On the design of a *Galculator*

Paulo Silva

Departamento de Informática
Universidade do Minho
Braga, Portugal

Third Joint Research Workshop on
Coinduction, Interaction and Composition
May 7 – 8, 2009
Braga

Outline

Outline

Software correctness

Current approaches

- Software correctness is an ambitious challenge
- Logic based approaches benefit from the help of theorem provers
- Sometimes proofs are hindered by the theory
- It is not always easy to devise the correct strategy

Alternatives

- Sometimes algebraic approaches are possible
- Algebras “abstract” the underlying logic
- Proofs become more syntactic

Galois connections can play an important role

Whole division implementation

Haskell code

$$
\begin{aligned}
x \text{ `}div\text{` } y \mid x < y &= 0 \\
\mid x \geqslant y &= (x - y) \text{ `}div\text{` } y + 1
\end{aligned}
$$

for non-negative x and positive y.

This is the code. Where is the specification?

Whole division specification

Implicit definition

$$c = x \div y \;\Leftrightarrow\; \langle \exists\, r \;:\; 0 \leqslant r < y :\; x = c \times y + r \rangle$$

Explicit definition

$$x \div y = \langle \bigvee\, z \;::\; z \times y \leqslant x \rangle$$

Galois connection

$$z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \qquad (y > 0)$$

Whole division specification

Implicit definition

$$c = x \div y \Leftrightarrow \langle \exists\, r \,:\, 0 \leqslant r < y \,:\, x = c \times y + r \rangle$$

Explicit definition

$$x \div y = \langle \bigvee z \,::\, z \times y \leqslant x \rangle$$

Galois connection

$$z \times y \leqslant x \Leftrightarrow z \leqslant x \div y \qquad (y > 0)$$

Whole division specification

Implicit definition

$$c = x \div y \;\Leftrightarrow\; \langle \exists\, r \;:\; 0 \leqslant r < y \,:\; x = c \times y + r \rangle$$

Explicit definition

$$x \div y = \langle \bigvee\; z \;::\; z \times y \leqslant x \rangle$$

Galois connection

$$z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \qquad (y > 0)$$

Whole division

Specification vs. Implementation

- We can *verify* if the implementation meets the specification.
- We can *calculate* the implementation from the specification.

Another useful Galois connection

$$a - b = c \quad \Leftrightarrow \quad a = c + b$$
$$a - b \leqslant c \quad \Leftrightarrow \quad a \leqslant c + b$$

Whole division

Specification vs. Implementation

- We can *verify* if the implementation meets the specification.
- We can *calculate* the implementation from the specification.

Another useful Galois connection

$$a - b = c \quad \Leftrightarrow \quad a = c + b$$
$$a - b \leqslant c \quad \Leftrightarrow \quad a \leqslant c + b$$

Proof.

$z \leqslant x \div y$

$\Leftrightarrow$ { $z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y$ assuming $x \geqslant 0, y > 0$ }

$z \times y \leqslant x$

$\Leftrightarrow$ { cancellation, thanks to $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$z \times y - y \leqslant x - y$

$\Leftrightarrow$ { distributivity }

$(z - 1) \times y \leqslant x - y$

$\Leftrightarrow$ { $z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y$ assuming $x \geqslant y$ }

$z - 1 \leqslant (x - y) \div y$

$\Leftrightarrow$ { $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$z \leqslant (x - y) \div y + 1$

Proof.

$$z \leqslant x \div y$$

$\Leftrightarrow$ { $z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y$ assuming $x \geqslant 0$, $y > 0$ }

$$z \times y \leqslant x$$

$\Leftrightarrow$ { cancellation, thanks to $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$$z \times y - y \leqslant x - y$$

$\Leftrightarrow$ { distributivity }

$$(z - 1) \times y \leqslant x - y$$

$\Leftrightarrow$ { $z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y$ assuming $x \geqslant y$ }

$$z - 1 \leqslant (x - y) \div y$$

$\Leftrightarrow$ { $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$$z \leqslant (x - y) \div y + 1$$

Proof.

