计算机形式验证方法研究综述

张瑞雪 郝春梅 王 旭
哈尔滨金融学院 黑龙江 哈尔滨 150030

【摘 要】对形式验证方法进行了综述和讨论，介绍了基于符号处理的形式推理方法，并详细讨论了时序电路、组合逻辑电路等价性的检验方法。

【关键词】形式验证 时序逻辑 等价性检验 BDD 模型检验
中图分类号：TP39 文献标识码：B 文章编号：1009-4067(2011)05-69-01

1．引言

集成电路的主流制造工艺正在向深亚微米发展，使用传统的基于模拟的方法对含有几百万门的电路和系统设计进行验证，已经不能满足需要，对于这样复杂的电路和系统，人们转而寻求其他的设计验证技术作为补充，形式化验证方法就是适应这个要求而产生的新技术。形式化方法可分为等价性检验、模型检验和定理证明方法[1]。

2．验证的方法

传统的验证方法有：模拟、测试、仿真，但是对于大型系统，模拟和测试都不可能是完全的，只能针对某些典型的情况或者随机地进行。模拟的基本原理是对逻辑设计结果施加一定的输入数据，观察其输出结果，并对其分析，存在三个问题：(1)输入数据要由用户给出，而输入数据的好坏决定了所能查出的错误的多少；(2)输出结果的分析要由有经验的人进行；(3)由于输入数据难以穷举，尽管能查出许多错误，但不能保证不存在错误。

形式化方法是保证设计正确性的另一条重要途径。它是用具有形式语义的记号和工具明确地表述所要设计的计算机系统的设计要求，即给出系统规范，并根据系统规范利用上述记号和工具对系统具有的性质和最终实现的正确性进行严格的证明。

2.1 形式验证的基本方法

等价性检验的主要目的是在一个设计经过变换后，穷尽地检验变换前后的功能的一致性，即证明设计的变换没有产生功能的变化。它可以验证对一个设计作变化前后功能是否一致，这种检验方法不必担心检验的完全性，保证了百分之百的覆盖率。等价性检验的基本原理是建立被比较的两个模型之间的关系。检验的依据是数学的定理和公理，以及设计实现所利用的标准单元库的精确描述。

对一个时序逻辑电路来说，我们可以把它看成一个有限状态机。电路功能的等价可以利用有限状态机的等价来判断。

对组合电路来说，不存在状态寄存器，其输出值不依赖于前面的输入值。这时只要对每个输入向量证明其输出向量相同。

组合验证领域里等价性检验可分为两大类：

(1)把两个组合电路的输出函数转换成一个单一的表示，当且仅当它们相应的输出部分的正则表示相同时，两个电路等价。通用的正则表示是基于二叉判定树(BDD)，在最坏情况下，布尔函数的正则表示随输入个数指数增加，会引起内存爆炸问题。

(2)利用输入测试向量进行验证。探寻使两个电路具有不同输出值的输入测试向量。

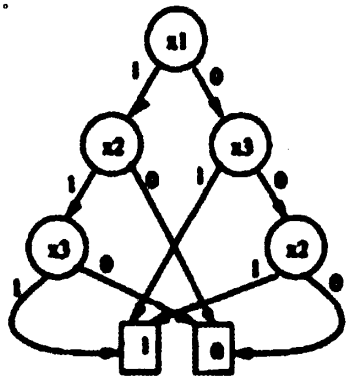

图1 BDD图

成功的系统中第一种方法用得比较多。BDD是布尔函数的一种二叉树表示形式。一个定义在$X=\{x_1,\cdots,x_n\}$上的BDD是一个有一个源点，至多两个汇点的有向无环图，汇点取值0或1，每一个内部节点由xn中的一个变量标识，且有两个出边，对应的边上变量取值0或1（如图1）。

BDD应满足两个约束条件：一、假设变量按$x_1< x_2<\cdots\cdots<x_n$顺序，那么从根节点到汇点的所有路径的变量序列都按这个规则排列。二、该图可遵循以下两个规则化简：(1) 合并规则：两个同构的子图应合并。(2) 消去规则：两个分支指向同一个顶点的顶点应删除。满足这两个条件的图称为简化的有序二叉判定图（ROBDD）。

因为ROBDD 是正则的，可以直接用来检验两个布尔网表的等价性。当且仅当两个电路的对应的输出的ROBDD相同时，这两个电路才等价。

ROBDD的大小依赖于变量的排序。给定一个组合电路网表，[2,3]讨论了一些队基本输入变量排序的启发式方法，可生成输出的ROBDD紧凑的表示。这些技术首次成功地证明了ROBDD可用来验证大规模的电路。变量排序的另一个显著的优点是引入动态变量再排序[4]。该方法试图定期地对变量进行重排，以减少存储需求。[5]提出了一种基于重排序技术的改进方法，通过分组筛选对称对来减少筛选操作。[6]提出了进一步改进的方法，引入了扩展对称的概念，来给更大的变量组分组。

[7,8]按深度优先搜索方法处理ROBDD，与传统的采用深度优先搜索算法的apply 方法[9]相比，能处理更大的，在任意给定的时间里，把几个不同层次的ROBDD存到主存里，剩下的存到辅存里，存在辅存里的ROBDD往往占空间更多。

3．结论

形式验证方法克服了传统的验证方法的缺陷。基于ROBDD的模型检验方法在选取良好排序的情况下，解决了空间爆炸问题。一阶逻辑的定理证明系统已经在实际中得到应用，但只适用于门级、寄存器传输级使用，而且不能用在时序逻辑电路的验证。高阶逻辑比一阶逻辑有比较的优势，它的描述能力比一阶逻辑强，但它的HDL逻辑推理更困难，容易产生悖论。有待于进一步研究。

参考文献

[1] 韩俊刚，杜慧敏. 数字硬件的形式化验证. 北京：北京大学出版社. 2001.

[2] 边计年，薛宏熙，苏明等. 数字系统设计自动化. 北京：清华大学出版社. 1996.

[3] S.Malik et. al. Logic Verification using Binary Decision Diagrams in a Logic Synthesis Environment. ZCCAD, 1988.

[4] M.Fujita, H. Fujisawa, and N. Kawato. valuation and Improvements of Boolean Comparison Method Based on Binary Decision Diagrams. ZCCAD, 1988.

[5] R. L. Rhdell. Dynamic Variable Ordering for Ordered Binary Decision Diagrams. ICCAD, 1993.

[6] S. Panda, F. Somenzi, and B. Plessier. Symmetry Detection and Dynamic Variable Ordering of Decision Diagrams. ZCCAD, 1994

[7] S. Panda and F. Somenzi. Who Are the Variables in Your Neighb(orhood. ICCAD, 1995.

[8] H. Ochi, K. Yasouka, and S. Yajima. readth-first manipulation of very large binary-decision diagrams. ICCAD.

[9] P. Ashar and M. Cheon. Efficient breadth-first manipulation of binary-decision diagrams. ICCAD, 1994.