Provability of Functionnal Reactive Programming type system

Esaïe Bauer and Alexis Saurin
IRIF – Université de Paris – CNRS – INRIA

December 2, 2021

Table des matières

Table of contents

Functionnal Reactive programming

History

Eliott and Hudak introduced it in 1997 with Functionnal Reactive animation

Functionnal Reactive programming

History

Eliott and Hudak introduced it in 1997 with Functionnal Reactive animation

Program paradigm concerned by propagating a reactive input (such as stream) to ensure properties or modify values over time

Functionnal Reactive programming

History

Eliott and Hudak introduced it in 1997 with Functionnal Reactive animation

Program paradigm concerned by propagating a reactive input (such as stream) to ensure properties or modify values over time

Exemple: Spreadsheet, graphical interface, web app

Linear Temporal Logic

Connectives:

$$\bigcirc A \qquad \Diamond A \qquad \Box A \qquad A \; U \; B$$

Linear Temporal Logic

Connectives:

$$\bigcirc A \qquad \Diamond A \qquad \Box A \qquad A\, U\, B$$

Pnueli used temporal logic to reason on reactive programs in 1977

Linear Temporal Logic

Connectives:

$$\bigcirc A \qquad \Diamond A \qquad \Box A \qquad A\ U\ B$$

Pnueli used temporal logic to reason on reactive programs in 1977

Yuse and Igarashi use temporal logic to encode multi-level generating code extensions with persistent code

Table of contents

Fair Reactive Programming (Cave, Ferreira, Panangaden and Pientka - 2013)

Functionnal Reactive Programming typed by a Linear Temporal Logic system

We will name this system FRP (for Fair Reactive Programming)

Fair Reactive Programming (Cave, Ferreira, Panangaden and Pientka - 2013)

Functionnal Reactive Programming typed by a Linear Temporal Logic system

We will name this system FRP (for Fair Reactive Programming)

Types of FRP

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

Fair Reactive Programming (Cave, Ferreira, Panangaden and Pientka - 2013)

Functionnal Reactive Programming typed by a Linear Temporal Logic system

We will name this system FRP (for Fair Reactive Programming)

Types of FRP

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

$$\Box A := \nu X.A \wedge \bigcirc X$$

$$\Diamond A := \mu X.A \vee \bigcirc X$$

$$A\, U\, B := \mu X.(B \vee (A \wedge \bigcirc X))$$

Temporal terms and derivation rules

$$\bullet t : \bigcirc A \qquad \text{let } \bullet x = t \text{ in } t_2 : C$$

Temporal terms and derivation rules

$$\bullet t : \bigcirc A \qquad \text{let } \bullet x = t \text{ in } t_2 : C$$

Sequents

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

Temporal terms and derivation rules

$$\bullet t : \bigcirc A \qquad \text{let } \bullet x = t \text{ in } t_2 : C$$

Sequents

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

Typing rules

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

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

Causality

Causality

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

$$\bigcirc A \to A$$

should no be provable:

$$\text{predictor1}(x : \bigcirc A) := \text{let } \bullet x' = x \text{ in } x'$$

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

$$\bigcirc A \to A$$

should no be provable:

$$\text{predictor1}(x : \bigcirc A) := \text{let } \bullet x' = x \text{ in } x'$$

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

should not be provable:

$$\begin{aligned} \text{predictor2 } (x : \bigcirc(A \vee B)) = \text{let } \bullet x' = x \text{ in case } x' \text{ of} \\ |\text{inl } a \to \text{inl } (\bullet a) \\ |\text{inr } b \to \text{inr } (\bullet b) \end{aligned}$$

Other rejected formula

$$A \to \bigcirc A$$

would not break causality, but we refute it anyway. (accepted in Krishnaswami and Benton 2011 but rejected in Krishnaswami 2013 paper for managing space)

$$\text{import } (x : A) = \bullet x$$

Some example of implementation

Type of Temporal Streams on A : $\Box A$ (namely $\nu X.A \wedge \bigcirc X$)

