大规模集成电路形式化等价性验证研究进展

张立明[1,2]，欧阳丹彤[1,2]，白洪涛[1,3]，王艺源[1,2]
（1. 吉林大学计算机科学与技术学院，吉林省长春市 130012；
2. 吉林大学符号计算与知识工程教育部重点实验室，吉林省长春市 130012；
3. 吉林大学公共计算机教学与研究中心，吉林省长春市 130012）

摘要：在集成电路设计中,验证的时间已占到整个设计周期的80%以上.因此对不同抽象层间的等价性验证方法的研究，从而提高验证的效率，缩短产品上市时间，显得非常重要.本文首先简单介绍了等价性验证的研究背景和发展趋势.然后分析了寄存器传输级(Register Transfer Level, RTL)的形式化等价性验证方法,并且分析了系统级模型(System Level Model, SLM)和 RTL 的形式化等价性验证方法.随后,介绍了电子设计公司关于形式化等价性验证的工具.最后,给出目前形式化等价性验证方法所面临的挑战和下一步的研究方向.

关键词：集成电路;等价性验证;形式化方法;RTL;SLM;可满足
中图分类号：TP18

The Research and Development of Formal Equivalence Checking in VLSI

ZHANG Liming[1,2], OUYANG Dantong[1,2], BAI Hongtao[1,3], WANG Yiyuan[1,2]
(1. School of Computer Science and Technology,Jilin University,Changchun 130012;
2. Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education,Jilin University,Changchun 130012;
3. Center for Computer Fundamental Education,Jilin University,Changchun 130012)

Abstract: In integrated circuit design, the verification time for the correctness can take up to 80 percent of the overall design process. Therefore, investigation into the equivalence checking method between different abstraction layers is indispensable, which can improve the efficiency of equivalence checking and reduce the overall time. This paper first presents a brief introduction on the background and development of formal equivalence checking. Then an analysis of formal equivalence checking methods is given, which including the equivalence between RTL(Register Transfer Level) and its variants and the equivalence between SLM (System Level Model) and RTL. Consequently, the typical formal equivalence checking tools developed by the electronic design company is introduced. Finally, we discuss the challenges that formal equivalence checking now facing, and the directions for future research.

Key words: integrated circuit; equivalence checking; formal method; RTL; SLM; satisfiability

0 引言

1975年摩尔提出了关于集成电路发展的“摩尔定律”,即电路芯片的电子器件数每18个月翻一番,而价格保持不变甚至下降,几十年的发展状况基本上符合了这个定律.随着集成电路

基金项目：国家自然科学基金(61272208,61133011,60973089,61003101)、国家教育部博士点专项基金(20100061110031)、中国博士后科学基金(2013M541302) 、吉林省科技发展计划项目基金(20101501,20100185)、浙江师范大学计算机软件与理论省级重中之重学科开放基金(ZSDZZZZXK12)
作者简介：张立明（1980-），男，吉林大学博士后，主要研究方向：自动定理证明，模型验证和基于模型的诊断
通信联系人：欧阳丹彤（1968-），女，吉林大学教授，博士生导师，主要研究方向：自动定理证明，模型验证和模型诊断. E-mail: ouyangdantong@163.com

设计的规模变得越来越大、功能越来越复杂,验证技术已经成为设计流程的主要瓶颈.据统计,设计验证的时间已占到整个设计周期的 80%以上.功能正确性是超大规模集成电路设计必须满足的要求.基于模拟仿真的方法是最常用的功能正确性测试手段,但随着集成电路设计规模的迅速增长、复杂度急剧提高,基于模拟验证方法的覆盖率逐步降低.这给错误留下了巨大的隐藏空间,如 Intel 公司奔腾 CPU 著名的浮点运算错误造成了四亿七千五百万美元的经济损失和美国阿里安 5 型火箭发动机控制系统的错误导致飞行试验失败等.

集成电路设计流程中包括许多步骤,在每一步中,集成电路设计被表示成不同抽象层次的模型,例如 SLM、RTL、Gate、物理版图级模型等.集成电路的设计流程实际上是一个对设计模型逐步精化的过程[1,2].在这个流程中,集成电路设计中的每一步都有可能引入错误.因此,芯片设计从其需求分析开始,经过设计和优化,到最终得到实际的芯片并投入应用,其中的每一步都需要进行严格的测试和验证.

等价性验证是指证明两个描述模型具有相同的功能,有时也称为逻辑验证或布尔比较[3].例如,RTL 模型和经过修改或优化后的 RTL 模型是否等价.等价性检验是目前在实际的芯片设计中应用最为广泛的形式化验证技术.基于模拟验证的方法需要产生各种测试激励,对于大型复杂的设计,模拟消耗了大量的时间.虽然模拟一直是最常用的功能验证方法,但它有两个主要的缺陷.首先指数级的时间复杂性,对于大型复杂的设计,人们不可能对整个输入向量空间进行穷举的模拟.正因如此,模拟验证能够发现错误的存在,但很难证明错误的存在,即它是不完备的方法.其次是难以定义合适的验证覆盖率,而且验证者很难给出理想的测试激励,使之能够覆盖到所定义的各种评估目标.为了克服上述困难,模拟方法要求更高效率的模拟器、更好的测试环境、更高效的计算机,当然还需要更多的时间、金钱和验证工程师.然而,由于市场的压力,又必须尽可能地缩短设计周期来加快产品面市,这就导致了模拟所能覆盖的功能越来越不完全.为此,人们转而借助于其它的验证技术来补充.从上个世纪八十年代以来,国内外对于形式化验证的研究取得了长足的进展,并被很快应用到实践中.

形式化验证方法利用数理逻辑来建模和推理,严格地证明一个电路设计（实现）满足给定的需求(设计规范).形式化验证方法现在已经发展成为基于模拟验证方法的一个重要补充.它的好处是可以隐式地穷举整个电路的输入变量空间,即它可以达到 100%的覆盖率,而且并不需要产生测试激励.研究表明,形式化验证方法可以成功检测到奔腾浮点除法器的错误.形式化验证方法逐步受到学术界和产业界的重视,成为当前超大规模集成电路广泛采用的、必不可少的验证手段.形式化验证方法作为传统模拟验证方法的补充和完善,具有重要的研究意义和实用价值.

