Fast Algebraic Rewriting Based on And-Inverter Graphs

Cunxi Yu, *Student Member, IEEE*, Maciej Ciesielski, *Senior Member, IEEE*, and Alan Mishchenko, *Senior Member, IEEE*

***Abstract*—Constructing algebraic polynomials using computer algebra techniques is believed to be state-of-the-art in analyzing gate-level arithmetic circuits. However, the existing approach applies algebraic rewriting directly to the gate-level netlist, which has potential memory explosion problem. This paper introduces an algebraic rewriting technique based on the And-Inverter Graph (AIG) representation of gate-level designs. Using AIG-based cut-enumeration and truth table computation, an efficient order of algebraic rewriting is identified, resulting in dramatic simplifications of the polynomial under construction.**

I. Introduction

IMPORTANCE of arithmetic verification problem grows with an increased use of arithmetic modules in embedded systems to perform computation-intensive tasks in multimedia, signal processing, and cryptography applications. One of the remaining challenges in formal verification is formal verification of gate-level integer arithmetic circuits, such as multipliers, used extensively in those applications. Despite a considerable progress in verification of random and control logic, advances in formal verification of arithmetic designs have been slow. This can be attributed to the difficulty in the efficient modeling of arithmetic circuits and datapaths without resorting to computationally expensive Boolean methods, such as BDDs, SAT, SMT, etc., that require "bit blasting", i.e., flattening the design to a bit-level netlist. However, recently, formal techniques based on *computer algebra* have been successfully applied to the verification problems of gate-level arithmetic circuits.

Computer algebra techniques, which construct the polynomial representation of a gate-level arithmetic circuit, are believed to offer best solution for analyzing arithmetic circuits [1][2][3][4][5]. These works address the verification problems of Galois field arithmetic [2] and integer arithmetic implementations, including abstractions and reverse engineering [3][4][5][1]. The verification problem is typically formulated as a proof that the implementation satisfies the specification, which is solved by polynomial division or algebraic rewriting. The results show that the computer algebra techniques provide several orders of magnitude performance improvement. The main advantage of computer algebra methods in verifying arithmetic circuits is that it provides a large number of polynomial reductions by eliminating non-linear terms. However, non-linear terms could explode exponentially after rewriting the variables in that term if they were not eliminated at the right time (order). The polynomial reduction is presented in Section II-E.

The order of rewriting or, equivalently, performing polynomial divisions has a significant impact on the performance of the computer algebra techniques [5][6]. However, these techniques may fail to find an efficient rewriting orders for the gate-level arithmetic circuits. Because they are applied directly to the gate-level netlist. Yu et al. [6] compared the performance of algebraic methods of combinational gate-level multipliers when different topological orders are used. It showed that an efficient topological order may not exist in the post-synthesized gate-level netlist. Even if such an order exists, it may be difficult to be identified because of the polynomial reductions hidden in the complex standard cells. In addition, redundant polynomials detected from combinational and sequential arithmetic circuits can provide significant polynomial reductions [7]. However, detecting such polynomials is limited by manual operations and depends on the structure of the circuits.

The approach presented in this paper aims at improving the efficiency of algebraic rewriting in the context of arithmetic verification. It addresses the problem by using a compact and uniform representation of the Boolean network called the *And-Inverter Graph* (AIG) [8]. Instead of directly applying algebraic rewriting to the gate-level netlist, it is applied to an AIG. In addition, this approach allows to automatically generate redundant polynomials, which significantly reduce the complexity of algebraic rewriting.

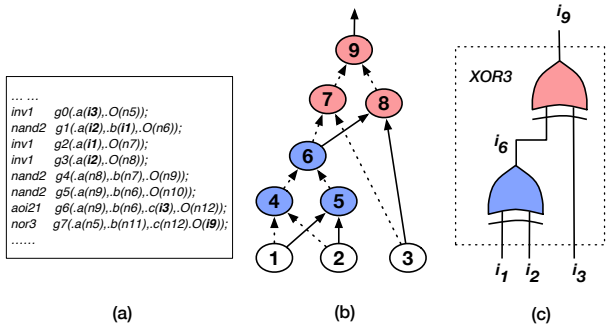

Fig. 1. a) Post-synthesized XOR3 gate-level netlist. b) AIG of the synthesized XOR3 gate-level netlist. (c) The extracted two XOR2 functions (nodes 6 and 9) and one XOR3 function (node 9).

