中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

Distinguished Lecture Series

New Frontiers in Formal Software Verification

Monday, April 9th, 2012 10:00am
Auditorium 106 at New IIS Building

Gerard Holzmann

Faculty Associate in Computer Science at
California Institute of Technology
Fellow at NASA/JPL

Abstract

Producing a convincing proof of correctness of any non-trivial piece of software is known to be time consuming and in itself error-prone. The most general proofs can be constructed with the help of theorem provers, but such proofs often take months of intensely focused work. Logic model checkers originally required the manual construction of faithful models of a software application, which similarly can be time-consuming and error-prone. About 12 years ago, though, this changed fundamentally when we learned to mechanically extract logic models from implementation level code, e.g., written in the widely used C programming language.

We first demonstrated this in the formal verification of the call processing code (written in C), developed at Lucent Technologies in the US for a new commercial telephone switch In this talk I will show how much progress has been made in the last ten years to reduce the time required by model checkers to perform correctness checks from hours to seconds. We will also discuss how this change is redefining what the frontiers are in formal software verification.

For more infomation: http://www.iis.sinica.edu.tw/