第 40 卷 第 1 期 计 算 机 工 程 2014 年 1 月
Vol.40 No.1 Computer Engineering January 2014

·开发研究与工程应用· 文章编号：1000—3428(2014)01—0301—04 文献标识码：A 中图分类号：TP331

基于 Mining-SEC 方法的电路等价性验证

王冠军[a]，童敏明[b]，周 勇[a]，赵 莹[a]

(中国矿业大学 a. 计算机科学与技术学院；b. 信息与电气工程学院，江苏 徐州 221116)

摘 要：针对时序电路的等价性验证难题，提出基于 Mining-SEC 的定界等价性验证方法。将待验证时序电路按时间帧展开为多项式符号代数表示的电路集合，利用时间序列数据挖掘方法挖掘其中的不变量和相应的全局约束，不变量可以是任意多项式。此外还可挖掘电路中的不合法约束和复杂的多项式关系，通过以上方法可以明显降低求解空间。使用基于 SMT 的验证引擎检验电路等价性。实验结果表明，该方法可以快速地实现验证收敛，得到平均 1~2 个量级的验证加速，并且可以有效消除虚假验证。

关键词：时间序列；数据挖掘；多项式符号代数；时序电路等价性检验；可满足性模理论；虚假验证

Equivalence Verification of Circuits Based on Mining-SEC Approach

WANG Guan-jun[a], TONG Min-ming[b], ZHOU Yong[a], ZHAO Ying[a]

(a. School of Computer Science and Technology; b. School of Information and Electrical Engineering, China University of Mining and Technology, Xuzhou 221116, China)

【Abstract】This paper researches the sequential circuit equivalence verification problem. Bounding equivalence verification method based on Mining-Sequential Equivalence Checking(SEC) is put forwarded. To be verified sequential circuit is expansion to a set of Polynomial Symbolic Algebra(PSA) representation in accordance with time frame. The invariants and global constraints are mined over the expression database according to time series. The invariants can be arbitrary polynomial. Moreover, the approach can also mine the illegal constraints and complex polynomial relationship, with this the solving space is pruned dramatically. The equivalence verification approach based on Satisfiablity Module Theory(SMT) engine is proposed. Experimental result shows that the approach can realize rapid convergence, 1~2 order of magnitude verification speedups is achieved and false verification is eliminated effectively.

【Key words】time series; data mining; Polynomial Symbolic Algebra(PSA); Sequential Equivalence Checking(SEC); Satisfiablity Module Theory(SMT); false verification

DOI: 10.3969/j.issn.1000-3428.2014.01.065

1 概述

时序电路等价性检验(Sequential Equivalence Checking, SEC)成为功能验证中的一项重要工作。目前时序电路的等价性验证有相当多的困难和挑战。传统的时序电路的等价性验证，通常采用基于有限状态机遍历的方法[1]。这类方法只能在逻辑门级上进行且计算复杂度太高，往往只能应用到小规模的设计验证，对于大型的实际设计，它们显得无能为力。另外一类方法是将时序电路等价性验证转化为组合电路等价性验证[2]。此类方法可以提高验证速度，但计算复杂度和计算代价较高。而当前基于数据挖掘技术的等价性验证成为研究热点[3-5]，这些方法利用数据挖掘技术对电路的布尔表达式进行挖掘，主要提取表达式中的各种不变量和全局约束，利用挖掘结果减少验证中的解空间搜索，上述方法在解决等价性验证中能够得到较好的验证加速，所以日益引起研究人员的重视。

本文在上述研究的基础上对 SEC 进行新的尝试。基于电路的多项式符号代数(Polynomial Symbolic Algebra, PSA)表示，在 RTL 级上进行时序电路的等价性验证。首先将待验证时序电路按时间帧展开为多项式符号代数表示的电路集合，利用时间序列数据挖掘技术搜索表达式中的不变量和各种全局约束，同时找出不合法的状态集，使用基于 SMT 引擎的等价性验证算法检验等价性。基于 SMT 的技术目前被广泛使用在各种解决 SEC 的方法中[6-8]。主要方法包括定

基金项目：国家自然科学基金资助项目(51104157)；中央高校基本科研业务费专项基金资助项目(2010NQA28)；国家大学生创业实践基金资助项目(201310290080)

