The Curry–Howard Correspondence between Temporal Logic and Functional Reactive Programming

Wolfgang Jeltsch

Brandenburgische Technische Universität Cottbus
Cottbus, Germany

Teooriapäevad Nelijärvel
Nelijärve, Estonia

February 4–6, 2011

Brandenburgische Technische Universität Cottbus

FRP Basics

- functional programming with support for describing temporal phenomena
- two new concepts:

  behavior a time-varying value

  $$\mathcal{B}\alpha \approx \mathsf{Time} \to \alpha$$

  event a time with an associated value

  $$\mathcal{E}\alpha \approx \mathsf{Time} \times \alpha$$

- event streams derivable via coinduction:

$$\mathcal{S}\alpha = \mathcal{E}(\alpha \times \mathcal{S}\alpha)$$

Some operations on behaviors and events

- transformation of embedded values:

$$\begin{aligned} \mathcal{B}f &: \mathcal{B}\alpha \to \mathcal{B}\beta && \text{for every } f : \alpha \to \beta \\ \mathcal{E}f &: \mathcal{E}\alpha \to \mathcal{E}\beta && \text{for every } f : \alpha \to \beta \end{aligned}$$

- further operations:

$$\begin{aligned} \mathsf{const} &: \alpha \to \mathcal{B}\alpha \\ \mathsf{zip} &: \mathcal{B}\alpha \times \mathcal{B}\beta \to \mathcal{B}(\alpha \times \beta) \\ \mathsf{sample} &: \mathcal{B}\alpha \times \mathcal{E}\beta \to \mathcal{E}(\alpha \times \beta) \\ \mathsf{switch} &: \mathcal{B}\alpha \times \mathcal{E}(\mathcal{B}\alpha) \to \mathcal{B}\alpha \end{aligned}$$

Some derived operations on event streams

Remember

$$\mathcal{S}\alpha = \mathcal{E}(\alpha \times \mathcal{S}\alpha)$$

- transformation of embedded values:

$$\mathcal{S}f : \mathcal{S}\alpha \to \mathcal{S}\beta$$
$$\mathcal{S}f = \mathcal{E}(\lambda(x, s)\ .\ (f(x), \mathcal{S}f(s)))$$

Remember

$$\text{switch} : \mathcal{B}\alpha \times \mathcal{E}(\mathcal{B}\alpha) \to \mathcal{B}\alpha$$

- multiple switching:

$$\text{switches} : \mathcal{B}\alpha \times \mathcal{S}(\mathcal{B}\alpha) \to \mathcal{B}\alpha$$
$$\text{switches}(b, s) = \text{switch}(b, \mathcal{E}\text{switches}(s))$$

Example: Controlling a light bulb

- three devices:

  two buttons send event streams s_1 and s_2 of type $\mathcal{S}1$

  one bulb receives a behavior b of type $\mathcal{B}\mathrm{Bool}$

- bulb switched on/off whenever one of the buttons is pressed

Remember

$$\mathcal{S}\alpha = \mathcal{E}(\alpha \times \mathcal{S}\alpha)$$

- bulb control for a single button with a given initial state:

$$\mathrm{control} : \mathrm{Bool} \times \mathcal{S}1 \to \mathcal{B}\mathrm{Bool}$$

$$\mathrm{control}(i, s) = \mathit{switch}(\mathrm{const}(i), \mathcal{E}(\lambda(\_, s')\ .\ \mathrm{control}(\neg i, s'))(s))$$

- combined bulb control for both buttons:

$$b = \mathcal{B}\mathrm{xor}(\mathit{zip}(\mathrm{control}(s_1, \bot), \mathrm{control}(s_2, \bot)))$$

Curry–Howard Correspondence

- correspondence between logic and type system:

$$
\begin{array}{ccc}
\text{proposition} & \longleftrightarrow & \text{type} \\
\uparrow & & \uparrow \\
\text{proof} & \longleftrightarrow & \text{expression}
\end{array}
$$

- some correspondences:
  - intuitionistic propositional logic $\longleftrightarrow$ simple types:

$$
\begin{aligned}
\langle \varphi \vee \psi \rangle &= \langle \varphi \rangle + \langle \psi \rangle \\
\langle \varphi \wedge \psi \rangle &= \langle \varphi \rangle \times \langle \psi \rangle \\
\langle \varphi \rightarrow \psi \rangle &= \langle \varphi \rangle \rightarrow \langle \psi \rangle
\end{aligned}
$$

  - intuitionistic predicate logic $\longleftrightarrow$ dependent types:

$$
\begin{aligned}
\langle \forall x \,.\, P[x] \rangle &= \Pi x \,.\, \langle P[x] \rangle \\
\langle \exists x \,.\, P[x] \rangle &= \Sigma x \,.\, \langle P[x] \rangle
\end{aligned}
$$

Linear Temporal Logic

- trueness of a proposition depends on time
- times are natural numbers
- propositional logic extended with four new constructs:

$\bigcirc\varphi$	φ will hold at the next time
$\Box\varphi$	φ will always hold
$\Diamond\varphi$	φ will eventually hold
$\varphi \rhd \psi$	φ will hold for some time, and then ψ will hold

- in this talk only $\Box$ and $\Diamond$ (continuous time also possible)

