

基于硬件模拟的 SAT 求解框架

何安平,毛乐乐,谌知学,吴尽昭

(广西民族大学 混杂计算与集成电路设计分析重点实验室,广西 南宁 530006)

摘 要: 使用硬件方法求解 SAT 问题,采用现场可编程门阵列(FPGA)技术,针对大规模实际系统的 CNF 公式实例,定制化编译和转换为 FPGA 芯片,并完全依据 FPGA 硬件完成 SAT 满足性求解过程.

关键词: 布尔可满足;现场可编程门阵列;合取范式

中图分类号: TN710.9

文献标识码: A

文章编号: 1000-7180(2016)09-0124-04

A Hardware Framework of SAT Solver

HE An-ping, MAO Le-le, CHEN Zhi-xue, WU Jin-zhao

(Guangxi Key Lab of Hybrid Computation and IC Design Analysis, Guangxi University for
Nationalities, Nanning 530006, China)

Abstract: In this paper, we customized the FPGA chip to fit the SAT problem, e. g., translating and compiling the large scale system, and then successfully solved the problem by FPGA autonomously.

Key words: SAT; FPGA; CNF

1 引言

布尔可满足性问题(SAT)即是计算机理论与应用的核心问题之一,也是第一个被证明的 NP 问题^[1]. 目前, SAT 已经应用在计算机系统结构设计等领域,特别在集成电路设计验证方面, SAT 具有极其广泛而深入的应用.

SAT 问题用于判断布尔逻辑公式是否存在一组满足解,即一组可以使布尔公式值为真的布尔变量的赋值. 一般而言, SAT 问题的布尔公式的标准形式是合取范式(conjunctive normal form, CNF), 判断 CNF 公式是否为真的工具被称为 SAT 求解器.

目前国内外对 SAT 问题的研究主要集中在软件求解方法上,如文献[1,2],每年的 SAT 国际大赛的参赛求解器几乎都为软件. 不过国内外也针对 SAT 问题研究了若干种 SAT 硬件求解器,这些求

解器均选用了计算能力强的现场可编程门阵列(FPGA),作为硬件实现平台. 已有的 SAT 硬件求解器,绝大多数采用应用型方法,如文献[3,4],以及国内中山大学在此方面的工作^[5],这种方法本质上是对软件 SAT 算法的硬件实现,即使用 FPGA 实现一些瓶颈算法,最终的求解器工作在软硬件协同的机制下. 这种方法的优点在于通用性,即只需要进行一次编译和配置的过程,然后可以对所有实例进行计算. 其缺点在于,这种解决机制本质上并没有将电路系统的特征引入 SAT 的求解中来,而仅仅使用了 FPGA 的可编程特征,所以这种方案依然会遇到与软件求解器相同的挑战.

另外一种方法就是所谓的实例型方法,如文献[6],其思路是针对每一个 SAT 实例独立开发和配置芯片,而后对芯片加电进行满足性计算. 相比应用型方法而言,这种方法的通用性较差,成本较高,但是这种方法充分发挥了数字电路系统的内在特征,

收稿日期: 2015-12-03; 修回日期: 2016-01-21

基金项目: 国家自然科学基金(61402121, 11371003, 11461006); 广西自然科学基金(2013GXNSFAA019342, 2012GXNSFGA060003); 广西高校科学技术研究项目(ZD2014044); 广西教育厅科研资助项目(201012MS274); 广西民族大学 2015 年研究生教育创新计划项目(gxun-chxs2015097)

完全避免了上述软件和应用型方法面临的挑战,将非常适用于大规模的 SAT 实例.

2 本文 SAT 求解方法概述

本文采用了实例型 SAT 求解系统,主要针对这种方法通用性差的特征,提出并开发出一种实例型自动求解机制和框架,主要思路为针对大规模实际系统的 CNF 公式实例,自动地定制化编译和转换为 FPGA 芯片,由 FPGA 硬件完成系统的 SAT 满足性求解过程.将 CNF 公式到电路的转换过程,FP-GA 芯片仿真、综合实现和验证,及 FPGA 配置、下载和计算求解统一起来,方便简洁地判断 CNF 式可满足性质.