作者简介：王冠军(1981－)，男，讲师、博士，主研方向：CAD/EDA 技术，机器人技术；童敏明，教授、博士生导师；周 勇，副教授；赵 莹，讲师、博士

收稿日期：2012-12-07 **修回日期：**2013-02-17 **E-mail：**zywgj@cumt.edu.cn

界模型检验(BMC)和无界模型检验(UMC)以及各种约束提取方法。

2 相关研究

2.1 时间序列数据挖掘

时间序列数据挖掘：基于一个或多个时间序列的数据挖掘称为时间序列数据挖掘，它可以从时序中抽取时序内部的规律用于时序的数值、周期、趋势分析和预测等。

由于时间序列数据挖掘的研究受到人们的广泛关注，加之数据挖掘研究领域的拓展，时间序列数据挖掘的研究发展迅速，其研究内容涵盖了时间序列的各个方向：分类和聚类，相似模式匹配，周期模式挖掘，序列模式挖掘，异常检测，分段研究等。时间序列分析方法中用得比较多的主要有概率模型和谱分析 2 种基本方式，其中，概率模型是研究得最为深入的时间序列分析方法，回归模型和随机过程模型是概率模型的主要研究内容。

2.2 多项式符号表示和运算

2.2.1 一元多项式的定义

一个一元多项式 $P_n(x)$ 可按升幂写成：

$$p_n(x)=p_0+p_1x+p_2x^2+\cdots+p_nx^n \tag{1}$$

它由 $n+1$ 个系数唯一确定。因此，在计算机里，它可以用一个线性表 p 来表示：

$$p=(p_0,p_1,p_2,\cdots,p_n)$$

每一项的指数 i 隐含在其系数 p_i 里。然而，在通常的应用中，多项式的次数可能很高且变化很大，使得顺序存储结构的最大长度很难确定。一般情况下的一元 n 次多项式可写成：

$$p_n(x)=p_0+p_1x^{e_1}+p_2x^{e_2}+\cdots+p_mx^{e_m} \tag{2}$$

其中，p_i 是指数为 e_i 的项的非零系数，且满足 $0\leqslant e_1\prec e_2\prec\cdots\prec e_m=n$，若用一个长度为 m 且每个元素有 2 个数据项的线性表：

$$((p_1,e_1),(p_2,e_2),\cdots(p_m,e_m)) \tag{3}$$

便可唯一确定多项式 $P_n(x)$，采用线性链表的数据结构可以实现一元多项式的表示和运算[9]。

2.2.2 一元多项式的运算

一元多项式的运算有如下 2 种：

(1)加法运算

多项式相加的运算规则相对简单，2 个多项式中所有指数相同的项，对应系数相加，若和不为 0，则构成和多项式中的一项，所有指数不同的项均复制到和多项式中。

(2)乘法运算

2 个一元多项式相乘的算法，可以利用 2 个一元多项式相加的算法来实现，因为乘法运算可以分解为一系列的加法运算。假设 $A(X)$ 和 $B(X)$ 为 2 个一元多项式，则两者乘积：

$$M(x)=A(x)\times B(x)=A(x)\times[b_1x^{e_1}+b_2x^{e_2}+\cdots b_nx^{e_n}]=\sum_{i=1}^{n}b_iA(x)x^{e_i} \tag{4}$$

2.2.3 多元多项式的符号表示

域上的多元多项式表示为：

$$f(x_1,x_2,\cdots,x_n)=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \tag{5}$$

其中，若每项全是 m 次的，则称它是域上的一个 n 元 m 次齐次多项式。

设 $f(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$，且有 $\deg(f(x_1,x_2,\cdots,x_n))=m$，把 $f(x_1,x_2,\cdots,x_n)$ 中次数为 i $(i=1,2,\cdots,m)$ 的所有单项式的和记作 $f_i(x_1,x_2,\cdots,x_n)$，它是 i 次齐次多项式，叫做 $f(x_1,x_2,\cdots,x_n)$ 的 i 次齐次成分。由于当 $i\neq j$ 时，$f_i(x_1,x_2,\cdots,x_n)$ 与 $f_j(x_1,x_2,\cdots,x_n)$ 的项不交叉、无重复，因此 $f(x_1,x_2,\cdots,x_n)$ 可唯一地表示为所有不同 i 次齐次成分之和：

$$f(x_1,x_2,\cdots,x_n)=\sum_{i=0}^{m}f_i(x_1,x_2,\cdots,x_n) \tag{6}$$

2.2.4 多元多项式运算

定义 1 域 k 上的 2 个 n 元多项式 $f(x_1,x_2,\cdots,x_n)=\sum_{\alpha}a_\alpha X^\alpha$ 与 $g(x_1,x_2,\cdots,x_n)=\sum_{\alpha}b_\alpha X^\alpha$ 的运算定义如下[10]：

