Abstract

Advancements in VLSI technology have enabled on-chip realisation of complete digital circuits. This has necessitated early detection of design errors to save production cost. Inadequacy of simulation as a tool for an exhaustive checking of a hardware system for fault-free operation has emphasised the need for improving the mechanism of verification for such a system. The present thesis dwells on application of inductive reasoning to some areas of hardware verification. A goal reduction oriented theorem proving approach has been adopted to solve the problem of verification of a hardware system. The work embodied in this thesis is based on HOL, the version of higher order logic developed at Cambridge University. Encoding the implementation, the initial condition (for sequential circuits) and the specification of a system by well formed formulae Imp, II and $Spec$ respectively, the principal task of verification is to prove the validity of the correctness theorem $Imp \wedge II \supset Spec$.

With a view to making the proof of correctness theorems of various forms of digital systems simple, elegant and applicable to generic designs, the present work has sought to explore the scope for inductive reasoning, wherever possible. In the process, the following results have emerged.

- Simple induction has been identified for the fsm problems where the interval of concern is parameterised by a single natural number variable. In the goal reduction paradigm, an inductive property is conjectured on obtaining recurrence of two structurally similar goals. Achieving the proof of such a property results in substantial simplification of the reasoning required to realise the proof of the correctness theorem of a generic implementation structure. Multiple induction is attempted for problems whose interval of interest involves consecutive subintervals and the input specification is parameterised by more than one natural number variables, one variable corresponding to each subinterval.

- The importance of various design constraints in restricting the search space in verification of complex digital systems has been investigated. The present work has also addressed the verification of large systems composed of separate data and control paths. The proof method has been enhanced to capture the transformation occurring in data states hand in hand with recurrence of a controller state. Case studies involving real life hardware systems have been performed to demonstrate the effectiveness of the proof algorithms.

- The work described in the present thesis has also gone on to apply inductive reasoning for verifying iterative circuits, both combinational and sequential. Forward as well as backward reasoning has been used to verify combinational iterative circuits. Inductive reasoning along two dimensions, namely space and time, has been applied for verification of iterative sequential circuits.