The Quest for Correctness-Beyond *a Posteriori* Verification

Joseph Sifakis

Verimag Laboratory

Abstract. In this presentation, I discuss the main achievements in the area of formal verification, in particular regarding their impact thus far on the development of Computer Science as a discipline and on future research directions.

The presentation starts with a short overview of formal verification techniques and their main characteristics, followed by an analysis of their current status with respect to: 1) requirements specification; 2) faithfulness of modeling; 3) scalability of verification methods. Compositional modeling and verification is the main challenge to tackling complexity. System verification should be tightly integrated into the design process, making use of knowledge about the system's structure and its properties.

I identify two complementary research directions for overcoming some of the current difficulties in compositional techniques: 1) Moving away from low-level automata-based composition to component-based composition, by developing frameworks encompassing heterogeneous components; 2) Using such frameworks to study compositionality techniques for particular architectures and/or specific properties.

I illustrate these ideas through the BIP (Behavior, Interaction, Priority) component framework which encompasses high-level composition of heterogeneous components.

BIP supports a design methodology for building systems in a three-dimensional design space by using property-preserving transformations. This allows efficient compositional verification techniques for proving invariants, and deadlock-freedom in particular.