自 1984 年起，ACM/IEEE 每年举办主要关注芯片、电路以及系统设计新工具和新方法的国际顶级会议（Design Automation Conference，DAC），此外还有诸如 Computer Aided Verification（CAV），Formal Methods world congress（FM），International Conference on Computer-Aided Design（ICCAD）等国际权威会议专门讨论形式化验证方法。近年来，在人工智能领域具有重要影响的 IJCAI、AAAI、ECAI 等也纷纷将形式化验证方法作为重要的研讨课题，IEEE Transactions on Computer-Aided Design 系列期刊重点关注和发表该领域相关论文；近年来，形式化验证方法的研究机构主要集中在欧美。美国的 Princeton University、Stanford University、Massachusetts Institute of Technology（MIT）、Carnegie Mellon University（CMU）和英国的 Oxford University、Cambridge University、德国 Technical University of Munich 和荷兰 University of Twente 等国际一流大学都有专门的研究小组并开设相关课程。国内的中科院计算所、软件所、清华大学、复旦大学、浙江大学、吉林大学、上海交大、哈

尔滨工业大学、西安邮电学院等高校和科研院所等较早开始了对于硬件形式化验证方法的研究,并取得了许多重要成果.这一研究领域成为推动信息技术发展的重要动力，对未来超大规模集成电路和核心软件产业起着至关重要的作用。

本文主要介绍集成电路的形式化等价性验证方法。在第二部分给出 RTL 和 RTL 的形式化等价性验证的研究与进展；在第三部分分析了 SLM 和 RTL 的形式化等价性验证的方法和技术；第四部分介绍了芯片验证公司验证工具的核心处理技术和方法.最后对形式化验证方法面临的问题和发展方向进行了分析.

1 RTL 和 RTL 的形式化等价性验证

RTL 和 RTL 的等价性验证问题主要是时序电路的等价性验证问题。通过匹配时序电路中寄存器等元件,将时序电路的等价性验证问题转化为组合电路的等价性验证问题已成为当前解决时序电路等价性验证问题的主流方法[4]-[10].组合电路验证是指验证两个无循环电路的等价性,是所有等价性验证的基础,许多商业化公司的验证工具采用了此种方法.下面介绍 RTL 和 RTL 的形式化等价性验证方法.

1.1 基于符号模拟的验证方法

组合电路形式化等价性验证的基本方法是使用基于符号模拟[8]的方法,可以自动计算每个电路输入和输出之间的关系,然后比较这些关系是否相等.符号模拟[9]是基于模拟方法的原理,结合电路输入模拟每个电路的功能进而计算电路的输出,而电路中的每个输入可以用变量来表达,所以基于符号模拟方法得到关于输入变量的符号表达式.

基于符号模拟的等价性验证方法基本思想是对于任意相同输入条件下的两个组合电路,计算两个电路输出是否总是相等.下面以 Gate 级电路为例,说明基于符号模拟的方法.图 1 中,输出 f 和 g 的符号模拟表达式分别为 a⊕((b∧c)∧d)和 a⊕(b∧(c∧d)).因此等价性验证就是计算两个符号表达式是否等价.

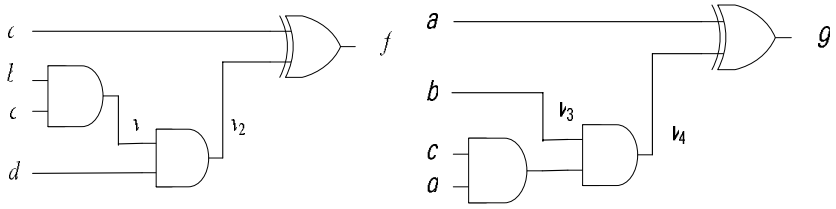

图 1 基于符号模拟等价验证方法示例

在符号模拟方法中可以使用任何表达形式来描述符号表达式.BDD[10]是描述布尔函数的最常见的一种方式,其描述形式是无冗余,紧凑和高效的布尔函数表达方式,BDD 是描述符号表达式较好的形式.

由于符号模拟的方法要描述所有的等号表达式,会引起空间爆炸问题,进而限制了符号模拟方法的验证规模.为了弥补符号模拟等价性验证方法的不足,许多研究者开始结合布尔可满足求解器进行等价性验证.下面介绍基于布尔可满足的等价性验证方法.

1.2 基于布尔可满足的验证方法

近年来,基于布尔约束可满足求解技术取得了较大进展,已经可以处理百万级的变量,同时也极大地提高了形式化等价性验证的效率.现在国外比较成熟的求解器有 Minisat[11], Grasp[12],Zchaff[13] walksat[14],C-sat[15]等,国内研究小组也对约束求解进行了多年的研究,并取得了相应的成果[16]-[23].结合 SAT 求解器的等价性验证方法需要将符号表达式或集成电路设

计转换成 SAT 可接受的 CNF 格式,然后进行求解.对于例 1,f 和 g 对应的符号表达式转换成 CNF 后分别为 (b∧c↔v1)∧(v1∧d↔v2)∧(a⊕v2↔f) 和 (c∧d↔v3)∧(b ∧v3↔v4)∧(a⊕v4↔g).

我们可以把以上这些约束和约束关系(O↔f⊕g)∧O 一起做为SAT求解器的输入,进行求解.如果 SAT 求解器得到的结果是可满足的,则存在相应的一组赋值,使得两个电路是不等价的;如果得到的结果是不可满足的,则说明两个电路是等价的.

布尔可满足的求解技术,使得等价性验证方法的求解效率和能力都有较大提高,但仍不能对许多工业上大规模的集成电路进行验证.为此,研究者开始把较大规模的验证问题分解成较小规模的验证问题,下面介绍基于此种思想的验证方法.

1.3 基于割集方法的验证

组合电路等价性验证方法的突破性进展是割集方法的引入[24],对于给定需要验证功能等价的两个组合电路,基于割集的方法[25]是根据电路结构的相似性,在电路内部引入候选等价结点,先验证候选等价结点对应子电路的等价性,进而验证电路的等价性.如果候选等价结点逻辑等价,则等价结点可以用新的输入变量代替,重复这个过程,可以将两个电路的等价性验证问题转化为一系列子电路的等价性验证问题.

基于割集的等价性验证方法中,采用一些启发式的策略来寻找到较好的候选等价结点是一个重要的研究领域.用鲁棒性较强的方法来寻找所有可能的候选等价结点复杂性很高,一种常见的方法是先对结构进行快速的比较,分离比较电路之间的差别.然后,用成百上千的随机模拟输入计算输出的值,具有相同的输出是较好的候选等价结点.

基于割集[26],[27]的验证方法把问题分解成较小规模的问题后再进行求解,进而提高了所能处理问题的规模,但此方法并不是完备的.当证明候选等价结点等价后会用新变量替代原来候选结点,引入的新变量忽略了原有的候选等价结点对应电路中的约束关系,可能导致等价的电路被证明不等价,即发生误判现象.