我们提出的 SAT 的硬件求解方法大致可以划分为翻译、封装、综合、配置与下载,以及求解 5 个环节:CNF 式是表达 SAT 问题的标准手段,要求解 SAT 问题,首先要对 CNF 式进行翻译处理,根据 CNF 式的逻辑定义用硬件描述语言对其进行行为级建模,将 CNF 式映射为与或非门电路形式,随后将状态机模块与 CNF 式所映射的电路封装在一起,从而在同一硬件环境下进行交互.其中状态机模块可以遍历生成 CNF 式中命题变量所对应的状态值,而后通过 EDA 工具进行综合、引脚配置转换成比特文件并下载到 FPGA 开发板,最后为 FPGA 芯片加电,整个流程全部由硬件系统完成 SAT 问题的判定,如图 1 所示.

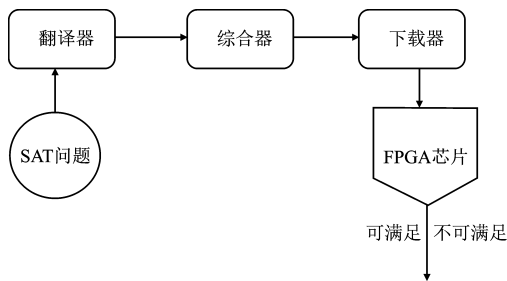


图 1 SAT 硬件求解流程

相对于软件求解 SAT 问题,文中提出的硬件求解器充分发挥了数字电路系统的内在特征,避免了软件求解器算法挑战,更适用于大规模 SAT 的实例.

3 硬件求解框架

文中的硬件求解方法的核心是 SAT 问题的翻译和封装,这两个步骤共同构成了所述的硬件求解框架.

3.1 CNF 的逻辑电路形式

CNF 式是表达 SAT 问题的标准手段,我们也采用这种表达方式作为待验证 SAT 问题的原始输入格式.CNF 式的翻译过程可以参照此公式的逻辑意义:CNF 式中子句内各文字间是逻辑析取的意义,即 $\vee$ 联接各文字组成子句;子句间的关系为逻辑合取,用逻辑联结词 $\wedge$ 联接.CNF 公式与寄存器传输级(RTL)数字电路的定义是一致的,而事实上布尔逻辑符合 RTL 级电路设计的基础理论,将 CNF 公式表示为逻辑电路是一种自然有效的方法.但对于大变量 CNF 公式的翻译,还需考虑技巧.

具体而言,根据描述 CNF 式的文件语法,每一行内的文字或逆文字之间是逻辑或的关系,并以 0 结束,我们开发的翻译器遵循门级 Verilog 语言的语法规则,将 CNF 式中的逻辑关系,替换为数字电路中的逻辑门电路,算法的伪代码如下所示.

算法 1 CNF 解析与转换算法

```
1: read CNF file;
2: for all literal  $x$  do
3: if  $x$  be a negative literal then
4: creat_INV_gate( $x$ );
5: else
6: creat_AND_gate( $x$ );done
7:for all Clause do
8:creat ClauseNet;
9: done
10:create CNFNet;
```

3.2 SAT 问题的封装

对 SAT 的一般硬件解决方案是将待验证电路作为 DUT(device under test),信号激励的产生机制用软件实现,而有软件交互完成 SAT 问题的求解功能,但这种方法因为有软件参与,并不能完全发挥硬件求解的速度优势,硬件电路常常等待软件系统的激励信号,所以我们采用的激励电路和待验证电路均为硬件实现,并自主完成验证过程的方案.

为求解 SAT 问题首先读取 CNF 式,根据上节所述的算法编写的翻译器将其自动翻译成门级数字电路,将 FPGA 的内在结构同 SAT 问题的求解自然地合为一体,由硬件电路系统的数字特征解决其对应的 SAT 问题.通过开发的激励模块可以遍历生成 CNF 式中命题变量所对应的状态值,将所生成的状态值并依次赋值到此 CNF 式所翻译成的数字电路系统中,将 CNF 模块与激励模块封装在一起,两者完全在硬件的环境下同一高速时钟的支配下进行同步交互,随后自主求解待验证 SAT 问题(如图 2 所示).将整个求解 SAT 问题封装在同一硬件系统

中并实现,简化了人机交互的繁琐,降低了人机交互时的出错率,同时发挥出硬件激励和求解的速度优势.

