Behavioural Distances for Higher-Order Languages with Continuous Probabilities. M2 Internship Proposal

Raphaëlle Crubillé
raphaelle.crubille@lis-lab.fr

LIS (Aix-Marseille Université)

Morris Context Equivalence (1969)

Comparing Two Programs

check whether two programs behaves *the same* no matter how the environment interacts with them (compiler optimisation, verification of a specification...);

When are two programs context equivalent?

- Environments are modelled as **contexts**–i.e. terms with a hole–thus by way of the underlying language
- Two terms are context equivalent if their **observable behaviour** is the same in **any** context.

Definition (Context Equivalence)

$M \;\equiv^{\mathrm{ctx}} N$ when:

$$\forall \text{ context } \mathcal{C},\ \mathsf{Obs}(\mathcal{C}[M]) = \mathsf{Obs}(\mathcal{C}[N]).$$

Observation in a Probabilistic Setting

Observing at type Nat

Probability that the program terminates:

$$Obs_n(M) = \text{Prob}(M \text{ returns } n)$$

Example

M and N are contextually distinguishable, but behave very **similarly**.

$$M(f) = f(0)$$
$$N(f) = \text{ if } (\text{rand}([0,1]) \geq \epsilon) \text{ then } f(0) \text{ else } f(1) \qquad \text{where } \epsilon \ll 1.$$

Quantitative Generalization of Contextual Equivalence

Definition (Contextual Distance)

$$\delta^{\text{ctx}}(M, N) = \sup_{\mathcal{C} \text{ a context, } n \in \mathbb{N}} \Big| \, \mathit{Prob}(C[M] \text{ returns } n) - \mathit{Prob}(C[N] \text{ returns } n) \, \Big|$$

Motivation:

- A statistical model is often approximated (deduced from statistical measure)
- security, e.g computational indistinguishability

Goal of this internship

Generalise definitions/ operational or denotational caracterisations of program distances from **discrete** probabilities to **continuous** probabilities.

Source: http://marseille-tourisme.com/