(1)相等：

$$f=g\Leftrightarrow\forall\alpha,\beta(\alpha=\beta\rightarrow a_\alpha=b_\beta)$$

(2)相加：

$$f+g=\sum_{\alpha}(a_\alpha+b_\alpha)X^\alpha$$

(3)相减：

$$f-g=f+(-g)$$

其中，$-g=\sum_{\alpha}(-b_\alpha)X^\alpha$；$-b_\alpha$ 为 b_α 在域 k 中的加法逆元。

(4)相乘：

$$f\times g=\sum_{\gamma}(\sum_{\alpha+\beta=\gamma}a_\alpha\times b_\beta)X^\gamma$$

3 基于 Mining-SEC 的等价性验证

本文将时间序列数据挖掘技术应用到了时序电路的等价性检验中。对于时序电路的等价性证明需要使用到以下定理：

定理 假定 2 个时序电路 L 和 S，它们具有相同的 PIs 和 POs。对 L 和 S 的触发器使用一对一映射形成 $<S^n,L^k>$，假定 $<S^n,L^k>=L^{n+k}$，那么 $L=S$。L、S 具有相同的初始状态，n、k 为时间帧。

借助以上定理将待检验电路 L 和电路 S 表示为多项式集合形式，$L=\{l\,|\,l$ 为按时间帧展开的多项式表示$\}$，$S=\{s\,|\,s$ 为按时间帧展开的多项式表示$\}$。验证 L 是否等于 S，首先利用 Mining-SEC 方法找出其中的约束和不变量，寻找约束和不变量的方法较为成熟，典型的方法参见

文献[11-12]，在获得约束和不变量后，利用约束和不变量进行解空间缩减，最后使用SMT验证引擎进行等价性判断，若 $L=S$，则两电路等价。完整的验证流程如图 1 所示。

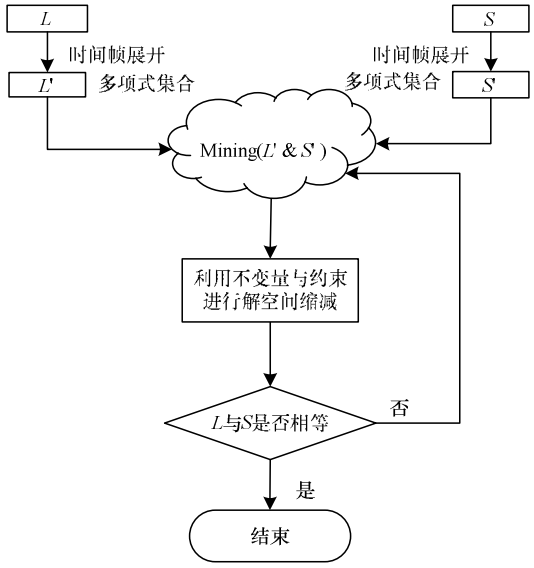

图 1　基于 Mining-SEC 的时序等价性验证

3.1　时序电路的多项式表示

首先讨论的时序电路仅限于同步时序电路。假定 S 是时序电路上状态变量的集合。对同步时序逻辑电路来说，集合 S 由所有输入变量和所有触发器的输出变量组成。一个状态是集合 S 中的各元素赋以确定的值后所得到的一个向量，即电路的一个状态，用 $<s_1 s_2 \cdots s_n>$ 表示，v_i 是电路中的一个多项式变量。S 是由所有电路状态组成的集合。电路中所有的状态转移均由转移关系表示。将时序电路转化为多项式的集合表示时要用到以下定义：