Some example of implementation

Type of Temporal Streams on A : $\Box A$ (namely $\nu X.A \wedge \bigcirc X$)

$$\text{coit app } f\ \ a : \Box(A \to B) \to \Box A \to \Box B :=$$

$$\text{let } ha, hf = \text{hd } a, \text{hd } f \text{ in}$$

$$\text{let } \bullet ta, \bullet tf = \text{tl } a, \text{tl } f \text{ in } (hf\ \ ha, \bullet\text{app } tf\ \ ta)$$

Table of contents

Linear Temporal Logic from Kojima and Igarashi ($LJ^{\bigcirc}$) - 2011

No $\Diamond$, $\Box$ and fixpoint, only $\bigcirc$ to deal with time

Linear Temporal Logic from Kojima and Igarashi ($LJ^{\bigcirc}$) - 2011

No $\Diamond$, $\Box$ and fixpoint, only $\bigcirc$ to deal with time

Sequents are made of formulas indexed with a natural number

Linear Temporal Logic from Kojima and Igarashi ($LJ^{\bigcirc}$) - 2011

No $\Diamond$, $\Box$ and fixpoint, only $\bigcirc$ to deal with time

Sequents are made of formulas indexed with a natural number

$$\frac{\Gamma^{\vec{m}}, A^{n+1} \vdash B^m}{\Gamma^{\vec{m}}, (\bigcirc A)^n \vdash B^m} \bigcirc_l \qquad \frac{\Gamma^{\vec{m}} \vdash A^{n+1}}{\Gamma^{\vec{m}} \vdash (\bigcirc A)^n} \bigcirc_r$$

Causality

$\vee$-rule

$$\frac{\Gamma^{\vec{m}}, A^n \vdash C^m \qquad \Gamma^{\vec{m}}, B^n \vdash C^m \qquad n \leq m}{\Gamma^{\vec{m}}, (A \vee B)^n \vdash C^m} \vee_I$$

Causality

∨-rule

$$\frac{\Gamma^{\vec{m}}, A^n \vdash C^m \qquad \Gamma^{\vec{m}}, B^n \vdash C^m \qquad n \leq m}{\Gamma^{\vec{m}}, (A \vee B)^n \vdash C^m} \vee_l$$

Thanks to the side condition, $\bigcirc(A \vee B) \rightarrow (\bigcirc A \vee \bigcirc B)$ is not provable in the system.

$\mathrm{FRP}^{\bigcirc}$

Same sequents than $\mathrm{LJ}^{\bigcirc}$.

FRP$^{\bigcirc}$

Same sequents than LJ$^{\bigcirc}$.

Additional side conditions:

$$\frac{\Gamma^{\vec{m}}, A^n \vdash C^m \qquad \Gamma^{\vec{m}}, B^n \vdash C^m \qquad n \leq m, \vec{m}}{\Gamma^{\vec{m}}, (A \vee B)^n \vdash C^m} \vee_l$$

$$\frac{\Gamma^{\vec{m}}, A^n \vdash B^n \qquad n \leq \vec{m}}{\Gamma^{\vec{m}} \vdash (A \to B)^n} \to_r$$

FRP$^{\bigcirc}$

Same sequents than LJ$^{\bigcirc}$.

Additional side conditions:

$$\frac{\Gamma^{\vec{m}}, A^n \vdash C^m \qquad \Gamma^{\vec{m}}, B^n \vdash C^m \qquad n \leq m, \vec{m}}{\Gamma^{\vec{m}}, (A \vee B)^n \vdash C^m} \vee_l$$

$$\frac{\Gamma^{\vec{m}}, A^n \vdash B^n \qquad n \leq \vec{m}}{\Gamma^{\vec{m}} \vdash (A \to B)^n} \to_r$$

μ and ν-free FRP is provably equivalent to FRP$^{\bigcirc}$.

