# Exécution symbolique et critères de test avancés ⋆

Sébastien Bardin, Nikolay Kosmatov et François Cheynier

CEA, LIST, Gif-sur-Yvette, F-91191, France
prénom.nom@cea.fr

Nous nous intéressons à la génération automatique de tests à partir du code source d'un programme. L'exécution symbolique dynamique (DSE) est une approche récente et particulièrement prometteuse [3,4]. Cependant, cette technique ne supporte pas nativement la plupart des critères de test classiques [1], comme les conditions multiples ou les mutations.

Notre objectif est de combler le fossé séparant la DSE des critères de test usuels. Nous définissons un nouveau critère, la couverture de labels, qui peut être vu comme un mécanisme de spécification pour décrire d'autres objectifs de tests (par ex. : décisions, conditions multiples, mutations faibles). Nous montrons que ce critère est expressif et peut être intégré efficacement dans la DSE. Ces résultats généralisent des travaux antérieurs [5,6]. Notamment, nous définissons des optimisations spécifiques à la DSE permettant de gérer les labels tout en évitant complètement l'explosion du nombre de chemins du programme, ce qui était la principale limitation des approches existantes. Les résultats expérimentaux montrent que ces optimisations permettent des gains particulièrement significatifs, aboutissant à une intégration des labels dans la DSE pour un surcoût marginal.

Il apparaît donc que les labels ont toutes les qualités requises pour être au centre d'un environnement générique de test automatisé : un mécanisme puissant de spécification de critères de tests, un calcul efficace de la couverture et enfin une intégration à moindre coût dans une des approches de génération automatique de tests les plus récentes.

## Références

1. P. Ammann, A. J. Offutt : Introduction to software testing. Cambridge University Press (2008)
2. S. Bardin, N. Kosmatov, F. Cheynier. : Efficient Leveraging of Symbolic Execution to Advanced Coverage Criteria. In : ICST 2014. IEEE, Los Alamitos (2014)
3. P. Godefroid, N. Klarlund, K. Sen : DART : Directed Automated Random Testing. In : PLDI 2005. ACM, New York (2005)
4. P. Godefroid, M. Y. Levin, D. Molnar : Automated Whitebox Fuzz Testing. In : NDSS 2008.
5. K. Jamrozik, G. Fraser, N. Tillmann, J. de Halleux : Generating Test Suites with Augmented Dynamic Symbolic Execution. In : TAP 2013. Springer, Heidelberg (2013)
6. M. Papadakis, N. Malevris, M. Kallia : Towards Automating the Generation of Mutation Tests. In : AST 2010 (with ICSE 2010).

⋆. Ces résultats ont été présentés à ICST 2014 [2]. Les auteurs ont été partiellement financés par le programme EU-FP7 (projet STANCE, bourse 317753) et l'ANR (projet BINSEC, bourse ANR-12-INSE-0002).