

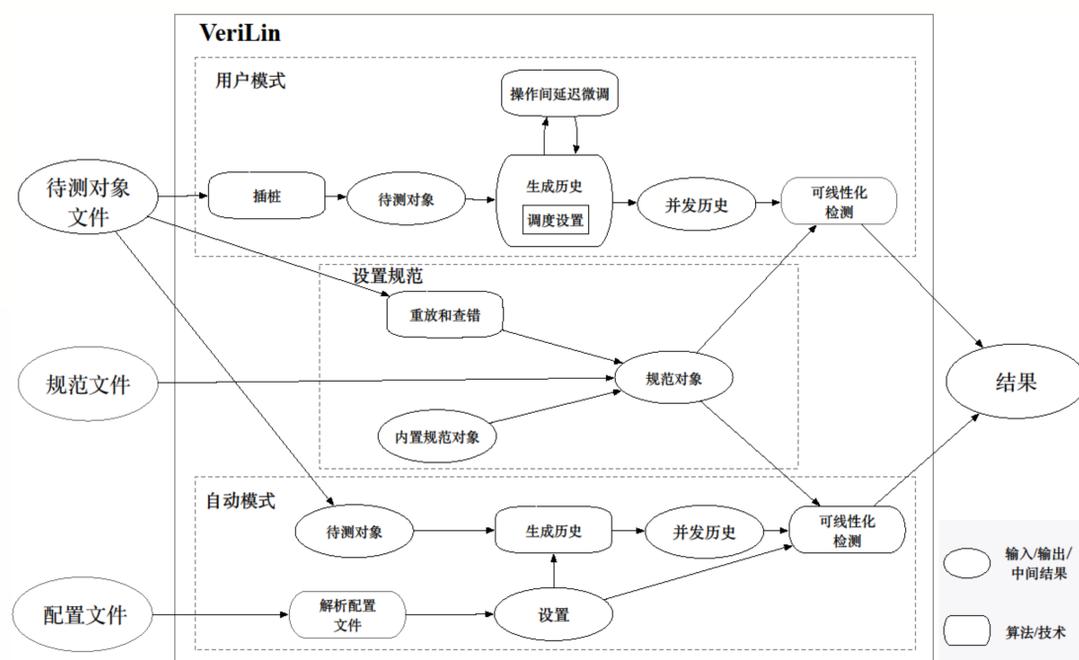
并发对象可线性化检测工具VeriLin

贾巧雯 吕毅 吴鹏 詹博华 郝继锋 叶宏 王超

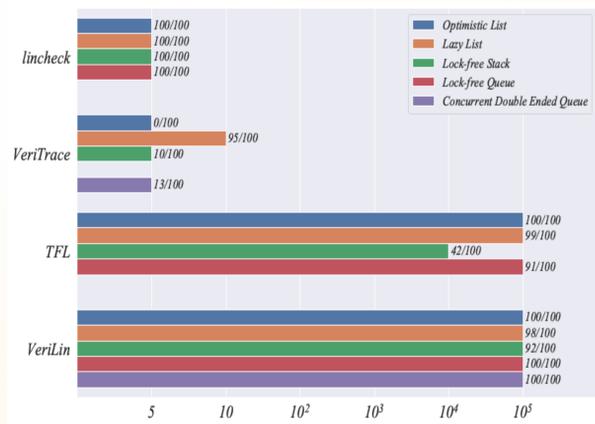
VeriLin: A Linearizability Checker for Large-Scale Concurrent Objects, TASE2023

联系人: 吕毅 lvyi@ios.ac.cn

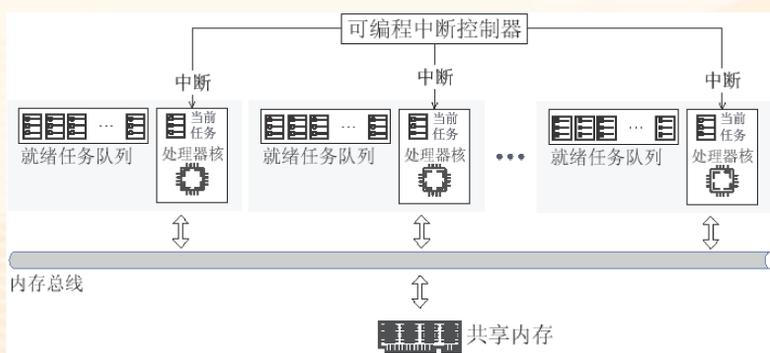
本文提出了大规模并发对象的可线性化(linearizability)检测算法。可线性化是并发对象正确性的重要描述方式,表示每个并发执行序列都存在对应的串行执行序列。针对复杂并发对象的可线性化性质检测问题,我们提出基于拓扑排序的检测算法,顺序执行历史的检测和微调操作内外延迟等在实践中行之有效的技术。我们实现的检测工具VeriLin集成了上述的算法和技术。



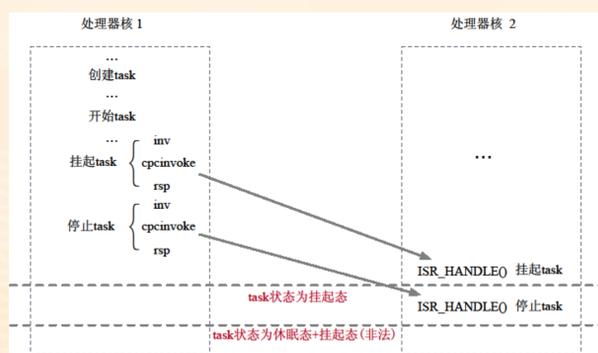
VeriLin在与其他可线性化检测工具的对比测试中取得了领先的效果。该工具也用于研究生课程中Train Ticketing System案例实现的自动化测试。



我们使用VeriLin对一个嵌入式多核操作系统内核的任务调度与管理模块进行验证。该模块包含超过4,500行代码,20余个共享变量。在应用VeriLin进行可线性化检测过程中,找到并确认了3处原始设计中的缺陷。这是第一次将可线性化检测成功用于带核间中断的多核操作系统内核验证。



多核任务调度与管理模块



核间中断相关错误示例