RESOLVING UNKNOWN COMPONENTS IN ARITHMETIC CIRCUITS USING COMPUTER ALGEBRA METHODS

Vikas Rao[1], Utkarsh Gupta[1], Irina Ilioaea[2], Priyank Kalla[1], and Florian Enescu[2]
[1]Electrical & Computer Engineering, University of Utah
[2]Mathematics & Statistics, Georgia State University

***Abstract*—Automatic correction of unknown components in a given circuit is a resource intensive process. Recent developments in realizing the functionality implemented by these unknown gates rely on incremental SAT solving. Despite using state-of-the-art SAT solvers, these approaches fail to verify multipliers beyond 12-bits and hence are infeasible in a practical setting. The current formal datapath verification methods which utilize symbolic computer algebra concepts, rely heavily on textbook structure of the circuits to realize an unknown component, and hence are not scalable. These approaches model circuit as a set of polynomials over integer rings, and use function extraction, simulation, and term rewriting using coefficient computation to arrive at a solution. The approach is not complete in the sense that the procedure cannot be extended to random logic circuits and finite field circuits due to ambiguities in coefficient computation. The approach also fails to verify circuits when redundant gates are introduced in the design. To overcome all these limitations, this paper describes a formal approach using finite field theory to automatically realize the function implemented by an unknown component, and verify the same. The paper introduces theory on resolving a single unknown component using ideal membership testing and Gröbner basis based reduction. We go onto pose the problem as a synthesis challenge and extend the solution space of the unknown component using concepts from quotient of ideals. Since the solution space is not unique, we will also discuss a systematic, goal driven search for simple implementable solutions. The paper presents results on some preliminary experiments performed over various arithmetic circuits to compare efficiency of our approach against recent methods.**