Un cadre logique pour raisonner sur les algorithmes probabilites : La semantique axiomatique de Hoare

En 81, Dexter Kozen a proposé une sémnantique dénotationnelle pour le langage impératif de référence, enrichi d'une instruction d'affection

$$X := \texttt{random}\ \gamma$$

où γ représente une distribution de probabilité. Dans ce cadre, un programme doit être considéré comme un **transformation de mesures de sous-probabilités**.

Certains travaux ont suivi qui s'appuient sur cette propostion pour développer un cadre semi-logique dans lequel est espérances mathématiques prennent la place des prédicats et formules logiques.

Dans un travail commun avec E. Zucca (DISI-Gènes), nous avons montré comme il est possible de construire un système d'inférence pour la sémantique axiomatique, aussitôt que le langage possède une sémantique dénotationnelle. La combinaison de ces deux travaux nous permet de développer naturellement un tel système pour les algorithmes aléatoires, et d'offrir ainsi un cadre logique pour développer des preuves de spécifications de la forme

$$\vdash \{P\}C\{Q\}$$

où P, Q sont des prédicats, ou des formules logiques construites en **logique intuitionniste**, et comportant comme formules atomiques des expressions telles que

$$Prob\,[A] \leq a$$

constamment présentes dans les preuves de tels algorithmes. De fait, la restriction au cadre intuitionniste est induit autant par ces formules que par les propriétés particulières du modèle d'interprétation des programmes aléatoires.

L'approche proposée préserve entièrement le système originel de Hoare. Il s'adapte sans le moindre effort en présence de mécanismes d'exceptions ou de blocs de commandes étiquetées.

Ce travail est né dans le cadre des TDs donnés aux cours de Bernard Ycart, sur la simulation des variables aléatoires. Il s'inscrit dans un groupe de travail autour de la preuve d'algorithmes probabilistes, comprenant Christine Paulin (LRI-Orsay) et Richard Lassaigne (PPS - P7). Christine Paulin étudie actuellement un moyen d'étendre ce travail au cas des langages fonctionnels.