下面以 Gate 级电路为例,说明基于割集等价性验证方法发生误判的现象.如图 2 所示,x 和 y 分别为两个电路中的候选等价结点,验证 x 和 y 是否等价所对应的约束关系为 (x↔b∧c∧d)∧(y↔b∧c∧d)∧(O↔x⊕y)∧O,通过调用 SAT 求解器,得到 x 和 y 等价.此时再用变量 x 和 y 分别代替候选等价结点对应的子电路,得到相应的约束关系为 (O1↔a∧¬x)∧(O2↔a⊕y)∧(O↔O1⊕O2)∧O 进一步验证得到两模型不等价.利用约束求解器可以得到此时模型不等价的赋值为 a=0,x=y=1 或 a=1,x=y=0.而在电路中,如果 a=0 则 x=y=0;如果 a=1 则 x=y=1,即 a=x=y.因此,对于得到模型不等价的两组赋值都不成立,所以存在误判,可以得到两模型等价.

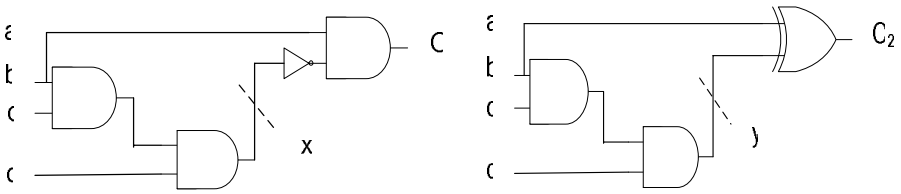

图 2 基于割集等价验证方法示例

许多研究人员对消除误判问题进行了研究,给出了相应的解决方法.Matsunaga 等[28]使用基于 ATPG 引擎的方法来消除误判,因为它很容易找到一个反例(测试向量)来证明两个结点是真正不等价的,因此当两个模型不等价时具有较好的效率.然而,当两个结点功能等价时,使

用 ATPG 引擎则要花费较多的运行时间.Reddy 等[29]采用基于 BDD 的算法来消除误判,此种方法存在空间爆炸问题,限制了验证求解问题的规模.此方法还需要将割集中的结点向后展开,直到能够证明等价或不等价为止,也大大降低了求解效率.其它研究还通过加入相应的约束关系[30,31],或借助堆结构来检查相应的约束关系[7]来避免误判现象的发生.

本研究小组也对消除误判方法进行了研究，在位级的形式化验证方法中，给出了结合约束满足消除误判的方法[32,33]；在字级的形式化验证方法中，给出了利用不可满足核消除误判的方法[34,35]。

1.4 基于布尔可满足的验证方法其它验证方法

国内对形式化验证方法的研究起步比较晚,近年来有些大学和科研院所开展了这方面的研究工作,严晓浪提出了避免内存爆炸的组合电路等价性验证方法和使用输出分组的电路可满足性的等价性验证算法等[36,37].马光胜研究了定点算术数据通路的等价性检验方法[38].唐璞山给出了改进的时间帧展开的时序电路等价验证算法[39]结合模拟蕴涵技术的电路验证方法[40]等.吴为民提出基于线性规划的 RTL 可满足性求解和性质检验[41]等方法.

通过对时序电路中寄存器等元件的匹配,可以将时序电路的等价性验证问题转化为组合电路的验证问题.但是如果两个时序电路中的状态编码不相同时,则很难验证时序电路的等价性.此时,只能应用状态遍历的验证方法或其它处理方法,导致其处理能力非常有限.一般情况下,当状态的位数超过几百时,状态遍历方法就很难得到验证结果.时序电路的形式化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并应用到时序电路验证中是急需解决的关键问题.

2 SLM 和 RTL 之间等价性验证

随着科技的进步,集成电路规模的日益增大,验证的难度越来越大.而激烈的市场竞争又要求产品上市时间越来越短,甚至电子产品上市时间决定着电子开发企业的发展命运.这使得电路的设计工作开始越来越多地从低层 RTL 设计转移到高层设计,即由细节层设计转移到抽象层设计.集成电路设计团队逐渐趋向于在系统级模型进行设计和验证,进而来减少设计和验证的时间.对于每一个集成电路设计,系统级模型一直伴随到设计的最后阶段,并在不同的阶段有不同的作用.在设计阶段,可以利用高层综合工具由 SLM 得到 RTL 模型,随后对得到的 RTL 模型根据面积和功耗要求进行优化.为了保证综合和优化后的 RTL 模型和 SLM 的功能等价,在验证阶段要使用形式化方法验证 RTL 和 SLM 的等价性.

在电路的设计和验证过程中,多数时间都参照系统级模型进行,很少对系统级模型进行修改,因此有时也称为黄金参考模型.系统级模型的采用,一方面利用高层综合工具直接得到相应的 RTL 级模型,大大加快了设计的速度;另一方面由于系统级模型在输入输出和内部结点与 RTL 模型的不同,也阻碍了组合电路验证方法的使用.

在形式化等价性验证方法中, SLM 到 RTL 验证是一个新兴活跃的研究领域.由于 SLM 和 RTL 在语义上的巨大差异,要求有能力的求解器处理现实中工业上的复杂设计.下面,我们介绍 SLM 和 RTL 的形式化等价性验证的求解技术.

2.1 synopsys 公司 Hector 的验证技术

SLM 在硬件设计工程中是最重要的功能模型,不仅表达了系统设计师的思想,而且是硬件设计师和验证人员工作的基础.SLM 是关于硬件设计较为抽象的模型,因此在 SLM 层次进行计算要比 RTL 进行计算的速度快几个数量级.在许多情况下,使用 C/C++来描述 SLM.设计

者可以在数小时内利用高层综合工具从 SLM 产生 RTL 代码,而使用传统的设计方法要花费数周的时间.为了保证设计流程中各模型间的等价性,要对综合后的 RTL 模型和 SLM 的等价性进行验证,而验证速度直接影响产品的上市时间,是基于系统级的集成电路设计方法中的一个瓶颈问题.下面我们以 Synopsys 公司的等价性验证工具 Hector[42]为例,介绍 SLM 和 RTL 的形式化等价性验证方法和技术.

如图所示,等价性验证模型中主要包括 SLM 和 RTL 模型,其中 SLM 的描述语言可以是 C++, SystemVerilog 或 SystemC.

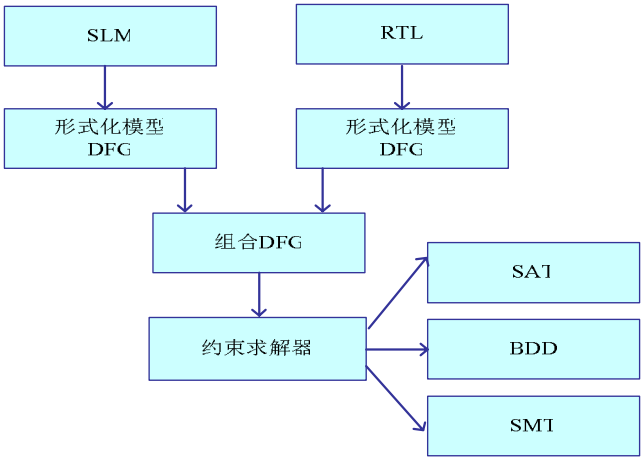

图 3　等价性验证流程图

在验证流程中,首先是将两个模型转换成形式化描述数据流控制图(Data Flow Graph,DFG).解析进来的两个模型都是字级(Word-Level)的,即 SLM 转换为字级有关输入输出关系的 DFG, RTL 模型转换为基于字级的网表.