II. Background

A. Formal Verification of Arithmetic Circuits

Verification of arithmetic circuits is performed using a variation of *combinational equivalence checking* (CEC) referred to

C. Yu and M. Ciesielski are with the Department of Electrical and Computer Engineering at University of Massachusetts, Amherst, MA, 01003, USA (ycunxi@umass.edu, xiangyuzhang@umass.edu, ciesiel@ecs.umass.edu).

A. Mishchenko is with EECS Department at University of California, Berkeley, Berkeley, CA 94720 (alanmi@berkeley.edu)

as *arithmetic combinational equivalence checking* (ACEC) [5]. Several approaches have been applied to equivalence check an arithmetic circuit against its functional specification, including *canonical diagrams*, *satisfiability* theories, *theorem proving*, etc. Different variants of canonical, graph-based representations have been proposed, including Binary Decision Diagrams (BDDs) [9], Binary Moment Diagrams (BMDs) [10] [11], Taylor Expansion Diagrams (TED) [12], and other hybrid diagrams. While BDDs have been used extensively in logic synthesis, their application to verification of arithmetic circuits is limited by the prohibitively high memory requirements for complex arithmetic circuits, such as multipliers. Boolean satisfiability (SAT) and satisfiability modulo theories (SMT) solvers have also been applied to solve ACEC problems [13]. Recently, several state-of-the-art SAT and SMT solvers have been applied to those problems, including MiniSAT[14], Lingeling[15], Boolector [16], Z3 [17], etc. However, the complexity of checking equivalence of large arithmetic circuits is extremely high [18][6]. Alternatively, the problem can be modeled as checking equivalence against the arithmetic function, e.g. checking whether the binary encoded output function is equivalent to the expected arithmetic function using bit-vector formulation of SMT. However, the complexity of this method is the same as the CEC method [6].

B. Computer Algebra Approaches

In computer algebra approach, the verification problem is typically formulated as a proof that the implementation satisfies the specification [1][2][4][3][5]. This task is accomplished by performing a series of divisions of the specification polynomial by a set of polynomials, representing components that implement the circuit. Techniques based on *Gröbner Basis* demonstrate that this approach can efficiently transform the verification problem into *membership testing* of the specification polynomial in the ideals [2][4]. Farahmandi et. al's work summary need to be added here. A different approach to arithmetic verification of gate-level circuits has been proposed using the algebraic rewriting technique, which transforms the polynomial at the primary outputs to a polynomial in terms of primary inputs [1], called *function extraction*. This approach has successfully been applied to 512-bit multipliers, due to a large number of polynomial reductions gained by rewriting a binary encoded polynomial of the outputs [6]. A similar approach has been applied to arithmetic combinational equivalence checking [5], with a novel approach of detecting vanishing polynomials using the reconvergent fanout information. Although those works showed good performance in solving arithmetic verification problems, they still suffer from potential polynomial (memory) explosion problem since they are applied to the original gate-level netlist.

C. Boolean network

Boolean network is a directed acyclic graph (DAG) with nodes representing logic gates and directed edges representing wires connecting the gates. And-Inverter Graph (AIG) is a combinational Boolean network composed of two-input AND-gates and inverters [8]. In an AIG, each node has at most two incoming edges. A node with no incoming edges is a primary input (PI). Primary outputs are represented using special output nodes. Each internal node in the AIG represents a two-input AND function. Based on DeMorgan's rule, the combinational logic of an arbitrary Boolean network can be transformed into an AIG [19], with the properly labeled edges to indicate the inversion of the signals. AIGs have been extensively used in logic synthesis, technology mapping [19] and formal verification [20].

