

组合电路等价性检验方法研究

曾 琼^{1,2}, 闫 炜¹

(1. 中国科学院成都计算机应用研究所, 成都 610041; 2. 成都信息工程学院计算机基础教学部, 成都 610041)

摘 要: 分析了数字电路等价性检验方法的基本原理, 对组合电路等价性检验方法进行了综合研究, 讨论了各种方法的特点, 指出了各种方法的优缺点及其适用场合, 总结了组合电路等价性检验方法的发展规律, 指出了未来的发展方向。

关键词: 等价性检验; 组合电路; 二叉判定图; 布尔可满足; 自动测试向量产生

Research on Combinational Circuits Equivalence Check Method

ZENG Qiong^{1,2}, YAN Wei¹

(1. Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu 610041;

2. Department of Computer Teaching, Chengdu University of Information Technology, Chengdu 610041)

【Abstract】 This paper analyzes general equivalence checking methods, discusses combinational equivalence checking methods, studies characteristics and applications of the methods. At the end of this paper, laws of evolution of combinational equivalence checking are summarized and the direction of study on the combinational equivalence checking is indicated.

【Key words】 Equivalence check; Combinational circuits; Binary decision diagram(BDD); Boolean satisfiability; Automatic test pattern generation (ATPG)

1 概述

随着芯片规模和复杂度的急剧增加, 大型设计的功能验证越来越困难和重要, 功能验证已经成为 SoC 设计的瓶颈。形式化验证方法是保证设计正确性的一条重要途径。它通过数学方法表达系统的刻画或系统的性质, 并根据数学理论来证明所设计的系统满足系统的刻画或具有期望的性质, 在不能证明所期望的性质时, 则可能发现设计错误。它是一种静态的验证方法, 可以节省大量的验证时间。一般来说, 形式化验证方法可以分为等价性检验、模型检验和定理证明方法。等价性检验是证明 2 个不同表示形式的设计具有相同的功能; 模型检验是证明设计满足给定的性质, 它适合于验证 RTL 设计的正确性; 定理证明是通过构造设计的数学模型, 并将需要验证的性质形式化为定理加以证明。目前定理证明还不如前两类方法成熟, 工业界还不多见^[1]。等价性检验是目前集成电路设计验证中应用最为广泛的形式化方法。

组合电路等价性检验通常包括功能性和结构性的验证方法^[2]。功能性方法是将电路表示成一种规范形式, 2 个电路等价, 当且仅当它们的规范形式同构。常用的规范形式有真值表、ROBDD 和 *BMDs^[2]等, 通常为了验证 2 个电路的原始输出是等价的, 需要按相同的输入变量序分别构造这 2 个输出函数的 ROBDD, 然后判断它们是否同构。但是表示一个布尔函数的 ROBDD 的大小依赖于变量排序, 常遇到内存爆炸的问题。结构性方法是通过识别电路内部的等价对, 并利用这些等价对的功能蕴含来简化验证任务。内部等价对常被称为断点(cutpoint), 识别潜在断点的常用方法有随机模拟、ATPG 方法、基于 BDD 的方法以及基于可满足性的方法。所有潜在的断点找出后, 依据一定的准则, 将整个系统验证分解为关于这些断点子集的较小验证任务, 分别进行验证。但是在选择断点的过程中可能出现误判问题(false negative)^[1],

即原本等价的 2 个电路被判为不等价。通常消除误判需花费较多的时间。组合电路等价性检验在数字电路验证过程中具有十分重要的意义, 它是当前研究热点。

2 数字电路等价性检验方法

等价性检验的主要目的是在一个设计经过变换之后, 穷尽地检验变化前后的功能一致性。即证明设计的变换没有产生功能的变化。它可以用来验证 2 个不同抽象级别的设计之间的功能等价性, 例如在 RTL 设计流程中验证 RTL 设计与门级设计、门级设计与门级设计、RTL 设计与 RTL 设计的等价性。它的基本原理是建立被比较的 2 个模型之间的关系。通常等价性检验程序能自动比较 2 个设计的关系, 而不需要用户的输入。它的优点是使用简单, 且很容易集成到设计流程中^[2]。下面简单介绍组合电路与时序电路的等价性检验方法的基本原理。

2.1 组合电路等价性检验方法

传统的组合电路等价性检验是通过构造 2 个电路的规范表示形式, 如 ROBDD。当且仅当它们的规范形式同构时, 2 个电路功能等价。BDD 的大小对原始输入变量排序极为敏感, 当电路规模较大时, 基于 BDD 的验证方法可能引起内存爆炸。为了克服这种局限性, 一般采用基于结构相似性的增量验证方法^[1]。因为在设计流程的 2 个设计版本之间通常保留了大量的结构相似性, 所以可利用这些相似性将整个电路的验证简化为一些较小的验证任务, 增量地完成。即首先使用随机模拟、名称信息或拓扑分析等方法, 产生候选等价对,

