Galois:

A Language for Proofs Using Galois connections and Fork Algebras

Paulo Silva[1] Joost Visser[2] José Oliveira[1]

[1]CCTC
University of Minho
Braga, Portugal

[2]Software Improvement Group
The Netherlands

PLMMS'09
August 21, 2009
Munich, Germany

Outline

Outline

Whole division

Prove

$$(a \div b) \div c \;=\; a \div (c \times b)$$

for b and $c \neq 0$.

- Easy if $\div$ is the real number division
- Also valid in natural numbers but the proof is not so straightforward

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

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

Proof.

$$
\begin{array}{ll}
 & n \leqslant (a \div b) \div c \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \times c \leqslant a \div b \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & (n \times c) \times b \leqslant a \\
\Leftrightarrow & \quad \{\ \text{multiplication is associative}\ \} \\
 & n \times (c \times b) \leqslant a \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \leqslant a \div (c \times b)
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & n \leqslant (a \div b) \div c \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \times c \leqslant a \div b \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & (n \times c) \times b \leqslant a \\
\Leftrightarrow & \quad \{\ \text{multiplication is associative}\ \} \\
 & n \times (c \times b) \leqslant a \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \leqslant a \div (c \times b)
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & n \leqslant (a \div b) \div c \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \times c \leqslant a \div b \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & (n \times c) \times b \leqslant a \\
\Leftrightarrow & \quad \{\ \text{multiplication is associative}\ \} \\
 & n \times (c \times b) \leqslant a \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \leqslant a \div (c \times b)
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & n \leqslant (a \div b) \div c \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \times c \leqslant a \div b \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & (n \times c) \times b \leqslant a \\
\Leftrightarrow & \quad \{\ \text{multiplication is associative}\ \} \\
 & n \times (c \times b) \leqslant a \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \leqslant a \div (c \times b)
\end{array}
$$

Proof.

$$
\begin{array}{ll}
 & n \leqslant (a \div b) \div c \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \times c \leqslant a \div b \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & (n \times c) \times b \leqslant a \\
\Leftrightarrow & \quad \{\ \text{multiplication is associative}\ \} \\
 & n \times (c \times b) \leqslant a \\
\Leftrightarrow & \quad \{\ z \times y \leqslant x \Leftrightarrow z \leqslant x \div y\ \} \\
 & n \leqslant a \div (c \times b)
\end{array}
$$

Objectives

Galculator = **Gal**ois connection + cal**culator**

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

Galois

- Language for mathematical reasoning
- Equivalent to first-order logic
- Typed language
- Front-end for the *Galculator*

Outline

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.

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

Proof.

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

Proof.

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

Proof.

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

Indirect equality

Definition (Indirect equality)

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

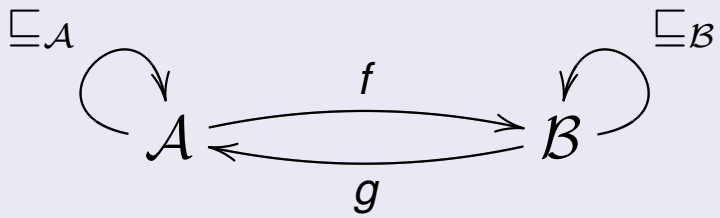
Galois connections

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

Point-free definitions

Definition (Galois connection)

