Equivalence Checking of Bounded Sequential Circuits based on Gröbner Basis

WANG Guanjun ZHAO Ying
Department of computer science and technology
China university of Mining and Technology
Xuzhou，P. R. China
E-mail: zywgj@cumt.edu.cn

Tong Minming
School of information and electrical engineering
China university of Mining and Technology
Xuzhou，P. R. China
E-mail: zywgj@cumt.edu.cn

***Abstract*—The sequential circuit equivalence verification problem is researched in this paper, bounding equivalence verification method based on Grobner basis is put forwarded. First, to be verified sequential circuit expansion to a set of Polynomial Symbolic Algebra Representation in accordance with time frame, so the sequential equivalence checking problem translate into combinational equivalence checking problem, The global constraints are mined over the expression database according to time series. Moreover, the approach can also mine the illegal constraints and complex polynomial relationship; with this the solving space is pruned dramatically. Then calculate the Grobner basis of the two sets, testing equivalence with equivalence checking algorithm. The experiment results show that this approach can realize rapid convergence, eliminate false verification effectively.**

Keywords- Sequential Equivalence Checking; Association Rule Mining; Polynomial Symbolic Algebra; Gröbner basis

I. INTRODUCTION

Formal verification [1] technology becomes mature in the past few decades and becomes verification methodology mainstream technology. Formal verification methods can be roughly divided into three categories: equivalence checking, model checking and theorem proving. Equivalence checking is the functional equivalence verification between two different descriptions. The traditional Equivalence checking of sequential circuits usually based on finite state machine traversal method [2]. Such methods can work at logic gate level and computational complexity is high, it can be applied to small-scale design verification only, they are powerless in practical design for large-scale design. Another method is change sequential circuit equivalence checking into combinational circuit equivalence checking [3], such methods can improve the verification speed greatly, become an important research direction now. methods[4]using storage element mapping method, the method to establish the storage element mapping between two circuits , the timing circuit is then decomposed into some corresponding combination module, followed by equivalence verification of the appropriate combination module.

II. BACKGROUND

Association rule mining

Data mining techniques include: Contains rules, signal correlation, clustering, association rules, statistical modeling. Beginning in 1993, association rule mining has attracted wide attention in the field of data mining, such as the classic Apriori algorithm is proposed by the Agrawal et al for mining association rules. However, this algorithm need to generate a lot of candidate item sets when generating association rules, efficiency is low. To solve this problem, Han et al proposed FP-GROWTH algorithm [5], Subsequently, similar algorithms have been proposed, such as COFI-TREE, CATS-TREE, CANTREE and so on. This article is mainly carried out constraints conflict detection using association rule mining. Here is the concept of conflict constraints.

Definition 1 conflict constraint

state pair (p^i, q^j) (i,j is time frame and $j > i > 0$)is a conflict constraint in FSM of M Iff $\forall k > i$,to all input sequence, when p^k in M, q^{k+j-i} never appears.

III. EQUIVALENCE VERIFICATION BASED ON GRÖBNER BASIS

Traditional sequential equivalence checking (SEC) approach is shown in Fig.1,sequential circuit L and S are connected according to Fig.1 first, if the output of OR gate is equal to 0 constantly, then $L = S$ .the equivalence checking problem can be solved with BDD representation or SAT engine.

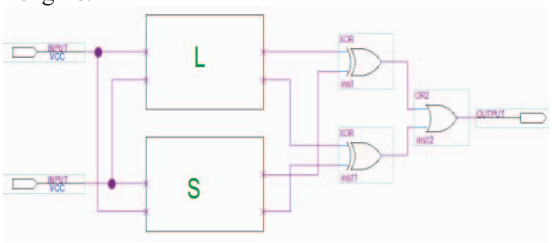

Fig.1.Traditional SEC Flow

Unlike the traditional approach, the Grobner basis theory is applied in sequential equivalence checking

978-1-4799-7005-6/14 $31.00 © 2014 IEEE
DOI 10.1109/ISCID.2014.235

problem, the polynomial symbolic algebra representation is also adopted in our paper. In order to solve the SEC problem theorem 1 is given first

Theorem 1 Let sequential circuits L and S, they have the same PIs and POs. $<S^n, L^k>$ is got when map the FFs of L and S one to one. Let $<S^n, L^k> = L^{n+k}$,then $L = S$.(L, S have the same initial state, n, k stands for time frame)

