Boolean Gröbner Basis based Verification Using the Unate Cube Set Algebra and an Implicit Data Structure

Abstract

In recent years, hardware verification using computer algebra and Gröbner basis based reduction has been applied to Galois field and integer arithmetic circuits. The basic idea behind these methods is modelling the circuit as polynomials and then using Gröbner basis based reduction to perform equivalence checking, membership testing or abstraction. However, the efficiency of these techniques is limited by the explicit data structures and technology-mapping library specific heuristics. By representing Boolean polynomials as characteristic sets using an implicit data structure like ZBDDs, we show how: i) monomial orderings based on the circuit's topology can be imposed on ZBDDs; ii) GB reduction can be significantly improved with ZBDDs by canceling multiple monomials in one-step of division; iii) the sparsity inherent in the formulated problem can be exploited to overcome the term explosion problem; and iv) the heuristics used for increasing the efficiency of the process can be implemented on the ZBDDs. Experiments performed over various "bit-blasted" arithmetic circuits demonstrate the scalability of our approach (some specific set of benchmarks can be listed here).