然后对 DFG 模型进行如下预处理:1) 根据模型中结点的结构信息等选择候选等价对.2)使用随机模拟方法删除候选等价对中的冗余.3)移除模型中的冗余信息,例如,变量的值为常值,用常值代替变量,移除变量.4)对模型使用重写共享技术,使模型最小化.

最后,结合割集的方法,调用 SAT 和基于模理论可满足性求解器(Satisfiability modulo theory, SMT)混合的求解技术对两个字级的 DFG 进行等价性验证.SMT 是基于字级的约束可满足求解器,基于 SMT 的求解器主要有 BAT[43],STP[44], Boolector[45],Beaver[46].

对于 SLM 和 RTL 的等价性验证的问题,最直接的解决方法是采用基于字级的技术来求解,如用 DFG 建模,用 SMT 进行求解.而不是将简单地转换成位级的 DFG,再进行位展开,然后使用任何基于位级的求解器（如 SAT,BDD,ATPG）来完成验证.虽然这些基于位级的求解器对解决 RTL 和 RTL 级验证是有效策略,但在 SLM 和 RTL 的工业模型验证方面效率低下,大型工业设计包含的算术运算符,成为基于位级方法的主要瓶颈问题.

基于字级的描述比基于位级方法有更多的优点.字级的描述比基于位级的方法占用了更少内存,因此可以适用于较大规模工业设计的等价性验证问题；并且基于字级的形式化描述比较接近系统级的设计代码,进而也有利于验证前候选等价结点的寻找和验证不等价后有关设计错误区域的诊断.

2.2　Calypto 公司 SLEC 的验证技术

基于模拟的等价性验证方法基本思想是给两个模型输入任意相同的测试向量,然后计算并比较输出向量是否相等来验证 SLM 和 RTL 是否等价.因此,基于模拟的方法需要大量的工作开发测试用例,而这些测试用例也不能对设计进行完全覆盖,以致于不能发现某些错误.

由于 SLM 和 RTL 模型在接口、内部结点和时钟的不同,阻碍了时序电路到组合电路的转换,进而不能采用基于组合电路的等价性验证方法.Calypto 公司的时序等价性验证工具 SLEC[47]是一个有效的验证 SLM 和 RTL 等价的工具,并且不要求 SLM 和 RTL 之间具有相同的输入/输出接口和内部状态.但 SLEC 的求解能力有限,可以验证两个模型中周期的延迟/吞吐量在 100S 之内包含 50 万-70 万个门的 SLM 和 RTL 模型的等价性.对于更大规模的工业设计,则需要转化成相应的子模型/子功能部分,再进行等价性验证.

SLEC 还提供集成电路设计中所需的一系列其它功能,主要体现在 RTL lint 签核、功率估算和分析、C 和 RTL 形式化等价验证、C 和 C 形式化等价验证、SystemC 模型生成、C 和 RTL 高层合成,进而可以最大限度地缩短设计周期,降低风险.

2.3 符号模拟方法

SLM 和 RTL 的等价性验证是一项重大挑战,主要是因为 SLM 是由系统设计师所撰写,而 RTL 实现是由硬件设计师创建.这一做法导致了两种描述模式是有明显不同.从 RTL 和 RTL 的验证问题到 RTL 和 SLM 验证问题,最明显不同的是 SLM 的出现,如果解决了高层模型的问题,即把 SLM 转换成 RTL,则 RTL 和 SLM 的验证问题就可以得到解决.

符号模拟是一个针对高层模型间验证的较好方法,SLM 可以用符号表示,对于符号表示中的赋值语句又可以看作为一个电路,即赋值语句右端为电路的输入,左端为电路的输出,因此可以很好地将 SLM 到 RTL 的验证问题用 RTL 到 RTL 的验证方法进行求解.还可以对符号模拟这种方法进一步扩展,进而可以处理数组,结构体,逻辑和算术运算,甚至指针[48].

对于系统级模型的处理,基本是采用符号模拟的方法.然而,如果用显示的遍历方法,则会导致指数级的空间和逻辑问题.如果采用合并路径的方法,同样存在指数级逻辑复杂性问题.Feng 等[49][50]使用基于符号模拟方法验证 SLM 和 RTL 模型的等价性,这种方法验证两个组成部分的所有路径,此方法是基于位级的方法,并且提出在展开循环前的插入分割点,以克服空间的复杂性.

2.4 基于问题分解的方法

许多学者对数组和存储器[51-54]之间的映射关系进行了研究,进而把问题分解成规模较小的问题后再进行求解.硬件设计者在从 SLM 得到 RTL 时,SLM 中对应的数组在 RTL 中会以存储器的形式描述.如果能够找出 SLM 中数组与 RTL 中存储器之间的对应关系,则会大大减小 SLM 和 RTL 之间等价性验证的复杂度.然而,由于 SLM 和 RTL 中描述语言的特点, 可以很容易地找出数组和存储器间的对应关系.许多学者[55]-[57]对锁存器匹配比较点的选择方法进行研究,Aagaard 等[58-60]也对不同环境中关于状态映射的等价性验证方法进行了研究,这些方法也可以推广到数组和存储器映射关系的研究中.

Pankaj 等[61]给出了周期不明显时序电路的验证方法,提出了关于锁存器的输入、输出、状态映射的概念,进一步可以形成一个关于两个周期不明显的集成电路设计之间等价性验证问题.把两个设计转化为自动机,进而将 SLM 和 RTL 的等价问题转化为自动机的等价问题,即当转化后的两自动机等价时 SLM 和 RTL 等价.并在得到不等价后,把转化后自动机上的反例转化为 RTL 上的反例.

Vasudevan[62]将时序等价性验证问题转换为组合等价性验证问题进行求解.此方法加入了时序比较点,用来分解等价性验证问题规模,转变为位级引擎可以处理的更小空间的问题.这种基于位级的方法无法处理多个周期的工业设计.此外,此方法中候选等价结点的选择具有很大的局限性,仅当两个观测点的描述具有相同名称时,才识别为候选等价点.