AIGs have been used to detect unobserved Boolean functions such as *Multiplexer* function [21] in an arbitrary gate-level circuits. This method is based on computing a *Cut* in the AIG. A cut *C* of node n is a set of nodes of the network called *leaves*, such that each path from PIs to n passes through the leaf nodes. Node n is the *root* of a *Cut*. A *Cut* is K-feasible if the number of leaves does not exceed K. The cut function is the function of node n in terms of the cut leaves. An AIG node n in an AIG structure that represents a Boolean function F, is called an F-node. Each node is an AND function and the edges indicate the inversions of Boolean signals[1]. An example of identifying XOR functions embedded in the AIG is shown in Figure 1. The AIG shown in Figure 1(b) represents a sub-circuit described in Figure 1(a). It includes a 3-feasible *Cut* of $node$ 9 and a 2-feasible *Cut* of $node$ 6, among other possible 3-feasible cuts. Let the function of the AIG node with index x be i_x. The function of $node$ 6 is $i_1 \oplus i_2$, and the function of $node$ 9 is $i_1 \oplus i_2 \oplus i_3$. Hence, $node$ 6 is an *XOR2*-node, and $node$ 9 is an *XOR3*-node. This means that an embedded XOR3 function consisting of two XOR2s exists and can be detected in the sub-circuit shown in Figure 1(a). Similarly, an AIG can be applied to identify embedded *Majority* functions.

D. Computer Algebraic Model

In this approach, the circuit is modeled as an AIG containing the following gates: INV, AND, embedded MAJ3, and embedded XOR3. This is in contract to using a standard-cell network model after synthesis and technology mapping [1]. The following algebraic equations describe the algebraic model used in this work.

TABLE I
BOOLEAN MODEL AND ALGEBRAIC MODEL OF INV, AND, XOR, AND MAJORITY OPERATIONS.

Operation	Boolean Model	Algebraic Model
INV(a)	$\bar{a}$	1-a
AND(a,b)	a $\wedge$ b	ab
XOR(a,b,c)	a $\oplus$ b $\oplus$ c	ab+ac+bc-2abc
Majority(a,b,c)	(a $\vee$ b) $\wedge$ (a $\vee$ c) $\wedge$ (b $\vee$ c)	a+b+c-2ab-2ac-2bc+4abc

Similarly to [1], the algebraic rewriting for a circuit is based on two polynomials referred to as *output signature* and *input signature*. The *input signature*, Sig_{in}, is a polynomial in terms of primary input variables that uniquely represents the integer function computed by the circuit, i.e., its *specification*. For example, an n-bit binary adder with inputs $\{a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1}\}$, is described by $Sig_{in} =$

[1]In Fig.1, the dash edges are inversion signals, e.g. $i_4 = \overline{i_1}\ \overline{i_2}$, $i_5 = i_1 i_2$.

$\sum_{i=0}^{n-1} 2^i a_i + \sum_{i=0}^{n-1} 2^i b_i$. In our approach, the input specification need not be known; it will be derived from the circuit implementation as part of the verification process. The *output signature*, Sig_{out}, of the circuit is a polynomial in terms of the primary output variables. Such a polynomial is uniquely determined by the n-bit encoding of the output, provided by the designer. This means that the binary encoding of the primary output variables is assumed to be known.

E. Simplified Polynomial Construction

According to [6], efficiency of algebraic rewriting of Sig_{out} is determined by the amount of simplifications during polynomial construction. This is because there is a large number of non-linear terms generated by *carry-out* (MAJ) and *sum*(XOR) functions, since multiplication is affected by a series of additions. Finding the maximum polynomial cancellations has been previously addressed by improving the topological order of the gates [6]. For example, let a sub-polynomial expression be Nx_1+$2Nx_2$+..., where x_1 = *XOR3(a, b, c)*, x_2 = *MAJ3(a, b, c)*, where *a, b, c* are the inputs of XOR3 and MAJ3 functions. According to Equation 1, when rewriting x_1 and x_2 together, four non-linear terms are eliminated, namely $2Nab$, $2Nbc$, $2Nac$ and $4Nabc$, generated by the algebraic models of XOR3 and MAJ3. However, if rewriting is applied directly to the gate-level netlist, its efficiency is lost when the MAJ3 and XOR3 functions are mapped into other standard cells by logic synthesis and technology mapping. For example, the XOR3 function mapped using standard cells is shown in Figure 1(a). In this case, there is no ordering that provides the required polynomial reductions.

