Curry-Howard Correspondance between Temporal Logic and Reactive Programming

Esaïe Bauer

Alexis Saurin & Thomas Ehrhard

13 octobre 2021

Who am I ?

Today

PhD student under the direction of Alexis Saurin & Thomas Ehrhard.

Who am I ?

Today

PhD student under the direction of Alexis Saurin & Thomas Ehrhard.

Internships

Worked with Marie Kerjean & Olivier Laurent.

Table des matières

Table des matières

Informal definitions

Temporal logic is a logic system where formulas have a truth value evolving over time.

Informal definitions

Temporal logic is a logic system where formulas have a truth value evolving over time.

Reactive programming is a programm paradigm concerned by propagating a reactive input (such as stream) to ensure properties or modify value over time.

Example : spreadsheet, graphical interface, web app

Temporal logic

Three connectives

We introduce three connectives :

$$\bigcirc A, \quad \Diamond A \quad \text{and} \quad \Box A$$

Temporal logic

Three connectives

We introduce three connectives :

$$\bigcirc A, \quad \Diamond A \quad \text{and} \quad \Box A$$

Formulas

$$\mathcal{F} ::= \mathcal{V}\text{ar} \mid \mathcal{F} \vee \mathcal{F} \mid \mathcal{F} \wedge \mathcal{F} \mid \mathcal{F} \to \mathcal{F} \mid \bigcirc \mathcal{F} \mid \mu X.F \mid \nu X.F \mid \bot \mid 1$$

Fixed point

Constructions with fixed point

$$\Diamond A ::= \mu X.A \vee \bigcirc X \text{ or } \Box A ::= \nu X.A \wedge \bigcirc X$$

$$\text{or } A \mathcal{U} B ::= \mu X.((A \wedge \bigcirc X) \vee B)$$

Fixed point over $\Box$ and $\Diamond$

$$\Box\Diamond A \quad \text{and} \quad \nu X.\mu Y.((A \wedge \bigcirc X) \vee \bigcirc Y)$$

both express that there will be an infinite number of A

Reactive programming and causality

Causality

$f(s_1, \ldots, s_n, s_{n+1}, \ldots) = f(s_1, \ldots, s_n, s'_{n+1}, \ldots)$ at time n

Reactive programming and causality

Causality

$f(s_1, \ldots, s_n, s_{n+1}, \ldots) = f(s_1, \ldots, s_n, s'_{n+1}, \ldots)$ at time n

$$\bigcirc(A \vee B) \rightarrow \bigcirc A \vee \bigcirc B$$

should not be provable.

FRP (Cave, Ferreira, Panangaden & Pientka)

$$\text{let } \bullet x = t_1 \text{ in } t_2 \qquad \bullet t$$

Sequents

$$\Theta; \Gamma \vdash A$$

Typing rules

$$\frac{; \Theta \vdash t : A}{\Theta; \Gamma \vdash \bullet t : \bigcirc A}\ \bigcirc_i \qquad \frac{\Theta; \Gamma \vdash t_1 : \bigcirc A \qquad \Theta, x : A; \Gamma \vdash t_2 : B}{\Theta; \Gamma \vdash \text{let } \bullet x = t_1 \text{ in } t_2 : B}\ \bigcirc_e$$

Reduction rules and normalization

Règle de réduction

$$\text{let } \bullet x = \bullet t_1 \text{ in } t_2 \rightarrow t_2[x := t_1]^{\bullet}$$

Reduction rules and normalization

Règle de réduction

$$\text{let } \bullet x = \bullet t_1 \text{ in } t_2 \to t_2[x := t_1]^\bullet$$

Strong Normalization

If $\Theta; \Gamma \vdash t : A$ is provable then t is strongly normalizing

Table des matières

Transforming FRP

FRP typing system seen as a sequent calculus, with step-indexed formula led to :

$$;\bigcirc A \to \bigcirc B \nvdash \bigcirc(A \to B)$$

Transforming FRP

FRP typing system seen as a sequent calculus, with step-indexed formula led to :

$$;\bigcirc A \to \bigcirc B \nvdash \bigcirc(A \to B)$$

Transforming FRP into a $\bar{\lambda}\mu$-*FRP*

Transforming FRP

FRP typing system seen as a sequent calculus, with step-indexed formula led to :

$$;\bigcirc A \to \bigcirc B \nvdash \bigcirc(A \to B)$$

Transforming FRP into a $\bar{\lambda}\mu$-*FRP*

Problem : in classical LTL, $\bigcirc(A \vee B) \vdash \bigcirc A \vee \bigcirc B$ is a theorem.

Circular proofs

Circular proofs

Circular proofs is a way of formalizing induction and coinduction in rule system.

Circular proofs

Circular proofs

Circular proofs is a way of formalizing induction and coinduction in rule system.

Formalizing such a system in a Coq Library