Boolean and 2-adic Numbers Based Techniques for Verifying Synchronous Designs

Gerard Berry
Centre de Mathematiques Appliquees (CMA)
Ecole des Mines de Paris
2004, Route des Lucioles
06902 Sophia-Antipolis, France

We present two distinct techniques to verify synchronous designs. The first technique applies to controllers written in Esterel or similar imperative languages. The problem is to efficiently compute the reachable state space (RSS) of large FSMs. We use structural information extracted from the program to cheaply compute an over-approximation of the RSS. This over-approximation can be used to simplify the logic and to remove registers, which makes the exact RSS computation much easier. We present other crucial optimizations implemented in the TiGeR BDD package we use for Esterel verification. The second technique is the usage of 2-adic number theory for verification of sequential arithmetic circuits, introduced by Jean Vuillemin. Infinite bitstreams are seen as numbers written low-order bits first. This makes it possible to consider the sequential transfer function of a circuit as a standard numerical function and to make sequential circuit correctness proofs by straight numerical calculations. Finally, we suggest to explore more deeply the relation between Boolean and number-based techniques.