$$z \leqslant x \div y$$

$$\Leftrightarrow \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \text{ assuming } x \geqslant 0,\, y > 0 \; \}$$

$$z \times y \leqslant x$$

$$\Leftrightarrow \quad \{ \text{ cancellation, thanks to } a - b \leqslant c \Leftrightarrow a \leqslant c + b \; \}$$

$$z \times y - y \leqslant x - y$$

$$\Leftrightarrow \quad \{ \text{ distributivity } \}$$

$$(z - 1) \times y \leqslant x - y$$

$$\Leftrightarrow \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \text{ assuming } x \geqslant y \; \}$$

$$z - 1 \leqslant (x - y) \div y$$

$$\Leftrightarrow \quad \{ \; a - b \leqslant c \Leftrightarrow a \leqslant c + b \; \}$$

$$z \leqslant (x - y) \div y + 1$$

Proof.

$$z \leqslant x \div y$$

$\Leftrightarrow$ { $z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y$ assuming $x \geqslant 0$, $y > 0$ }

$$z \times y \leqslant x$$

$\Leftrightarrow$ { cancellation, thanks to $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$$z \times y - y \leqslant x - y$$

$\Leftrightarrow$ { distributivity }

$$(z - 1) \times y \leqslant x - y$$

$\Leftrightarrow$ { $z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y$ assuming $x \geqslant y$ }

$$z - 1 \leqslant (x - y) \div y$$

$\Leftrightarrow$ { $a - b \leqslant c \Leftrightarrow a \leqslant c + b$ }

$$z \leqslant (x - y) \div y + 1$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \{\ z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y \text{ assuming } x \geqslant 0,\ y > 0\ \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \{\ \text{cancellation, thanks to } a - b \leqslant c \Leftrightarrow a \leqslant c + b\ \} \\
 & z \times y - y \leqslant x - y \\
\Leftrightarrow & \{\ \text{distributivity}\ \} \\
 & (z - 1) \times y \leqslant x - y \\
\Leftrightarrow & \{\ z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y \text{ assuming } x \geqslant y\ \} \\
 & z - 1 \leqslant (x - y) \div y \\
\Leftrightarrow & \{\ a - b \leqslant c \Leftrightarrow a \leqslant c + b\ \} \\
 & z \leqslant (x - y) \div y + 1
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \text{ assuming } x \geqslant 0,\, y > 0 \; \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \quad \{ \; \text{cancellation, thanks to } a - b \leqslant c \Leftrightarrow a \leqslant c + b \; \} \\
 & z \times y - y \leqslant x - y \\
\Leftrightarrow & \quad \{ \; \text{distributivity} \; \} \\
 & (z - 1) \times y \leqslant x - y \\
\Leftrightarrow & \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \text{ assuming } x \geqslant y \; \} \\
 & z - 1 \leqslant (x - y) \div y \\
\Leftrightarrow & \quad \{ \; a - b \leqslant c \Leftrightarrow a \leqslant c + b \; \} \\
 & z \leqslant (x - y) \div y + 1
\end{array}
$$

□

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \{ \ z \times y \leqslant x \ \Leftrightarrow \ z \leqslant x \div y \ \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \{ \ \text{transitivity, since } x < y \ \} \\
 & z \times y \leqslant x \ \wedge \ z \times y < y \\
\Leftrightarrow & \{ \ \text{since } y \neq 0 \ \} \\
 & z \times y \leqslant x \ \wedge \ z \leqslant 0 \\
\Leftrightarrow & \{ \ z \leqslant 0 \text{ entails } z \times y \leqslant x \text{, since } 0 \leqslant x \ \} \\
 & z \leqslant 0
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \{ \ z \times y \leqslant x \ \Leftrightarrow \ z \leqslant x \div y \ \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \{ \ \text{transitivity, since } x < y \ \} \\
 & z \times y \leqslant x \ \wedge \ z \times y < y \\
\Leftrightarrow & \{ \ \text{since } y \neq 0 \ \} \\
 & z \times y \leqslant x \ \wedge \ z \leqslant 0 \\
\Leftrightarrow & \{ \ z \leqslant 0 \text{ entails } z \times y \leqslant x, \text{ since } 0 \leqslant x \ \} \\
 & z \leqslant 0
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \{\ z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y\ \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \{\ \text{transitivity, since } x < y\ \} \\
 & z \times y \leqslant x \ \wedge\ z \times y < y \\
\Leftrightarrow & \{\ \text{since } y \neq 0\ \} \\
 & z \times y \leqslant x \ \wedge\ z \leqslant 0 \\
\Leftrightarrow & \{\ z \leqslant 0 \text{ entails } z \times y \leqslant x, \text{ since } 0 \leqslant x\ \} \\
 & z \leqslant 0
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \; \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \quad \{ \; \text{transitivity, since } x < y \; \} \\
 & z \times y \leqslant x \;\wedge\; z \times y < y \\
\Leftrightarrow & \quad \{ \; \text{since } y \neq 0 \; \} \\
 & z \times y \leqslant x \;\wedge\; z \leqslant 0 \\
\Leftrightarrow & \quad \{ \; z \leqslant 0 \text{ entails } z \times y \leqslant x, \text{ since } 0 \leqslant x \; \} \\
 & z \leqslant 0
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & z \leqslant x \div y \\
\Leftrightarrow & \quad \{ \; z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \; \} \\
 & z \times y \leqslant x \\
\Leftrightarrow & \quad \{ \; \text{transitivity, since } x < y \; \} \\
 & z \times y \leqslant x \;\wedge\; z \times y < y \\
\Leftrightarrow & \quad \{ \; \text{since } y \neq 0 \; \} \\
 & z \times y \leqslant x \;\wedge\; z \leqslant 0 \\
\Leftrightarrow & \quad \{ \; z \leqslant 0 \text{ entails } z \times y \leqslant x \text{, since } 0 \leqslant x \; \} \\
 & z \leqslant 0
\end{array}
$$