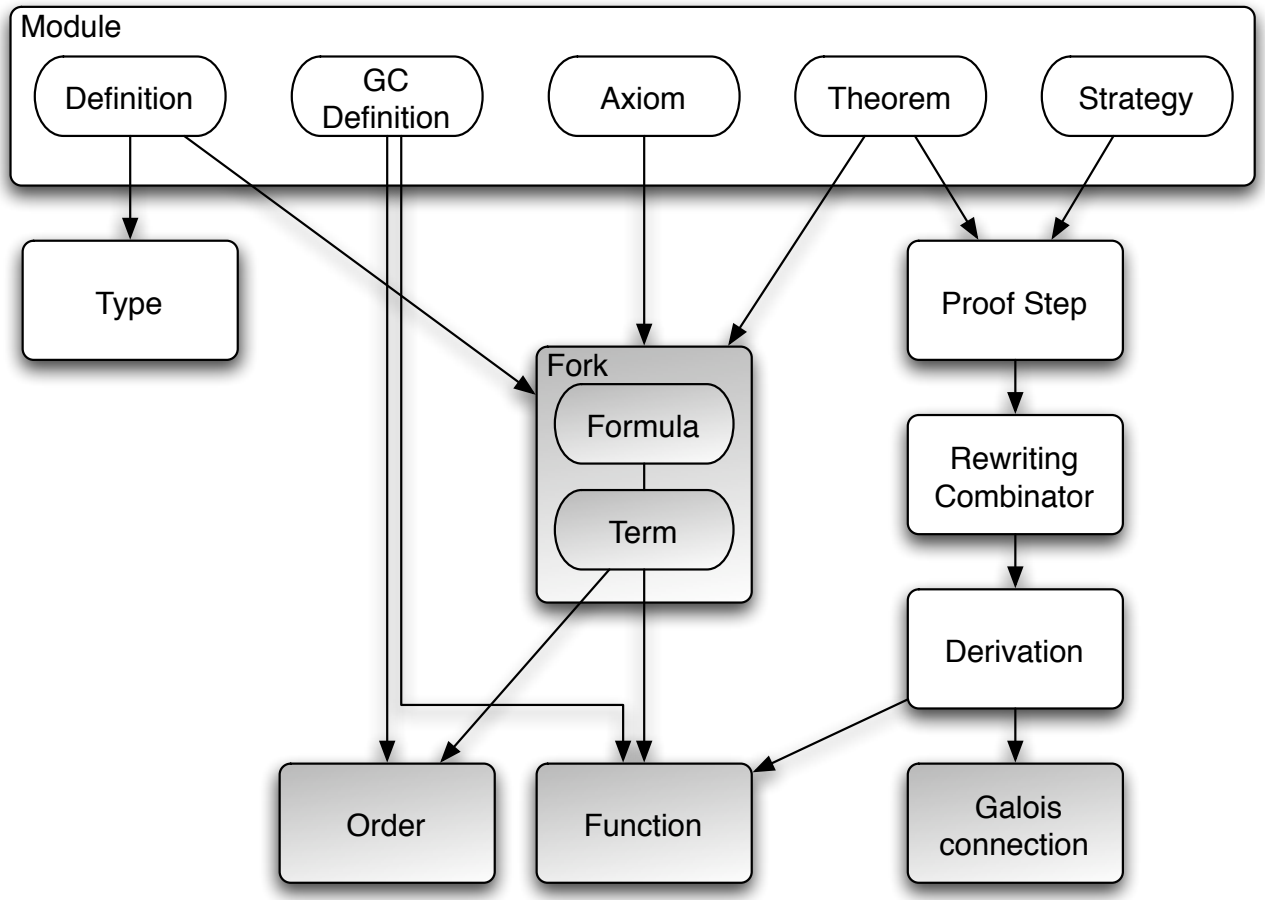
$$f^\circ \circ \sqsubseteq_{\mathcal{B}} \quad = \quad \sqsubseteq_{\mathcal{A}} \circ g$$

Definition (Indirect equality)

