1 Publishable Summary

1.1 Summary description

A serious limitation for most model-checking techniques to verify infinite-state systems rests on the fact that they are mainly interested on the control and less on the data values stored by local or global program variables. Nowadays, verification techniques dedicated to systems heavily manipulating data are not so well represented within the research community dealing with model-checking techniques.

The project DATAVERIF aims at developing verification techniques for systems heavily manipulating data in order to ensure the satisfaction of properties that are essentially related to data. This is an important topic since we need formal methods to guarantee the correctness of computer systems. To do so, the project advocates the use of SMT solvers, such as CVC4 developed at New York University, in the design of verification techniques and algorithms. The project includes questions about the relevancy of logics to specify properties on resources (data, memory, etc.) and about the design of associated verification methods (symbolic methods, automata).

Project No 301166 **Project Acronym** DataVerif

Project Full Name Temporal Reasoning with Data for Verification

Period covered August 1st, 2012 to July 31st, 2015

Start date of project August 1st, 2012

Research Fellow S. Demri `demri@lsv.ens-cachan.fr`

Scientist in charge (NYU) C. Barrett `barrett@cs.nyu.edu`

Scientist in charge (CNRS) L. Fribourg `fribourg@lsv.ens-cachan.fr`

1.2 Description of the work performed since august 2012

- We studied model-checking problems for multi-pushdown systems based on LTL-like dialects, naturally allowing to express liveness properties, when some bounds are fixed.
- We studied fragments of separation logic known to be an assertion language for the verification of program with pointers. We characterized the complexity, decidability status and expressive power of several fragments. For one interesting fragment, we provided an algorithm that could be used in the SMT solver CVC4.
- We studied the complexity of model-checking problems for flat counter systems for several specification languages. A prototype implementation using CVC4 has been done by supervised PhD student Amit Kumar Dhar. Research fellow has also implemented a prototype to enumerate path schemas and to eliminate redundant ones in (arbitrary) counter systems by using CVC4 solver for queries about linear arithmetic.

- Numerous invited talks given by research fellow related to DATAVERIF, including one at FROCOS'13 and TABLEAUX'13 (Nancy), and another one at AIML'14 (Groningen).
- The research fellow has served as program committee co-chair for the international conference IJCAR 2014 at VSL'14.
- About nine research articles produced during the period, most of them already published in top-ranked venues.

1.3 Main results so far

- Considering the verification of multi-pushdown systems, we have studied a LTL-like specification language based on CaReT. Under this logic, we show model-checking problem of MPDS restricted to k-context bounded runs is in EXPTIME, when k is encoded in unary.
- Main results about separation logic are the following: separation logic 1SL1 (one record field, one variable) has a PSPACE-complete satisfiability problem and separation logic 1SL2 (one record field, two variables) is as expressive as weak second-order logic (even if we drop out separation conjunction).
- Main results about model-checking flat counter systems are the following: model-checking linear mu-calculus formulae [resp. FO formulae] over flat counter systems is PSPACE-complete and model-checking CTL* formulae over flat counter systems is polynomially equivalent to satisfiability in Presburger arithmetic.
- Supervised PhD student Amit Kumar Dhar has implemented a prototype about the algorithms designed for flat counter systems. Research fellow has implemented a prototype about path schema enumeration in (arbitrary) counter systems using the SMT solver CVC4 developped at NYU.

1.4 Expected final results

- Publications of research articles about formal verification and SMT solvers and delivery of talks in conferences and seminars. Proposal of master internships dealing with verification and SMT techniques.
- Implementation of two prototypes using the SMT solver CVC4, one to verify counter systems and another one to decide formulae from fragments of separation logic.
- Design of course proposals dealing with infinite-state systems, verification of data properties and theories decided by SMT solvers. Research fellow and Morgan Deters (New York University) will give a course at the summer school ESSLLI'15, Barcelona, August 2015.