FRP$^{\bigcirc}$

Same sequents than LJ$^{\bigcirc}$.

Additional side conditions:

$$\frac{\Gamma^{\vec{m}}, A^n \vdash C^m \qquad \Gamma^{\vec{m}}, B^n \vdash C^m \qquad n \leq m, \vec{m}}{\Gamma^{\vec{m}}, (A \vee B)^n \vdash C^m} \vee_l$$

$$\frac{\Gamma^{\vec{m}}, A^n \vdash B^n \qquad n \leq \vec{m}}{\Gamma^{\vec{m}} \vdash (A \to B)^n} \to_r$$

μ and ν-free FRP is provably equivalent to FRP$^{\bigcirc}$.

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

Table of contents

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

W is a non-empty set,

Kripke models

IM-frame

Quadruplet $(W, \leq, \text{R}, \Vdash)$ such that :

- W is a non-empty set,
- $\leq$ is a partial order on W,

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

- W is a non-empty set,
- $\leq$ is a partial order on W,
- R is a binary relation on W,

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

- W is a non-empty set,
- $\leq$ is a partial order on W,
- R is a binary relation on W,
- $\Vdash$ is a relation between elements of W and propositionnal variables

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

- W is a non-empty set,
- $\leq$ is a partial order on W,
- R is a binary relation on W,
- $\Vdash$ is a relation between elements of W and propositionnal variables

Interpretation of formulas

$$w \Vdash A \to B \Leftrightarrow (\forall w' \geq w, (w' \Vdash A) \Rightarrow (w' \Vdash B))$$

Kripke models

IM-frame

Quadruplet $(W, \leq, \mathrm{R}, \Vdash)$ such that :

- W is a non-empty set,
- $\leq$ is a partial order on W,
- R is a binary relation on W,
- $\Vdash$ is a relation between elements of W and propositionnal variables

Interpretation of formulas

$w \Vdash A \rightarrow B \Leftrightarrow (\forall w' \geq w, (w' \Vdash A) \Rightarrow (w' \Vdash B))$

$w \Vdash \bigcirc A \Leftrightarrow (\forall v, w \, \mathrm{R} \, v \Rightarrow v \Vdash A)$

Correctness and Completness

Two axioms:

axiom 1:

$$(\leq, \text{R}, \leq) = \text{R}$$

axiom 2:

$$\forall w, v, w \text{ R } v \rightarrow (\exists w', w \leq w' \text{ and } \forall u, (w' \text{ R } u) \Leftrightarrow (v \leq u)$$

Correctness and Completeness

Two axioms:
axiom 1:

$$(\leq, \text{R}, \leq) = \text{R}$$

axiom 2:

$$\forall w, v, w \text{ R } v \rightarrow (\exists w', w \leq w' \text{ and } \forall u, (w' \text{ R } u) \Leftrightarrow (v \leq u)$$

Correctness and Completeness for $LJ^{\bigcirc}$ (Kojima and Igarashi - 2011)

IM-frame together with axiom 1 and 2 are correct and complete relatively to $LJ^{\bigcirc}$.

Correctness and Completeness

Two axioms:

axiom 1:

$$(\leq, \mathrm{R}, \leq) = \mathrm{R}$$

axiom 2:

$$\forall w, v, w \mathrel{\mathrm{R}} v \rightarrow (\exists w', w \leq w' \text{ and } \forall u, (w' \mathrel{\mathrm{R}} u) \Leftrightarrow (v \leq u))$$

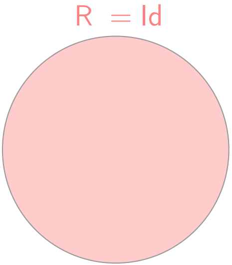
Correctness and Completeness for $LJ^{\bigcirc}$ (Kojima and Igarashi - 2011)

IM-frame together with axiom 1 and 2 are correct and complete relatively to $LJ^{\bigcirc}$.

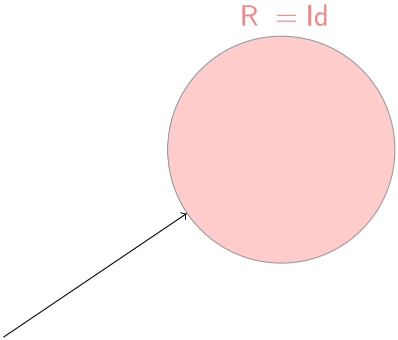
Correctnness and Completeness for $FRP^{\bigcirc}$

IM-frame satisfying axiom 1 are correct and complete relatively to $FRP^{\bigcirc}$.

Kripke models

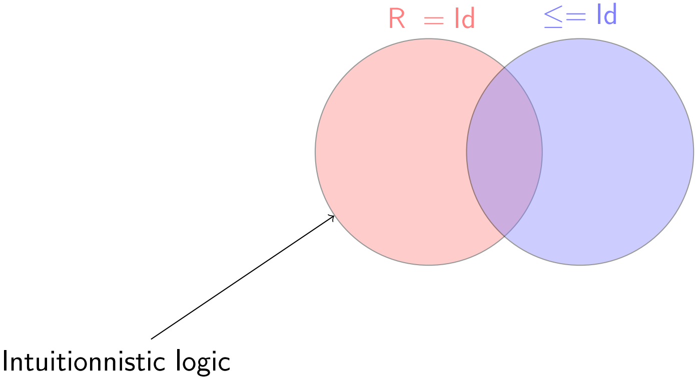


Kripke models