III. Approach

This section presents the algebraic rewriting approach based on AIGs. Similarly to [1], the algebraic rewriting process rewrites the output signature for all AIG nodes in a reverse topological order. As discussed in Section II-E, the rewriting order that provides a large number of polynomial reductions, has significant impact on the rewriting performance. However, there are many reverse topological orders available in an AIG, since many nodes can have the same topological depth. This approach detects a reverse topological order for algebraic rewriting that provides the maximum polynomial reduction. This is achieved by detecting pairs of MAJ3 and XOR3 nodes using AIG-based *cut enumeration*.

Algorithm 1 Algebraic Rewriting in AIG

Input: Gate-level netlist, output signature Sig_{out}
Output: *Pseudo-Boolean* expression extracted by rewriting

1: Structural hashing the gate-level netlist into AIG, denoted *G(V, E)*.
2: Detect all XOR3 and MAJ3 nodes in *G(V, E)*.
3: Pair the XOR3 and MAJ3 if they have identical signals, denoted as P.
4: Topological sort *G(V,E)* considering each element in P as one node.
5: i = 0; $F_i = Sig_{out}$
6: **while** there are no elements remained in the reverse topological order **do**
7: Rewrite: $F_{i+1} = F_i$ by substituting the variables with algebraic equations;
8: i = i + 1
9: **return** $F = F_i$ (to be compared with Sig_{in})

A. Outline of the Approach

The proposed flow is outlined in Algorithm 1. The inputs to the algorithm are: the gate-level netlist and the output signature Sig_{out}. The flow includes three basic steps: 1) converting the gate-level implementation into AIG; 2) detecting all pairs of XOR3 and MAJ3 nodes with identical inputs; topological sorting the AIG nodes while considering the detected pairs as one element; and 3) applying algebraic rewriting from POs to PIs following the reverse topological order determined in step 2). Note that XOR2 and MAJ2(AND2) are the special cases of XOR3 and MAJ3, where one of the inputs is constant zero. The second step is performed as follows:

- Computing all 3-feasible (3-input) cuts of all AIG nodes.
- Computing truth tables of all cuts.
- Storing cuts in the hash table by their ordered set of inputs.
- Detecting pairs of 3-input cuts with identical inputs belonging to different nodes, such that the Boolean functions of the two cuts with the shared inputs belong to the *NPN* classes of XOR3 and MAJ3, respectively.

Note that, in this approach, matching the XOR3 and MAJ3 nodes does not require the inputs and outputs polarity to be the same. Instead, all the cut-points are matched without considering their complemented attributes. For example, instead of being an exact XOR3, the function of a 3-feasible cut can be either XOR3 or XNOR3. Similarly, instead of being exactly MAJ3, the function can be one of the eight functions forming the *NPN* class of MAJ3 [22]. To compute the cuts, the 3-input cut enumeration is performed in a topological order as described in [23]. The truth tables of the cuts are obtained as a by-product of the cut enumeration. Thus, when two fanin cuts are merged during the cut computation and the resulting cut is 3-feasible, the truth tables of fanin cuts are permuted to match the fanin order of the resulting cut. These truth tables are then ANDed or XORed, depending on the node function, to get the resulting truth table. For the case of 3-input cuts, a dedicated pre-computation reduces the runtime of truth table computation to a small fraction of that of cut enumeration.

