

前 言

在软件定义一切的时代，软件使能的系统遍布在人类社会的各个方面、在不同程度发挥着重要的作用，软件可信保障既是迫切需求又是重要挑战。对软件的语义及其行为空间进行深入理解是软件可信保障的重要依据与前提。然而，随着计算机技术的快速发展与应用的日趋普及，软件系统规模和复杂性持续增大，如何对大规模、复杂软件系统的语义进行理解，并指导软件分析、测试、验证乃至优化活动是当前领域关注的重要问题。特别是在当前开源时代下，如何对大规模代码高效构建准确的语义认知，并基于相关认知与理解进行后续自动化分析，具有重要意义。

为反映程序语义理解及其应用相关研究前沿进展与实践，并推动国内相关研究向深度发展，我们组织“程序语义深度理解前沿进展”专题，邀请领域专家对抽象解释、符号执行、模糊测试等程序语义理解的重要技术手段进行综述总结与进展报告，并围绕 **JAVA** 指针分析、中断驱动代码原子性违反检测、智能合约优化等领域重要问题进行专题讨论。

抽象解释是程序分析的基础理论之一，在安全攸关软件的分析与验证方面发挥了重要的作用，近年来也被拓展到人工智能、安全等领域。陈立前等人的“抽象解释及其应用研究进展”一文对近年来抽象解释在理论本身、基于抽象解释的可信人工智能和智能合约、信息安全及量子计算等的可信保证等方向的最新进展进行了系统、全面的总结、分析和介绍。

符号执行是一种重要的程序分析技术，常用于程序的测试输入生成和缺陷自动检测，近年来受到了学术界和工业界的广泛关注。然而，符号执行仍面临路径空间爆炸和约束求解这两个关键挑战，严重阻碍了符号执行的进一步发展和应用。针对相关问题，周彭和左志强的“基于多线程并行的符号执行引擎设计与实现”一文提出了一种基于多线程并行化的符号执行解决方案，将路径探索过程均摊到多个工作线程中，在线程间共享约束求解信息，提高求解缓存的命中率，实现符号执行效率的提升。

近年来，模糊测试技术在工业界大规模系统的测试中得到广泛应用。王明哲等人的“模糊测试中的静态插桩技术”一文对模糊测试以及模糊测试背景下的静态插桩技术进行介绍，分别介绍了安全特性强化插桩和导向信息收集插桩这两类静态插桩技术及其应用场景，并且结合最新的工业界和学术界的成果对不同目的的静态插桩技术进行解释剖析。

指针分析是程序分析中的一个经典问题，得到了相关领域长期以来的持续关注。谭添等人的“**Java** 指针分析综述”一文系统综述了 **Java** 指针分析的重要内容：指针分析算法、上下文敏感、堆对象抽象、复杂语言特性处理、非全程序指针分析，并系统性地梳理和讨论了近年来 **Java** 指针分析的研究进展，为相关研究人员快速了解相关问题领域提供参考。

航天嵌入式软件是一种典型安全攸关软件，原子性违反是航天嵌入式软件中断并发缺陷中的一类常见缺陷类型。研究适合航天嵌入式软件原子性违反的检测方法具有重要实用价值。于婷婷等人的“中断驱动型航天嵌入式软件原子性违反检测方法”一文针对航天嵌入式软件中原子性违反缺陷的表现形式开展了实证研究，并基于实证研究得到的特征，提出了一

种精度高、效率高的中断驱动型程序原子性违反静态检测方法.

智能合约的 Gas 优化是近年来的一个热点问题. 宋书纬等人的“智能合约 Gas 优化综述”一文针对智能合约的执行过程中的 Gas 消耗问题进行了系统性的调研与分析, 对 Gas 优化相关工作与研究方向进行了整理与总结, 为智能合约开发者, 以及智能合约执行优化等相关方向的研究者, 提供了指引与展望.

深入理解程序语义是通向软件可信保障的必由之路. 希望本专题的出版能够抛砖引玉, 对系统软件、软件工程及其相关领域的研究人员有所帮助和启发, 以进一步促进相关研究. 由于时间仓促、容量有限, 本专题无法全面覆盖相关领域的所有最新研究工作, 敬请各位同行谅解和批评指正. 衷心感谢《计算机研究与发展》提供了宝贵机会出版此专题论文! 衷心感谢各位作者、审稿专家和编辑部工作人员的全力支持和辛勤付出, 使得本专题能顺利出版!

卜磊 (南京大学)

陈振邦 (国防科技大学)

2023 年 1 月