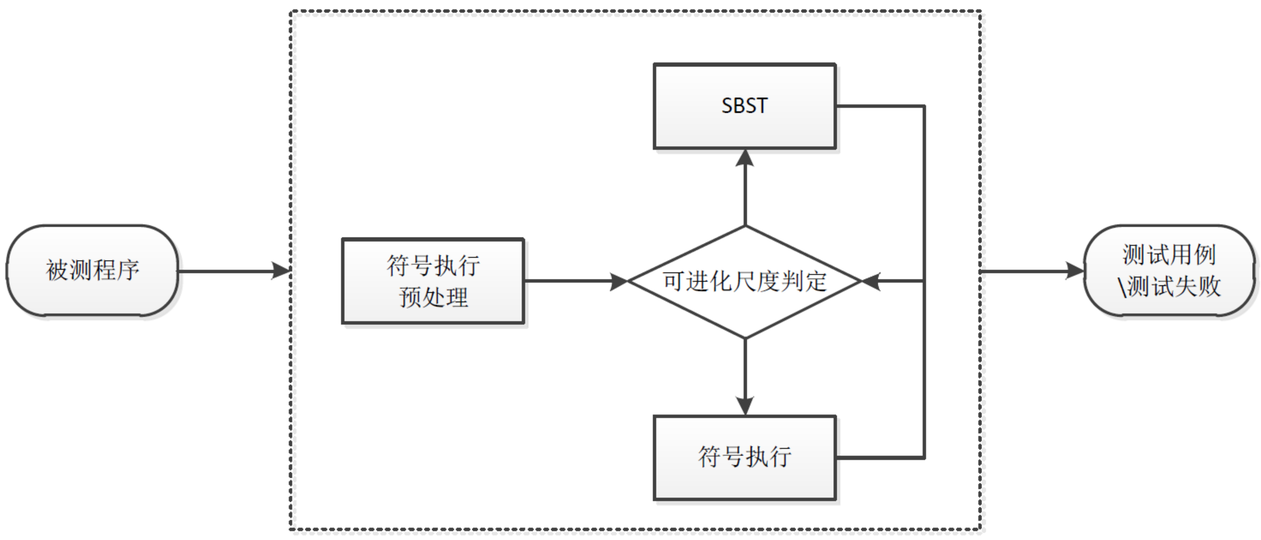
基于可进化尺度的搜索测试与动态符号执行的结合

朱自明，焦莉，徐雄，“Combining Search-based Software Testing and Dynamic Symbolic Execution by Evolvability Metric”，International Conference on Software Maintenance and Evolution (ICSME)，2018。
联系方式：{zhuzm, ljiao, xux}@ios.ac.cn

摘要

- 在软件测试领域中，基于搜索的软件测试（Search-based Software Testing，SBST）和动态符号执行技术（Dynamic Symbolic Execution，DSE）被认为是最为有效的两种测试用例生成技术。然而，这两种测试技术都存在着各自不可忽视的问题。
- SBST将测试用例的生成问题转化为搜索优化问题，因此能够很好地处理程序中各种复杂的约束，而其最主要的缺陷是启发式信息缺失和效率较低的问题。
- 符号执行能够通过约束求解器高效地生成目标测试用例，而如何求解复杂约束一直是制约符号执行发展的一个重要因素。
- SBST和符号执行是互为补充的两种测试技术，因此，本文致力于将SBST与符号执行相结合，优势互补，提升软件测试的性能。

测试框架



切换机制

- 基于可进化尺度（EM）的切换机制：
- 给定n个测试数据，其相应的适度值表示如下：

$$F = f_1, f_2, \ldots, f_n .$$

- 每个测试数据与当前最优测试数据的欧式距离表示如下：

$$D = d_1, d_2, \ldots, d_n .$$

- 则：

$$EM = \frac{Cov(F,D)}{\sigma(F) \bullet \sigma(D)}$$

- 其中Cov(F, D)表示F与D的协方差，σ(F)和σ(D)分别是F和D的标准差。

实验结果

- 本方法（GA_DSE）与其他方法（SBST, DSE, Comb_Ap）的实验数据检验结果：

	p-value	$\widehat{A}_{12}$
GA_DSE vs DSE	0.001	0.818
GA_DSE vs SBST	0.001	0.886

	APC		ATC	
	p-value	$\widehat{A}_{12}$	p-value	$\widehat{A}_{12}$
GA_DSE vs Comb_Ap	0.049	0.661	0.233	0.571