Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Automatic Abstraction for Congruences

Prof. Andy King

School of Computing, University of Kent, Canterbury, Kent, UK

Sala de Grados • 7 de noviembre de 2011 • 16:00
entrada libre hasta completar el aforo

resumen:

One approach to verifying bit-twiddling algorithms is to derive invariants between the bits that constitute the variables of a program. Such invariants can often be described with systems of linear congruences where the modulo is a power of two. The classic technique for discovering invariants is to, first, find the transfer functions that simulate the statements of the program and then, second, repeatedly apply these transfer functions to compute a fixpoint which yields the invariants. Because of the low-level nature of these invariants and the large number of bits that are involved, it is important that the transfer functions can be derived automatically; it is too much to do my hand. We show how this is possible using repeated SAT solving, and thus provide a way of mechanically deriving bit-level invariants.

sobre Andy King:

Andy King is a Reader in computer science at the University of Kent in Canterbury, UK. He majored in mathematics and computer science at the University of Bath before going to study for a PhD in theoretical computer science at the University of Southampton.

He is currently the head of the Programming Languages and Systems (PLaS) research group in the school of computing, though he also holds a Royal Society Industrial Fellowship under which he is seconded, part-time, to a computer security firm in London where he is researching into reverse engineering. He has written approximately 70 peer-reviewed academic papers.