

超大规模数字系统控制器的验证实现

卢英¹, 李炜², 张义超¹, 郭星¹

(1. 安徽大学 计算机科学与技术学院, 安徽 合肥 230039;

2. 安徽大学 计算智能与信号处理教育部重点实验室, 安徽 合肥 230039)

摘要:数字系统的验证是一个复杂的过程。结合当前数字电路设计的高复杂度、高度集成化的特性,介绍了模拟验证和形式验证两种验证方法,并对它们进行了分析与比较,然后详细介绍了基于STG图同构求解的控制器综合验证方法。该方法需要两组有限状态机的STG(状态转换图),通过验证两个STG是否同构来验证控制器综合结果的正确与否。实践证明该方法可以有效地克服算法级描述到底层实现之间跨度太大的问题。

关键词:超大规模数字系统;电子设计自动化;模拟验证;形式验证;状态转换图

中图分类号:TN79

文献标识码:A

文章编号:1673-629X(2008)10-0170-03

Implementation on Verification of Controller in Very Large Digital Systems

LU Ying¹, LI Wei², ZHANG Yi-chao¹, GUO Xing¹

(1. Institute of Computer Science and Technology, Anhui University, Hefei 230039, China;

2. Ministry of Education Key Laboratory of Intelligence Computing and Signal Processing, Anhui University, Hefei 230039, China)

Abstract: Digital system's verification is a complex issue. In connection with the high complexity and integration of current digital circuit, introduces simulation verification and formal verification which are analyzed and compared, and then detailedly introduces the verification of controller synthesis based on STG's (state transition graph) isomorphism. The verification of controller synthesis requires two finite state machines' STG, whose isomorphism is checked to see the corresponding controller synthesis' correctness. Practice shows that the method can effectively overcomes the wide span between algorithm-level description and bottom implementation.

Key words: very large digital system; electronic design automation; verification of simulation; formal verification; state transition graph

0 引言

近年来,由于数字电路设计规模不断增大和设计复杂度的提高,使得超大规模集成电路(VLSI, Very Large Scale Integrated)的设计无论采用手工或自动的综合过程,都很难保证电路的逻辑设计正确无误。随着系统设计复杂性的不断增加,设计正确性的验证过程变得非常费时,设计人员在设计验证上的时间常常是设计时间的二至三倍,计算机模拟方法已无法满足需要^[1]。为解决设计验证这一难题,人们发展了形式验证,该方法是数学化,而不是像模拟那样,是试验性质的。其克服了模拟方法的不足,它对指定描述中所

有可能的输入组合一次进行了验证而不是仅仅对其一个子集进行多次试验。控制器综合是指规范行为描述到实现之间的转换,这种转换是在算法级抽象层次上完成的,也就是完成算法级描述到RTL级结构实现之间的转换。目前面向低级抽象层次的验证技术已经趋向成熟,而近年来数字系统设计自动化研究领域中的控制器综合技术的迅速发展给验证研究带来新的难题。控制器综合文中主要研究基于完全确定有限状态机模型^[2]的控制器综合的正确性验证,给出了基于图同构求解的验证方法。文中将控制器综合前有限状态系统的抽象行为描述和控制器综合结果的结构通过逆向分析方法实现的等价的行为描述分别用有限状态机的状态转换图来表示,然后利用基于STG图同构求解的方法及图论中的理论和方法验证控制器综合结果的正确性。主要阐述了能够适应控制器综合特点的基于STG图同构求解的控制器综合结果验证方法。

收稿日期:2008-03-02

基金项目:安徽省自然科学基金资助计划项目(2006KJ013A)

作者简介:卢英(1984-),女,安徽泗县人,硕士研究生,研究方向为计算机与VLSI设计自动化;李炜,副教授,硕导,研究方向为嵌入式系统和CIMS技术。

1 验证方法概述

1.1 验证的基本概念

当设计者设计或修改了一个电路后,需要进行正确性验证;不论是在自上而下或是自下而上对大规模集成电路进行设计中,验证过程都是必需的,只有经过验证才能保证设计中的错误被早期发现、早期消除。

从上可以总结出所谓的验证是指采用某种方法来确定在给定系统规范说明的前提下所构造的系统模型(或系统实现)是否满足规范说明。简单的说,验证就是对两个系统进行比较以判断两个系统是否相同。对应于 VLSI 设计的过程,验证分为设计验证(Design Verification)和实现验证(Implementation Verification)两部分,如图1所示。

