ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Lăcrămioara Aștefănoaei
Visited Location : Pop Art, INRIA, Grenoble
Duration of Visit: 03.01.2011 – 31.12.2011
Scientific coordinator: Pascal Fradet, Gregor Gössler

I - Scientific activity

At INRIA, in the team Pop Art, I worked on the following topics:

- **Analysis of Logical Causality.** Together with Gregor Gössler, we worked on extending and implementing some definitions for the analysis of logical causality with the scope to find violations of specifications in component-based systems. Causality is an important topic as it allows one not only to explain what went wrong but also who is to blame. The applications are numerous: from software integration to liability issues needed in courts. Gregor Gössler introduced me to this interesting problem and his innovative approach to analyse causality. In this approach components are black boxes, we are given only their specifications and their observed behaviour recorded in log files. From these and from a global specification of the whole system we are able, in the case of a global failure, to point to a group of components whose behaviours led to the failure. The proposed definitions allow a fine-grained analysis of causality. Furthermore, they are generic enough to be applied to different modelling frameworks: either working with components specified as transition systems, or as timed automata, for instance, the definitions apply just as well. This strong point we also exploited in LoCA (*Lo*gical *C*ausality *A*nalysis), a tool we have implemented in Scala, a programming language that combines object oriented and functional features. Our choice of implementation language brings mainly two advantages: portability (Scala compiles to Java code) and succinctness together with an elegant mapping of the definitions. We have illustrated the suitability of the causality definitions in two specific frameworks for the design of components: finite transition systems interacting by synchronising some of their actions and respectively timed systems. For the latter, our tool integrates with the UPPAAL model-checking tool. LoCA make it possible for a user to experiment with the causality definitions: he or she must provide the specifications of the components, a global specification of the whole system and a log file recording the behaviours which are analysed. During the implementation, we confronted with quite a number of "small" research problems which turned out to be interesting on their own. These results we plan to put together and materialise in a future publication.

- **Total correctness of Structured Gamma Schedulers.** Together with Pascal Fradet, I tried to work on the definition of a weakest precondition calculus for Structured Gamma schedulers. This subject is part of a greater research theme which involves the study of correctness of concrete programs written in Structured Gamma with respect to abstract Gamma specifications. The abstractions specify the functionality as high-level Gamma reactions. An usual approach to obtain efficient programs which preserve the functionality of the abstractions is by means of refinement. The refinement concerns two orthogonal directions. On the one hand, the data involved in the reaction is refined by specifying a

more precise data type (for instance, a "bag" of elements may be refined into a list). On the other hand, the inherent nondeterminism in the application of the reactions in the specifications is reduced (control refinement) by implementing specific schedulers which make use of selection functions. With respect to correctness, a weakest precondition calculus would allow us to prove that the refined program terminates in a stable state. Because of possible recursive schedulers and because of the genericity of the reactions, the definition of a weakest precondition calculus turns to be slightly more tricky. This makes the problem (which in fact also resembles one of the subjects I touched upon in my Ph.D thesis) even more interesting, however, mostly because of time, my effort did not lead to any valuable results. I would, nevertheless, further work on this topic if the occasion appears.

II- Publication(s) during your fellowship

[ASDL2012] Gregor Gössler, Daniel Le Métayer, Eduardo Mazza, Marie-Laure Potet and Lăcrămioara Aştefănoaei: "Apport des méthodes formelles pour l'exploitation de logs informatiques dans un contexte contractuel"

Abstract. Dans cet article, nous presentons la démarche adoptée dans le projet LISE pour spécifier de maniere formelle les responsabilitès des parties dans un contrat portant sur des logiciels. Nous décrivons deux options, l'une reposant sur une attribution a priori des responsabilités en fonction des dysfonctionnements constatés dans les logs, l'autre sur une analyse de causalité, et nous les illustrons sur un exemple de système de reservation d'hôtels.

III -Attended Seminars, Workshops, and Conferences

- *Pop Art seminar, biweekly seminars organised by Alain Girault*
  ** talk on 13.01.2011: "An executable Theory of Multi-Agent Systems Refinement"*

- *"Seminaire au Vert", organised by Pascal Fradet, 27.11.2011, Chamonix, France*
  ** talk on 28.11.2011: "Loca: A Prototype for the Verification of Logical Casuality"*