Rectification of Arithmetic Circuits using Computer Algebra Techniques

Vikas Rao
Department of Electrical and Computer Eng.
University of Utah
Vikas.k.rao@utah.edu

Formal verification of Arithmetic circuits checks whether or not a gate-level circuit correctly implements a given specification model. In cases where this equivalence check fails the presence of a bug is detected it is required to: i) debug the circuit, ii) identify a set of nets (signals) where the circuit might be rectified, and iii) compute the corresponding rectification functions at those locations. As a preliminary work, I addressed the problem of debugging and correction (rectification) in finite field arithmetic circuits[1]. I presented techniques that determine whether the circuit can be rectified at one particular net (gate output) i.e. a single-fix rectification issue is addressed. Starting from an equivalence checking setup modeled as a polynomial ideal membership test, I analyzed the ideal membership residue to identify potential single-fix rectification locations. Subsequently, Nullstellensatz principles were used to ascertain if indeed a single-fix rectification can be applied at any of these locations. If a single-fix rectification exists, a rectification function is derived by modeling it as the synthesis of an unknown component problem[2].

As part of my future work, I intend to deep-dive into the theory of permissible functions to explore the synthesis side of the problem in finding a more deterministic solution from the given solution space. There is also a need for further investigation on how the current procedure can be extended to cover integer arithmetic circuits. Further research also needs to address exploring the current approach for the case of multi-fix rectification.

References

[1] V. Rao, U. G. A. Srinath, I. Ilioaea, P. Kalla, and F. Enescu, "Post-Verification Debugging and Rectification of Finite Field Arithmetic Circuits using Computer Algebra Techniques - accepted," in *Formal Methods in Computer-Aided Design(FMCAD)*, 2018.

[2] V. Rao, U. Gupta, I. Ilioaea, P. Kalla, and F. Enescu, "Resolving Unknown Components in Arithmetic Circuits using Computer Algebra Meth-

ods - poster presentation," in *International Workshop on Logic and Synthesis(IWLS)*, 2018.