IIM > Vol.2 No.2, February 2010

OPEN ACCESS

Probabilistic Verification over GF(2m) Using Mod2-OBDDs

PDF (Size:275KB) PP. 95-103 DOI: 10.4236/iim.2010.22012

Author(s)

J.L. Imana

ABSTRACT

Formal verification is fundamental in many phases of digital systems design. The most successful verification procedures employ Ordered Binary Decision Diagrams (OBDDs) as canonical representation for both Boolean circuit specifications and logic designs, but these methods require a large amount of memory and time. Due to these limitations, several models of Decision Diagrams have been studied and other verification techniques have been proposed. In this paper, we have used probabilistic verification with Galois (or finite) field GF(2m) modifying the CUDD package for the computation of signatures in classical OBDDs, and for the construction of Mod2-OBDDs (also known as ?-OBDDs). Mod2-OBDDs have been constructed with a two-level layer of ?-nodes using a positive Davio expansion (pDE) for a given variable. The sizes of the Mod2-OBDDs obtained with our method are lower than the Mod2-OBDDs sizes obtained with other similar methods.

KEYWORDS

Verification, Probabilistic, OBDD, Mod2-OBDD, Galois Field GF(2m)

Cite this paper

J. Imana, "Probabilistic Verification over GF(2m) Using Mod2-OBDDs," *Intelligent Information Management*, Vol. 2 No. 2, 2010, pp. 95-103. doi: 10.4236/iim.2010.22012.

References

[1] C. Y. Lee, "Representation of switching circuits by binary-decision programs," Bell Systems Technology Journal, Vol. 38, pp. 985–999, 1959.

[2] S. B. Akers, "Binary decision diagrams," IEEE Transactions on Computers, Vol. C-27, pp, 509–516, 1978.

[3] L. Fortune, J. Hopcroft, and E. M. Schmidt, "The complexity of equivalence and containment for free single variable program schemes," in: Goos, Hartmanis, Ausiello, Baum (Eds.), Lecture Notes in Computer Science, Springer-Verlag, New York, Vol. 62, pp. 227–240, 1978.

[4] R. E. Bryant, "Graph based algorithms for Boolean function representation," IEEE Transactions on Computers, Vol. C-35, pp. 677–690, 1986.

[5] R. Drechsler, B. Becker, and N. G?ckel, "A genetic algorithm for variable ordering of OBDDs," International Workshop on Logic Synthesis, pp. P5c:5.55–5.64, 1995.

[6] P. W. C. Prasad, A. Assi, A. Harb, and V. C. Prasad, "Binary decision diagrams: An improved variable ordering using graph representation of boolean functions," International Journal of Computer Science, Vol. 1, No. 1, pp. 1–7, 2006.

[7] J. R. Burch and V. Singhal, "Tight integration of combinational verification methods," IEEE/ACM International Conference on CAD, pp. 570–576, 1998.

[8] A. Kuehlmann and F. Krohm, "Equivalence checking using cuts and heaps," Proceedings of Design Automation Conference, pp. 263–268, 1997.

[9] V. Paruthi and A. Kuehlmann, "Equivalence checking using cuts a structural SAT-solver, BDDs and

• Open Special Issues
• Published Special Issues
• Special Issues Guideline

IIM Subscription

Most popular papers in IIM

About IIM News

Frequently Asked Questions

Recommend to Peers

Recommend to Library

Contact Us

simulation, " International Conference Computer Design, 2000.

[10] E. Goldberg, M. R. Parasad, and R. K. Brayton, " Using SAT for combinational equivalence checking, " IEEE/ ACM Design, Automation and Test in Europe, Conference and Exhibition ' 01, pp. 114 – 121, 2001.

[11] J. Marques-Silva and T. Glass, " Combinational equivalence checking using satisfiability and recursive learning, " IEEE/ACM Design, Automation and Test in Europe, pp. 145 – 149, 1999.