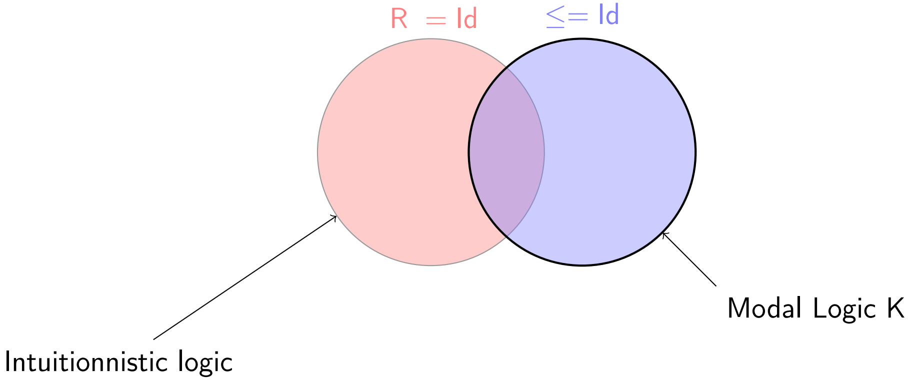


Intuitionnistic logic

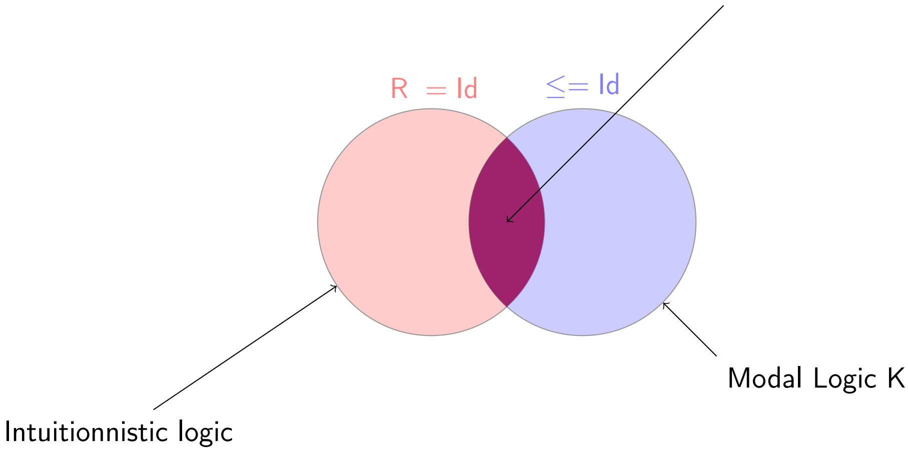
Kripke models



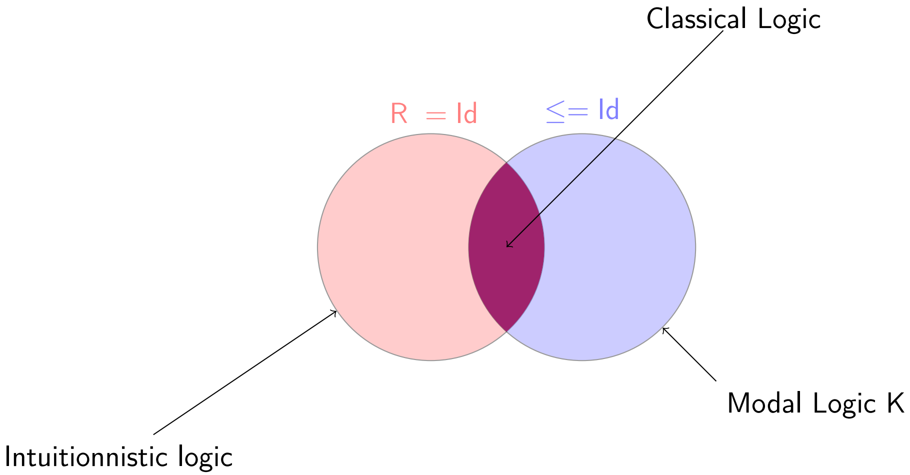
Kripke models



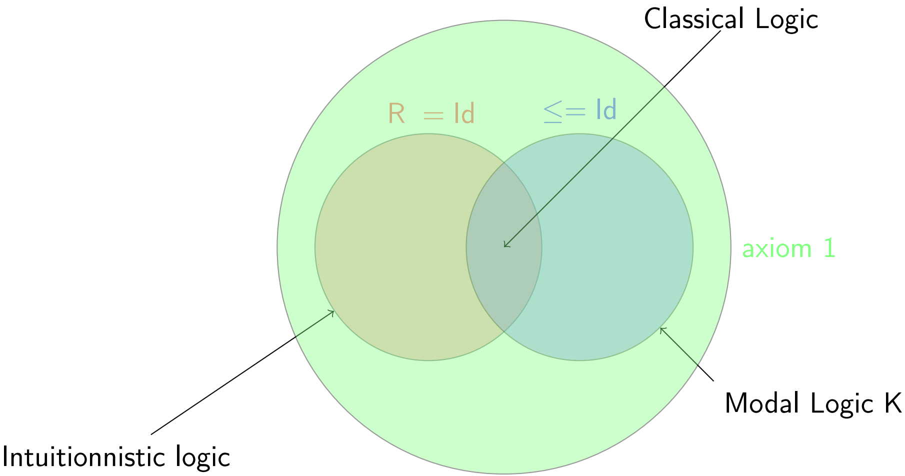
Kripke models



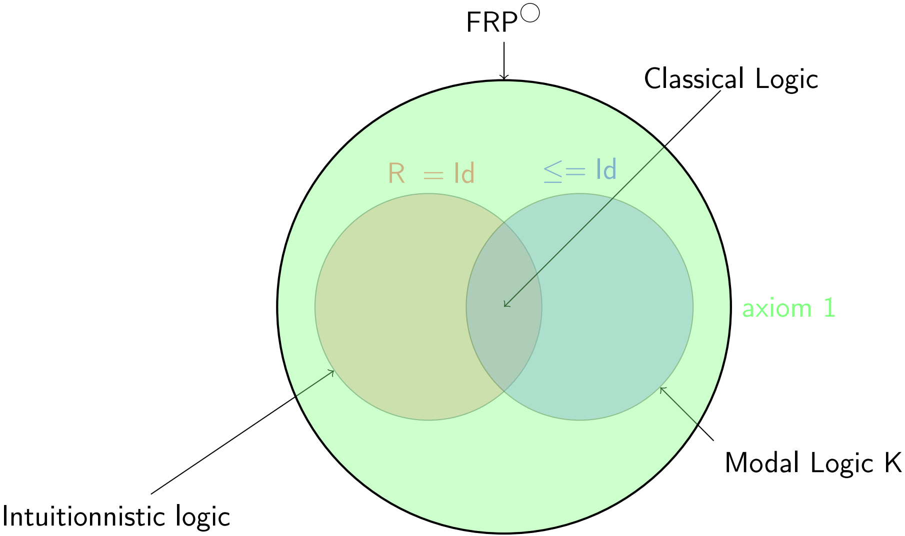
