Alt-Ergo Fuzz

Stage 3-6 mois, niveau M1 à M2 Recherche.

Présentation d'OCamlPro :

OCamlPro SAS est une société issue de l'INRIA, créée en avril 2011, pour promouvoir l'utilisation du langage de programmation OCaml dans le milieu industriel. Elle participe activement à des programmes de recherche et de développement visant à améliorer la sûreté et la sécurité des applications informatiques en général. Vous

trouverez plus d'informations sur notre site web: https://www.ocamlpro.com/

Présentation d'Alt-Ergo :

Alt-Ergo est un solveur automatique de formules mathématiques open source conçu pour la vérification des programmes. Il est basé sur la Satisfiabilité Modulo Théories (SMT). Les solveurs de cette famille ont fait des progrès impressionnants et sont devenus très populaires au cours des dix dernières années. Ils sont maintenant utilisés dans divers domaines tels que la conception matérielle, la vérification de logiciels et les tests formels.

Alt-Ergo est très efficace pour prouver les formules générées dans le contexte de la vérification déductive des programmes. Il a été conçu et mis au point à l'origine pour être utilisé sur la plate-forme Why. Aujourd'hui, il est utilisé comme back-end de différents outils et dans différents contextes, notamment via la plateforme Why3. Par exemple, la suite Frama-C s'en sert pour prouver des formules générées à partir de code C, et la boîte à outils SPARK l'utilise pour vérifier des formules produites à partir de programmes Ada.

De plus, Alt-Ergo est utilisé pour prouver des formules issues de modélisations B et de vérification de protocoles cryptographiques. La figure ci-dessous montre les principaux outils qui s'appuient sur Alt-Ergo pour prouver les formules qu'ils génèrent.

Contexte du Stage :

Le fuzzing est une technique utilisée pour effectuer des tests via des jeux de données aléatoires. Dans le cadre du solveur SMT Alt-Ergo, cela se traduit par la génération aléatoire de fichier à prouver respectant une certaine syntaxe. Alt-Ergo utilise principalement deux langages d'entrée, son langage natif basé sur le langage de la plateforme Why ainsi que la syntaxe standardisée de la communauté : smt-lib.
Pour le langage smt-lib2, il existe déjà quelques travaux (smtfuzz et testsmt) de fuzzing sur des outils supportant ce langage comme z3 et cvc4. En revanche, aucun travail n'a été effectué sur le langage natif d'Alt-Ergo, langage qui est utilisé pour communiquer avec Alt-Ergo par divers outils, comme la plateforme Why3.

Sujet détaillé du stage :

Le premier but de ce stage serait de faire un état des lieux des travaux effectués sur le fuzzing des outils supportant le standard smt-lib, ainsi qu'étudier les résultats de tels outils de fuzzing sur Alt-Ergo. Dans un second temps, le but sera de créer un fuzzer pour le langage d'entrée d'Alt-Ergo.