L and S is represented with polynomial set according to theorem 1, $L = \{l \mid l$ is the polynomial representation unroll according to time frame$\}$, $S = \{s \mid s$ is the polynomial representation unroll according to time frame$\}$,our goal is to verify $L = S$? to solve this problem, *Gröbner* basis G of $<L>$ is computed first. Then *Gröbner* basis G' of $<S>$ is computed. If $G = G'$,then the two circuits is equivalence. The verification flow is shown in Fig.2:

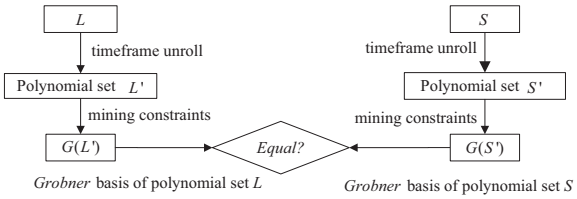

Fig.2.Verification flow based on Gröbner basis

A. *The polynomial representation of sequential circuits*

The sequential circuits discussed in our paper are synchronous sequential circuits. Let S be the set of state variable of sequential circuits. To synchronous sequential circuits, set S composed with all input variable and all FFs.A vector is got by assignment value to the elements in S ,called a state, denoted as $<s_1 s_2 \cdots s_n>$. v_i is a polynomial variable in circuits. S is a set of all states in circuits. The state transitions are represented by transition relation. To a circuit with inputs of m and FFs of n , $S =< x_0, \cdots, x_{m-1}, s_0, s_1 \cdots s_{n-1} >$ (x_i is the input variable and v_j is the state variable), $S =< x_0, \cdots, x_{m-1}, s_0, s_1 \cdots s_{n-1} >$ is the current state, $S' =< x_0', \cdots, x_{m-1}', s_0', s_1' \cdots s_{n-1}' >$ is the next state in circuit. to every state variable s_j' ,they have a constrain function f_j ,so: $s_j' = f_j(s_j)$ .every synchronous sequential circuits can be expressed in polynomial function $f_t'(x) = f_t(x_0', \cdots, x_{m-1}', s_0', s_1' \cdots s_{n-1}')$ (x_i' is the value in time t and v_j' is the state value in time t). Suppose the time frame of synchronous sequential circuits is n ,then we can get the polynomial set $f(x) = \{f_{t_1}(x), \cdots, f_{t_n}(x)\}$ ($f_{t_i}(x)$ is the polynomial function in time t_i).

B. *Constraints mining*

The simulation vector was inputted to DUT firstly, then the test vector response is got ,after that we can divided the simulation data according to time frame, polynomial set is got with every time frame count as FFs.Association rule mining is applied to the polynomial sets. After mining we can get the representation polynomial set. If cross time frame state pair is empty with this polynomial set, then it's a candidate point. The constrained polynomial equation is got with these points. The complexity of compute *Gröbner* basis is then reduced when the equation applied to polynomial sets. The constrains mining flow is shown in Fig.3;

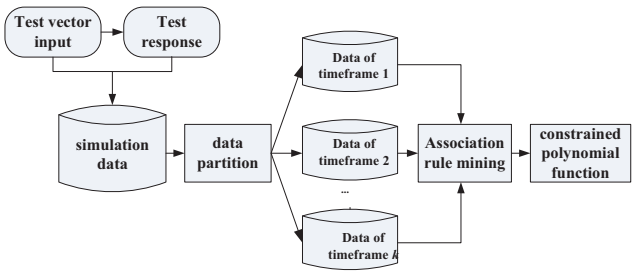

Fig.3.Constrained mining flow

In the process of polynomial mining of simulation data, the learning framework based on *sup* and *conf* is established. *sup* and *conf* stands for the frequency and accuracy[6] in polynomial function of FFs.the define is as follows:

$$sup = \frac{|X|}{|M|} \,\&\, conf = \frac{|X \cap Y|}{|X|} \qquad (1)$$

M denotes the whole test data. X denotes the test data covered by a FF polynomial. Y denotes the test response in the test database.

With the above definition, we can compare the two parameters of FFs with the predefined threshold value; parameters will be added to the verification set if greater than the threshold value. On the basis find the states of these flip-flops will not appear simultaneous to form the corresponding constraints. In the equivalence checking process, we can add constraints to these sequential circuit polynomial sets. So the complexity of the circuits to be verified is reduced. For example， if $(\overline{S_3}^3, S_4^4)$ is a constraint ， then its corresponding polynomial set $(S_3^3 + \overline{S_4}^4), (S_3^4 + \overline{S_4}^5), \cdots, (S_3^{K-1} + \overline{S_4}^K)$ will be added to the under verify polynomial sets.