□

Objectives

Galculator

- Build a proof assistant based on Galois connections, their algebra and associated tactics

Outline

1. Introduction
   - Motivation
   - Objectives
2. Theoretical background
   - Indirect equality
   - Galois connections
   - Point-free transform
3. Galculator
4. Conclusion
   - Conclusion
   - Future work

Indirect inequality

Definition (Indirect inequality)

$$a \sqsubseteq b \quad \Leftrightarrow \quad \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle$$
$$a \sqsubseteq b \quad \Leftrightarrow \quad \langle \forall\, x \ :: \ b \sqsubseteq x \Rightarrow a \sqsubseteq x \rangle$$

Proof.

$$
\begin{array}{ll}
 & a = b \\
\Leftrightarrow & \quad \{ \text{ Anti-symmetry } \} \\
 & a \sqsubseteq b \wedge b \sqsubseteq a \\
\Leftrightarrow & \quad \{ \text{ Indirect inequality } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle \wedge \langle \forall\, x \ :: \ x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Rearranging quantifiers } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \wedge x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Mutual implication } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle
\end{array}
$$

□

Proof.

$$a = b$$

$\Leftrightarrow$ { Anti-symmetry }

$$a \sqsubseteq b \wedge b \sqsubseteq a$$

$\Leftrightarrow$ { Indirect inequality }

$$\langle \forall\, x \;::\; x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle \wedge \langle \forall\, x \;::\; x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle$$

$\Leftrightarrow$ { Rearranging quantifiers }

$$\langle \forall\, x \;::\; x \sqsubseteq a \Rightarrow x \sqsubseteq b \wedge x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle$$

$\Leftrightarrow$ { Mutual implication }

$$\langle \forall\, x \;::\; x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle$$

Proof.

$$
\begin{array}{ll}
 & a = b \\
\Leftrightarrow & \quad \{ \text{ Anti-symmetry } \} \\
 & a \sqsubseteq b \wedge b \sqsubseteq a \\
\Leftrightarrow & \quad \{ \text{ Indirect inequality } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle \wedge \langle \forall\, x \ :: \ x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Rearranging quantifiers } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \wedge x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Mutual implication } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle
\end{array}
$$

□

Proof.

$$a = b$$

$\Leftrightarrow$ { Anti-symmetry }

$$a \sqsubseteq b \wedge b \sqsubseteq a$$

$\Leftrightarrow$ { Indirect inequality }

$$\langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle \wedge \langle \forall\, x \ :: \ x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle$$

$\Leftrightarrow$ { Rearranging quantifiers }

$$\langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \wedge x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle$$

$\Leftrightarrow$ { Mutual implication }

$$\langle \forall\, x \ :: \ x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle$$

□

Proof.

$$
\begin{array}{ll}
 & a = b \\
\Leftrightarrow & \quad \{ \text{ Anti-symmetry } \} \\
 & a \sqsubseteq b \wedge b \sqsubseteq a \\
\Leftrightarrow & \quad \{ \text{ Indirect inequality } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \rangle \wedge \langle \forall\, x \ :: \ x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Rearranging quantifiers } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Rightarrow x \sqsubseteq b \wedge x \sqsubseteq b \Rightarrow x \sqsubseteq a \rangle \\
\Leftrightarrow & \quad \{ \text{ Mutual implication } \} \\
 & \langle \forall\, x \ :: \ x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle
\end{array}
$$

