Une extension probabiliste pour Event-B

Mohamed Amine Aouadhi, Benoit Delahaye, Arnaud Lanoix

Une extension probabiliste pour Event-B *

Mohamed Amine Aouadhi Benoît Delahaye Arnaud Lanoix

Université de Nantes
LS2N UMR CNRS 6004

Dans l'article *"Moving from Event-B to Probabilistic Event-B"* accepté à la conférence internationale *SAC-SVT 2017* [1] nous présentons des travaux autour d'une extension probabiliste à *Event-B*.

Afin de vérifier les systèmes de plus en plus complexes, il est nécessaire d'ajouter aux techniques de modélisation et aux outils de vérification actuels de nouvelles facettes permettant de prendre en compte tous les aspects de ces systèmes. L'une de ces facettes est le *raisonnement probabiliste* qui permet par exemple de modéliser des incertitudes ou de simuler des comportements aléatoires.

Event-B [2] est un langage et une méthode de vérification basée sur des techniques de preuves et principalement dédié à la modélisation de systèmes à événements discrets. [3] suggère que les probabilités devraient être introduites dans Event-B comme un raffinement du *non-déterminisme*. Dans Event-B, le non-déterminisme apparaît à plusieurs endroits : *i)* lors du *choix de l'événement à activer* parmi l'ensemble des événements activables, *ii)* lors du *choix des valeurs* des paramètres des événements et *iii)* lors de la résolution des *affections non-déterministes* de la forme $x :| Q(x,x')$ (forme prédicative) ou $x :\in \{E_1 \ldots E_n\}$ (forme énumérée). À notre connaissance, les travaux existants jusqu'ici [4, 5, 6, 7] ne se sont intéressés qu'au remplacement des affections non-déterministes par des affections probabilistes (quantifiées ou non).

Dans [1], nous proposons une extension probabiliste à Event-B dans laquelle toutes les sources de non-déterminisme sont remplacées par des choix probabilistes : *i)* un *poids* est ajouté à chaque événement afin de pouvoir établir la probabilité d'activation de cet événement, *ii)* le choix des valeurs des paramètres est réalisé à partir d'une distribution *uniforme* et *iii)* nous proposons deux nouvelles *affectations probabilistes quantifiées* afin de remplacer les affections non-déterministes : $x :\oplus Q_x(x,x')$, où le choix des valeurs possibles pour x est résolu à l'aide d'une distribution *uniforme*, et $x := E_1 \ @ \ p_1 \oplus \ldots \oplus E_n \ @ \ p_n$, où chaque valeur E_i est choisie avec une *probabilité* p_i. Nous donnons de nouvelles Obligations de Preuves (OPs) nécessaires pour démontrer la consistence d'un *modèle Event-B probabiliste*. Afin de démontrer la correction de notre proposition, nous montrons que la sémantique

*This work is partially supported by the ANR national research program PACS (ANR-14-CE28-0002).

opérationnelle d'un modèle Event-B probabiliste s'exprime par une chaîne de Markov à temps discrets comportant un nombre potentiellement infini d'états [8]. Finalement, nous étendons [4] afin d'établir les OPs nécessaires afin de montrer la *convergence presque-sûre* d'un ensemble d'événements dans un modèle Event-B probabiliste.

Comme illustré en Fig. 1, nous avons commencé le développement d'un plugin pour *Rodin* [9] permettant la modélisation et la vérification de modèles Event-B probabilistes.

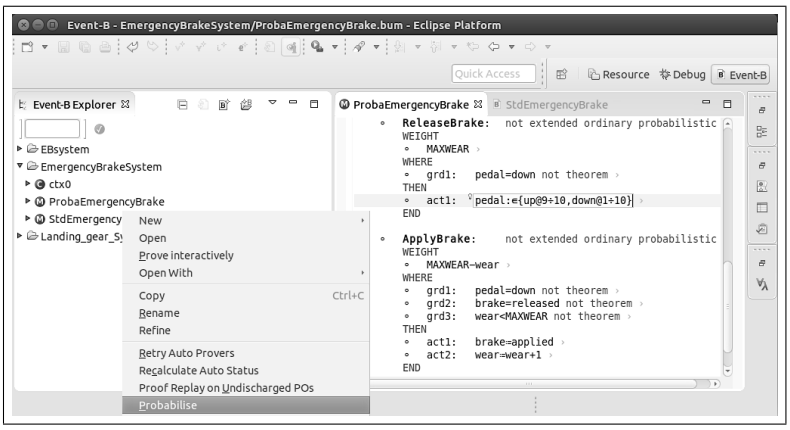

FIGURE 1 – Plugin probabiliste pour *Rodin*

Références

[1] Mohamed Amine Aouadhi, Benoît Delahaye, and Arnaud Lanoix. Moving from event-b to probabilistic event-b. In *Proceedings of the 32th Annual ACM Symposium on Applied Computing (to appear)*. ACM, 2017.

[2] Jean-Raymond Abrial. *Modeling in Event-B : system and software engineering*. Cambridge University Press, 2010.

[3] Carroll Morgan, Thai Son Hoang, and Jean-Raymond Abrial. The challenge of probabilistic event b—extended abstract—. In *ZB 2005 : Formal Specification and Development in Z and B*, pages 162–171. Springer, 2005.

[4] Stefan Hallerstede and Thai Son Hoang. Qualitative probabilistic modelling in event-b. In *Integrated Formal Methods*, pages 293–312. Springer, 2007.

[5] Emre Yilmaz. *Tool support for qualitative reasoning in Event-B*. PhD thesis, Master Thesis ETH Zürich, 2010, 2010.

[6] Anton Tarasyuk, Elena Troubitsyna, and Linas Laibinis. Integrating stochastic reasoning into event-b development. *Formal Aspects of Computing*, 27(1) :53–77, 2015.

[7] Anton Tarasyuk, Elena Troubitsyna, and Linas Laibinis. Towards probabilistic modelling in event-b. In *Integrated Formal Methods*, pages 275–289. Springer, 2010.

[8] Christel Baier, Joost-Pieter Katoen, et al. *Principles of model checking*, volume 26202649. MIT press Cambridge, 2008.

[9] Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, Thai Son Hoang, Farhad Mehta, and Laurent Voisin. Rodin : an open toolset for modelling and reasoning in event-b. *International journal on software tools for technology transfer*, 12(6) :447–466, 2010.