C. *The Gröbner basis computing of polynomial set*

Gröbner basis theory applied widely, the irreducible *Gröbner* basis computation based on polynomial symbolic algebra is discussed in our paper. Some symbols are defined first: Let the n variable polynomial ring in field k represents as $A = k[x_1, x_2, \cdots, x_n]$.

Definition 2 (monomial ordering)

Let X_1 and X_2 be the product of variable x, Y_1 and Y_2 be the product of variable y .define:

$$X_1Y_1 < X_2Y_2 \Leftrightarrow \begin{cases} X_1 <_x X_2 \\ X_1 = X_2 \text{ and } Y_1 <_y Y_2 \end{cases} \quad (2)$$

From above, $<$ is term ordering, this term ordering called monomial ordering where variable x bigger than variable y .

Theorem 2 (monomial theorem)

Let I be the non-zero ideal of polynomial ring $k[y_1,\cdots,y_m,x_1,\cdots,x_n]$ in finite field k , term ordering $<$ is monomial ordering where variable x bigger than variable y ,Let $G=\{g_1,\cdots,g_t\}$ the *Gröbner* basis of ideal I ,then $G\bigcap k[y_1,\cdots,y_m]$ is the basis of ideal $I\bigcap k[y_1,\cdots,y_m]$.

Polynomial ring $A=k[x_1,x_2,\cdots,x_n]$ is the unique factor decomposition ring in finite field. The *Gröbner* basis generated problem can be solved with Theorem 2.the algorithm is shown as follows:

Algorithm1.the *Gröbner* basis generated based on PSA

step1: Let $f,g\in k[x_1,x_2,\cdots,x_n]$

step2: Let $d=\gcd(f,g)$ is the greatest common divisor of f and g （ $lc(d)=1$ ） d is computed by f and g .

step3: compute $l=lcm(f,g)$ is the least common multiple of f and g ， where $lc(l)=lc(f).lc(g)$

step4: compute $f.g=lcm(f,g)\gcd(f,g)$

$<lcm(f,g)>=<f>\bigcap<g>$

step5: get $\gcd(f,g)=\dfrac{fg}{lcm(g,f)}$

step6: compute the irreducible *Gröbner* basis G of ideal $<\omega f,(1-\omega)g>$ in ring $k[x_1,x_2,\cdots,x_n,\omega]$ according to monomial ordering of x less than ω .

D. Equivalence verification algorithm based on Grobner basis

Equivalence checking algorithm based on Grobner basis is shown in our paper; the detailed flow is shown in algorithm 2.

algorithm 2. Equivalence checking algorithm based on Grobner basis

input：sequential circuits L,S ;

output： $L=S$? (L,S equivalence or not)

{

Construct the polynomial set of L first; unroll L according to time frame.

Construct the polynomial set of S ; unroll S according to time frame.

/*compute the Grobner basis of L and S under their variable ordering */

for given time step n :

For(t=1;t<=n;t++)

{

If($L(t)!=S(t)$ break;

Elsif($t==n+1$)

Return(EQUAL);

}

Return(UNEQUAL);

IV. EXPERIMENT

Our verification experiment is conducted on Intel platform. All the verification work running with PowerEdge T410.the configuration is as follows (CPU:Xeon E5506, Frequency:2.13 GHz, Memory:4 GB, OS:Linux, Harddisk: 500GB).

To verify the experiment results, we selected seven common benchmark circuits, the size of these circuits are moderate, the representation time with an average time of about 15.20s, average verification time is about 161.3s, compared to existing verification methods [7], verification efficiency is improved with varying degrees. The corresponding result is shown in Table 1.

TABLE I. THE VERIFICATION EXPERIMENT RESULT WITH THE BENCHMARKS

circuit	Time frames	verification time of literature [6] (/s)	Time of Compute Grobner basis(/s)	Mining time + Time of Compute Grobner basis (/s)	Speed up
S1196	40	319.5	12.9	103.6	3.08
S1494	40	623.4	24.3	236.9	2.63
S4863	40	1423.3	35.8	421.3	3.38
S6669	30	146.9	41.2	86.1	1.71
S38417	30	352.6	32.4	152.8	2.31
b14	15	95.6	7.8	75.2	1.27
b21	15	125.6	10.3	57.6	2.18

From the experiment result in Table 1 we can see, although the polynomial decomposition in finite field can effectively reduce verification time, but the time cost of change sequential circuit into a polynomial algebraic symbol represents is also increased (including the Gröbner basis computing cost). But considering the whole time cost, there is a considerable advantage of our approach in solving the sequential circuit equivalence problem.

