Preuve de programmes aléatoires

Bibliothèque Coq

Christine Paulin

Université Paris Sud et INRIA Futurs

AVERROES - Grenoble - 10/02/06

Plan

- Méthode générale
- Bibliothèque
- Systèmes de transitions probabilistes

Langage de base

Des expressions e représentant des calculs probabilistes

- Primitive constants and functions: c
- Random primitives : `random`(n), `flip` ...
- Conditional: **if** b **then** e_1 **else** e_2
- Local binding: **let** $x = a$ **in** b
- Abstraction: **fun** $(x : \tau) \Rightarrow e$
- Application: $(e_1\ e_2)$

Comment les représenter dans Coq ?

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision opérationnelle

- Espace Ω des suites de tirages aléatoires indépendants: booléens, tirages uniformes . . .
- Un état global ω de type Ω.
  Dans Coq possibilité d'utiliser une stream implantant un générateur de nombres aléatoires
- Un appel à `random` consomme une partie de ω.
- Une expression $e : \tau$ est interprétée comme une fonction $[e] : \Omega \rightarrow \tau \times \Omega$.
- $\Pr(\{e|P(e)\}) = \Pr_{Omega}\{\omega|P(\pi_1([e](\omega)))\}$
- Possibilité d'estimation par simulation.

Vision probabiliste

- Chaque expression de type τ définit une distribution sur τ.
- Représentations possibles des distributions
  - $(\tau \to \{0,1\}) \to [0,1]$
  - $(\tau \to \mathbb{R}^+) \to \mathbb{R}^+$
  - $(\tau \to [0,1]) \to [0,1]$
- $\Pr(P(e)) = [e](\mathbb{I}_P)$
- Possibilité de sémantique axiomatique $k \leq [e](f)$

Vision probabiliste

- Chaque expression de type τ définit une distribution sur τ.
- Représentations possibles des distributions
  - $(\tau \to \{0,1\}) \to [0,1]$
  - $(\tau \to \mathbb{R}^+) \to \mathbb{R}^+$
  - $(\tau \to [0,1]) \to [0,1]$
- $\Pr(P(e)) = [e](\mathbb{I}_P)$
- Possibilité de sémantique axiomatique $k \leq [e](f)$

Vision probabiliste

- Chaque expression de type τ définit une distribution sur τ.
- Représentations possibles des distributions
  - $(\tau \to \{0,1\}) \to [0,1]$
  - $(\tau \to \mathbb{R}^+) \to \mathbb{R}^+$
  - $(\tau \to [0,1]) \to [0,1]$
- $\Pr(P(e)) = [e](\mathbb{I}_P)$
- Possibilité de sémantique axiomatique $k \leq [e](f)$

Vision probabiliste

- Chaque expression de type τ définit une distribution sur τ.
- Représentations possibles des distributions
  - $(\tau \to \{0,1\}) \to [0,1]$
  - $(\tau \to \mathbb{R}^+) \to \mathbb{R}^+$
  - $(\tau \to [0,1]) \to [0,1]$
- $\Pr(P(e)) = [e](\mathbb{I}_P)$
- Possibilité de sémantique axiomatique $k \leq [e](f)$

Axiomatisation de $[0,1]$

- $0,1 : U$, $\forall x, 0 \leq x \leq 1$, $0 \neq 1$
- $(x,y) \mapsto x + y$ borné par 1, $(x,y) \mapsto x \times y$, $x \mapsto 1 - x$
- $n \mapsto \frac{1}{n+1}$, $\frac{1}{n+1} = 1 - n \times \frac{1}{n+1}$ $x \neq 0 \Rightarrow \exists n, \frac{1}{n+1} \leq x$
- $\texttt{lub} : (\texttt{nat} \to U) \to U$
- Vision classique : $\neg\neg x \leq y \Rightarrow x \leq y$, totality de l'ordre $(x \leq y) \vee_c (y \leq x)$

Formalisme suffisant pour déduire les opérations et propriétés usuelles : $x - y$, $\texttt{max}$ ...

Représentation des distributions

Définition d'un record $(\texttt{distr}\ \tau)$
$fg : \tau \to U, k : U$

- $\mu : (\tau \to U) \to U$
- $f \leq 1 - g \Rightarrow \mu(f + g) = \mu(f) + \mu(g)$
- $\mu(1 - f) \leq 1 - \mu(f)$
- $\mu(k \times f) = k \times \mu(f)$

Représentation des programmes

- $\texttt{Munit} : \tau \to \texttt{distr}\ \tau$
  mesure de dirac.
- $\texttt{Mlet} : \texttt{distr}\ \tau \to (\tau \to \texttt{distr}\ \sigma) \to \texttt{distr}\ \sigma$.
  mesure produit.
- $\texttt{Mif} : \texttt{distr bool} \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau$.
- $\texttt{Mfix} : ((\tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma$
  hypothèse de monotonicité, itération à partir de 0.
- Primitives aléatoires
  - $\texttt{Random} : \texttt{int} \to \texttt{distr int}$
  - $\texttt{Flip} : \texttt{distr bool}$
  - tirage dans un ensemble fini, tirage uniforme. . .