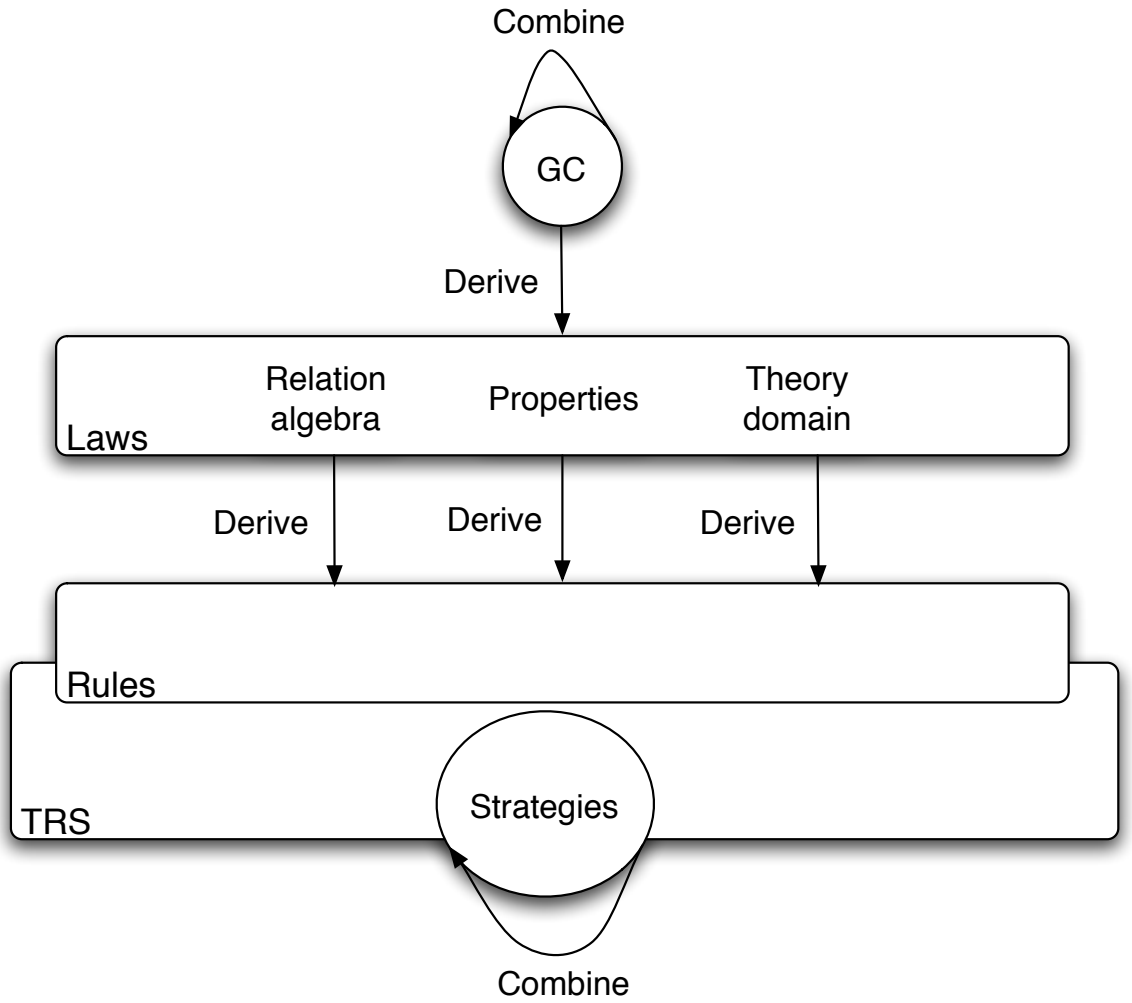
$$f = g \quad \Leftrightarrow \quad \preceq \circ f = \preceq \circ g$$
$$f = g \quad \Leftrightarrow \quad f^\circ \circ \preceq = g^\circ \circ \preceq$$

Outline

Sub-languages of *Galois*



Architecture of *Galculator*



Outline

Summary

Fork algebras

- Equivalent to first-order logic (same expressive and deductive power)
- Single inference rule: substitution of equals for equals
- Equational
- No variables
- Integrates Galois connections and indirect equality

Galois connections

- Provide structure
- Introduce semantic information in syntactic reasoning

Summary

Galois

- Follows the mathematical concepts
- Alternative to first-order languages
- Typed approach

Galculator

- Proof assistance prototype based on Galois connections
- Innovative approach
- Uses a point-free equational approach

Future work

- Mechanization of point-free transform
- Automated proofs
- Extension of the type system
- Free-theorems
- Evaluation of the language
- 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`