2.5 其它等价性验证方法

国外在 SLM 和 RTL 的等价性验证方面做了许多研究.最直接的方法是把时序电路按时间帧展开,然后调用时序可满足性求解引擎[63,64]和时序 ATPG 引擎[65,66]进行求解,进而得到时序电路的等价性.Smria 等[67]给出了关于 C 和 RTL 间的组合电路的等价性验证方法,此方法把 C 直接转换成为 HDL,然后用 RTL 和 RTL 的等价性验证工具进行求解. 验证 SLM 和 RTL 的等价性需要强有力的可满足求解技术,位级和字级混合的推理技术将是有效的解决方法,并且在很多实际工业问题的等价验证中已经证明是有效的求解技术.Alizadeh[68]对 SLM 和 RTL 之间的等价性验证引入了混合的求解技术,混合求解技术主要包括基于位级的 SAT 或 BDD 和字级的无冗余的 TED 表达形式.在等价性验证时,并不需要把 SLM 转换成位级再与 RTL 进行等价性验证.

Matsumoto[69-71]提出了基于内容差异分析的等价性验证方法,文中先提取两个目标模型内容的差异,然后使用程序切片方法做依赖性分析,进而得出这两个模型的实际差异.然后,采用符号模拟的方法处理这些差异,最后给出等价性验证结果.当两个目标模型在功能以及结构比较相似时,这种验证技术效率较高.

Alan 等[72]把路径空间爆炸问题转化为逻辑爆炸问题,并用 BDD 进行表示,此方法的处理能力有限.koelbl 和 pixley[73]提出了使用电路表示代替符号模拟表达的方法,极大地减小了空间爆炸问题,还给出了基于两层表达的方法来减小路径条件的爆炸问题,分别把分支选择和路径条件描述为布尔变量和 BDD 形式.

Clark[74,75]给出了基于边界的等价性验证求解器 CBMC,主要结合基于边界技术求解,把要验证的 C 模型转化为布尔形式,并在转化时引入了关于指针和网表循环的改进技术；对 SLM 综合后转换为布尔公式,进而调用位级可满足求解器进行验证.由于 CBMC 把验证问题转化到布尔形式,调用基于位级的可满足求解器进行求解,因此限制了其求解能力.

3 形式化验证工具

形式化验证方法受到了工业界的高度重视，从学术科研领域逐步走向实际研究与应用。在当今的数字设计领域中,为了使自己的产品在竞争中脱颖而出,人们正在将越来越多的功能集成进自己设计的产品中,促使总体系统进而变得日益复杂.功能等价性验证是电子设计人员目前面临的主要挑战之一,美国的自动化设计公司 Cadence、Synopsys、Calypto、Mentor 等提供了成熟的验证工具和平台.

3.1 Cadence 公司验证工具

Cadence 是全球最大的电子设计技术、设计服务和程序方案服务供应商.其解决方案旨在提升和监控半导体、网络工程、计算机系统和消费电子产品、电信设备以及其它各类型电子产品的设计.其总部位于美国加州圣何塞（San Jose）,在全球各地设有销售办事处、设计及研发中心. Cadence 公司的电子设计自动化产品涵盖了电子设计的整个流程,包括系统级设计,功能验证,集成电路综合及布局布线,模拟、混合信号及射频集成电路设计,全定制集成电路设计,集成电路物理验证,电路板设计和硬件仿真建模等.下面简要介绍 Cadence 公司推出的形式化等价性验证平台和工具.

Cadence 公司的 Incisive Confromal 验证某一设计在各个关键步骤中不同版本模型的功能等价性,并且还可以帮助设计师们及时识别并且纠正刚刚产生的错误.进而可在整个设计流程中实现更快、更准确的错误监测和纠正.同时,该工具具有完整的验证覆盖率,使重新流片的风

险大大降低.

2004 年 Cadence 设计系统公司宣布,Cadence Incisive Conformal 等价性验证方案业已成为富士通有限公司全球的标准化方案,用于验证其高度复杂的上百万门级片上系统设计专用集成电路(ASIC). Incisive Confromal 之所以能够成为富士通公司的等价性验证方案,就在于其突出的容量与性能.借助这款工具,公司进而可以轻松地布置设计团队.富士通采用 Conformal 验证工具加快了多媒体、消费品以及通讯应用产品上市时间,并使其高度复杂的芯片的首次硅片成功率极大提高.

随着上千的流片设计获得成功,Incisive Confromal 等价性验证解决方案在本行业获得了最广泛的支持,该技术能够验证较大范围内的各种复杂电路,包括复杂的数据通道、数字逻辑、存储器以及用户定制逻辑；此外,还可以帮助设计师找到传统等价性验证工具不能找出但在实现过程中出现的错误.

2009 年中科院计算所开始采用 Cadence 公司的 Incisive Xtreme Ⅲ系统来验证下一代多核处理器设计.计算所为开发先进的 65 和 45 纳米多核处理器而部署 Incisive Xtreme Ⅲ系统,使计算所的工程师可以在确认软件操作的同时加速系统级验证.Xtreme Ⅲ系统满足了计算所的目标,在加速软硬件开发的同时降低昂贵的重制风险.进而加速其下一代 6400 万门以上龙芯3 号高级多核处理器RTL 设计和验证流程的开发.

Incisive Xtreme Ⅲ系统使得计算所得以加速仿真生产力,并且发现了至少 10 个关键性的系统级故障,这些故障在系统级环境中要运行数十亿个周期后才能被发现.该系统提供一个灵活的高性能软硬件协同开发验证平台,提供热交换和 VCD-on-Demand.这些性能可以帮助计算所的开发人员快速架设系统,比传统调试方法更容易发现系统级故障.Cadence 的技术可以提高龙芯 3 号开发的整体生产力、可预测性和品质.

2010 年深圳的无晶圆厂集成电路设计领先企业芯邦科技股份有限公司开始采用 Cadence Incisive Xtreme III 系统来加速其 RTL 设计流程,并且为下一代数字消费和网络芯片提供验证流程.芯邦是一家国内领先的芯片供给商,其芯片的目标应用领域有数字音视频处理、移动存储、网络通信和消费电子等. Cadence Incisive Xtreme III 系统以及 Incisive Enterprise Simulator 的部署,使芯邦的工程师能加速全芯片 SoC 验证,加速倍数可达 500 倍.

3.2 synopsys 公司验证工具

Synopsys 公司是提供电子设计自动化软件工具的主导企业,为全球集成电路设计提供先进的集成电路设计技术与验证平台,致力于复杂的芯片上系统的开发.同时,Synopsys 公司还提供设计服务,为客户简化设计过程,提高产品上市速度.Synopsys 公司总部设在美国加利福尼亚州 Mountain View,有超过 60 家分公司分布在北美、欧洲、日本与亚洲.下面简要介绍 Synopsys 公司推出的形式化等价性验证工具和平台.

Formality 采用形式化验证的技术来判断一个设计的两个版本在功能上是否等价.通过比较 RTL 和 Gate 或 Gate 和 Gate 的等价性来保证它满足原始的设计需求.在集成电路设计的流程中,用户使用形式化方法验证 RTL 与综合后 Gate 网表的功能等效性.这个验证可以用于整个设计周期,如时钟树综合、优化、网表编辑等之后,以便在流程的每一阶段都能在 Gate 级保持与设计规范的功能等价.这样在整个设计周期中就不再需要耗时的 Gate 级仿真.Formality 通过完备的验证覆盖将硅片失败的可能性降到最低.