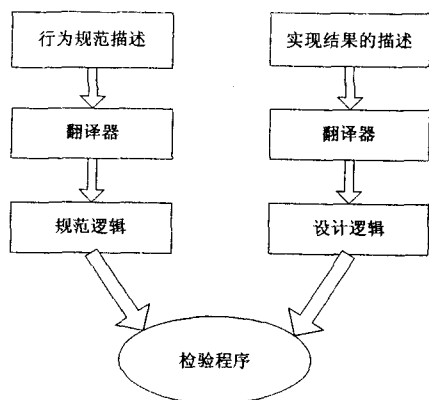


图1 数字电路的验证过程

设计验证是针对一个设计规范说明来检查其实现的正确与否;实现验证是为了保证综合过程的准确无误。验证的目的包含以下三个方面:

- (1)验证系统原始描述的正确性;
- (2)验证设计结果的逻辑功能是否符合原始规定的逻辑功能;
- (3)验证设计结果中不含有设计规则的错误。

验证方法一般包含模拟、形式验证及其他方法。

1.2 验证方法的分类

1.2.1 模拟验证

在目前流行的设计方法和实际设计流程中,设计正确性的验证通常采用的是模拟验证方法。模拟验证采用仿真运行的手段,为设计人员提供了可行的判别数据,在实际中发挥着巨大的作用。

模拟,或称仿真,是指从电路的描述(语言描述或图形描述)抽象出模型,然后将外部激励信号或数据施加于此模型,通过观察该模型在外部激励信号作用下的反应来判断该电路系统是否实现预期的功能^[1]。模拟系统的基本数据包括电路模型、外部输入激励波形、输出响应波形三部分。模拟过程如下:

- (1)在输入端施加作为外部激励的数据;

(2)计算机根据步骤(1)中的激励和内部电路模型计算出各点的响应,得到输出波形;

- (3)比较得到的结果是否和预期的功能相同。

但是这种技术的不足之处也是十分明显的,主要表现在以下三个方面:

1)模拟不是完备的验证方法,只能证明有错而不能证明无错。因此,模拟一般适用于在验证初期发现大量和明显的设计错误,而对于复杂和微妙的错误,该方法难以胜任。

2)模拟验证的效果严重依赖于测试向量的选取。但是合理而充分地选取测试量本身就是一个十分艰巨的任务。

- 3)模拟方法的效率不高。

电路规模小的时候,这些不足所造成的影响还不明显;随着电路规模的迅速增长,模拟验证的不足便突出地摆在了设计人员的面前。人们开始认识到,必须提供多种设计正确性的验证手段,这时另一种验证方法——形式验证得到了越来越多的关注。

1.2.2 形式验证

形式验证是指从数学上完备地证明或验证电路的实现方案是否确实实现了电路设计描述的功能。

该方法首先是得到预设计系统的形式描述;然后给出将被验证的系统模型(或是系统实现);最后再构造一个验证器,并利用其来验证设计结果是否正确。

与模拟验证相比,形式验证有如下的优点:

- (1)此验证方法是完备的,可以完全断定设计的正确性。
- (2)此验证方法是对指定设计描述的所有可能情况进行验证。

(3)此验证方法可以进行从系统级到门级的验证,而且验证时间短,有利于尽早发现错误。

形式验证也有其致命的弱点:首先是在对原始设计进行抽取后所得到的描述上进行的。抽取模型和原始设计不可避免地存在鸿沟。抽取过粗,则可能忽略某些设计错误;抽取过细,则可能将本来正确的设计判断成错误的。其次,目前的两种最基本的形式验证技术,即定理证明和模型检验,都有其固有的缺陷需要继续研究克服。最后,形式验证到目前为止仍然不能有效地验证电路的性能,例如电路的时延和功耗等^[3]。由于这一系列原因,形式验证目前还不能取代模拟验证,两者各有优势,互为补充,缺一不可。

近年来数字系统设计自动化研究领域控制器综合技术的迅速发展给验证带来新的难题。控制器综合结果的正确性验证研究成为一个薄弱环节,控制器综合验证策略的确定迫在眉睫。

2 基于 STG(状态转换图)图同构求解的控制器综合结果验证

2.1 控制器综合

控制器综合实质是有限状态机综合,即对数据流综合生成的 FSM(有限状态机)进行分解、状态化简、状态分配等处理,选取时序元件,导出状态转换函数和控制输出函数。控制器综合的目标是获取芯片面积优化的高性能控制电路结构形式^[3]。基于篇幅限制只能简要介绍一些基本概念和等价性验证算法。