基金项目: 国家自然科学基金资助项目(60373113); 国家“973”计划基金资助项目(2004CB318000)

作者简介: 曾 琼(1976—), 女, 硕士、讲师, 主研方向: 形式化刻画与验证; 闫 炜, 博士

收稿日期: 2006-03-13 E-mail: zmiao106@yahoo.com.cn

然后按扇入优先的拓扑顺序，逐步简化电路，最后选择合适的方法验证各候选等价对是否等价。常用的方法有 BDD, ATPG, SAT、可置换性及递归学习、多种算法相结合的方法^[3]。增量验证算法的主要步骤如下：

```
Verify(circuit specification, circuit implementation)
{
    Generate candidate list;
    Sort candidates in fanin-first topological order;
    For each candidate pair (u, v) in list
    {
        check(u, v);
        if (u equal to v)
            add pair (u, v) to the equivalent list;
    }
    if (all corresponding primary output pairs are in the equivalent list)
        return SUCCEED;
    else
        return FAILED;
}
```

2.2 时序电路等价性检验方法

对于规模不大的时序电路，使用有限状态机遍历的方法，即把 2 个电路看成有限状态机，构造它们的积自动机，如图 1 所示。

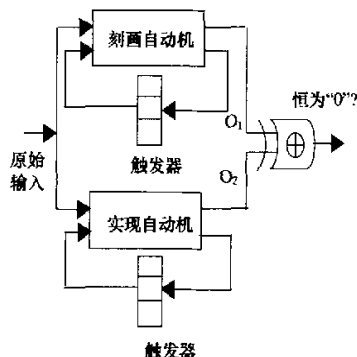


图 1 积自动机

Brand^[3]将这种计算模型称为 miter。它是通过把 2 个状态机相应的每一对原始输入连接到一起，同时把相应的每一对原始输出连接到一起，而这些异或门就构成了积自动机的输出。如果对于每一个输入序列，积自动机的每个原始输出恒为 0，那么 2 个电路等价。即对于任何输入向量和可达状态，积自动机的原始输出响应总为 0。证明状态机等价性的第 1 步是从初始状态开始，计算所有可达状态。该过程是基于有限状态机遍历的。尽管最近十多年里，由于 BDD 方法的研究进展使得基于有限状态机遍历算法有了很大进步，但对大型设计仍然可能会因构造 BDD 的表示导致内存爆炸^[1]。当时序电路规模较大时，可以采用类似组合电路验证的基于结构相似性的增量方法。虽然基于结构相似性的增量方法可以验证较大规模的电路，但是等价性检验方法关于设计的输入数和触发器数目的最坏情况复杂度仍然是指数式的。对于百万门级的大型设计，尤其是含有许多触发器时，使用有限状态机遍历的方法常会因状态空间太大而引起内存爆炸。实际的 EDA 厂商推出的等价性检验工具大都采用组合验证方法来验证时序电路。然而当 2 个电路不存在触发器的一一对应关系时，上述方法失效，只能应用状态遍历的验证方法，导致其处理能力非常有限。时序电路的形式验证一直是困扰学术界的难题，如何发挥组合验证技术的优势与提高处理能力是急需解决的关键问题。

3 组合电路等价性检验经典算法

组合电路等价性检验是工业界设计验证中的重要组成部分。BDD、SAT 和 ATPG 方法是组合电路等价性检验中常用的经典算法。下面以 BDD、SAT 和 ATPG 方法为中心，对已有的一些较为成熟的算法进行回顾，并对其优缺点进行了分析和评述。

3.1 基于 BDD 的组合电路等价性检验方法

BDD 是 Akers 在 1978 年提出的一种表示和操作布尔函数的有效方法，1986 年 Bryant 又提出了 OBDD，它是正则的布尔函数表示。OBDD 是一个具有 1 个根结点和 2 个终结点的有向无环图；将电路的状态集合、转换关系及状态遍历都映射为布尔函数，每个结点对应一个布尔函数，布尔函数常用操作均可在 BDD 上通过图的遍历方法实现。

基于 BDD 的组合电路等价性检验方法采用结构性检验方法，结合功能性方法进行验证。首先提取 2 个被比较电路的内部相似性，推导出各断点之间的关系，如等价性、蕴涵及可置换性等。然后使用这些关系，把等价性检验过程分解为关于这些断点子集的较小的验证任务，分别完成。算法从原始输入向原始输出方向遍历 2 个电路，从已知断点演绎出新的断点，直到所有的相应原始输出被证明等价，或找到某个输入向量使得 2 个电路输出不匹配。