Vera 验证系统支持高层次的功能验证.Vera 验证系统已被 NEC、Sun、Cisco 等公司广泛使用,用来验证其实际的产品,如从定制、半定制电路到高复杂度的微处理器,从单片 ASIC 到

多片 ASIC 组成的计算机和网络系统.Vera 验证系统的基本技术原理是产生灵活的并能自我验证的测试向量,然后将其应用到测试用例中以尽可能充分测试所设计的集成电路.Vera 验证系统适用于各个层次的等价性验证,还具有以下特点,与设计环境的紧密集成、数据及协议建模、启发式及完全随机测试和功能代码覆盖率分析.

公司刚刚推出了新的混合形式化验证工具 Magellan.Magellan 将新的 VCS 仿真工具引擎和高性能形式化工具引擎内置的强大能力相结合,进而帮助工程师发现可能隐藏于设计深层的需要仿真几千个周期才能发现的设计错误.Magellan 支持由 Verilog 和 VHDL 所做的设计,并正在构建符合成熟的 System Verilog 标准的工具,从而加强了 Synopsys 的 Discovery 验证平台的能力.

Magellan 还可以排除可能会产生不利影响的误报,并且发送确定性结果,进一步提升验证的能力.与传统的 RTL 形式化验证工具不同的是,Magellan 使用其内置的 VCS 引擎对其形式化工具引擎所发现的特性反例进行验证.新增了 Magellan 之后,现在 Synopsys 的 Discovery 验证平台实现了层次化验证,实现其强大的可验证设计技术,其中通过 VCS 和 Vera 将模块级设定和断言作为芯片级监控手段自动地重复使用.其在统一验证平台下进行层次化验证的能力,确保了两模型等价性,同时提升了设计者的整体验证能力和水平.

3.3 Calypto 公司的验证工具

Calypto 公司提供功耗优化和功能验证工具,帮助设计人员设计高质量集成电路产品.公司总部在 Santa Clara,在日本,印度,欧洲和北美洲设有办事处.Calypto 的客户包括全球 500 强企业,如 Nvidia,Qualcomm,Renesas, Freescale 和 ST 微电子公司.并与多家电子设计自动化公司合作,如 Synopsys,Mentor Graphics 和 Cadence.

Calypto 设计公司的验证工具 SLEC 是面向时序电路等价性验证第一款产品.SLEC 具有多个求解器,主要包括 Word Solver、HW intent extraction 和 Induction based proofs.Word Solver 是基于字级的可满足性求解器,是以字为单位进行处理,相对于以位为单位的处理方法缩短了处理时间.HW intent extraction 可以从 C++描述中找到设计者的意图,进而提高验证的效率.最重要的求解器是 Induction based proofs.可以通过削减所需检测的状态数,提高验证的效率.

2005 年,Calypto 公司宣布 Mentor 的“Catapult C”和 SLEC 可配合使用,能够对动作合成之前的 C++与动作合成之后的 RTL 的等价性进行验证.在此之前,由于没有对二者进行验证的有效手段,因此很多时候对于动作合成工具的导入就会犹豫不决.如果 SLEC 能够像 Calypto 所介绍的那样运行,那么就将消除导入动作合成工具面对的问题,进而加速集成电路的设计和验证效率.

4 结束语

当前主流集成电路已经达到了几千万甚至上亿门电路的规模,高端图形芯片甚至包含了数十亿个晶体管.在这样的复杂度下,等价性验证成为集成电路生产周期的瓶颈.随着我国大规模集成电路业的兴起,我们的工业界也越来越离不开验证系统和工具的辅助.目前验证类软件和工具主要集中在美国设计自动化公司（Cadence、Synopsys、Mentor、Calypto）里,国内则完全是一个空白,这对我们自主知识产权的芯片设计和创新是严重的制约.据国内知名的<电子工程专辑>网站统计,国内以中星微电子为代表的具有自主芯片设计能力的公司已超过 600 家,若国内研究的关键问题得以解决和自有知识产权技术建立的原型系统能够逐步成熟并投入市场,则对于缩小我国与世界信息技术发达国家的差距,提升我国基础芯片研发能力,

增强国防实力具有重要且深远的意义.

本文首先分析了 RTL 和 RTL、SLM 和 RTL 的形式化等价性验证方法,然后介绍了自动化电子设计公司关于形式化等价性验证工具和平台.形式化等价性验证工具和方法的研究已经取得了较大进展,但还存在如下的问题要进一步研究.

在 RTL 和 RTL 或 SLM 和 RTL 的形式化等价性验证中,多是采用基于割集的方法,进而把规模较大问题转换成规模较小的问题进行处理.而由于验证候选等价结点等价后会用新变量替代原来候选结点,引入的新变量忽略了原有的候选等价结点对应电路中的约束关系,可能导致发生误判现象.至今,还没有较好的消除误判的解决方法,对消除误判方法的研究是一个重要的研究内容.

在集成电路的验证流程中,如果验证工具发现两模型不等价,设计者和验证人员都面临着一个非常棘手的任务,即找到修改后模型中的错误或者尽可能压缩可疑的设计错误区域,进而方便随后模型的纠正,这就是所谓的设计错误诊断问题.国内学者对基于模型的诊断的研究取得了较好的成果[76,77],将基于模型的诊断研究成果应用到设计错误的诊断上是一个值得研究的方向.

[参考文献] (References)

[1] Thomas Kropf. Introduction to Formal Hardware Verification[M]. Springer: Berlin ,New York ,Hong Kong ,Tokyo, 1999.

[2] Park J, Pixley C, Burns M, et al. An Efficient Logic Equivalence Checker for Industrial Circuits [J].Journal of Electronic Testing: Theory and Applications, 2000, 16 (1):91-106.

[3] Farzad Nekoogar. Timing Verification of Application-Specific Integrated Circuits [M]. Prentice Hall PTR: New Jersey, 1999.

[4] R.B.Jones, J.W.O'Leary, et al. Practical Fromal Verificaiton in Microprocessor Design [J].IEEE Design & Test of Computers, 2001,18 (4):16-25.

[5] Soha Hassoun, Tsutomu Sasao, et al. Logic Synthesis and Verification [M]. Kluwer Academic Publisher: Boston ,Dordrecht ,London, 2002.

[6] Saglamdemir M.O., Sen A., Dundar G. A formal equivalence checking methodology for Simulink and Register Transfer Level designs Synthesis[C]. Proceedings of International Conference on Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), 2012 ,221-224.

[7] J.R.Burch, V.Singhal. Robust Latch Mapping for Combinational Equivalence Checking [C]. in Proceedings of International Conference on Computer Aided Design (ICCAD), San Jose, 1998,563-569.