As soon as the XOR3 and MAJ3 pairs are detected, algebraic rewriting will be applied to the AIG network in a constrained reverse topological order, in which each XOR3 and MAJ3 pair is considered as one element. This means that at one topological depth, whenever either XOR3 or MAJ3 node of a pair (or its complement) is rewritten, the subsequent rewritten node is of the other type. The AIG nodes with the same topological depth that do not belong to any pair are ordered in the decreasing order of their integer IDs. The algebraic rewriting ends when all elements in AIG network have been rewritten. The algorithm returns the extracted input signature.

Example 1 (2-bit CSA-multiplier): The mapped gate-level netlist of a 2-bit CSA-multiplier is shown in Figure 2(a). First, the gate-level netlist is converted to an AIG representation, Figure 2(b). Then, a set of XOR3 nodes X, and a set of MAJ3 nodes M are detected. X = {*14, 18*}, M = {12, 16}. *Node 14* is *XOR3(10, 11, 0)* and *node 12* is *MAJ3(10, 11, 0)*, where *nodes 10 and 11* and constant zero *0* are the inputs; *node 18* is

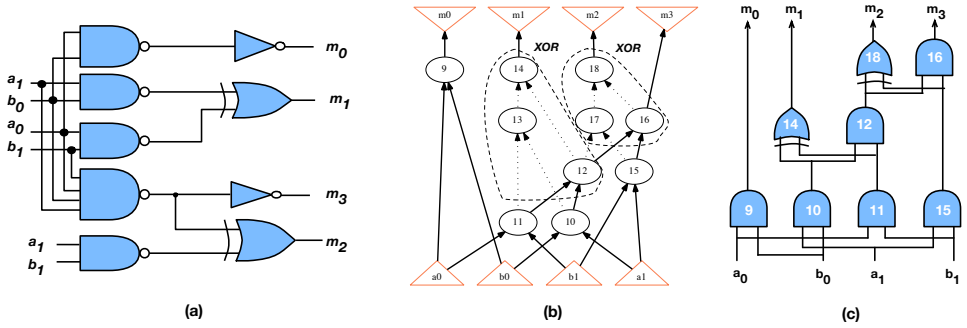

Fig. 2. (a) Post-synthesized 2-bit multiplier gate-level netlist; (b) The AIG of the 2-bit multiplier shown in Figure 2(a); (c) Detected unobserved functions from the AIG and the correspondences to AIG nodes. The index value in Figure 2(c) corresponds to the hash value of each node in Figure 2(b).

XOR3(12, 15, 0) and *node 16* is *MAJ3(12, 15, 0)*. Hence, two pairs of XOR3 and MAJ3 are generated, *(14, 12)* and *(18, 16)*. The order of rewriting is determined as follows: 1) *node 18* is the node with highest depth; it is detected as a XOR3 and paired with a MAJ3 *node 16*; hence, the first rewriting starts from node 18 and 16, and ends at node 12 and 15; 2) similarly to the first rewriting, the second rewriting starts from nodes 14 and 12, and ends at nodes 11 and 10; 3) the remaining AIG nodes are ordered by their index value in decreasing order. The logic network after detecting all XOR3 and MAJ3 functions are shown in Figure 2(c).

