ISCAS 中国科学院软件研究所学术年会’2023
暨计算机科学国家重点实验室开放周

关键技术

CHA：Chisel语言的类SVA时序断言扩展及形式验证关键技术

于世禛，董一凡，李勇，吴志林，杨大卫，张立军

联系人：于世禛　13121802177 yusz@ios.ac.cn

□ □ □ □

- Chisel□ □ □ □ □ Scala□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 化、复用性高的特点，已经被广泛应用于 RISC-V处理器和片 □ □ □ □ □ □
- Chisel□ □ □ □ □ □ □
  - □ □ □ □ □ □ □ □ □ □
  - 在 Chiseltest中有部分扩展，可以以 past算子的形式描述简 □ □ □ □ □ □ □ □ □ □ **表达能力弱**，**表达性质困难** □ □ □

BOOM　XIANGSHAN　Nutshell

使用Chisel 开发的处理器设计

关键技术介绍

- 前端对Chisel 断言语言添加类SVA的**序列**/性质算子，提高性质表达能力

序列算子与SVA算子的对应关系

	布尔序列	序列交叠	序列连接	**序列析取**	重复0次	-
SVA	u	##0	##1	or	[*0]	[*1:$]
Ours	u	##0	##1	|	[*0]	[*1:$]

性质算子与SVA算子的对应关系

	交叠蕴含	性质取反	性质合取	性质析取	nexttime	always	s_eventually	s_until
SVA	|->	not	and	or	nexttime	always	s_eventually	s_until
Ours	|->	!	&&	||	X	G	F	U

- 后端维护断言的编译过程，结合模型检测技术支持对硬件设计进行形式化验证

Chisel
设计
断言
FIRRTL 编译器
High FIRRTL
Low FIRRTL
High-fir Annotation
Low-fir Annotation
时序性质
迁移系统
迁移系统
Büchi 自动机
乘积迁移系统
Spot
ChiselTest
btor2文件
模型检测工具
结果
输出

1. 利用Target-Annotation 机制维护断言与设计中的信号在编译过程中的一致性
2. 对时序性质进行简单改写，调用spot工具翻译成自动机，解析自动机转化为迁移系统
3. 通过迁移系统乘积的方式将断言与硬件设计做同步
4. 实现L2S算法将自动机判空问题转化为安全性质检查问题，调用硬件模型检测工具求解

案例介绍

Host Adapter
cyc_o
stb_o
ack_i
err_i
adr_o
dat_o
we_o
sel_o
dat_i
Device Adapter
cyc_i
stb_i
ack_o
err_o
adr_i
dat_i
we_i
sel_i
dat_o

针对左图所示的一组Wishbone 协议适配器

在Chisel 设计中添加扩展后的断言

assert(stb |–> (stb U ack) || G stb)

验证该断言成立，证明该设计符合此条规范

应用领域

- 可应用于形式化验证Chisel 硬件设计
  - 支持了assume/assert 断言原语
  - 支持描述安全性质（safety property ）与活性性质（liveness property ）
  - 支持使用限界模型检测算法寻找设计中的bug，也支持使用 K-induction 等算法证明设计的正确性