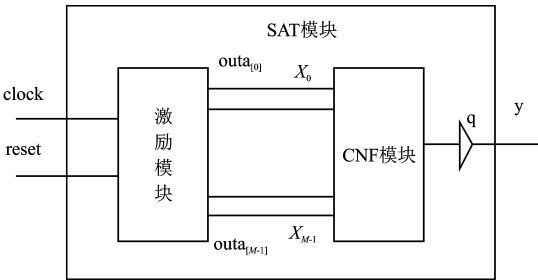


图 2 SAT 硬件封装示意图

4 FPGA 实现

FPGA 规模较大,适应于时序、组合等逻辑电路应用场合,可以代替几十甚至上百块通用 IC 芯片. FPGA 的集成度很高,可以完成极其复杂的时序和组合逻辑电路功能,它既解决了 ASIC 不可编程、功能有限的缺点,又克服了原有可编程器件电路数有限的缺点,本文采用 Xilinx 公司 Virtex-7 系列 xc7vx485t-2ffg1761 型号的 FPGA,此型号的 FPGA 采用高速全局时钟以及新型六输入 LUT 架构,在资源占用率方面具有显著优势,与同类器件相比,可以使用较小的 Virtex-7FPGA 来实现同样的设计,节省电路板空间并降低功耗和成本,同时六输入 LUT 实现减少寄存器之间逻辑数,从而提高了性能,适应于高速、高密度的 SAT 硬件求解系统.

图 3 描述了基于 FPGA 的 SAT 求解器的设计流程. 本文所研究的 SAT 硬件求解系统采用实例型框架,其思路是针对每一个 SAT 实例独立开发和配置芯片,经过翻译模块对 CNF 式翻译,继而进行编译仿真,综合实现、下载,最后对芯片上电进行满足性计算.

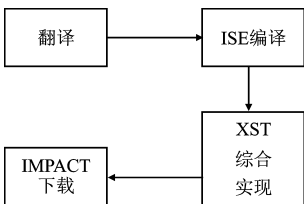


图 3 基于 FPGA 的 SAT 求解器

首先根据算法 1 开发的翻译模块可以将 CNF 式直接自动转换为门级电路描述,通过激励模块遍历生成 CNF 公式中命题变量所对应的状态值并映射到此电路,并将此电路嵌入设计的硬件求解框架.

为了验证所设计的硬件求解器能否符合要求,利用 Xilinx 公司的开发工具 ISE 进行编译,对程序设计中的语法进行检查,随后编写测试向量进行波形仿真验证,一旦仿真波形符合要求,将以此为模板进行生成器的开发,以后无论遇到何种变量和子句的 CNF 式都可以自动生成相应的 SAT 求解框架.

编译仿真通过后,利用 Xilinx 公司内嵌在 ISE 软件中的综合工具 XST 将描述 SAT 问题的 Verilog 语言翻译成由与、或、非门和 RAM、触发器等基本逻辑单元组成的网表,并根据目标和约束条件优化生成的网表,XST 是 Xilinx 公司自己的综合工具,对部分 Xilinx 芯片独有的结构具有更好的融合性. 完成输入以及针对 Virtex-7 系列 xc7vx485t-2ffg1761 型号的 FPGA 进行管脚分配后,就可以进行综合和实现了,最后生成比特文件.

最后通过内嵌在 ISE 软件中的 iMPACT 配置工具使用 JTAG 模式直接将比特文件配置到此型号 FPGA 芯片中. iMPACT 能生成 PROM 各种格式的下载文件,并校验配置数据是否正确. 或者使用 ChipScope Pro 软件,设定触发以及数据线宽度和采集长度,并将其和 ICON(Integrated Controller Pro core)核关联起来,然后完成设计以及相关核的综合,将设计中输出端信号和时钟信号连接起来,下一步完成整体系统的实现并下载到此型号 FPGA 中,最后将输出端信号连接到 LED 灯,当 CNF 式可满足时,LED 灯常亮,或者打开 ChipScope Analyzer 设定触发条件,观察波形.

5 实验与性能分析

本文在测试平台上实现了 SAT 硬件求解器,测试平台由一台主机和一块 FPGA 算法加速器构成,主机配置为 Intel 四核 I5 处理器,4.0 GB 内存,硬件加速器是 Xilinx 公司 Virtex-7 系列的 XC7VX485T-2FFG1761C,简称 VC707. 所使用的 EDA 工具 ISE 是 Xilinx 公司推出的非常通用的 FPGA 工具软件,不仅包括逻辑设计所需的一切,还具有大量简单易用的内置式工具和向导,使得 I/O 分配,功耗分析,时序驱动设计收敛、HDL 仿真等关键步骤变得容易而直观. ISE 的主要功能包括设计输入、综合、仿真、实现和下载,覆盖了 FPGA 开发的全过程.

