A. M. Turing Award Lecture:

Verification Engineering: A Future Profession

Amir Pnueli

Weizmann Institute of Science

It is time that formal verification (of both software and hardware systems) be demoted from an art practiced by the enlightened few to an activity routinely and mundanely performed by a cadre of Verification Engineers (a new profession), as a standard part of the system development process.

In the talk, we will assess how far we are from the realization of this obvious necessity in terms of:

1. The current state of the art of existing verification approaches and tools of the two prevalent kinds: Model Checking and Deductive Verification. The power, accessibility, friendliness, ease of use and operation of existing tools, and the size of systems they can verify. The qualification and sophistication required of a potential user.

2. The degree of acceptability and future expectations of formal verification within different industrial sectors.

3. The educational background and a proposed curriculum for the new discipline of Verification Engineering.

4. Integration of formal verification with other commonly practiced methods of validation such as testing and simulation.

5. The main obstacles standing in the way: the needs for user interaction. We will analyze the various places where user creativity is called for, such as in the design of powerful abstractions, reduction by symmetry and similarity, and the construction of auxiliary invariants and progress measures. It will be shown that, for particular classes of applications, it is possible to identify verification patterns and application-specific heuristics that can significantly reduce the amount of fresh intellectual effort needed for the consideration of each new instance of a system in this class.

Re-usability of verification modules should go hand in hand with re-usability of system modules.