B. Detecting Redundant Polynomials

Significant simplification of algebraic polynomial construction can be achieved not only by performing algebraic rewriting using a reverse topological order, as discussed above, but also by detecting redundant polynomials, such as *don't-care* polynomials and *vanishing* polynomials [5][7]. Specifically, this section focuses on detecting *don't-care polynomials* defined in [7], i.e., a set of polynomials that are included in the arithmetic function but excluded from the design. These polynomials are identified by observing that in some designs, such as truncated multipliers, the removed signals contain algebraic information needed to cancel algebraic terms of the remaining output bits. Arithmetic operators are often truncated to reduce power consumption or speed up the critical path. Polynomial associated with the most significant bit (MSB) of an adder or a multiplier is an example of such a polynomial. Note that the logic obtained by removing such output bits is either a carry-out or a sum function of a full adder, implemented by MAJ3 and XOR3 functions. Hence, using the approach of detecting pairs of XOR3 and MAJ3 (Section III-A), the XOR3/MAJ3 nodes that do not belong to any such pairs can also be identified. For example, in a n-bit CSA-multiplier with *2n-1* output bits (with a MSB removed), MAJ3 with same inputs as an unpaired XOR3 is missing. Since one pair of XOR3 and MAJ3 is a full adder, removing the carry bit (and the MAJ3) makes the function an addition *modulo 2*. In this case, the algebraic model of XOR3 (Equation 1) reduces to *a + b + c - 2ab - 2ac - 2bc + 4abc mod 2*. In other words, the algebraic model of a $\oplus$ b $\oplus$ c in this case becomes *a + b + c*. Specifically, the negation of the removed terms, *-2ab - 2ac - 2bc + 4abc, gives the redundant polynomials detected for each unpaired XOR3*.

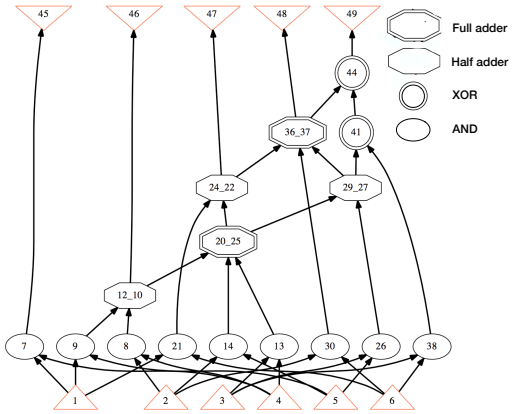

Fig. 3. Detecting *MAJ3-XOR3* of a 3-bit post-synthesized CSA-multiplier with MSB z_5 deleted.

Example 2 (3-bit CSA-multiplier with MSB z_5 detected): The AIG after detecting XOR3 and MAJ3 pairs of a 3-bit synthesized CSA-multiplier with MSB deleted is shown in Figure 3. The detected XOR3 and MAJ3 pairs are represented using the ID of the root node of the XOR3 and MAJ3 nodes. We can see that there is one XOR3 (composed of two XOR2 nodes, *41* and *44*) with inputs i_{36_37}, i_{27_29} and i_{38}, that cannot be paired with any MAJ3. This is simply because the synthesis process removed the redundant logic (last carry out) when the MSB has been removed. In this case, the algebraic model of that XOR3 reduces to $2^4 z_4(i_{49}) = 2^4(i_{36\_37} + i_{27\_29} + i_{38})$.

IV. Results

The technique described in this paper was implemented in ABC [19]. It applies algebraic rewriting to the AIG and generates the polynomial signature. The experiments were conducted on a PC with Intel(R) Xeon CPU E5-2420 v2 2.20 GHz x12 with 32 GB memory. The experiments include gate-level rewriting of Carry-Save-Adder (CSA) multipliers and radix-4 Booth multipliers, up to 512 bits. The results are compared with *functional extraction* [1] and the Grobner Basis based approach [5][18], using post-synthesized circuits. The results show that the proposed technique is more efficient than the state-of-the-art technique for extracting the polynomial expressions for those arithmetic circuits.

TABLE II
RESULTS OF APPLYING AIG-BASED ALGEBRAIC REWRITING TO PRE- AND POST-SYNTHESIZED CSA MULTIPLIERS COMPARED TO *functional extraction* PRESENTED IN [1]. **t(s)* IS THE RUNTIME IN SECONDS. **mem* IS THE MEMORY USAGE IN MB. **256B* IS 256-BIT BOOTH MULTIPLIER. *TO* = OUT OF 24 HOURS.

