'$, then

1. $a = \tau$ and $t' \mathrel{\mathcal{R}} u'$, or
2. $u (\xrightarrow{\tau})^* u_1 \xrightarrow{a} u_2 (\xrightarrow{\tau})^* u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$.

$\mathcal{R}$ is a branching bisimulation if it is a weak bisimulation with the additional requirements that $t \mathrel{\mathcal{R}} u_1$ and $t' \mathrel{\mathcal{R}} u_2$ in item 2.

$t \underline{\leftrightarrow}_W u$ iff $t \mathrel{\mathcal{R}} u$ for some weak bisimulation $\mathcal{R}$.

$t \underline{\leftrightarrow}_B u$ iff $t \mathrel{\mathcal{R}} u$ for some branching bisimulation $\mathcal{R}$.

Examples

$a\tau t \underline{\leftrightarrow}_W at \qquad \tau t + t \underline{\leftrightarrow}_W t \qquad a(t + \tau u) \underline{\leftrightarrow}_W a(t + \tau u) + au$

$$a(\tau(t + u) + u) \underline{\leftrightarrow}_B a(t + u)$$

Weak Semantics over CCS: Definitions and Basic Results

Two Variations on Bisimilarity

A symmetric binary relation $\mathcal{R}$ over closed CCS terms is a weak bisimulation iff for all $t \mathrel{\mathcal{R}} u$, if $t \xrightarrow{a} t'$, then

1. $a = \tau$ and $t' \mathrel{\mathcal{R}} u'$, or
2. $u(\xrightarrow{\tau})^* u_1 \xrightarrow{a} u_2(\xrightarrow{\tau})^* u'$ for some u' such that $t' \mathrel{\mathcal{R}} u'$.

$\mathcal{R}$ is a branching bisimulation if it is a weak bisimulation with the additional requirements that $t \mathrel{\mathcal{R}} u_1$ and $t' \mathrel{\mathcal{R}} u_2$ in item 2.
$t \leftrightarroweq_W u$ iff $t \mathrel{\mathcal{R}} u$ for some weak bisimulation $\mathcal{R}$.
$t \leftrightarroweq_B u$ iff $t \mathrel{\mathcal{R}} u$ for some branching bisimulation $\mathcal{R}$.

Theorem

$\leftrightarroweq_W$ and $\leftrightarroweq_B$ are equivalence relations and the largest weak and branching bisimulation, respectively. However, they are not congruences!

Rooted Bisimulations

$t \underline{\leftrightarrow}_{RW}\, u$ iff

1. if $t \xrightarrow{a} t'$, then $u(\xrightarrow{\tau})^* u_1 \xrightarrow{a} u_2(\xrightarrow{\tau})^* u'$ for some u' such that $t' \underline{\leftrightarrow}_{\mathcal{W}}\, u'$, and
2. if $u \xrightarrow{a} u'$, then $t(\xrightarrow{\tau})^* t_1 \xrightarrow{a} t_2(\xrightarrow{\tau})^* t'$ for some t' such that $t' \underline{\leftrightarrow}_{\mathcal{W}}\, u'$.

$t \underline{\leftrightarrow}_{RB}\, u$ iff

1. if $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \underline{\leftrightarrow}_{\mathcal{B}}\, u'$, and
2. if $u \xrightarrow{a} u'$, then $t \xrightarrow{a} t'$ for some t' such that $t' \underline{\leftrightarrow}_{\mathcal{B}}\, u'$.

Rooted Bisimulations

$t \leftrightarroww_{RW} u$ iff

1. if $t \xrightarrow{a} t'$, then $u(\xrightarrow{\tau})^* u_1 \xrightarrow{a} u_2(\xrightarrow{\tau})^* u'$ for some u' such that $t' \leftrightarroww_{\mathcal{W}} u'$, and
2. if $u \xrightarrow{a} u'$, then $t(\xrightarrow{\tau})^* t_1 \xrightarrow{a} t_2(\xrightarrow{\tau})^* t'$ for some t' such that $t' \leftrightarroww_{\mathcal{W}} u'$.

$t \leftrightarroww_{RB} u$ iff

1. if $t \xrightarrow{a} t'$, then $u \xrightarrow{a} u'$ for some u' such that $t' \leftrightarroww_{\mathcal{B}} u'$, and
2. if $u \xrightarrow{a} u'$, then $t \xrightarrow{a} t'$ for some t' such that $t' \leftrightarroww_{\mathcal{B}} u'$.

Theorem

$\leftrightarroww_{RW}$ and $\leftrightarroww_{RB}$ are the largest congruences over CCS included in $\leftrightarroww_{W}$ and $\leftrightarroww_{B}$, respectively.

Weak Semantics over CCS: Negative Results

Theorem (A., Anastasiadi, Castiglioni, Ingólfsdóttir, Luttik; LICS 2021 and TCS 2025)

Let $\sim$ be a congruence over CCS such that $\underline{\leftrightarrow}_{RB} \subseteq \sim \subseteq \underline{\leftrightarrow}_{RW}$. Then $\sim$ has no finite (ground-)complete axiomatisation.

Proof Sketch

1. Identify an infinite family e_n $(n \geq 1)$ of equations that are sound modulo $\underline{\leftrightarrow}_{RB}$. The one for $\underline{\leftrightarrow}$ works!
2. Prove that no finite set of equations that are sound modulo $\underline{\leftrightarrow}_{RW}$ can prove them all!
3. Proof-theoretic approach. Warning! Non-trivial details! For instance,

$$a\mathbf{0} + a\mathbf{0} \ \underline{\leftrightarrow}_{RW}\ a\mathbf{0}$$

can be proved using the τ-laws.

