西北大学信息科学与技术学院

本科毕业设计/作品验收/毕业答辩评语表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 院系 | | 信息科学与技术学院 | | | | | 专业 | | 软件工程 | | | |
| 学号 | | 2021117283 | | | | | 姓名 | | 雷璟锟 | | | |
| 毕业论文  （设计）题目 | | | | 嵌入式JS引擎模糊测试方法研究 | | | | | | | | | |
| 文献综述成绩 | | | 81 | | 作品验收成绩 | 75 | | 毕业论文成绩 | | 78 | 毕业答辩  成绩 | 80 |
| 注：上述各项成绩采取百分制。 | | | | | | | | | | | | |
| 答辩小组成员（姓名，职称）：范训礼（教授） ，周伟（讲师） ，吴昊（讲师） | | | | | | | | | | | | |
| 答辩小组组长签字： 2025年5月19日 | | | | | | | | | | | | |
| 作品验收情况表 | |  |  |  | | --- | --- | --- | | 验收项目 | 验收内容 | 验收结果 | | 作品选题 | 选题符合专业培养目标，能够达到综合训练目标，题目难度高，工作量大，具有实践指导意义 | 通过 | | 作品功能 | 系统具备从GitHub等平台提取函数构建初始测试样本的功能；能设计基于参数类型推断的测试用例变异方法，生成大量语法语义正确、高覆盖率的测试用例；可对多个主流的JavaScript嵌入式引擎进行模糊测试，并对发现的缺陷进行案例分析 | 通过 | | 技术实现 | 系统采用的技术路线合理，代码实现规范，模块划分清晰，具备良好的可扩展性和可维护性 | 通过 | | 实用性 | 系统能够有效应用于嵌入式JavaScript引擎的测试工作，对提升嵌入式系统的稳定性与性能具有实际意义 | 通过 | | 创新性 | 系统提出了一种基于参数类型推断的测试用例变异方法，结合差分测试实现了模糊测试框架，与现有模糊测试工具相比，在代码覆盖率、漏洞发现率等方面具有优势 | 通过 | | 文档资料 | 作品的文档资料齐全，包括设计说明书、用户手册等，文档内容完整、规范，能够清晰地阐述作品的设计思路、实现过程和使用方法 | 通过 | | | | | | | | | | | | | |
| 毕业论文评语表  （含文献综述） | 论文选题契合专业培养目标，能够达成综合训练目的，题目难度较高，工作量饱满。选题具备实践指导价值。  该生在文献资料查阅方面表现出较强能力，能够全面收集相关资料，写作中体现出较强的知识综合运用与问题分析能力。文章篇幅符合学院规定，内容完整，层次结构合理，核心观点突出，逻辑清晰，但个人见解略有不足。文题契合，论点明确，论述紧密围绕主题。语言表达流畅，格式规范；参考文献丰富且时效性强。 | | | | | | | | | | | | |
| 答辩记录 | 一、学生陈述（5分钟）  陈述内容：  研究背景与意义：该同学首先介绍了物联网技术快速发展背景下，JavaScript 在嵌入式系统开发中的重要地位，以及嵌入式 JavaScript 引擎测试的必要性。阐述了传统测试方法在嵌入式设备低内存、弱算力等资源受限特性下难以有效挖掘引擎潜在缺陷的问题，引出本研究的必要性。  研究内容与方法：详细介绍了基于参数类型推断的测试用例变异方法，包括从 GitHub 等平台提取函数构建初始测试样本、设计参数类型推断方法以及基于类型推断的变异算法。重点讲解了如何通过分析函数体内参数的行为模式推断其可能的数据类型，并据此生成大量语法语义正确、高覆盖率的测试用例。  系统设计与实验评估：阐述了 EJSFuzz 测试系统的架构设计，包括语料库处理模块、测试用例处理模块、差分模糊测试模块等，并介绍了实验设置、实验步骤以及评估指标。通过与 Fuzzilli、AFL 等模糊测试工具的对比实验，展示了 EJSFuzz 在代码覆盖率、漏洞发现率等方面的优势。  结论与展望：总结了本研究的主要贡献，包括提出基于参数类型推断的测试用例变异方法、实现 EJSFuzz 测试系统以及验证其有效性。同时，对未来的研究方向提出了展望，如改进差分测试局限性、优化类型推断方案以及增强缺陷定位与分析能力。  二、答辩小组提问（10 分钟）  问题 1：在实验过程中，你是如何评估 EJSFuzz 系统的代码覆盖率和漏洞发现率的？  回答：对于代码覆盖率，我使用了专业的代码覆盖率工具对 EJSFuzz 生成的测试用例在多个嵌入式 JavaScript 引擎上进行运行，统计了语句覆盖率、分支覆盖率等指标。通过对比不同引擎的覆盖率结果，以及与 Fuzzilli、AFL 等工具生成的测试用例的覆盖率进行对比分析，来评估 EJSFuzz 的代码覆盖率表现。在漏洞发现率方面，记录了在一定时间内 EJSFuzz 触发的引擎缺陷数量，并与 Fuzzilli、AFL 等工具在同一实验环境下触发的缺陷数量进行对比，计算漏洞发现率，从而评估 EJSFuzz 在漏洞挖掘方面的能力。  问题 2：你认为你的研究在实际应用中可能面临哪些挑战？  回答：我认为我的研究在实际应用中可能面临以下挑战：首先，差分测试存在局限性，当不同引擎对同一测试用例产生相异的输出时才能有效识别潜在缺陷，但如果被测引擎对某一语言特性的实现均存在错误，则会产生相同的错误输出，导致此类缺陷无法被检测。其次，类型推断方案通过静态的参数行为计数来实现，可推断的参数类型受条件限制未能涵盖 Object 类型以及其他嵌套类型，在面对复杂嵌套类型和动态类型场景时，测试用例的变异方向可能不够丰富。最后，在对触发缺陷的测试用例进行分析时，由于引擎触发崩溃导致执行中断，给缺陷定位与分析带来了巨大的挑战，需要进一步优化差分测试模块，设计一套故障分析方案，用于记录触发崩溃的调用栈、内存快照等关键信息。 | | | | | | | | | | | | |
| 毕业答辩评语表 | 该生的毕业论文选题具有较高的难度和较大的工作量，符合专业培养目标，能够达到综合训练的要求，具有较强的实践指导意义。在研究过程中，该生查阅了大量文献资料，综合运用了多学科知识，全面分析了问题，展现出了较强的研究能力。论文内容完整，层次结构合理，主要观点突出，逻辑关系清楚，语言表达流畅，格式规范，参考文献丰富且时效性强，未发现抄袭现象。在答辩过程中，该生陈述清晰，回答问题准确，展现出扎实的专业素养和良好的应变能力。 | | | | | | | | | | | | |