Verification of Sequential Galois Field Circuits using Algebraic Geometry *

Xiaojun Sun
University of Utah
Department of Electrical & Computer Engineering
Salt Lake City, USA
xiaojun.sun@utah.edu

Priyank Kalla
University of Utah
Department of Electrical & Computer Engineering
Salt Lake City, USA
kalla@ece.utah.edu

ABSTRACT

Circuits working in Galois fields are increasingly employed in designs like Ellptic Curve Cryptography (ECC). This work proposes a new method to effectively verify sequential circuits in Galois fields. Algebraic geometry is intriduced to describe circuits behavior and redefine implicit state space traversal. Moreover, Gröbner basis representation is adopted for word-level abstraction on circuit variables to address state explosion problem with BDDs. Experiments are run with F4-style reduction engine to get more competitive results.

Categories and Subject Descriptors

EDA5.1 [**Verification**]: Functional, transaction-level, RTL, and gate-level modeling and verification of hardware design

General Terms

Verification, Algorithms

Keywords

Verification, Sequential, Galois Fields, Algebraic Geometry

1. INTRODUCTION

Verification for sequential circuits has been extensively discussed for decade. Binary Decision Diagram (BDD) is the first and most widely used canonical technique among those for sequential verification [9]. It is easy to manipulate any Boolean expressions with BDD and use them to enumerate implicit states. However, an issue that BDDs have to face is the size explosion when Boolean variables increase significantly. Several modifications have been made to improve this problem by optimizing original BDD [6] [8], or by reducing Boolean variables from circuits[4] [7]. Some variants of BDD representation have also been developed such as Linear Taylor Expansion Diagram (LTED) [1].

Another sort of approaches are based on satisfiability theory (SAT). SAT-solver is applied to state space traversal and work through eliminations on Boolean constrains [5]. By exploiting SAT-based algorithm, direct reachability induction is proposed [3]. Still SAT-based approaches need to struggle with size explosion problem.

2. RELATED WORKS

G. Avrunin [2] introduced algebraic geometry into formal verification. In his paper, the corresponding relation between varieties of ideals and circuit variables is discussed, and concepts such as intersect of varieties, ideal and its generators and algebraic closure are explored. Yet, a self-contained system of algebraic geometry representation theory has not been well-defined.

T. Pruss, el(which one should I cite?) developed a word-level abstraction method based on Gröbner basis theory...

J. Lv, el (should I cite this part) gave out a F4-style reduction algorithm which can help speed up Gröbner basis calculation...

3. REFERENCES

[1] B. Alizadeh and M. Fujita. Sequential equivalence checking using a hybrid boolean-word level decision diagram. In *Advances in Computer Science and Engineering*, pages 697–704. Springer, 2009.

[2] G. S. Avrunin. Symbolic model checking using algebraic geometry. In *Computer Aided Verification*, pages 26–37. Springer, 1996.

[3] P. Bjesse and K. Claessen. Sat-based verification without state space traversal. In *Formal Methods in Computer-Aided Design*, pages 409–426. Springer, 2000.

[4] J. R. Burch, E. M. Clarke, and D. E. Long. Representing circuits more efficiently in symbolic model checking. In *Proceedings of the 28th ACM/IEEE Design Automation Conference*, pages 403–407. ACM, 1991.

[5] O. Coudert, C. Berthet, and J. C. Madre. Verification of synchronous sequential machines based on symbolic execution. In *Automatic verification methods for finite state systems*, pages 365–373. Springer, 1990.

[6] W. Günther, A. Hett, and B. Becker. Application of linearly transformed bdds in sequential verification. In *Proceedings of the 2001 Asia and South Pacific Design Automation Conference*, pages 91–96. ACM, 2001.

*First version, only contains abstract and introduction part.

[7] J.-H. Jiang and R. K. Brayton. On the verification of sequential equivalence. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 22(6):686–697, 2003.

[8] A. Narayan, A. J. Isles, J. Jain, R. K. Brayton, and A. L. Sangiovanni-Vincentelli. Reachability analysis using partitioned-robdds. In *Proceedings of the 1997 IEEE/ACM international conference on Computer-aided design*, pages 388–393. IEEE Computer Society, 1997.

[9] H. J. Touati, H. Savoj, B. Lin, R. K. Brayton, and A. Sangiovanni-Vincentelli. Implicit state enumeration of finite state machines using bdd's. In *Computer-Aided Design, 1990. ICCAD-90. Digest of Technical Papers., 1990 IEEE International Conference on*, pages 130–133. IEEE, 1990.