Weak Semantics over CCS: Positive Results

Theorem (A., Castiglioni, Ingólfsdóttir, Luttik TCS 2025)

1. Assume that A is finite and $\|$ is "pure interleaving". Then, $\underline{\leftrightarrow}_{RB}$ and $\underline{\leftrightarrow}_{RW}$ have a finite equational axiomatisation over CCS with $\|\!\_$.
2. Assume that A is infinite. Then $\underline{\leftrightarrow}_{RB}$ has an equational axiomatisation over CCS with $\|\!\_$ and $|$ that consists of finitely many axiom schemas.

Weak Semantics over CCS: Positive Results

Theorem (A., Castiglioni, Ingólfsdóttir, Luttik TCS 2025)

1. Assume that A is finite and $\|$ is "pure interleaving". Then, $\leftrightarrow_{RB}$ and $\leftrightarrow_{RW}$ have a finite equational axiomatisation over CCS with $\|\!\!\lfloor$.
2. Assume that A is infinite. Then $\leftrightarrow_{RB}$ has an equational axiomatisation over CCS with $\|\!\!\lfloor$ and $|$ that consists of finitely many axiom schemas.

Proof technique

Normal forms and distinguishing substitutions, using unique parallel decomposition. Normal forms for item 1:

$$\sum_{i \in I} a_i t_i + \sum_{j \in J} x_j \|\!\!\lfloor u_j,$$

where each t_i and u_j is a normal form.

Weak Semantics over CCS: Positive Results

Proof technique

Normal forms and distinguishing substitutions, using unique parallel decomposition. Normal forms for item 1:

$$\sum_{i \in I} a_i t_i + \sum_{j \in J} x_j \,\|\!\!\lfloor\, u_j,$$

where each t_i and u_j is a normal form.

Some equations for CCS with $\|\!\!\lfloor$

$$x \,\|\!\!\lfloor\, \tau y \leftrightarroweq_{RB} x \,\|\!\!\lfloor\, y \qquad x \,\|\!\!\lfloor\, (\tau y + z) \leftrightarroweq_{RW} x \,\|\!\!\lfloor\, (\tau y + z) + (x \,\|\!\!\lfloor\, y)$$

A derivable equation modulo $\leftrightarroweq_{RB}$

$$x \,\|\!\!\lfloor\, \tau(y + z) + y \leftrightarroweq_{RB} x \,\|\!\!\lfloor\, (y + z)$$

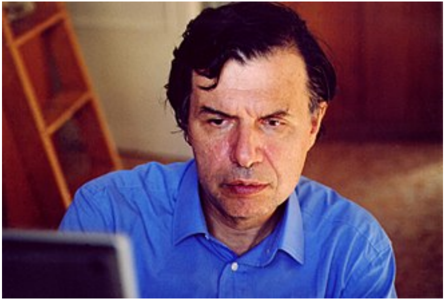
Some Open Problems

- Missing pieces in the axiomatisability puzzle for weak bisimulation semantics.
- Existence of finite complete axiomatisations for 2-nested simulation and possible future semantics over CCS when A is a singleton.
- PolyConc: Removing (some of) our assumptions from the CSL 2021/ToCL 2022 result. ☹
- Find general sufficient conditions ensuring finite axiomatisability of bisimilarity over process algebras.
- Find ways to transfer negative results across languages.
- Several very hard ☹, negative results to prove.

Join the fun!

"The future lies in standing on the shoulders of crowds."
(Nature, 16 June 2021)

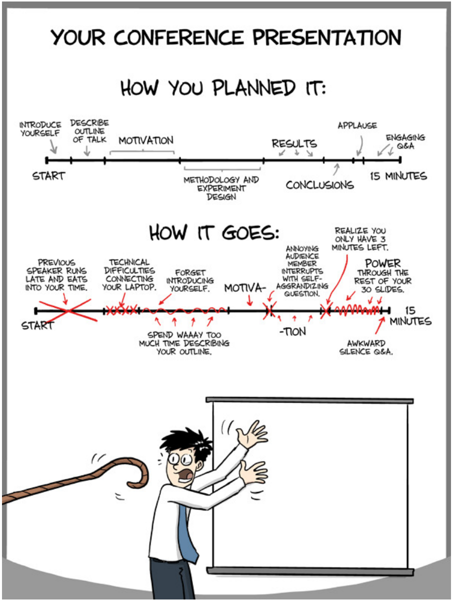
Conclusion: Bonus Take-home Message ☺



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: Bonus Take-home Message ☺



Conclusion: Bonus Take-home Message ☺

Four Requirements of a Good Lecture/Talk

1. Every lecture should make only one main point.
   Audience = herd of cows [Gian-Carlo Rota]
2. Never run overtime.
   Fifty minutes = one microcentury [John von Neumann].
3. Relate to your audience.
   Tip: Everyone in the audience has come to listen to your lecture with the secret hope of hearing their work mentioned.
4. Give them something to take home.

Conclusion: Bonus Take-home Message ☺

Four Requirements of a Good Lecture/Talk

1. Every lecture should make only one main point.
   Audience = herd of cows [Gian-Carlo Rota]
2. Never run overtime.
   Fifty minutes = one microcentury [John von Neumann].
3. Relate to your audience.
   Tip: Everyone in the audience has come to listen to your lecture with the secret hope of hearing their work mentioned.
4. Give them something to take home.

Advice (reloaded)

Scientific presentations are too often confusing, boring and overstuffed. Less is more!

Conclusion: Thanks to all my collaborators (sample below)!










Thank you for your attention!

We are grateful to the Icelandic Research Fund for funding our theoretical research.