□

Indirect equality

Definition (Indirect equality)

$$a = b \quad \Leftrightarrow \quad \langle \forall\, x \; :: \; x \sqsubseteq a \Leftrightarrow x \sqsubseteq b \rangle$$
$$a = b \quad \Leftrightarrow \quad \langle \forall\, x \; :: \; a \sqsubseteq x \Leftrightarrow b \sqsubseteq x \rangle$$

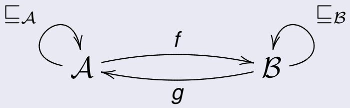
Galois connections

Definition (Galois connection)

Given two preordered sets $(\mathcal{A}, \sqsubseteq_{\mathcal{A}})$ and $(\mathcal{B}, \sqsubseteq_{\mathcal{B}})$ and two functions $\mathcal{B} \xleftarrow{f} \mathcal{A}$ and $\mathcal{A} \xleftarrow{g} \mathcal{B}$, the pair (f, g) is a Galois connection if and only if, for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$:

$$f\ a \sqsubseteq_{\mathcal{B}} b \quad \Leftrightarrow \quad a \sqsubseteq_{\mathcal{A}} g\ b$$

Graphical notation



or $(\mathcal{A}, \sqsubseteq_{\mathcal{A}}) \xleftarrow{(f,g)} (\mathcal{B}, \sqsubseteq_{\mathcal{B}})$

Properties

Property	Description
$f\ a \sqsubseteq_B b \Leftrightarrow a \sqsubseteq_A g\ b$	*"Shunting rule"*
$a \sqsubseteq_A a' \Rightarrow f\ a \sqsubseteq_B f\ a'$	*Monotonicity (LA)*
$b \sqsubseteq_B b' \Rightarrow g\ b \sqsubseteq_A g\ b'$	*Monotonicity (UA)*
$a \sqsubseteq_A g\ (f\ a)$	*Lower cancellation*
$f\ (g\ b) \sqsubseteq_B b$	*Upper cancellation*
$f\ (g\ (f\ a)) = f\ a$	*Semi-inverse*
$g\ (f\ (g\ b)) = g\ b$	*Semi-inverse*
$g\ (b \sqcap_B b') = g\ b \sqcap_A g\ b'$	*Distributivity (UA over meet)*
$f\ (a \sqcup_A a') = f\ a \sqcup_B f\ a'$	*Distributivity (LA over join)*
$g\ \top_B = \top_A$	*Top-preservation (UA)*
$f\ \bot_A = \bot_B$	*Bottom-preservation (LA)*

Galois connections — Algebra

Identity connection

$$(\mathcal{A}, \sqsubseteq_{\mathcal{A}}) \xleftarrow{(id,id)} (\mathcal{A}, \sqsubseteq_{\mathcal{A}})$$

Composition

if $(\mathcal{A}, \sqsubseteq) \xleftarrow{(f,g)} (\mathcal{B}, \preceq)$ and $(\mathcal{B}, \preceq) \xleftarrow{(h,k)} (\mathcal{C}, \leqslant)$ then $(\mathcal{A}, \sqsubseteq) \xleftarrow{(h \circ f, g \circ k)} (\mathcal{C}, \leqslant)$

Composition is *associative* and the identity is its *unit*.
Galois connections form a category.

Galois connections — Algebra

Converse

$$\text{if } (\mathcal{A}, \sqsubseteq) \xleftarrow{(f,g)} (\mathcal{B}, \preceq) \text{ then } (\mathcal{B}, \succeq) \xleftarrow{(g,f)} (\mathcal{A}, \sqsupseteq)$$

Relator

For every relator $\mathcal{F}$

$$\text{if } (\mathcal{A}, \sqsubseteq) \xleftarrow{(f,g)} (\mathcal{B}, \preceq) \text{ then } (\mathcal{F}\mathcal{A}, \mathcal{F} \sqsubseteq) \xleftarrow{(\mathcal{F}f,\mathcal{F}g)} (\mathcal{F}\mathcal{B}, \mathcal{F} \preceq)$$

