Commercial Verification

Robert P. Kurshan
AT&T Bell Labs
Murray Hills
New Jersey, USA
k@research.bell-labs.com

Abstract

Recently, increasing complexity of hardware designs and theoretical breakthroughs in algorithmic verification have provided the opportunity for formal verification to emerge from academia to commerce. Suddenly, there are at least four serious design tools based upon the theory of formal verification, available in the commercial market, with more on the way. I will discuss the basis and future of this new trend.

Algorithmic model-checking of finite-state programs had its "coming out" in 1990, with the establishment of the annual COMPUTER-AIDED VERIFICATION conference. However, the field this conference represents has a longer history, founded on automata theory and logic, with roots in the works of Pnueli, Clarke, Emerson and others.

The benefits of finite-state verification are easy to state and understand: control-intensive programs and hardware may be designed, developed, tested and validated

- significantly FASTER,
- more RELIABLY

than previously possible. Why faster? Because errors may be eliminated earlier in the design cycle, than otherwise possible, reducing the need for more time-consuming re-design, retro-fit and regression testing at later points in the design cycle. Why more reliably? Because, unlike conventional simulation test with its well-known problem of inadequate coverage, verification constitutes, in effect, the result of simulating every possible behavior. Unlike automated theorem-proving, which is user-intensive and logically undecidable, the techniques which have come to be known as "[finite-state] model-checking" are algorithmic, and may be run with very little user interaction or training.

The basic formulation of a model-checking problem involves a (finite-state) PROGRAM P and a list of properties or TASKS T that P is intended to perform. The domain of T may be automata, ω-automata, tree-automata or a variety of temporal logics. At the heart of the model-checking problem is its computational complexity, which is intractable as a function of the number of components or variables in P. Much of the recent work (which has allowed model-checking nonetheless to be feasible for many practical problems), is centered on heuristics which can overcome this intractability in many cases. A recent reference on this subject is:

> R. Kurshan, *Computer-Aided Verification of Coordinating Processes*, Princeton Univ. Press (1994). ISBN: 0–691–03436–2

With the advent of recent theoretical breakthroughs and faster computers, the field has emerged from academia to industry, with the recent release of a number of commercial products. As with many new products, there has been a certain initial reluctance to embrace these very broadly. Part of that reluctance is a prudent skepticism during the initial shake-out. Another part may be driven by ignorance and suspicion of something new. However, this natural reluctance is starting to give way, under the weight of the necessity to deal with the staggeringly complex concurrent systems currently being designed into contemporary hardware and software.

For the designers of control-intensive hardware and software in a "critical path", be it performance-critical, safety-critical, security-critical or commercially-critical, the cost of failure outweighs — many times over — the (fairly small) cost of trying some of the new tools and techniques on a pilot project. The reports of success from those who have, are beginning to have a cascade effect on the applications of this (still very new) technology.

Biography

Robert P. Kurshan is a distinguished member of the technical staff at Bell Laboratories, Murray Hill, N.J., USA. He got a Ph.D. in Mathematics in 1968 from University of Washington. From 1969 till present he is with Mathematics and Computer Science Research Centers, Bell Labs. From 1975 till 1976 he held the Krantzburg Chair for Visiting Scientists, Dept. of Mathematics, Technion, Israel. From 1984 till 1985 he was a visiting professor at the Dept. of Electrical Engineering, Technion, Israel.

His areas of research are ring theory, analytical number theory, coding theory, digital signal processing, approximation theory, formal verification. He is author of a book titled *Computer-aided Verificaion of Coordinating Processes*, published by Princeton University Press in 1994. He created the COSPAN verification system in 1985, which recently has been productized as the commercial hardware verification system FormalCheck.