它可以分为 3 个阶段：(1)对 2 个电路做适量的、一致的随机模拟，比较各结点的输出响应，将具有相同特征的结点作为潜在断点。(2)利用 ROBDD 按次序验证潜在断点的等价性。如果当前结点对被证明是等价的，便加入到等价结点表中。(3)检验所有的原始输出对是否在等价结点表中，如果是，则 2 个电路等价；否则不等价。

为了验证一对候选结点的等价性，需要利用已知的断点来推导。使用全局 BDD 表示布尔函数常碰到内存爆炸问题，如果能够找到某个合适的断点集，即结点的迁移扇入集(TFI)的割集(cutset)，那么只需比较这对结点关于该割集的局部 BDD，即根据割集中的元素，而不是原始输入来表示 BDD，便能检验它们的等价性。

Y Matsunaga^[4]提出使用启发式方法导出合适的割集，即：(1)包含在候选结点迁移扇入集中较多个元素的 TFI 中的结点，即如果从该结点到候选结点有较多的通路，应选入割集。(2)结点之间存在迁移扇入或扇出的关系的结点同时选入割集中，可能发生误判问题。相互独立的结点应选入割集。对于消除误判，Matsunaga 提出使用 BDD 进行功能蕴涵的方法。这种方法往往由于 BDD 过大而导致算法失效。

实验结果表明，基于 BDD 的方法对 C432 电路，在 P4 PC 机上的运行时间是 0.04s，它能够在很短的时间内验证一些规模较小的电路的等价性，但是它不能有效地表示一些重要的布尔函数，尽管应用了有效的启发式方法进行变量排序，仍存在内存爆炸问题。对于上千门的电路往往会由于 BDD 呈指数增长而导致算法失效。在实际应用时，通常结合 ATPG 的方法来提高算法的效率。

3.2 基于 SAT 的组合电路等价性检验方法

SAT 方法的主要思想是把等价性检验问题转化为可满足性问题^[2]。它把异或门应用到 2 个待比较的电路中。电路 F 和电路 G 等价当且仅当对所有的输入都不会使 miter 输出 1。SAT 问题是一个著名的 NP 完全问题，在最坏的情况下，其复杂度呈指数增长。研究 SAT 算法具有重大的理论和实践意义。

在分析 SAT 算法前, 首先引入几个基本概念。n 个布尔变量 x_1, \dots, x_n 的合取范式(CNF)是 m 个子句 $\omega_1, \dots, \omega_m$ 的合取, 而每个子句是一个或多个文字的析取, 这里文字是指布尔变量 x 及其否定形式 x' 。SAT 算法的基本思想是选取变量并赋值 1, 如果所有子句都可满足, 则 CNF 范式可满足, 否则进行回溯, 并对变量赋值 0 继续, 如果回到初始状态, 则 CNF 范式不可满足。

组合电路的 CNF 公式是指电路中每个门输出对应的 CNF 公式的合取, 而每个门的 CNF 公式表示了该门的有效输入/输出赋值关系。对 miter 对应的 CNF 公式, 如果 miter 输出赋值为 1 时可满足, 则 2 个电路不等价; 反之则等价。当 miter 输出为 1 时, 如果至少存在一组赋值, 使得 miter 对应 CNF 公式为 1。即存在一组原始输入赋值, 使得 2 个待验证电路输出值不相等, 则这 2 个电路不等价。

迄今为止, 已经提出了许多 SAT 算法, 从最初的 Davis-Putnam 和 DPLL 算法, 到最近的回溯搜索算法^[5]以及局部搜索等算法。目前, 随着高效可满足性解算器诸如 zChaff^[5]等的提出, 可满足性解算器已日益显示出其强健的和灵活的推理能力, 也已成为重要验证引擎之一。可满足性解算器结合了高级修剪技术和新的策略来对问题空间的搜索。有效的搜索修剪技术主要是基于 no-good 学习, 基于制导的回溯、回跳等技术。而新近高效的搜索策略则对回溯搜索组织引入了变奏, 如弱提交搜索、搜索重新启动和随机回溯等技术。

SAT 算法在使用 zChaff 可满足性解算器进行推理前, 采用了多种方法来简化验证任务。实验表明, 使用基于 SAT 的方法对无冗余的 C432 电路进行等价性检验, 在 SUN ULTRA 10 工作站上的运行时间是 0.7s。SAT 其实是牺牲时间换取节省内存空间。SAT 方法适合于解决较大规模组合电路等价性检验。