A semantics for □–◇–LTL

- meaning of a temporal formula is a formula of predicate logic with a free variable t that denotes the current time
- atomic propositions p correspond to predicates $\hat{p}$ that take a time argument
- semantics for propositional logic fragment:

$$
\begin{aligned}
[\![p]\!] &= \hat{p}(t) & [\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \wedge [\![\psi]\!] \\
[\![\top]\!] &= \top & [\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \vee [\![\psi]\!] \\
[\![\bot]\!] &= \bot & [\![\varphi \rightarrow \psi]\!] &= [\![\varphi]\!] \rightarrow [\![\psi]\!]
\end{aligned}
$$

- semantics for □ and ◇:

$$
\begin{aligned}
[\![\Box\varphi]\!] &= \forall t' \in [t, \infty) \,.\, [\![\varphi]\!][t'/t] \\
[\![\Diamond\varphi]\!] &= \exists t' \in [t, \infty) \,.\, [\![\varphi]\!][t'/t]
\end{aligned}
$$

$\square$–$\diamond$–LTL as a type system

- type inhabitation depends on time
- simple type system extended with two new type constructors $\blacksquare$ and $\blacklozenge$
- meaning of a temporal type is a dependent type with a free variable t that denotes the current time
- semantics for $\blacksquare$ and $\blacklozenge$:

$$[\![\blacksquare\alpha]\!] = \Pi t' \in [t, \infty) \,.\, [\![\alpha]\!][t'/t]$$
$$[\![\blacklozenge\alpha]\!] = \Sigma t' \in [t, \infty) \,.\, [\![\alpha]\!][t'/t]$$

- compare this to the intuition behind $\mathcal{B}$ and $\mathcal{E}$:

$$\mathcal{B}\alpha \approx \text{Time} \rightarrow \alpha$$
$$\mathcal{E}\alpha \approx \text{Time} \times \alpha$$

- $\square$–$\diamond$–LTL corresponds to a strongly typed form of FRP where $\mathcal{B} = \blacksquare$ and $\mathcal{E} = \blacklozenge$

Start time consistency

Remember

$$\llbracket \mathcal{B}\alpha \rrbracket = \Pi t' \in [t, \infty) \; . \; \llbracket \alpha \rrbracket [t'/t]$$
$$\llbracket \mathcal{E}\alpha \rrbracket = \Sigma t' \in [t, \infty) \; . \; \llbracket \alpha \rrbracket [t'/t]$$

- each behavior and each event has a dedicated start time t:
  - behavior: only has a value at its start time and afterwards
  - event: can only fire at its start time or afterwards
- type system ensures start time consistency:
  - an inhabitant of some type α at some time t deals only with behaviors and events that start at t
  - values within behaviors and events use their occurrence times as start times

Start time consistency and zipping

Remember

$$\text{zip} : \mathcal{B}\alpha \times \mathcal{B}\beta \to \mathcal{B}(\alpha \times \beta)$$

- meaning of zip's type:

$$(\Pi t' \in [t, \infty) \, . \, [\![\alpha]\!][t'/t]) \times (\Pi t' \in [t, \infty) \, . \, [\![\beta]\!][t'/t])$$
$$\downarrow$$
$$\Pi t' \in [t, \infty) \, . \, [\![\alpha]\!][t'/t] \times [\![\beta]\!][t'/t]$$

- type system ensures reasonable conditions:
  - **pre** argument behaviors have to start at the same time
  - **post** result behavior starts at the same time as the argument behaviors

Start time consistency and switching

Remember

$$\text{switch} : \mathcal{B}\alpha \times \mathcal{E}(\mathcal{B}\alpha) \to \mathcal{B}\alpha$$

- meaning of $\mathcal{E}(\mathcal{B}\alpha)$:

$$\Sigma t' \in [t, \infty) \,.\, \Pi t'' \in [t', \infty) \,.\, [\![\alpha]\!][t''/t]$$

- behavior has to start at the time of switching
- avoids problems with accumulating behaviors
- take again the light bulb example:
  - bulb control b starts when button inputs s_1 and s_2 start
  - switching to b later typically causes problems:

semantics	b always begins with $\perp$ at switching time
efficiency	b's value is (re)computed at switching time

Distributivity of $\Diamond$ over finite disjunctions

- in classical modal and temporal logics, $\Diamond$ distributes over finite disjunctions:

$$\Diamond(\varphi \vee \psi) \rightarrow \Diamond\varphi \vee \Diamond\psi$$

$$\Diamond\bot \rightarrow \bot$$

- different approaches for intuitionistic logics:
  - keep both laws
  - keep only $\Diamond\bot \rightarrow \bot$
  - drop both

FRP suggests temporal constructivity

- distributivity laws correspond to these FRP types:

$$\mathcal{E}(\alpha + \beta) \to \mathcal{E}\alpha + \mathcal{E}\beta$$
$$\mathcal{E}0 \to 0$$

- no combinators of these types, since these would be non-causal
- makes it plausible to drop both distributivity laws from intuitionistic temporal logic
- logic is now constructive with respect to time:
  - no access to the whole time scale
  - time-dependent knowledge can be expressed

Conclusions and Outlook

- Curry–Howard Correspondence between $\Box$–$\Diamond$–LTL and FRP
- development of a precise correspondence leads to interesting concepts, e.g.:
  - a type system that ensures start time consistency
  - a form of constructivity that allows us to express time-dependent knowledge
- further interesting things:
  - FRP analogs to $\bigcirc$ and $\triangleright$
  - common categorical semantics for LTL and FRP
  - induction and coinduction in LTL and FRP
- see also my seminar talk in Tallinn next Thursday