Logic vs. algebra

Logic	Algebra
Propositional logic	Boolean algebra
Intuitionistic propositional logic	Heyting algebra
Predicate logic	*??*

Relation algebras

- Extension of Boolean algebras
- Original work of De Morgan, Peirce and Schröder
- Further developed by Tarski in his attempt to formalize set theory without variables
- Amenable for syntactic manipulation
- Only one inference rule is needed: substitution of equals by equals

Equational reasoning

Relation algebras

- Extension of Boolean algebras
- Original work of De Morgan, Peirce and Schröder
- Further developed by Tarski in his attempt to formalize set theory without variables
- Amenable for syntactic manipulation
- Only one inference rule is needed: substitution of equals by equals

Equational reasoning

Fork algebras

Limitation of relation algebras

Relations algebras can express first-order predicates with at most three variables

Fork algebras

- Extend relation algebras with a pairing operator
- Equivalent in expressive and deductive power to first-order logic

Fork algebras

Limitation of relation algebras

Relations algebras can express first-order predicates with at most three variables

Fork algebras

- Extend relation algebras with a pairing operator
- Equivalent in expressive and deductive power to first-order logic

Point-free transform summary

Pointwise	Pointfree
$\neg(bRa)$	$b(\neg R)a$
$bRa \wedge bSa$	$b(R \cap S)a$
$bSa \vee bSa$	$b(R \cup S)a$
$True$	$b \top a$
$False$	$b \perp a$
$b = a$	$b\ id\ a$
aRb	$bR^{\circ}a$
$\langle \exists\ c\ ::\ bRc \wedge cSa \rangle$	$b(R \circ S)a$
$\langle \forall\ x\ ::\ xRb \Rightarrow xSa \rangle$	$b(R \setminus S)a$
$\langle \forall\ x\ ::\ aRx \Rightarrow bSx \rangle$	$b(S / R)a$
$bRa \wedge cSa$	$(b, c)\langle R, S \rangle a$
$bRa \wedge dSc$	$(b, d)(R \times S)(a, c)$
$\langle \forall\ a, b\ ::\ bRa \Rightarrow bSa \rangle$	$R \subseteq S$
$\langle \forall\ a, b\ ::\ bRa \Leftrightarrow bSa \rangle$	$R = S$

Point-free definitions

Definition (Galois connection)

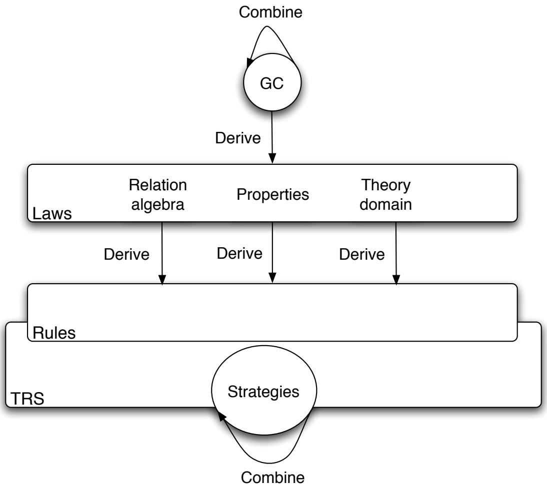
$$f^{\circ} \circ \sqsubseteq_{\mathcal{B}} \quad = \quad \sqsubseteq_{\mathcal{A}} \circ g$$

Definition (Indirect equality)

$$f = g \quad \Leftrightarrow \quad \preceq \circ f = \preceq \circ g$$
$$f = g \quad \Leftrightarrow \quad f^{\circ} \circ \preceq = g^{\circ} \circ \preceq$$

Outline

Design Principles



Outline

Conclusion

- Proof assistant prototype based on Galois connections
- Innovative approach
  - Combination of Galois connections and point-free calculus
- Non-trivial example of the application of distinctive features of functional languages
  - Generalized algebraic data types
  - Existential data types
  - Combinatorial approaches (parsing, rewriting)
  - Support for embedded domain specific languages
  - Computations as monads
  - Higher-order functions
  - **New:** Polymorphic type representation with unification
  - ...

Future work

- Automated proofs
- Free-theorems
- Integration with host theorem provers (e.g., *Coq*)

Download

Source code and documentation available from
`www.di.uminho.pt/research/galculator`

Contact

Questions to `paufil@di.uminho.pt`