Modelli di computazione per la verifica formale

Workshop FORMA e sostanza — DIBRIS

Enrico Ghiorzi

6 Luglio 2023

What I have been up to:

- PhD in category theory (enriched and internal categories)
- categorical semantics of inductive data types (ADTs, nested types, GADTs) at Appstate
- formal methods applied to autonomous (robotic) systems, at IIT (synthesis of temporal logic contrastive exaplnations)
- CONVINCE project on verification and monitoring of autonomous systems, at DIBRIS

Contents

Definition

A category $\mathbf{C}$ is given by

- a class of objects $\mathrm{Ob}_{\mathbf{C}}$
- a class of morphisms $\mathrm{Morph}_{\mathbf{C}}$
- a composition operation $\circ$
- an identity operation id

such that

- each morphism $f \in \mathrm{Morph}_{\mathbf{C}}$ has a domain and a codomain object, and we write $f\colon A \to B$
- each object A has an identity morphism $\mathrm{id}_A \colon A \to A$
- consecutive morphisms $f\colon A \to B$ and $g\colon B \to C$ can be composed into $g \circ f\colon A \to C$
- composition is associative, and unitary with respect to identity

Example

The category **Set** has

- Sets as objects
- Functions between sets as morphisms
- Composition of functions as composition
- Identity function on a set as identity

Example

The category $\mathbf{Set}_{\mathrm{fin}}$ has

- Finite sets as objects
- Functions between finite sets as morphisms
- Composition of functions as composition
- Identity function on a finite set as identity

Definition

Given categories $\mathbf{C}$ and $\mathbf{D}$, a functor $F\colon \mathbf{C} \to \mathbf{D}$ is given by

- an object component $F_0\colon \mathrm{Ob}_{\mathbf{C}} \to \mathrm{Ob}_{\mathbf{D}}$
- a morphism component $F_1\colon \mathrm{Morph}_{\mathbf{C}} \to \mathrm{Morph}_{\mathbf{D}}$

preserving composition and identity

$$F_1(g \circ_{\mathbf{C}} f) = F_1(g) \circ_{\mathbf{D}} F_1(f) \qquad F_1(\mathrm{id}_A) = \mathrm{id}_{F_0(A)}$$

Definition

A coalgebra of an (endo)functor $F\colon \mathbf{C} \to \mathrm{CtC}$ on a carrier object A is a morphism $A \to F(A)$

A morphism of coalgebrae $A \xrightarrow{\alpha} F(A)$ and $B \xrightarrow{\beta} F(B)$ is a morphism $f\colon A \to B$ such that

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"] & F(A) \arrow[d, "F(f)"] \\ B \arrow[r, "\beta"] & F(B) \end{tikzcd}$$

Deterministic Automata

Definition (Jacobs)

A deterministic automaton with

- set of inputs I
- set of outputs O

is a coalgebra for the functor **Set** $\to$ **Set**

$$F(-) = (-)^I \times O$$

that is, a function

$$X \xrightarrow{\langle t,o \rangle} X^I \times O$$

where

- $t \colon X \times I \to X$ is the transition function
- $o \colon X \to O$ is the observation function

Non-Deterministic Automata

Definition (Jacobs)

A non-deterministic automaton with

- set of inputs I
- set of outputs O

is a coalgebra for the functor $\mathbf{Set} \to \mathbf{Set}$

$$\mathsf{F}(-) = \mathcal{P}(-)^{\mathsf{I}} \times \mathsf{O}$$

that is, a function

$$\mathsf{X} \xrightarrow{\langle \mathsf{t},\mathsf{o} \rangle} \mathcal{P}(\mathsf{X})^{\mathsf{I}} \times \mathsf{O}$$

where

- $\mathsf{t} \subseteq \mathsf{X} \times \mathsf{I} \times \mathsf{X}$ is the transition relation
- $\mathsf{o} \colon \mathsf{X} \to \mathsf{O}$ is the observation function

Example

A labelled program graph is a non-deterministic automata with trivial output $O = \mathbb{1}$.

Example

Replacing **Set** with $\mathbf{Set}_{\mathrm{fin}}$ we model finite automata.

Morphisms of non-deterministic automata

Definition

Given non-deterministic automata as coalgebras

$$X \xrightarrow{\langle t_X, o_X \rangle} \mathcal{P}(X)^I \times O \quad \text{and} \quad Y \xrightarrow{\langle t_Y, o_Y \rangle} \mathcal{P}(Y)^I \times O$$

a homomorphism between them is given by a function $f \colon X \to Y$ such that

$$\begin{array}{ccc} X & \xrightarrow{\langle t_X, o_X \rangle} & \mathcal{P}(X)^I \times O \\ {\scriptstyle f}\big\downarrow & & \big\downarrow{\scriptstyle \mathcal{P}(f)^I \times id_O} \\ Y & \xrightarrow{\langle t_Y, o_Y \rangle} & \mathcal{P}(Y)^I \times O \end{array}$$

where $\mathcal{P}(f)^I$ sends $h \colon I \to \mathcal{P}(X)$ into $i \in I \mapsto f(h(i)) \subseteq Y$.

Lemma (Jacobs)

$f\colon X \to Y$ *is a homomorphism of coalgebras iff*

- $x \downarrow o \implies f(x) \downarrow o$ *for* $x \in X$ *and* $o \in O$
- $x \xrightarrow{i} x' \implies f(x) \xrightarrow{i} f(x')$ *for* $x, x' \in X$ *and* $i \in I$
- $f(x) \xrightarrow{i} y \implies \exists x' \in X.\, f(x') = y$ *and* $x \xrightarrow{i} x'$ *for* $x \in X$, $y \in Y$ *and* $i \in I$

- For some functors F there is a “special” coalgebra: the terminal coalgebra
- Via terminal coalgebrae, the behavior of an algebra can be defined
- Bisimilarity is carachterized via behavior: two states have the same behavior if and only if they have the same behavior
- As corollary: bisimilarity on the final coalgebra is equality
- Other models of computation can be modeled with other categorical models, then they can be put in relation via functors