3.3 基于 ATPG 的组合电路等价性检验方法

SAT 是对 CNF 范式求解可满足性问题, 而 ATPG 是直接布尔网上求解可满足性问题。ATPG 即自动测试向量产生, 原来是在模拟测试中用来诊断电路故障的, 这里用来证明联接电路的输出是恒为 0 是否可测。如果不可测, 则原来 2 个电路等价, 否则就不等价。ATPG 直接在电路结构上求解可满足性问题, 与电路结构关系很紧密, 其算法也具有这个特点。在 ATPG 算法中, 蕴涵、确认和传播是 3 个基本和重要的操作。常用的 ATPG 算法主要有 D 算法、九值算法、PODEM 算法和 FAN 算法等。其中, FAN 算法是目前国际上公认的比较有效的测试产生方法。它有效地减少了在测试产生中的回溯次数和缩短了回溯之间的处理时间。例如, 对 C7552 电路,

PODEM 算法和 FAN 算法的运行时间之比为 10/1。在此之后的许多改进方法都是基于 FAN 算法做出的或是改进推广了 FAN 的技术。

使用 ATPG 方法在进行等价性检验时, 占用的内存较少, 但大量回溯时间复杂度较高。近年来, 递归学习的算法也有长足的进步。该算法的主要思想是尽可能地找出数字硬件逻辑图中, 各个逻辑端口之间的逻辑约束关系(指直接和间接逻辑蕴涵关系), 这就可以尽可能地减少在寻找测试向量过程中错误判定的可能性, 甚至完全避免错误判定, 从而避免回溯。

4 结束语

本文分析了数字电路等价性检验的一般方法。重点分析和评述了组合电路等价性检验方法的 3 种算法, 并简单介绍了其扩展技术。

组合电路等价性检验方法各有优缺点, 用 BDD 进行等价性检验速度较快, 但 BDD 的结点数可能会随变量个数增加而呈指数倍增大, 从而导致空间爆炸。而完全的 SAT 算法基本是对变量的回溯搜索为基础, 时间复杂度较高, 可能导致算法超时。在实际运用时, 通常结合电路结构应用各种启发式方法, 选择合适算法进行等价性检验。

ATPG 算法的效率普遍还不高, 今后有较大改进的余地, 寻求简化 ATPG 问题的方法是当前亟待解决的问题, 目前结合符号模拟、SAT 和 ATPG 来进行组合电路的等价性检验, 已经取得一定效果。该领域将来的工作是应用一些最新的理论成果, 如抽象和细化技术, 提高等价性验证算法的运行效率, 特别是 ATPG 算法和 SAT 算法, 解决 SAT 方法处理时序电路的问题。

参考文献

- 1 Huang S Y, Cheng K T. Formal Equivalence Checking and Design Debugging[M]. London: Kluwer Academic Publishers, 1998.
- 2 Moliter P, Mohnke J. Equivalence Checking of Digital Circuits: Fundamentals, Principles, Methods[M]. Boston, Dordrecht, London: Kluwer Academic Publishers, 2004.
- 3 Brand D. Verification of Large Synthesized Designs[C]//Proceedings of International Conference of Computer-aided Design. 1993: 534-537.
- 4 Matsunaga Y. An Efficient Equivalence Checker for Combinational Circuits[C]//Proc. of Design Automation Conference. 1996: 629-634.
- 5 Moskewicz M, Madigan C, Zhao Y, et al. Chaff: Engineering An Efficient SAT Solver[C]//Proc. of Design Automation Conference. 2001: 530-535.
- 6 李光辉, 邵明, 李晓维. 基于 BDD 的组合电路等价性检验方法[J]. 微电子学与计算机, 2003, 20(2): 48-51.

(上接第 252 页)

4 结束语

本文根据当前汽车外观造型设计的现状, 探讨了汽车构件的设计与复用, 并依据实际需要与当前计算机技术, 探讨了构件的存储、构件库的组织与结构, 笔者结合自己的实践, 感觉此方案具有很好的可行性。当然, 该系统还有很多地方有待于深入、完善, 下一步将探讨单个构件的智能生成与智能装配。

参考文献

- 1 之水. 为车做嫁衣——带你了解汽车设计全程[EB/OL]. 2004.

<http://auto.sina.com.cn/news/2004-11-05/85519.shtml>

- 2 National Materials Advisory Board. Enabling Technologies for Unified Life-cycle Engineering of Structural Components[M]. Washing, National Academy Press, 1991.
- 3 邱莉梅, 刘弘. 支持创新概念设计的多 Agent 系统[J]. 计算机集成制造系统, 2003, 9(12).
- 4 杨美清, 朱冰, 梅宏. 软件复用[J]. 软件学报, 1995, 6(9): 525-533.
- 5 杨美清. 软件复用及相关技术[J]. 计算机科学, 1999, 26(5): 1-4.