Représentation des programmes

- $\texttt{Munit} : \tau \to \texttt{distr}\ \tau$
  mesure de dirac.
- $\texttt{Mlet} : \texttt{distr}\ \tau \to (\tau \to \texttt{distr}\ \sigma) \to \texttt{distr}\ \sigma$.
  mesure produit.
- $\texttt{Mif} : \texttt{distr bool} \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau$.
- $\texttt{Mfix} : ((\tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma$
  hypothèse de monotonicité, itération à partir de 0.
- Primitives aléatoires
  - $\texttt{Random} : \texttt{int} \to \texttt{distr int}$
  - $\texttt{Flip} : \texttt{distr bool}$
  - tirage dans un ensemble fini, tirage uniforme. . .

Représentation des programmes

- $\texttt{Munit} : \tau \to \texttt{distr}\ \tau$
  mesure de dirac.
- $\texttt{Mlet} : \texttt{distr}\ \tau \to (\tau \to \texttt{distr}\ \sigma) \to \texttt{distr}\ \sigma$.
  mesure produit.
- $\texttt{Mif} : \texttt{distr bool} \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau$.
- $\texttt{Mfix} : ((\tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma$
  hypothèse de monotonicité, itération à partir de 0.
- Primitives aléatoires
  - $\texttt{Random} : \texttt{int} \to \texttt{distr int}$
  - $\texttt{Flip} : \texttt{distr bool}$
  - tirage dans un ensemble fini, tirage uniforme. . .

Représentation des programmes

- $\texttt{Munit} : \tau \to \texttt{distr}\ \tau$
  mesure de dirac.
- $\texttt{Mlet} : \texttt{distr}\ \tau \to (\tau \to \texttt{distr}\ \sigma) \to \texttt{distr}\ \sigma$.
  mesure produit.
- $\texttt{Mif} : \texttt{distr bool} \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau$.
- $\texttt{Mfix} : ((\tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma$
  hypothèse de monotonicité, itération à partir de 0.
- Primitives aléatoires
  - $\texttt{Random} : \texttt{int} \to \texttt{distr int}$
  - $\texttt{Flip} : \texttt{distr bool}$
  - tirage dans un ensemble fini, tirage uniforme. . .

Représentation des programmes

- $\texttt{Munit} : \tau \to \texttt{distr}\ \tau$
  mesure de dirac.
- $\texttt{Mlet} : \texttt{distr}\ \tau \to (\tau \to \texttt{distr}\ \sigma) \to \texttt{distr}\ \sigma$.
  mesure produit.
- $\texttt{Mif} : \texttt{distr}\ \texttt{bool} \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau \to \texttt{distr}\ \tau$.
- $\texttt{Mfix} : ((\tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma) \to \tau \to \texttt{distr}\ \sigma$
  hypothèse de monotonicité, itération à partir de 0.
- Primitives aléatoires
  - $\texttt{Random} : \texttt{int} \to \texttt{distr}\ \texttt{int}$
  - $\texttt{Flip} : \texttt{distr}\ \texttt{bool}$
  - tirage dans un ensemble fini, tirage uniforme. . .

Logique axiomatique

Application

$$\frac{k \leq [a](f) \quad \forall x, f\ x \leq [e\ x](g)}{k \leq [e\ a](g)}$$

Conditionnelle

$$\frac{k_1 \leq [e_1](f) \quad k_2 \leq [e_2](f)}{k_1 \times [b](\mathbb{I}_{.=\texttt{true}}) + k_2 \times [b](\mathbb{I}_{.=\texttt{false}}) \leq [\textbf{if}\ b\ \textbf{then}\ e_1\ \textbf{else}\ e_2](f)}$$

Point fixe

$$\frac{\forall f : A \to \texttt{distr}\ B, (\forall x, p_n\ x \leq [f\ x](q)) \Rightarrow (\forall x, p_{n+1}\ x \leq [F\ f\ x](q))}{\forall x, \texttt{lub}\ (p_n\ x)_n \leq [\textbf{fix}\ F\ x](q)}$$

Règle dérivée

$$\frac{1 \leq [a](\mathbb{I}_P) \quad \forall x, (P\ x) \Rightarrow k \leq [b](f)}{k \leq [\textbf{let}\ x = a\ \textbf{in}\ b](f)}$$

Applications

- Distribution bernouilli, loi binomiale
- Terminaison probabiliste tirages pile ou face
- Itération d'un choix probabiliste

Systèmes de transitions probabilistes

Tentative de modélisation

- Relation de transitions probabiliste : $\texttt{step} : \tau \to \texttt{distr}\ \tau$
- Extention à une distribution sur les chemins de longueur k issus d'une état s :
  $\texttt{path} : \texttt{distr}\ (\texttt{nelist}\ \tau)$

Traitement du non-déterminisme

(McIver, Morgan)

- Algorithmique distribuée
- Raffinement
- Probabilités approchées
- Notion de **sous-distribution**
  - $\mu(f + g) \leq \mu(f) + \mu(g)$
  - $\texttt{choice} : \texttt{sdistr}\ \tau \to \texttt{sdistr}\ \tau \to \texttt{sdistr}\ \tau$
  - $\texttt{choice}\ e_1\ e_2\ f = \texttt{min}\ (e_1\ f)\ (e_2\ f)$

Conclusion

- Une base conséquente pour raisonner sur les programmes probabilistes
- Des variations à explorer : non-déterminisme, mesure de fonctions à valeur réelles . . .
- Nécessité de traiter des exemples plus complexes, d'automatiser la construction du modèle, les preuves.

Références

- Bibliothèque : contribution Coq V8.1
- Contribution AVERROES `http://www.lri.fr/~paulin/library.pdf`
- Article soumis