FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, edificio norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

SEMINARIO

CENTRO DE MODELAMIENTO MATEMATICO

EXPOSITOR

MARTIN BODIN

Postdoctorado CMM

TITULO

INTRODUCTION TO FORMAL VERIFICATION

ABSTRACT:

Software is pervasive. In particular, a lot of programs are nowadays produced to be executed in safety critical contexts. It is crucial to certify these programs. There are several methods of certification. By far the most used is testing. But testing can be costly, and more importantly, it only covers a finite number of cases. Formal verification is a vastly different approach: it aims at building a mathematical proof that the program meets its specification, thus covering all possible cases. To increase the level of certification, this proof can even be computer-checked by a proof assistant, such as Coq.

In the last years, several projects formally verifying real-world programs got mature. One of the most impressive is the CompCert project, which consists in an optimising compiler for the C language. This compiler has been proved correct in Coq, providing it the highest certification level a program can have. This project involved a large amount of effort, as all the compiler behaviours were specified and proven by hand. Mosts programs do not need such a high guarantee: the certification can focus on simpler and more generic properties, such as the absence of runtime error (division by zero, pointer exception, etc.). These other properties can be certified by analysers which can run through large amount of code, leaving only the analyser to be certified by hand. Such an approach has proven to be very helpful for software development, as illustrated by the usage of the Infer analyser in Facebook. I personally believe that the field is only starting to attack the certification of real-world projects, and that new methods of certification for industrial projects will appear in the next years.

This presentation aims at giving some bases on how formal verification works, at showing what the proof certificates of Coq can look like, as well as explaining the different techniques to certify different programs and properties.

Martes 23 de mayo a las 16:30 hrs, Sala de Seminario John Von Neumann CMM, séptimo piso de Beauchef 851 Torre Norte.

CONICYT
Ministerio de Educación

cnrs