# bits	*Pre-Syntheized*				*Post-Synthesized*				
	[1]		This approach		[1]	[5]	[18]	This approach	
	t(s)	mem	t(s)	mem	t(s)	t(s)	t(s)	t(s)	mem
64	1.9	74	0.08	34	5.50	593	TO	0.11	34
128	8.1	288	0.78	117	39.6	TO	TO	0.91	120
256	32.6	1157	7.80	441	285	TO	TO	8.23	439
256B	TO	-	33.7	423	TO	TO	TO	39.5	431
512	130	4427	31.7	1695	-	-	-	-	-

TABLE III
RESULTS OF APPLYING AIG-BASED ALGEBRAIC REWRITING TO POST-SYNTHESIZED COMPLEX ARITHMETIC CIRCUITS COMPARED TO *functional extraction* PRESENTED IN [1]. **MO* = MEMORY OUT OF 8 GB.

Benchmarks (256-bit)	[1]		This approach	
	runtime(s)	mem(MB)	runtime(s)	mem(MB)
$F=A\times B+C$	179.1	1182	5.1	447
$F=A\times(B+C)$	209.3	1120	5.1	451
$F=A\times B\times C$	-	MO	37.5	2871
$F=1+A+A^2+A^3$	-	MO	47.1	3331

We evaluate our AIG-based algebraic rewriting approach using pre-synthesized and post-synthesized CSA multipliers shown in Table II, and post-synthesized complex arithmetic circuits shown in Table III. The gate-level arithmetic circuits are unsigned and are taken from [1]. Booth multipliers are generated by *%blast -b* command using ABC [19]. The runtime and memory usage are compared to *functional extraction* [1]. In Table III, the functions of the arithmetic circuits are shown in the first column. The bit-width varies between 64 and 512 bits[2]. We can see that the runtime of the proposed approach outperforms other approaches for the post-synthesized multipliers for any bit-width. The memory usage has been reduced on average 60%, compared to *function extraction* [1]. Also, the complexity of extracting the polynomial expression using functional extraction is increased when the multipliers are synthesized. For example, extracting post-synthesized 256-bit multiplier using functional extraction requires 9x more runtime and more memory. However, using the proposed approach, the runtime of extracting pre- or post-synthesized multipliers are almost the same. More importantly, we can see that our approach surpass *functional extraction* on complex arithmetic designs (Table III).

V. CONCLUSION

This paper presented a method to improve the efficiency of algebraic rewriting used in arithmetic verification. The method is based on And-Inverter Graph (AIG) representation of the Boolean network. This approach allows for formal verification of practical multipliers that are heavily optimized and mapped using 14nm technology library. Another contribution of the paper is a technique that automatically detects redundant polynomials to reduce the complexity of algebraic rewriting.

ACKNOWLEDGMENT

This work was supported by an award from National Science Foundation, No. CCF-1319496 and No. CCF-1617708. The co-author affiliated with UC Berkeley was supported in part by NSA grant "Enhanced equivalence checking in crypto-analytic applications". The authors would like to thank Dr. A. Sayed-Ahmed, for his help to get comparison results.

[2]512-bit post-synthesized multipliers are not reported in [1].

REFERENCES

[1] M. Ciesielski, C. Yu, W. Brown, D. Liu, and A. Rossi, "Verification of Gate-level Arithmetic Circuits by Function Extraction," in *52nd DAC*. ACM, 2015, pp. 52–57.

[2] J. Lv, P. Kalla, and F. Enescu, "Efficient Grobner Basis Reductions for Formal Verification of Galois Field Arithmatic Circuits," *IEEE Trans. on CAD*, vol. 32, no. 9, pp. 1409–1420, September 2013.

[3] E. Pavlenko, M. Wedler, D. Stoffel, W. Kunz, A. Dreyer, F. Seelisch, and G. Greuel, "STABLE: A new QF-BV SMT solver for hard verification problems combining Boolean reasoning with computer algebra," in *DATE*, 2011, pp. 155–160.

[4] F. Farahmandi and B. Alizadeh, "Groebner basis based formal verification of large arithmetic circuits using gaussian elimination and cone-based polynomial extraction," *Microprocessors and Microsystems*, vol. 39, no. 2, pp. 83–96, 2015.