(1)行为域、结构域、综合。

数字电路设计包括行为、结构和物理三个领域。行为域是指电路的功能;结构域是指电路的逻辑组成。在行为域只须说明行为功能,不必设计任何达到这一行为的实现方式;结构域仅仅说明要实现某一行为的功能要素的体系结构及其间的互联关系;而物理域不设计任何的功能信息。

(2)等价性验证。

文中所要进行的等价性验证是基于图同构^[4]证明,在验证控制器综合前后的有限状态机模型的等价性时,只要根据定义 3 判断其初始点等价,就可以验证控制器综合结果的正确性。

定义 1 状态机 M 称为完全确定的有限状态机,如果 M 在任意状态下对任意可能的输入,满足有确定的输出和有唯一确定的下一状态。

定义 2 设 M_a 和 M_b 为两个完全确定的有限状态机,对任意两个状态 $S_i \in S_a, S_j \in S_b$,当且仅当对每一对输入 $x \in X$,若同时满足以下条件:输出相同,即 $O(S_i, X) = O(S_j, X)$ (“=”表示相同);下一状态等价,即 $N(S_i, X) \equiv N(S_j, X)$ (“ \equiv ”表示等价),则称 S_i 和 S_j 等价。

定义 3 如果两个完全确定的有限状态机 M_a 和 M_b 的初始状态等价,则 M_a 和 M_b 等价。

2.2 基于 STG 图同构求解的控制器综合验证

基于 STG 图同构求解的控制器综合的正确性,需要两组有限状态机的状态转换图(STG),一组是控制器综合前系统的抽象行为描述 STG_{org},另外一组是控制器综合结果的结构实现等价的行为描述所构成的 STG_{ext}。通过判断两图是否同构来验证控制器综合结果的正确性,证明过程如图 2 所示。

先讲解图的同构问题,然后介绍图同构求解的等价性证明方法。

(1)图的同构^[4,5]。

假设控制器综合结果的结构实现等价的行为描述所构成的 STG 为 $G_1(V_1, E_1)$,即 STG_{ext};综合前的

行为描述的抽象模型的 STG 为 $G_2(V_2, E_2)$,即 STG_{org}。当控制器综合结果正确时,应有 $G_1(V_1, E_1) \cong G_2(V_2, E_2)$ (“ \cong ”表示同构)。

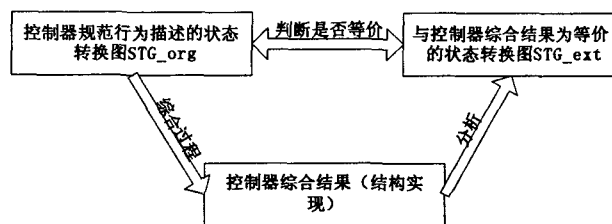


图 2 控制器的综合和验证过程

(2)等价性证明方法。

文中利用完全确定的有限状态机进行图的同构证明,目的是让算法效率更高。利用下面所提出的算法,在验证控制器综合前后的状态图的等价时,只要判断其初始顶点是否等价就可以判断两图是否等价。

基本思想:从 STG_{org} 与 STG_{ext} 的初始顶点对开始,判定两个图是否同构,假定有限状态机有 n 个状态,算法中 m 代表匹配的顶点数。

(1)先判定初始顶点对的输出函数是否相等,如果相等则 $m++$,否则转向(3);

(2)求解该顶点对的所有下一顶点对,如果下一顶点不能完全匹配,则两图不同构,转向(3),否则 $m++$,同时转向(2);

(3) $m < n$,则两图不同构,算法提前结束; $m = n$,两图同构,算法结束。

等价性证明算法:

```
FSM_EQUAL( $G_1, G_2$ ) //判断两图  $G_1, G_2$  是否同构
{
    InitQueue(Queue); //新建一个队列并初始化
    EnQueue(Queue,  $G_1.v_0, G_2.v_0$ ); //  $G_1$  和  $G_2$  的初始顶点  $V_0$  入队
    While(! QueueEmpty(Queue)) //判断两图是否同构
    {
        OutQueue(Queue,  $v_1, v_2$ ); //取出队列 Queue 当前的对头元素  $v_1, v_2, v_1$  是  $G_1$  中的顶点,  $v_2$  是  $G_2$  中的顶点
        If((Flag[ $v_1.q$ ] != NULL) || (Flag2[ $v_2.q$ ] != NULL))
        {
            If(Flag[ $v_1.q$ ] ==  $v_2.q$  && Flag2[ $v_2.q$ ] ==  $v_1.q$ ) //如果两个顶点至少有一个被标记 continue
            else return (false);
        }
        If( $v_1.Y \neq v_2.Y$ ) return (false); //如果对应的顶点队的输出不相同,则不同构,直接返回错误信息
        Flag[ $v_1.q$ ] =  $v_2.q$ ;
        Flag2[ $v_2.q$ ] =  $v_1.q$ ;
        For( $G_1$  中的每条边  $e_1(v_1.q, q_1, F)$ )
        {
```

