Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Region Logic for Local Reasoning about Global Invariants

Prof. Anindya Banerjee

Research Professor
Fundación IMDEA Software

Aula 6 • 18 de febrero de 2010 • 16: 00
entrada libre hasta completar el aforo

resumen:

Shared mutable objects pose challenges in reasoning, especially for data abstraction and modularity. We present a novel logic for error-avoiding partial correctness of programs featuring shared mutable objects. Using a first order assertion language, the logic provides heap-local reasoning about mutation and separation, via ghost fields and variables of type region (finite sets of object references). A new form of modifies clause specifies write, read, and allocation effects using region expressions; this supports a frame rule that allows a command to read state on which the framed predicate depends. We show the logic in use in proving the correctness of design patterns such as the composite pattern, the verification of which has been proposed as a challenge problem for specification and verification of sequential object-based programs.

sobre Anindya Banerjee:

Anindya Banerjee is Research Professor at the Madrid Institute of Advanced Studies in Software Technologies (IMDEA-SW), Madrid. His research interests are in language-based computer security, program analysis and verification, type systems and concurrency. He is a recipient of the Career Award from the United States National Science Foundation.

Immediately prior to his current position, Anindya was full professor of Computing and Information Sciences at Kansas State University. In 2007—2008 he spent a sabbatical year in the Programming Languages and Methodology group at Microsoft Research, Redmond and spent Summer 2007 as Academic Visitor in the Advanced Programming Tools group at IBM TJ Watson Research Center.