

# **VERA: VERification Approchée**

## **Report on April 30th 2005**

Michel de Rougemont, LRI

This research project studies various notions of approximation in the context of formal verification. Given a program, a system, a protocol, it is often a hard problem to prove that it satisfies a specification. We propose an approach where we can efficiently prove that it approximately satisfies a specification.

We introduce the notion of approximate verification, based on the theoretical notion of property testing, generalized to trees and to Model-Checking. We also study the verification of probabilistic processes.

### **Topics**

- Testers and Correctors on Trees
- Approximate Model-Checking
- Games and Protocols

The two first topics were covered in the the two first years and the last topic is kept for the last year.

### **Members of the project**

- Algorithms et Complexity, LRI, Paris XI
- Logic group, Paris VII

Additional members who joined the original group:

- M.C. Gaudel, Software Engineering LRI
- Thomas Héroult, Parallelism, LRI

Visitors:

- Eldar Fisher, Technion, Israel
- Pankaj Singh, IIT Kanpur, India

### **Software developments**

- [APMC: Approximate Probabilistic Model Checking](#) (Logic, Paris VII)
- [XML corrector](#) (Algorithms and Complexity, LRI, Paris XI)

# 1. Testers and Correctors on trees

The main subjects are:

- Testers for regular trees
- Correction of XML data
- Approximate equivalence of automata

## Publications

- F. Magniez, M. de Rougemont [Property testing for regular tree languages \(ICALP 2004\) \(.pdf\)](#)
- U. Boobna, M. de Rougemont [Correctors for XML data \(XSym 2004\) \(.pdf\)](#)
- E. Fischer, F. Magniez, M. de Rougemont [Property and Equivalence Testing on strings\(ECCC\) \(.pdf\)](#)
- K. Friedl, G. Ivanyos, M. Santha, Efficient Testing of groups (STOC 2005)

## Software development

- XML tree corrector : this software was developed by Pankaj Singh (Master student from India, Kanpur). Given an invalid XML file, it finds a close valid file, if the distance is less than  $\epsilon$ . The software is accessible on:

<http://www.lri.fr/~mdr/xml/>

# 2. Approximate Model Checking

The main subjects are:

- **Probabilistic abstraction .**

Given a program and a property to check, which admits some tester, we study how to find, in a general way, some probabilistic abstraction, defined in [LLMPR]. Such an abstraction is a program transformation allowing to abstract certain variables with respect to the tester. Then we can apply the test to concrete programs and approximatively check a property in constant time.

- **Probabilistic Model Checking.**

Model Checking has been recently extended to probabilistic protocols, which can be represented by probabilistic transition systems (Markov chains). The objective is to compute the satisfaction probability of some temporal property as reachability, liveness or safety. The main problem is the space complexity of these methods. A natural issue is to approximate this probability. Although the problem is not approximable in full generality, there exist some randomized approximation schemes in polynomial time for certain classes of properties [LP]. We apply some sampling techniques, as Monte-Carlo method, to probabilistic protocols in order to generate randomized execution paths and approximatively verify these quantitative properties.

## Publications

- T. Herault, R. Lassaigne, F. Magniette, and S. Peyronnet: Approximate Probabilistic Model Checking Proc. of the 5th Conf. on Verification, Model Checking and Abstract Interpretation (VMCAI 2004) Lecture Notes in Computer Science n° 2937, p.73-84.
- M. Duflot, L. Fribourg, T. Herault, R. Lassaigne, F. Magniette, Stephane Messika, S. Peyronnet and C. Picaronny Proc. of the 4th Int. Workshop on Automated Verification of Critical Systems (AVoCS 2004) Electronic Notes in Theoretical Computer Science 2004.
- F. Afrati, H. Leiss, M. de Rougemont [Definability and compression, LICS 2000 et Fundamenta Informaticae 2003](#).
- S. Laplante, R. Lassaigne, F. Magniez, S. Peyronnet, M. de Rougemont [Probabilistic abstraction for model-checking, LICS 2002](#).
- H. Leiss, M. de Rougemont [Automata on Lempel-Ziv structures \(.pdf\)](#), or [\(.ps\)](#), [CSL 2003](#)

### 3. Future developments

A very fruitful collaboration was started with Eldar Fischer (Technion), leading to a polynomial time algorithm to decide approximate equivalence of two regular expressions. We hope to push this approach to Model Checking in the context of distributed computing, considered as games with N players.