(下转第 176 页)

```

}
GetGPRSMess mGPRS=NULL; /* 获得 GPRS 发送来的信息
COM 组件 */
SendCommand mSCmd=NULL; /* 给下位机发送命令 COM
组件 */
AlarmInfor mAlm=NULL; /* 本地报警 COM 组件 */
.....
CMainDlg dlg; /* 登陆主界面 */
m_pMainWnd = &dlg;
return FALSE;
}
BOOL CMointerApp:: ExitInstance ()
{
if(mGPRS!= NULL) /* 释放资源 */
mGPRS->Release();
.....
}

```

4 结束语

给出了一种无线抄表系统的方案,通过 GPRS 无线自动抄表,具有速度快、准确率高等特点,方便电力公司抄表工作,由于不需要人员深入小区住户家里进

行抄表,加强了小区住民的安全感。实践证明,采用多次收发机制,数据丢失率几乎为 0,抄表工作一般在 2 分钟内完成。

该系统备受电力公司和普通百姓的青睐,具有良好的市场前景和应用价值。

参考文献:

- [1] 里吉斯.通用分组无线业务(GPRS)技术与应用[M].北京:人民邮电出版社,2004.
- [2] 陈 曠.ARM 嵌入式技术实践教程[M].北京:北京航空航天大学出版社,2005.
- [3] 尚 宇,郅 琦. $\mu C/OS-II$ 在 LPC2210 上的移植研究[J].计算机技术与发展,2007,17(2):103-105.
- [4] Kruglinski D J. Programming Visual C++ 6.0 技术内幕[M].第 5 版.希望图书创作室译.北京:北京希望电子出版社,2002.
- [5] 邓中亮,何双亮.基于 ARM 的嵌入式操作系统 $\mu C/OS-II$ 的移植研究[J].计算机技术与发展,2007,17(10):4-6.
- [6] 程广河,郝凤琦,张让勇,等.嵌入式环境中的软件构件化研究[J].计算机技术与发展,2007,17(9):139-141.
- [7] 黄燕平. $\mu C/OS$ ARM 移植要点详解[M].北京:北京航空航天大学出版社,2005.

(上接第 172 页)

```

If(在图  $G_2$  中有边  $e_2(v_2..q, q_2, F)$  使得  $e_1.F = e_2.F$ )
{
记状态标记为  $q_1$  的  $G_1$  中的顶点是  $G_1.v_3$ ;
记状态标记为  $q_2$  的  $G_2$  的的顶点是  $G_2.v_4$ ;
EnQueue(Que,  $G_1.v_3, G_2.v_4$ );
}
else return(false);
}
Return (true);
}

```

算法中 G_1, G_2 是两个图,目的就是判断 G_1 和 G_2 等价, q 表示状态, Y 表示输出, F 是输出函数,其中的 Que 是队列的名称。从上面的算法可以看出向队列中增加新顶点对的条件是顶点对中的两个顶点都没有被标记。

3 结束语

数字系统设计自动化研究领域中的控制器综合具有面向高抽象层次,支持大规模高复杂度的设计目标等,原来的验证技术已经满足要求,经过研究发现基于

STG 图同构求解的方法可完成控制器综合的验证。该验证方法直接考查控制器综合的输入与输出的一致性,直接面向目标的功能描述,可接收较大规模较高复杂度的设计目标,不依赖测试激励输入,利于控制综合优势的发挥。

参考文献:

- [1] 边计年,薛宏熙,苏 明,等.数字系统设计自动化[M].北京:清华大学出版社,2005.
- [2] 秦永彬,许道云.有穷自动机中的等价性与等价归并算法[J].济南大学学报:自然科学版,2006,20(4):354-358.
- [3] Devades S, Ghosh A, Keutzer K. Logic synthesis[M]. Hightstown: McGraw-Hill, Inc, 1994.
- [4] Kong F G, Li Q, Zhang F J. An artificial neural network approach to mechanism kinematic chain isomorphism identification[J]. Mechanism and Machine Theory, 1999, 34(2): 271-283.
- [5] He P R, Zhang W J, Li Q. Some further development on the eigensystem approach for graph isomorphism detection[J]. Journal of Franklin Institute, 2005, 342(6): 657-673.