[8] Randal E. Bryant. A methodology for hardware verification based on logic simulation [J]. Journal of the ACM, 1991, 38(2):299-328.

[9] Salim Ismail A.A. On the Verification of a WiMax Design Using Symbolic Simulation[D]. Canada: Concordia University,2012.

[10] R. E. Bryant. Graph-based algorithms for boolean function manipulation [J]. IEEE Transactions on Computers, 1986,35(8):677-691.

[11] Niklas Eén, Armin Biere. Effective preprocessing in SAT Through Variable and Clause Elimination [C]. Proceedings of 8th International Conference on Theory and Applications of Satisfiability Testing, 2005, 61-75.

[12] J. P. Marques-Silva, K. A. Sakallah. GRASP-A New Search Algorithm for Satisfiability [C]. Proceedings of IEEE/ACM International Conference on Computer-Aided Design, 1996, 220-227.

[13] M. W. Moskewicz, C. F. Madigan, Y. Zhao, et al. Chaff: Engineering an efficient SAT solver [C]. Proceedings of Design Automation Conference (DAC'01), 2001, 530-535.

[14] Bart Selman , Henry Kautz , Bram Cohen. Local search strategies for satisfiability testing [J].DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 1993, 521-532.

[15] Feng Lu , Li-C. Wang , Kwang-ting Cheng, et al. A Circuit SAT Solver with Signal Correlation Guided Learning [C]. Proceedings of the conference on Design, Automation and Test in Europe, Munich, 2003, 892-897.

[16] H. Lin, JG Sun, YM Zhang. Theorem proving based on extension rule [J]. Journal of Automated Reasoning, 2003, 31:11-21.

[17] 孙吉贵, 刘叙华. 模态归结弱包含删除策略[J]. 计算机学报, 1994, 17(5): 321-329.

[18] 孙吉贵, 刘叙华. Cialdea 一阶模态归结系统的不完备性及其改进[J].计算机学报, 1995, 18(6):401-408.

[19] 孙吉贵,李莹,朱兴军,等. 一种新的基于扩展规则的定理证明算法[J]. 计算机研究与发展, 2009, 14(1): 9-14.

[20] 王湘浩, 刘叙华. 广义归结[J]. 计算机学报, 1982, 5(2): 81-92.

[21] Liming Zhang, Hailin Zeng, Fang Yang, Dantong Ouyang. Dynamic Theorem Proving Algorithm for Consistency-based Diagnosis [J]. Expert Systems With Applications, 2011, 38(6):7511-7516.

[22] Liming Zhang, Dantong Ouyang,Jian Zhao, Hongtao Bai. The parallel theorem proving algorithm based on

semi-extension rule[J]. Applied Mathematics and Information Science,2012,6(1S):70-75.
[23] 赖永, 欧阳丹彤, 蔡敦波, 等. 基于扩展规则的模型计数与智能规划方法[J]. 计算机研究与发展, 2009, 46(3): 459-469.
[24] C. L. Berman, L. H Trevillyan. Functional comparison of logic designs for VLSI circuits [C]. Proceedings of International Conference on Computer-Aided Design, 1989, 456-459.
[25] A. Kuehlmann and F. Krohm. Equivalence checking using cuts and heaps [C]. Proceedings of 34th Design Automation Conference, 1997, 263-268.
[26] 黄伟,唐璞山.基于切割法的时序电路等价验证[J].复旦学报自然科学版,2006,45(1):102-106.
[27] 杨军,郑飞君,卢永江,葛海通,严晓浪.结合通用割集和专用割集的组合电路验证方法.浙江大学学报工学版,2006,9(40):1511-1515.
[28] Y. Matsunaga. An efficient equivalence checker for combinatorial circuits [C]. Proceedings of the 33th ACM/IEEE Design Automation Conference, Las Vegas,1996, 629-634.
[29] S. M. Reddy, W. Kunz, D. K. Pradhan, Novel verification framework combining structural and OBDD methods in a synthesis environment [C]. Proceedings of the 32th ACM/IEEE Design Automation Conference, San Francisco, 1995, 414-419.
[30] J. Jain, A. Narayan, M. Fujita, et al. Formal verification of combinational circuits [C]. Proceedings of International Conference on VLSI Design, 1997,218-225.
[31] C. van Eijk, G. Janssen .Exploiting structural similarities in a BDD-based verification method [C]. Proceedings of the 2nd International Conference on Theorem Provers in Circuit Design, 1995, 110-125.
[32] 张立明,欧阳丹彤,白洪涛.结合约束满足消除误判的等价性验证方法[J].吉林大学学报(工学版),2011,41(5):1374-1377.
[33] Zhang, Guiling, Ouyang Dantong, Bai Hongtao, Zeng, Hailin, Ma Tiemin, Zhang Yuehua.Formal model extraction for combinational equivalence checking[J], Journal of Convergence Information Technology,2012, 7(8): 371-380.
[34] Hailin Zeng, Dantong Ouyang, Liming Zhang, Guiling Zhang. Verilog Combinational Equivalence Checking based on SMT Constraint Solver [J]. ICIC Express Letters Part B: Applications. 2011, 2(5):1087-1092.
[35] 曾海林.基于 SMT 约束求解器的 Verilog 组合电路等价性验证[D].吉林：吉林大学，2012.
[36] 杨军,卢永江,葛海通,郑飞君,严晓浪. 一种避免内存爆炸的组合电路等价性验证方法[J].电路与系统学报, 2007,12(3): 21-25.
[37] 郑飞君,严晓浪,葛海通,杨军,卢永江.使用输出分组和电路可满足性的等价性验证算法[J].计算机辅助设计与图形学学报, 2005,17(11):2484-2488.
[38] 李东海,马光胜,胡靖.定点算术数据通路的等价性检验方法[J].计算机辅助设计与图形学学报, 2009,21(1): 27-32.
[39] 丁敏,唐璞山.改进的时间帧展开的时序电路等价验证算法[J]. 计算机辅助设计与图形学学报,2006,18(1):53-61.
[40] 柯宪明,唐璞山.结合模拟蕴含技术的电路验证方法[J]. 微电子学与计算机,2007,24(2):58-61.
[41] 郑伟伟,吴为民,边计年.基于线性规划的 RTL 可满足性求解和性质检验[J]. 计算机辅助设计与图形学学报,2006,18 (14): 538-544.
[42] Alfred Koelbl, Reily Jacoby, Himanshu Jain, et al. Solver Technology for System-level to RTL Equivalence Checking [C]. Proceedings of Automation and Test in Europe, 2009.
[43] P. Manolios, S. K. Srinivasan, D. Vroon. Automatic memory reductions for rtl model verification [C]. Proceedings of International Conference on Computer Aided Design, 2006, 786-793.
[44] V. Ganesh, D. L. Dill. A decision procedure for bit-vectors and arrays [C]. Proceedings of International Conference on Computer Aided Verification, Berlin, Germany: Springer-Verlag, 2007,524-536.
[45] Robert Brummayer, Armin Biere. Boolector: An efficient SMT solver for bit-vectors and arrays [C]. Proceedings of Tools and Algorithms for the Construction and Analysis of Systems, 2009, 5505:174-177.
[46] Susmit Jha , Rhishikesh Limaye , Sanjit A, et al. Beaver: Engineering an Efficient SMT Solver for Bit-Vector Arithmetic[C]. Proceedings of the 21st International Conference on Computer Aided Verification, Grenoble, France,2009.
[47] Calypto Design Systems. calypto.com/products.
[48] E. Clarke, D. Kroening. Behavior consistency of C and Verilog programs using bounded model checking [C]. Proceedings of DAC, ACM Press, 2003,368-371.
[49] X. Feng, A. Hu. Early Cutpoint Insertion for High-Level Software vs. RTL Formal Combinational Equivalence Verification [C]. Proceedings of the 43th Design Automation Conference (DAC), 2006, 1063-1068.
[50] Todman T., Luk W.Verification of streaming designs by combining symbolic simulation and equivalence checking[C]. Proceedings of the 22nd International Conference on Field Programmable Logic and Applications (FPL), 2012,203-208.
[51] A. R. Bradley, Z. Manna, H. B. Sipma. What's decidable about arrays[C]. Proceedings of VMCAI, 2006,427-442.
[52] Nguyen H., Hsiao M.S.Sequential equivalence checking of hard instances with targeted inductive invariants and efficient filtering strategies[C]. Proceedings of International Conference on High Level Design Validation and Test Workshop (HLDVT), 2012,1-8.
[53] J. McCarthy. Towards a mathematical science of computation [C].Proceedings of IFIP Congress, 1962, 21-28.
[54] A. Stump, C. W. Barrett, D. L. Dill, et al. A decision procedure for an extensional theory of arrays [C]. Proceedings of Logic in Computer Science, 2001,29-37.

