UNIVERSIDAD
COMPLUTENSE
MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA
POSGRADO

Safety in AI Systems: SMT-Based Verification of Deep Neural Networks

Guy Katz

Hebrew University of Jerusalem

Facultad de Informática

Sala de Grados – Miércoles 24 de abril de 2024 - 11:00

Entrada libre hasta completar el aforo

Resumen:

Deep neural networks have emerged as a widely used and effective means for tackling complex, real-world problems. However, a major obstacle in applying them to safety-critical systems is the great difficulty in providing formal guarantees about their behavior. In this talk we will discuss how SMT solving can be used to prove various safety properties of neural networks, and to measure their robustness to various kinds of attacks. We will also demonstrate how abstraction/refinement techniques can be used to render neural network verificaiton more scalable. Finally, we will discuss some of the real-world applications of this technology, in the aerospace domain.

Sobre Guy Katz:

Guy Katz is an associate professor at the Hebrew University of Jerusalem, Israel. He received his Ph.D. at the Weizmann Institute of Science in 2015. His research interests lie at the intersection between Formal Methods and Software Engineering, and in particular in the application of formal methods to software systems with components generated via machine learning.

His research is currently supported by grants from the European Research Council (ERC Starting Grant), the Israeli Science Foundation (ISF), the US-Israel Binational Science Foundation (BSF), the Israel Innovation Authority, and Airbus.

Further information and publications at: https://www.katz-lab.com/