Figures 4 and 5 also compares time frame unroll with or without constraints. Experimental comparison shows effectiveness of our constraint extraction approach. The solid line represents the circuit unrolls with constraints. Dash line on behalf of the original circuit unrolls with no constraints. When the constraint extraction technique is incorporated herein our research, the unroll time frames corresponding to a significant increase. It shows that our constraint extraction method is effective.

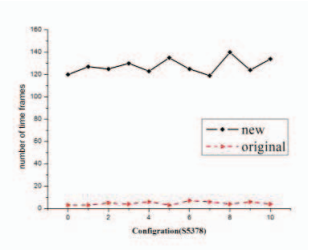

Fig.4. Timeframe unroll with or without constraints (S5378)

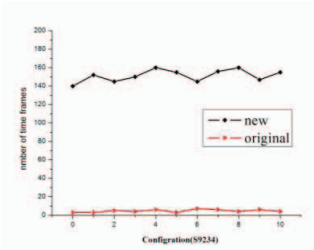

Fig.5.Timeframe unroll with or without constraints (S9234)

In addition, compared with the literature [6], our method also has advantage. literature[6] using the SAT-based verification engine, the verification cannot be effectively resolved in terms of complexity circuit, and the verification method in our paper works with word level polynomial representation and SMT computing engine is used, it can effectively cope with the complexity of the circuit. Comparative validation results for the same type of circuit in this paper under the constraints are shown in Figure 6 and Figure 7:

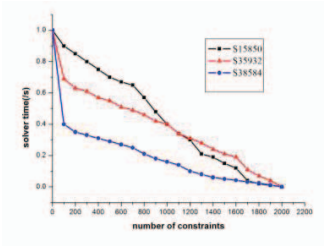

Fig.6.SAT solver with different constraints

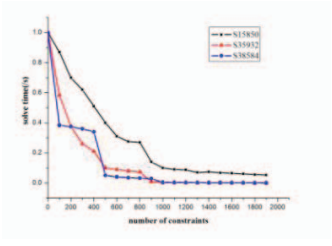

Fig.7. SMT solver with different constraints

From the comparison of two figures, it can be found that the processing time based on SMT method also has advantage than the method based on SAT engine. Our next work will concentrated in reducing circuit representation and complexity of Gröbner basis computing.

V. CONCLUSION AND PROSPECT

There has been some new research hotspot literature recently in this domain. Research [8-10] are conducted with formal verification techniques based on the algebraic polynomial symbol model in finite field, some results are achieved, it also shows the vitality of the polynomial symbolic algebra. Polynomial equivalence checking will continue to be a relatively new research direction on this basis. Our next work will focus on the use of symbolic algebraic polynomial model to establish and perfect sequential finite field arithmetic circuit verification.

VI. ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (No.51104157). The fundamental research funds for the Central Universities (2010NQA28)., National college students' entrepreneurial practice project (201310290080).the National Natural Science Foundation of China (Grant No. F020502).

REFERENCES

[1] Paruthi, V.. Large-scale application of formal verification: From fiction to fact , Formal Methods in Computer-Aided Design (FMCAD), 2010 .175-180P

[2] Stoffel, D.; Wedler, M.; Warkentin, P.; Kunz. W. Structural FSM traversal .IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2004, 23(5) : 598 – 619P

[3] P.Savoj, H.; Berthelot, D.; Mishchenko, A.; Brayton, R.Combinational techniques for sequential equivalence checking Formal Methods in Computer-Aided Design (FMCAD), 2010 .145 - 149 P

[4] LI Guang-hui,ZENG Song-wei. Research on Storage Elements Mapping for Sequential Equivalence Checking, computer science.2009,36(4):285- 288P

[5] Han Jia wei, Pei Jian, Yin Yi wen.Mining frequent patterns without candidate generation[C].Proc of the ACMSIGMOD Int conf on Management of Data.New York: ACM, 2000:1-12.

[6] Chia-Ling Chang.Speeding up Bounded Sequential Equivalence Checking with Data Mining.[D].National chiao Tung university.2009.

[7] W.Wu and M.S.Hsiao.Mining Global Constraints for improving Bounded Sequential Equivalence Checking. In Proc Design Automation Conf.(DAC), 2010,743-748P

[8] Yang Zhi,Ma Guangsheng,and Zhang Shu..Equivalence Verification of High-Level Datapaths Based on Polynomial Symbolic Algebra.Journal of Computer Research and Development,2009,46(3):513-520P

[9] Theo A.Drane and George A.Constantinides.Leap in formal verification of Datapath.2011,www.dac.com.,1-14P

[10] Lv J, Kalla P, Enescu F. Efficient Gröbner Basis Reductions for Formal Verification of Galois Field Arithmetic Circuits[J]. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 2013, 32(9): 1409-1420.