将输出端与 Xilinx 公司开发板中的 LED 灯引脚相连,通过 LED 灯的指示判断 SAT 是否可满足. 图 4 为一 CNF 式的仿真波形图. 输出端 y 最后输出

为高电平,说明此 CNF 式是可满足的.

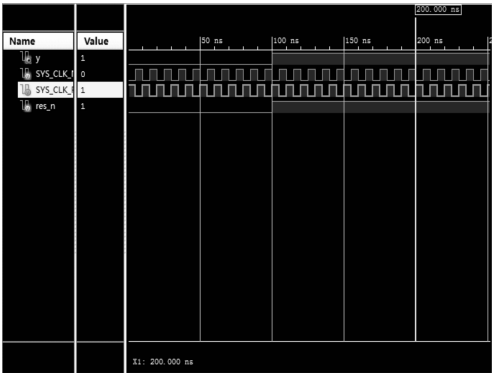


图 4 CNF 式的仿真波形

通过 ISE 软件对例 1 的 CNF 式进行综合下载到 FPGA 上来验证其可满足性,LED 灯亮表明与仿真结果相同,实现硬件对 SAT 问题的验证,见图 5.

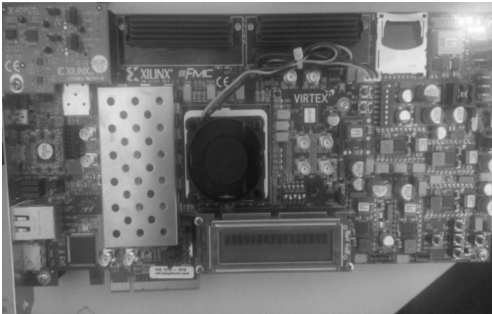


图 5 开发板 LED 灯判断 SAT 是否可满足

测试 SAT 问题硬件求解器的运行情况,结果显示 FPGA 求解的计算结果与软件的计算结果是完全一致的,表 1 所示为 SAT 硬件求解器实验结果.

6 结束语

布尔可满足(SAT)是计算机领域的基础问题之一,传统软件实现的 SAT 满足性求解器已经无法应对实际系统中变量数目激增的巨大挑战. 本文提出一种基于硬件仿真的 SAT 求解方法,基于 FPGA 硬件方便快速地判断 CNF 式是否可满足,采用实例型方法,针对每一个 SAT 实例独立开发和配置芯片,而后对芯片加电进行满足性计算. 相比应用型方法而言,这种方法充分发挥了数字电路系统的内在计算能力,具有潜在的求解大规模的 SAT 问题的能力.

表 1 SAT 硬件求解器实验结果

序号	变量/子句	综合时间/s	硬件求解时间/s
1	5/15	164	10×10^{-9}
2	10/24	163	175×10^{-9}
3	15/36	164	5.76×10^{-6}
4	20/48	164	170.26×10^{-6}
5	25/60	158	5.41×10^{-3}
6	30/72	165	0.38
7	35/84	162	5.57
8	40/96	168	177.86
9	45/108	160	5 677.45

参考文献:

[1] 张建民,沈胜宇,李思昆. 可满足性求解技术研究[J]. 计算机工程与科学,2010,31(1):500-504.

[2] 黄文奇,金人超. 求解 SAT 问题的拟物拟人算法——Solar[J]. 中国科学(E辑),1997,27(2):179-186.

[3] J T D. Sousa, J P Marques-Silva, M Abramovici. A configware/software approach to SAT solving[C] // Proc Ninth IEEE Int’ Symp Field-Programmable Custom Computing Machines. California; IEEE,2001;239-298.

[4] N A Reis, J T de Sousa. On implementing a configware/software SAT solver[C]// Proc 10th IEEE Int’l Symp Field-programmable Custom Computing Machines. Napa,California; IEEE,2002;282-283.

[5] 周进,赵希顺. 基于硬件可编程逻辑(FPGA)的 SAT 算法的综述[J]. 电子世界,2012,33(6):61-63.

[6] P Zhong, M Martonosi, P Ashar, et al. Using configurable computing to accelerate boolean satisfiability [J]. IEEE trans Computer-Aided Design of Integrated Circuits and Systems, 1999,18(6):861-868.

作者简介:

何安平 男,(1981-),博士,副教授. 研究方向为形式化方法.

毛乐乐 男,(1989-),硕士研究生. 研究方向为可满足性问题求解方法.

湛知学(通讯作者) 男,(1991-),硕士研究生. 研究方向为可满足性问题求解方法. E-mail:137391629@qq.com

吴尽昭 男,(1965-),博士,教授. 研究方向为形式化方法.