[12] D. Brand, " Verification of large synthesized designs, " IEEE/ACM International Conference on Computer-Aided Design, pp. 534 – 537, 1993.

[13] W. Kunz, " HANNIBAL: An efficient tool for logic verification based on recursive learning, " IEEE/ACM International Conference on CAD, pp. 538 – 543, November 1993.

[14] R. E. Bryant, " Symbolic Boolean manipulation with ordered binary decision diagrams, " ACM Computing Surveys, Vol. 24, No. 3, pp. 293 – 318, 1992.

[15] M. Blum, A. K. Chandra, and M. N. Wegman, " Equivalence of free Boolean graphs can be decided probabilistically in polynomial time, " Information Processing Letters, Vol. 10, No. 2, pp. 80 – 82, 1980.

[16] J. Jain, J. Bitner, D. Fussell, and J. Abraham, " Probabilistic verification of Boolean functions, " Formal Methods in System Design, Kluwer, Vol. 1, pp. 61 – 115, 1992.

[17] R. E. Bryant and Y. Cheng, " Verification of arithmetic functions with binary moment diagrams, " Carnegie Mellon University Technical Report: CMU-CS-94-160, May 1994.

[18] R. Drechsler, B. Becker, and S. Ruppertz, " K*BMDs: A new data structure for verification, " IEEE European Design and Test Conference, pp. 2 – 8, 1996.

[19] U. Kebschull, E. Schubert, and W. Rosentiel, " Multilevel logic based on functional decision diagrams, " European Design Automation Conference, pp. 43 – 47, 1992.

[20] Y. T. Lai and S. Sastry, " Edge-valued binary decision diagrams for multi-level hierarchical verification, " 29th Design Automation Conference, pp. 608 – 613, 1992.

[21] J. Gergov and C. Meinel, " Mod2-OBDDs: A data structure that generalizes exor-sum-of-products and ordered binary decision diagrams, " Formal Methods in System Design, Kluwer, Vol. 8, pp. 273 – 282, 1996.

[22] S. Waack, " On the descriptive and algorithmic power of parity ordered binary decision diagrams, " Proceedings of 14th Symposium on Theoretical Aspects of Computer Science, LNCS 1200, Springer, 1997.

[23] J. L. Ima?a, J. M. Sánchez, and F. Tirado, " Bit-parallel finite field multipliers for irreducible trinomials, " IEEE Transactions on Computers, Vol. 55, No. 5, pp. 520 – 533, May 2006.

[24] ?. K. Ko? and B. Sunar, " Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields, " IEEE Transactions on Computers, Vol. 47, No. 3, pp. 353 – 356, March 1998.

[25] R. Lidl and H. Niederreiter, " Finite fields, " Addison-Wesley, Reading, MA, 1983.

[26] J. C. Madre and J. P. Billón, " Proving Circuit correctness using formal comparison between expected and extracted behaviour, " Proceedings of 25th ACM/IEEE Design Automation Conference, pp. 308 – 313, 1988.

[27] P. A. Scott, S. E. Tavares, and L. E. Peppard, " A fast VLSI multiplier for GF(2m), " IEEE Journal on Selected Areas in Communications, Vol. 4, pp. 62 – 66, 1986.

[28] C. Meinel and H. Sack, " ?-OBDDs – A BDD structure for probabilistic verification, " Pre-LICS Workshop on Probabilistic Methods in Verification (PROBMIV ' 98), Indianapolis, IN, USA, pp. 141 – 151, 1998.

[29] F. Somenzi, " CUDD: CU decision diagram package, " Uni- versity of Colorado at Boulder. http://vlsi.colorado. edu/ ~ fabio/CUDD/.

[30] K. S. Brace, R. L. Rudell, and R. E. Bryant, " Efficient implementation of a BDD package, " 27th ACM/IEEE Design Automation Conference, pp. 40 – 45, 1990.