定义 2 对于一个状态转换系统 Ts，它从初始状态出发，连续展开 k 个时序对应的多项式集合递归地定义为：

$$[[Ts]]_0 = \tau(\phi_0)[X / X[0]]$$

其中，$\phi_0 = \vee_{s\in s_0}(\wedge_{\alpha\in L(S)}\alpha)$，并且对 $k=1$，有：

$$[[Ts]]_k = Gbasis([[Ts]]_{k-1} \cup T(X[k-1], X[k]), \prec)$$

其中，$\prec$ 为一个合适的项序。

对有 m 个输入和 n 个触发器的电路来说，$S=<x_0, x_1, \cdots, x_{m-1}, s_0, s_1 \cdots s_{n-1}>$(其中，$x_i$ 为输入变量；v_j 为内部状态变量)，$S=<x_0, x_1, \cdots, x_{m-1}, s_0, s_1, \cdots, s_{n-1}>$ 是电路的当前状态，$S'=<x_0', x_1', \cdots, x_{m-1}', s_0', s_1', \cdots, s_{n-1}'>$ 是电路的下一状态。对于每一个内部状态变量 s_j'，都有一个约束函数 f_j 使得：$s_j' = f_j(s_j)$。这样，任意一个同步时序电路均可按时间帧展开为多项式函数 $f_t'(x) = f_t(x_0', x_1', \cdots, x_{m-1}', s_0', s_1', \cdots, s_{n-1}')$(其中，$x_i'$ 为输入变量在 t 时刻取值；v_j' 为 t 时刻内部状态量)。假定同步时序电路的时间帧为 n，则可得到电路的多项式集合为 $f(x) = \{f_{t_1}(x), f_{t_2}(x), \cdots, f_{t_n}(x)\}$ ($f_{t_i}(x)$ 为 t_i 时间帧的多项式函数)。

3.2　时序电路的多项式表示

本节给出基于 Mining-SEC 方法的等价性算法，具体算法如下：

算法 基于Mining-SEC方法的时序电路等价性验证算法

输入 时序电路 L、S

输出 L=S ?(即电路 L、S 是否等价)

{首先构造电路 L 对应的多项式集合；按时间帧展开电路 L；然后同样构造电路 S 对应的多项式集合；按时间帧展开电路 S;

/*调用 Mining-SEC 方法计算 L、S 在各自结点变元排序之下的不变量(Invariant)和全局约束集 Constraint Set*/

对于给定的时间步 n:

```
For(t=1; t<=n; t++)
{ while(satisfy(Constraint Set))
  { Search(L,S); //利用 Invariant 降低解空间
    If(L(t)!=S(t) break;
    Elseif(t==n+1)
      Return(EQUAL);
  }
}
Return(UNEQUAL);
```

4　实验验证

实验环境设置如下：所有验证在 SUN Ultra 40 M2 上完成，硬件参数：CPU 类型 AMD Opteron；CPU 主频 2.2 GHz；操作系统 Solaris 10 Pre-Installed；内存容量 4 GB；随机硬盘容量 250 GB)。

SMT 验证引擎(Mining-SEC checker)利用 C++语言实现。为便于比较验证结果，选取了 9 个常见的 ISCAST 和 ITC 实验电路，如表 1 所示，电路规模适中，电路平均表示时间为 37.80 s 左右，平均验证时间为 269.93 s 左右，和传统的验证方法相比，验证效率均有不同程度的提高。

表 1　常见 benchmark 时序电路验证结果

实验电路	电路门数	表示时间/s	验证时间/s
S832	429	3.46	0.14
S1494	531	4.55	0.20
S4863	1 817	9.12	0.56
b09gray_onehot	2 908	112.34	1 945.89
b10gray_onehot	13 940	25.34	46.53
b11gray_onehot	5 924	40.21	102.60
b12gray_onehot	13 169	60.36	315.43
b14	5 924	30.21	2.60
b21	8 954	21.35	15.43
平均	5 955	37.80	269.93

本文方法属于动态多目标优化问题。实验结果表明，本文方法在最坏情况下也可以在多项式时间内完成，但是使用并行计算技术却不能获得良好的加速效果。一般说来，任何 SEC 都可表示为线性规划(LP)问题解决，且

能在多项式时间内完成，但多项式的幂次较高。实际上 SEC 问题是 P-hard 问题，P 类复杂性问题使用串行算法可在多项式时间内解决，其中的一些问题使用多个处理器(K 个)和并行算法能在 $O(\log(n)^K)$ 时间内完成。因此，从这个角度来说，本文算法属于 NC 问题，那么 NC 是否等于 P，这个问题上笔者认为是相等的(也有人认为是不等的)，目前双方均没有找到相应的理论证明。

此外，从表 1 的实验综合结果来看，虽然域上多项式分解可以有效地降低验证时间，但与此同时时序电路转化为多项式符号代数表示时间耗费相应增加(包括计算不变量和全局约束的时间耗费)。但综合计算以上时间，本文方法在解决时序电路等价性时还有相当的优势，下一步的工作可以在减少电路的表示复杂度和提高挖掘效率等方面进行研究。

5 结束语

本文给出一种时序电路中通过挖掘触发器复杂多结点多项式关系进行等价性验证的新方法。该方法利用时序电路的多时帧展开挖掘触发器中的不合法约束和复杂的多项式关系，这是对原有的基于布尔表达式的 SEC 的一种扩展，通过上述方法可以大幅降低等价性验证的求解空间，提高求解效率。下一步的工作主要集中于提取高质量的约束来继续降低搜索工作量以及验证复杂和大型电路设计，并将该方法集成到下一代的工业验证工具中。

参考文献

[1] Stoffel D, Wedler M, Warkentin P, et al. Structural FSM Traversal[J]. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, 2004, 23(5): 598-619.

