# 面向MC/DC的符号执行编译优化

洪伟疆[1,2]，刘怡君[1]，陈振邦[1]，董威[1]，王戟[1,2]
[1]国防科技大学计算机学院，中国长沙市，410073
[2]国防科技大学高性能计算国家重点实验室，中国长沙市，410073

**摘要：**符号执行是一种系统地探索程序路径空间的有效方式，常用于自动软件测试与错误查找。通常待分析的程序会被编译成二进制或中间表示，在此基础上进行符号执行。在此过程中，编译器的优化选项往往会影响符号执行的有效性和效率。修订条件/判定覆盖（MC/DC）是一种广泛应用于任务关键型软件的重要测试覆盖准则；据我们所知，目前尚未开展面向MC/DC的符号执行编译优化推荐工作。本文采用先进的符号执行工具开展了大量实验，研究编译器优化对使用符号执行以满足程序MC/DC的影响。结果表明，指令组合（IC）优化是符号执行面向MC/DC的关键和主导优化选项。在此基础上，设计并实现了一个基于支持向量机的编译优化推荐方法，在Coreutils和NECLA两个测试集上开展实验。结果表明，所提方法在67.47%的Coreutils程序和78.26%的NECLA程序上取得了最佳MC/DC结果。

**关键词：**编译优化；修订条件/判定覆盖（MC/DC）；优化推荐；符号执行
https://doi.org/10.1631/FITEE.1900213