Verification of hardware circuits still remains a challenge to our community. Binary Decision Diagrams (BDDs) and SAT solvers based verification cannot scale-up with the current circuit sizes. In recent years, computer algebra and Gröbner basis based verification have been proposed and improved upon. The circuit is modeled as an ideal of polynomials and its Gröbner basis is computed using the Buchberger's algorithm. The expensive cost of Buchberger's algorithm can be avoided by extracting a term order from the circuit's topology. Verification approaches based on this ordering have been shown to perform well on large Galois field arithmetic circuits [4] [7]. However, using similar approaches for integer arithmetic circuits, results in a term explosion problem. Several heuristics based on the circuit topology and hierarchy have been suggested to avoid this blow-up.

The authors in [3] perform fan-out rewriting to increase the chances of term cancellation before their blow-up. The work in [2] uses a number of heuristics, including fan-outs and levelization, to improve the reduction process. The term explosion in certain mulitplier architectures is attributed to vanishing monomials that eventually reduce to zero but result in an intermediate blow-up [8].

For the approaches discussed above, the polynomials are implemented explicitly using symbolic data structures. The sparsity inherent in these polynomials cannot be exploited using these data structures. Zero-Suppressed Binary Decision Diagrams (ZBDDs) [5] find numerous applications in fields requiring set manipulation. Boolean polynomials can be considered as sets of their monomials which can be represented using ZBDDs [1]. As a result, ZBDDs, being an implict data structure, are better for representing these polynomials as characteristic functions. The approach presented in [8] depends on the structural hierarchy of the circuit. If this information is unavailable or if the netlist is bit-blasted, the heuristic of vanishing monomial cannot be applied. A similar but more generalized heuristic is required for these cases.

Contributions: We present an implementation of symbolic computer algebra algorithms, specifially targeted for circuit verification, using the unate cube set algebra and ZBDDs. The basic unate cube set algebra operations using ZBDDs are discussed in [6]. We show that the process of reduction can be performed by accessing the subgraphs of the ZBDD and using the modulo-2 sum and product algorithms described in [1]. Based on the term orders derived from the circuits, ZBDDs gives further opportunities to speed up Gröbner basis reduction implicitly by cancelling multiple monomials. As ZBDD is a canonical data structure, the result of the reduction for the output bits of the circuit can be used for verifiction. The heuristcis presented in [8] and [2], can further be extracted from arbitrary bit-blasted netlists using our approach. We present algorithms for performing these computations and experiments to support our implementations.

Paper Organization: Section II discusses the related previous work in computer algebra based abstraction and equivalence checking for verification of circuits. Section III covers the preliminary concepts related to Binary decision diagrams, boolean polynomials and Gröbner basis reduction. Section IV describes the use of ZBDDs for polynomial abstraction from circuits including the algorithm for performing the multi-term cancellation. Section V discusses the heuristics required for speeding up the reduction process and their implementation on ZBDDs. Our experiments on galois field and arithmetic circuits are presented in section VI, and finally, section VII concludes the paper.

References

[1] Michael Brickenstein and Alexander Dreyer. Polybori: A framework for grbner-basis computations with boolean polynomials. *Journal of Symbolic Computation*, 44(9):1326 – 1345, 2009. Effective Methods in Algebraic Geometry.

[2] M. Ciesielski, C. Yu, W. Brown, D. Liu, and A. Rossi. Verification of gate-level arithmetic circuits by function extraction. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6, June 2015.

[3] Farimah Farahmandi and Bijan Alizadeh. Groebner basis based formal verification of large arithmetic circuits using gaussian elimination and cone-based polynomial extraction. *Microprocess. Microsyst.*, 39(2):83–96, mar 2015.

[4] J. Lv, P. Kalla, and F. Enescu. Efficient gröbner basis reductions for formal verification of galois field multipliers. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2012*, pages 899–904, March 2012.

[5] Shin-ichi Minato. Zero-suppressed bdds for set manipulation in combinatorial problems. In *Proceedings of the 30th International Design Automation Conference*, DAC '93, pages 272–277, New York, NY, USA, 1993. ACM.

[6] Shin-ichi Minato. Calculation of unate cube set algebra using zero-suppressed bdds. In *Proceedings of the 31st Annual Design Automation Conference*, DAC '94, pages 420–424, New York, NY, USA, 1994. ACM.

[7] T. Pruss, P. Kalla, and F. Enescu. Equivalence verification of large galois field arithmetic circuits using word-level abstraction via Gröbner bases. In *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE*, pages 1–6, June 2014.

[8] A. Sayed-Ahmed, D. Groe, U. Khne, M. Soeken, and R. Drechsler. Formal verification of integer multipliers by combining gröbner basis with logic reduction. In *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 1048–1053, March 2016.