Kripke models



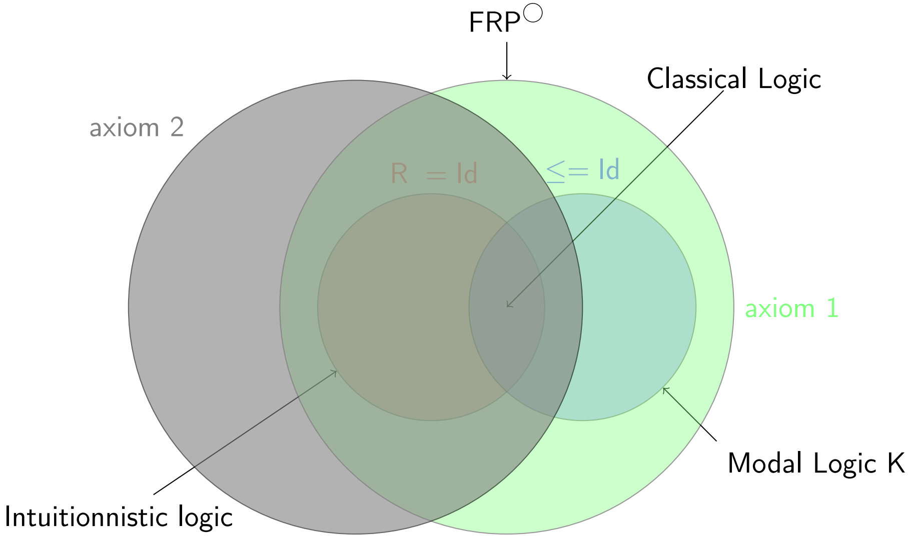
Kripke models



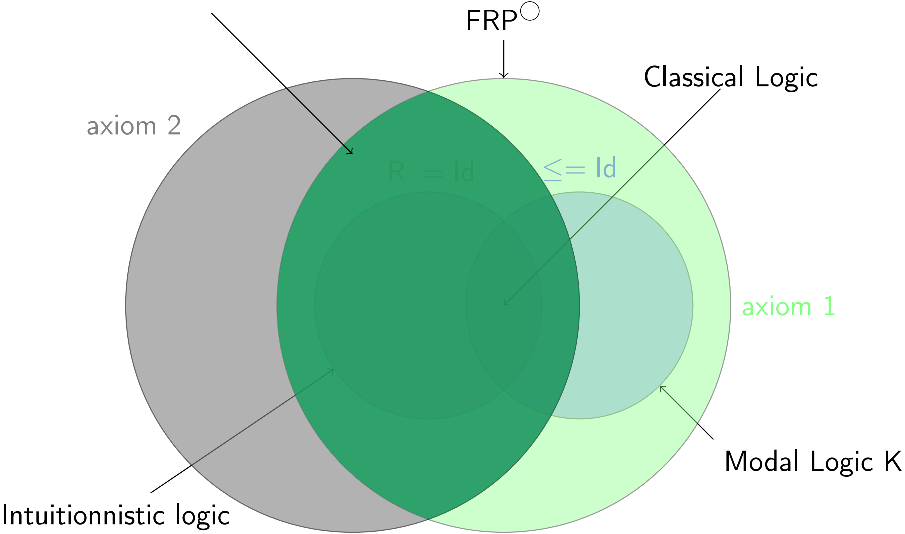
Kripke models



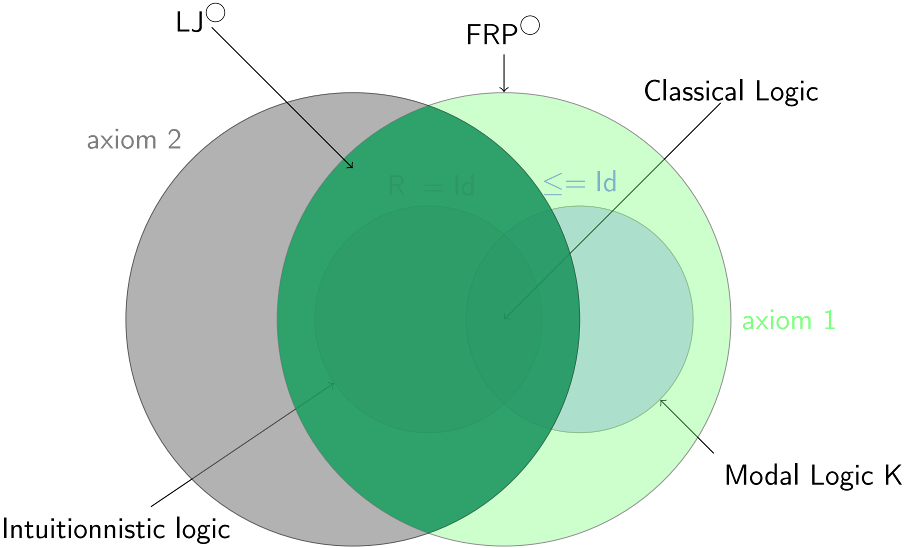
Kripke models



Kripke models



Kripke models



Kripke models