[55] D. Anastasakis, R. Damiano, H.-K. T.Ma, et al. A practical and efficient method for compare-point matching[C]. Proceedings of the 39th conference on Design automa-tion, 2002,305-310.
[56] Malazgirt G.A.,Culha E. , Sen, A.,et al.A Verifiable High Level Data Path Synthesis Framework[C]. Proceedings of the 15th Euromicro Conference on Digital System Design (DSD), 2012,397-404.
[57] C. van Eijk, J. Jess. Detection of equivalent state variables in finite state machine verification [C]. Proceedings of the International Workshop on Logic Synthesis 1995, 3-35.
[58] M. Aagaard, B. Cook, N. A. Day, et al. A framework for microprocessor correctness statements[C]. Proceedings of CHARME, 2001,433-448.
[59] P. Bjesse, J. Kukula. Automatic generalized phase abstraction for formal verification[C]. Proceedings of ICCAD, 2005,1076-1082.
[60] A. Koelbl, J. R. Burch, C. Pixley. Memory modeling in ESL-RTL equivalence checking[C]. Proceedings of DAC, 2007,205-209.
[61] Pankaj Chauhan, Deepak Goyal, Gagan Hasteer, et al. Non-cycle-accurate sequential equivalence checking[C]. Proceedings of DAC, 2009, 460-465.
[62] S. Vasudevan, V. Viswanath, J. Abraham, et al. Automatic Decomposition for Sequential Equivalence Checking of System Level and RTL Descriptions [C].Proceedings of Formal Methods and Modes for Co-Design, Memocode, 2006,71-80.
[63] F. Lu, M. K. Iyer, G. Parthasarathy, et al. An efficient sequential sat solver with improved search strategies [C]. Proceedings of DATE, 2005,1102- 1107.
[64] M. R. Prasad, A. Biere, A. Gupta. A survey of recent advances in sat-based formal verification[C]. Proceedings of STTT , 2005,7(2):156- 173.
[65] S.-Y. Huang, K.T. Cheng, K.C. Chen. Verifying sequential equivalence using atpg techniques [J]. ACM Trans. Des. Autom. Electron. Syst, 2001, 244-275.
[66] J. A. Abraham, V. M. Vedula, D. G. Saab. Verifying properties using sequential atpg [C]. Proceedings of International Test Confer- ence, 2002, 194-200.
[67] L. Smria, R. Mehra, B. Pangrle, et al. Rtl c-based methodology for designing and verifying a multi-threaded processor [C]. Proceedings of the 39th conference on Design automation, 2002, 123-128.
[68] B. Alizadeh, M. Fujita. A Hybrid Approach for Equivalence Checking Between System Level and RTL Descriptions [C]. Proceedings of the International Workshop of Logic and Synthesis, 2007, 298-304.
[69] H. Saito, T. Ogawa, T. Sakunkonchak, et al. An equivalence checking methodology for hardware oriented C-based specifications[C]. Proceedings of the International High-Level Design, Validation, and Test Workshop, 2002, 139-144.
[70] T. Matsumoto, H. Saito, M. Fujita. An equivalence checking method for c descriptions based on symbolic simulation with textual differences[C]. Proceedings of IEICE Transactions on Fundamentals of Electronics, Communications and Com- puter Sciences, 2005, 3315-3323.
[71] A. J. Hu, D. L. Dill, A. J. Drexler, et al. Higher-level specification and verification with BDDs [C]. Proceedings of Computer-Aided Verification: 4th Intl Workshop, 1992. LNCS 663.
[72] S. Minato. Generation of BDDs from hardware algorithm descriptions [C]. Proceedings of ICCAD, 1996.
[73] A. Koelbl, C. Pixley. Constructing efficient formal models from high-level descriptions using symbolic simuluation [C]. Proceedings of Parallel Programming, 2005, 33(6):645-666.
[74] H. Jain, D. Kroening, E. Clarke. Verification of SpecC using Predicate Abstraction [C]. Proceedings of Formal Methods and Modes for Co-Design ,Memocode, 2004, 7-16.
[75] E. Clarke , D. Kroening. Hardware verification using ANSI-C programs as a reference[C]. Proceedings of ASPDAC, 2003, 308-311.
[76] Xiangfu Zhao, Liming Zhang, Dantong Ouyang, et al. Deriving all minimal consistency-based diagnosis sets using SAT solvers [J]. Progress in Natural Science, 2009, 19 (4): 489 - 494.
[77] Xiangfu Zhao, Dantong Ouyang. Model-based diagnosis of discrete event systems with an incomplete system model [C]. Proceedings of 18th European Conference on Artificial Intelligence (ECAI-08), Patras, Greece, IOS Press, Amsterdam, 2008, 189-193.