[5] A. Sayed-Ahmed, D. Große, U. Kühne, M. Soeken, and R. Drechsler, "Formal Verification of Integer Multipliers by Combining Grobner Basis with Logic Reduction," in *DATE'16*, 2016, pp. 1–6.

[6] C. Yu, W. Brown, D. Liu, A. Rossi, and M. J. Ciesielski, "Formal Verification of Arithmetic Circuits using Function Extraction," *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 35, no. 12, pp. 2131–2142, 2016.

[7] C. Yu and M. Ciesielski, "Formal Verification Using Don't-Care and Vanishing Polynomials," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2016, pp. 284–289.

[8] A. Mishchenko, S. Chatterjee, and R. Brayton, "DAG-aware AIG Rewriting A Fresh Look at Combinational Logic Synthesis," in *43rd DAC*. ACM, 2006, pp. 532–535.

[9] R. E. Bryant, "Graph-based algorithms for boolean function manipulation," *IEEE Trans. on Computers*, vol. 100, no. 8, pp. 677–691, 1986.

[10] R. E. Bryant and Y. Chen, "Verification of Arithmetic Circuits with Binary Moment Diagrams," in *Proceedings of the 32st Conference on Design Automation, San Francisco, California, USA, Moscone Center, June 12-16, 1995.*, 1995, pp. 535–541.

[11] Y.-A. Chen and R. Bryant, "*PHDD: An Efficient Graph Representation for Floating Point Circuit Verification," School of Computer Science, Carnegie Mellon University, Tech. Rep. CMU-CS-97-134, 1997.

[12] M. Ciesielski, P. Kalla, and S. Askar, "Taylor Expansion Diagrams: A Canonical Representation for Verification of Data Flow Designs," *IEEE Trans. on Computers*, vol. 55, no. 9, pp. 1188–1201, Sept. 2006.

[13] E. Goldberg, M. Prasad, and R. Brayton, "Using SAT for combinational equivalence checking," in *Proceedings of the conference on Design, automation and test in Europe*. IEEE Press, 2001, pp. 114–121.

[14] N. Sorensson and N. Een, "Minisat v1. 13-a sat solver with conflict-clause minimization," *SAT*, vol. 2005, p. 53, 2005.

[15] A. Biere, "Lingeling, plingeling and treengeling entering the sat competition 2013," *Proceedings of SAT Competition*, pp. 51–52, 2013.

[16] A. Niemetz, M. Preiner, and A. Biere, "Boolector 2.0," *Journal on Satisfiability, Boolean Modeling and Computation*, vol. 9, 2015.

[17] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," in *Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2008, pp. 337–340.

[18] T. Pruss, P. Kalla, and F. Enescu, "Efficient Symbolic Computation for Word-Level Abstraction From Combinational Circuits for Verification Over Finite Fields," *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 35, no. 7, pp. 1206–1218, 2016.

[19] A. Mishchenko *et al.*, "ABC: A system for sequential synthesis and verification," *URL http://www. eecs. berkeley. edu/˜ alanmi/abc*, 2007.

[20] A. Mishchenko, S. Chatterjee, R. Jiang, and R. K. Brayton, "FRAIGs: A unifying representation for logic synthesis and verification," ERL Technical Report, Tech. Rep., 2005.

[21] C. Yu, M. J. Ciesielski, M. Choudhury, and A. Sullivan, "DAG-aware logic synthesis of datapaths," in *Proceedings of the 53rd Annual Design Automation Conference, DAC 2016, Austin, TX, USA, June 5-9, 2016*, 2016, pp. 135:1–135:6.

[22] Z. Huang, L. Wang, Y. Nasikovskiy, and A. Mishchenko, "Fast Boolean matching based on NPN classification," in *International Conference on Field-Programmable Technology, FPT, Kyoto, Japan*, 2013.

[23] P. Pan and C. Lin, "A New Retiming-Based Technology Mapping Algorithm for LUT-based FPGAs," in *FPGA*, 1998, pp. 35–42.