[2] Savoj H, Berthelot D, Mishchenko A, et al. Combinational Techniques for Sequential Equivalence Checking[C]//Proc. of Conference on Formal Methods in Computer-aided Design. [S. l.]: ACM Press, 2010: 145-149.

[3] Goel N, Hsiao M S, Ramakrishnan N, et al. Mining Complex Boolean Expressions for Sequential Equivalence Checking[C]// Proc. of the 19th IEEE Asian Test Symposium. Washington D. C., USA: IEEE Computer Society, 2010: 442- 447.

[4] Hu Wei, Huy N, Hsiao M S. Sufficiency-based Filtering of Invariants for Sequential Equivalence Checking[C]//Proc. of IEEE International High Level Design Validation and Test Workshop. [S. l.]: IEEE Press, 2011: 1-8.

[5] Chang Chia-Ling, Wen C H P, Bhadra J. Speeding up Bounded Sequential Equivalence Checking with Cross-timeframe State-pair Constraints from Data Learning[C]//Proc. of International Test Conference. [S. l.]: IEEE Press, 2009: 1-8.

[6] Kong Weiqiang, Katahira N, Qian Wanpeng. An SMT-based Approach to Bounded Model Checking of Designs in Communicating State Transition Matrix[C]//Proc. of International Conference on Computational Science and Its Applications. [S. l.]: IEEE Press, 2011: 159-167.

[7] 赵燕妮, 边计年, 邓澍军. 利用 SMT 约束分解方法求解 RTL 可满足性问题[J]. 计算机辅助设计与图形学学报, 2010, 22(2): 234-239.

[8] Milicevic A, Kugler H. Model Checking Using SMT and Theory of Lists[C]//Proc. of the 3rd International Conference on NASA Formal Methods. Berlin, Germany: Springer-Verlag, 2011: 282-297.

[9] 杜振军. 布尔过程论及其在复杂高速芯片设计自动化应用中的研究[D]. 哈尔滨: 哈尔滨工程大学, 2003.

[10] 王冠军. 基于 PSA 和有限域理论的高级综合研究[D]. 哈尔滨: 哈尔滨工程大学, 2009.

[11] Lu Feng, Cheng Kwang-Ting. SEChecker: A Sequential Equivalence Checking Framework Based on K-th Invariants[J]. IEEE Transactions on Very Large Scale Integration Systems, 2009, 17(6): 733-746.

[12] Wu Weixin, Hsiao M S. Mining Global Constraints for Improving Bounded Sequential Equivalence Checking[C]// Proc. of the 43rd Annual Design Automation Conference. New York, USA: ACM Press, 2006: 743-748.

编辑 顾逸斐

(上接第 300 页)

[7] 谢志强, 辛 宇, 杨 静. 基于设备空闲事件驱动的综合调度算法[J]. 机械工程学报, 2011, 47(11): 139-147.

[8] 谢志强, 李志敏, 郝淑珍, 等. 工序间存在零等待约束的复杂产品调度研究[J]. 自动化学报, 2009, 35(7): 983-989.

[9] Xie Zhiqiang, Hao Shuzhen, Ye Guangjie, et al. A New Algorithm for Complex Product Flexible Scheduling with Constraint Between Jobs[J]. Computers & Industrial Engineering, 2009, 57(3): 766-772.

[10] Xie Zhiqiang, Ye Guangjie, Zhang Dali, et al. New Non-standard Job Shop Scheduling Algorithm[J]. Chinese Journal of Mechanical Engineering, 2008, 21(4): 97-100.

[11] 谢志强, 王 悦, 杨 静. 存在批量为 2 的批处理设备的综合调度算法[J]. 北京工业大学学报, 2011, 37(10): 1470- 1476, 1481.

[12] 谢志强, 杨 静, 杨 光, 等. 可动态生成具有优先级工序集的动态 Job-Shop 调度算法[J]. 计算机学报, 2008, 31(3): 502-508.

[13] 谢志强, 邵 侠, 杨 静. 存在设备无关延迟约束的综合柔性调度算法[J]. 机械工程学报, 2011, 47(4): 177-185.

[14] 熊禾根, 李建军, 孔建益, 等. 考虑工序相关性的动态 Job Shop 调度问题启发式算法[J]. 机械工程学报, 2006, 42(8): 51-55.

编辑 顾逸斐