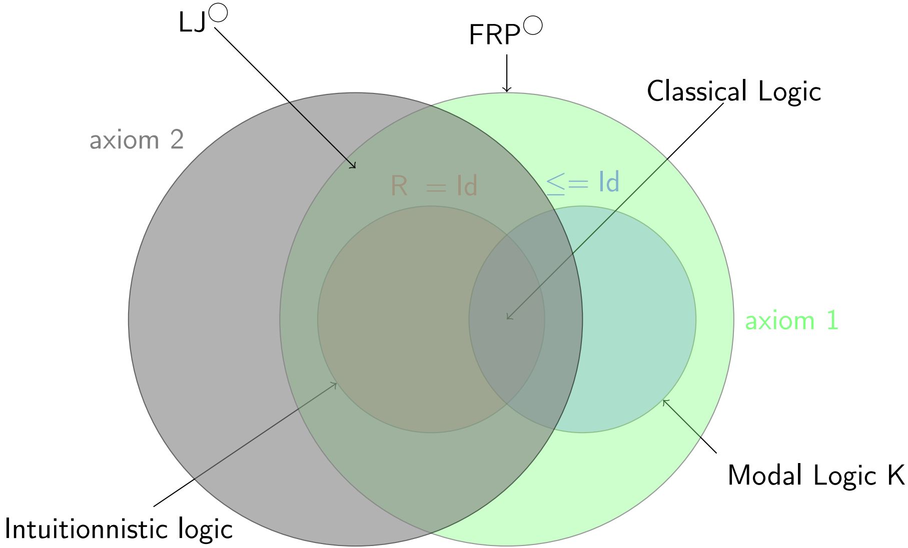


Table of contents

Future works

Extending our results to full FRP (with fixpoints)

Future works

Extending our results to full FRP (with fixpoints)

Consider a classical setting for FRP ($\lambda\mu - calculus$ from Parigot)