Ecole Doctorale STIC
Sciences & Technologies de l'Information et de la Communication

ED STIC - Proposition de Sujets de Thèse

pour la campagne d'Allocation de thèses 2011

Titre du sujet :	Résolution de contraintes numériques sur les vecteurs de bits pour la vérification de logiciels
Mention de thèse :	Informatique
HDR Directeur de thèse inscrit à l'ED STIC :	Rueher Michel

Co-encadrant de thèse éventuel :

Nom :	Bardin
Prénom :	Sébastien
Email :	sebastien.bardin@cea.fr
Téléphone :	0686808722

Email de contact pour ce sujet :	michel.rueher@gmail.com
Laboratoire d'accueil :	I3S

Description du sujet :

Le Laboratoire de Sûreté Logicielle (LSL) du CEA-LIST développe trois outils de génération automatique de
tests : GaTEL pour le code Scade, PathCrawler pour le code C et OSMOSE pour certains codes binaires.
Ces trois outils partagent un même moteur de résolution basé sur la Programmation par Contraintes (CP) [1] :
COLIBRI.
Les techniques usuelles de résolution considèrent une sémantique idéalisée des valeurs manipulées par un
programme, typiquement sous forme d'entiers. Cependant, raisonner directement sur des mots machine
donnerait la possibilité de traiter des mécanismes jusque là très mal pris en comptes

(débordements,
opérations bit à bit, etc.), ce qui permettrait d'une part d'améliorer la précision des analyses existantes, et
d'autre part de cibler de nouveaux champs d'applications, par exemple des analyses de sécurité du code ou
la vérification de composants sur étagère.
La théorie des vecteurs de bits (BV) [6] permet de modéliser finement les contraintes apparaissant dans
l'exécution d'un programme bas niveau. L'approche standard de résolution, dite bit-blasting, consiste à
transformer le problème initial en une formule booléenne équivalente puis à utiliser un SAT solveur.
L'avantage est de se reposer complètement sur la puissance des SAT solveurs actuels. L'inconvénient
majeur est que cette approche gère assez mal les opérations arithmétiques. A l'inverse, le cadre CP(BV)
développé récemment au LSL [3] consiste à transformer un problème BV en un problème d'arithmétique
bornée équivalent, puis à le résoudre par des techniques de programmation par contraintes (CP) dédiées.
Une telle approche devrait permettre en principe d'éviter les inconvénients du
bit-blasting, et nous espérons pouvoir concurrencer l'approche standard sur les problèmes d'arithmétique de
vecteurs de bits.
Cette thèse a pour ambition d'étudier l'apport des techniques de Programmation par Contraintes dans la
résolution des formules BV typiquement rencontrées en vérification de programmes. En s'appuyant d'une part
sur les avancées réalisées sur BV dans la communauté SMT (Satisfiability Modulo Theory) [4,5] et d'autre
part sur le travail préliminaire mené au CEA sur CP(BV) [3], l'étudiant pourra développer une approche
originale de résolution de BV, l'implanter et l'évaluer expérimentalement. Le défi principal sera de réussir à
dépasser les approches actuelles sur certaines classes de formules utiles à la vérification.
L'étudiant devra se concentrer sur les points mal gérés par le bit-blasting et importants pour la vérification de
programmes, par exemple l'arithmétique de vecteurs de bits ou les opérations sur les flottants. Un point de
départ intéressant pourra être d'identifier dans la littérature des fragments de BV solubles efficacement, et de
s'en inspirer pour ajouter des mécanismes de raisonnement global dans CP(BV).
Les retombées à attendre de cette thèse pour le LSL sont de deux ordres. D'une part, comme ces travaux

visent à étendre les capacités de COLIBRI, ils bénéficieront directement aux trois outils de génération de
tests du laboratoire, soit en améliorant directement leurs performances (OSMOSE), soit en élargissant leurs
champs d'application (GaTEL et PathCrawler). D'autre part, le LSL peut aussi espérer un impact académique
international de premier plan : la résolution de contraintes bas-niveau est l'un des sujets chauds du moment
en vérification automatique, l'approche envisagée est très originale et des résultats prometteurs ont déjà été
obtenus par le LSL, donnant lieu à une publication au meilleur niveau international [3].

Références :

[1] K. R. Apt. Principles of Constraint Programming. Cambridge University Press (2003)
[2] S. Bardin and P. Herrmann. Structural testing of executables. In: ICST 2008. IEEE (2008)
[3] S. Bardin, P. Herrmann and F. Perroud. An Alternative to SAT-based Approaches for Bit-Vectors. In:
TACAS 2010. Springer (2010)
[4] R. Bruttomesso and N. Sharygina. A scalable decision procedure for fixed-width bit-vectors. In: ICCAD
2009. ACM (2009)
[5] D. Cyrluk, O. Moller and H. Ruess. An efficient decision procedure for the theory of fixed-size bit-vectors.
In: CAV 1997. Springer (1997)
[6] D. Kroening and O. Strichman. Decision Procedures: An Algorithmic Point of View. Springer (2008)

URL : http://www.essi.fr/~rueher/PhD/SujetThese-bv-clp.pdf

English version: