Abstract

Transforming a specification from language into a language supported by a verification tool is a widely adopted way of doing formal verification. It enables the reuse of existing languages and tools.

Model-checker is an approach for formal verification. It is used in the designing phase of a system. In model checking a model is made from an existing design and that model is then used to verify the design. Spin model-checker is such a model verifier. The model that Spin verified is written in Promela.

Nowadays, the cost of program errors is increasing from day to day, so software reliability becomes a critical problem to the whole world. C is a programming language widely used for developing all types of software. Hence, the security of software written in C accounts for important proportion of software reliability.

This thesis will describe a mediate method of model checking C codes to find potential problems using Spin. The translator we developed uses a technique inspired by the technique of translation syntax directed translation techniques for doing the translation from C to Promela. C# was the language we used for programming.

Keywords : Verification, Spin model-checker, Syntax-directed translation, C language, Promela, C#

Résumé

La transformation d'une spécification du langage vers un langage pris en charge par un outil de vérification est un moyen largement adopté en vérification formelle. Il permet la réutilisation des langages et des outils existants.

Le Model-checker est une approche pour la vérification formelle. Il est utilisé dans la phase de conception d'un système. Dans model-checking un modèle est construit à partir d'une conception existante et ce modèle est ensuite utilisé pour vérifier la conception. Spin model-checker est un vérificateur de modèle. Le modèle que Spin vérifié est écrit dans Promela.

Aujourd'hui, le coût des erreurs de programme est en augmentation de jour en jour, ce qui fait que la fiabilité du logiciel devient un problème critique pour le monde entier. C est un langage de programmation largement utilisé pour développer tous types de logiciels. Par conséquent, la sécurité des logiciels écrits en C représente la proportion importante de la fiabilité des logiciels.

Ce mémoire décrit une méthode médiate de model checking codes C pour trouver les problèmes potentiels à l'aide de Spin. Le traducteur que nous avons développé utilise une technique inspiré par la technique de traduction dirigée par la syntaxe pour faire la traduction de C à Promela. C # a été le langage utilisé pour l'implémentation.

Mots-clés : Vérification, Model-checker Spin, Translation dirigée par la syntaxe, Langage C, Promela, C#

ملخص

التحويل من لغة إلى لغة أخرى معتمدة من قبل وسيلة للتحقق هو نهج أعتمد على نطاق واسع للقيام بالتحقق الشكلي، يسمح بإعادة استعمال اللغات حوالأدوات الموجودة.

نموذج التحقق هو نهج للتحقق الشكلي. يمكن استخدامه في مرحلة تصميم نظام، في نموذج التحقق يبمى النموذج من خلال تصميم منجز، حيث يستعمل هذا النوذج للتحقق. نموذج (C) هو محقق يعمل على النماذج التي مكتوبة في لغة (Promla).

في الوقت الحاضرتكلفة أخطاء البرمجيات تتزايد من يوم إلى آخر، لذلك موثوقية البرمجيات اصبحت مسألة حساسسة بالنسبة للعالم، C هي لغة برمجة مستعملة على نطاق واسع لتطوير جميع أنواع البرمجيات، وبالتالي فإن أمن البرمجيات المكتوبة بلغة C تمثل نسبة كبيرة من موثوقية البرمجيات.

في هذه المذكرة نصف طريقة لنموذج التحقق لفحص نموذج برنامج C من جل الكشف على المشاكل الكامنة بالاستعانة بأداة التحقق من النماذج SPIN.

المترجم الذي قمنا بإنجازه يستعمل طريقة مستوحاة من تقنية الترجمة الموجهة بالنحو بهدف الترجمة من C إلى Promla . #C هو اللغة المستعملة في تطوير البرنامج.

كلمات مفتاحية: أدة التحقق من النماذج SPIN، الترجمة الموجهة بالنحو، لغة C، Promla،#C