

一个针对安卓应用的可扩展的流,上下文,对象,数据成员以及路径敏感的程序分析框架

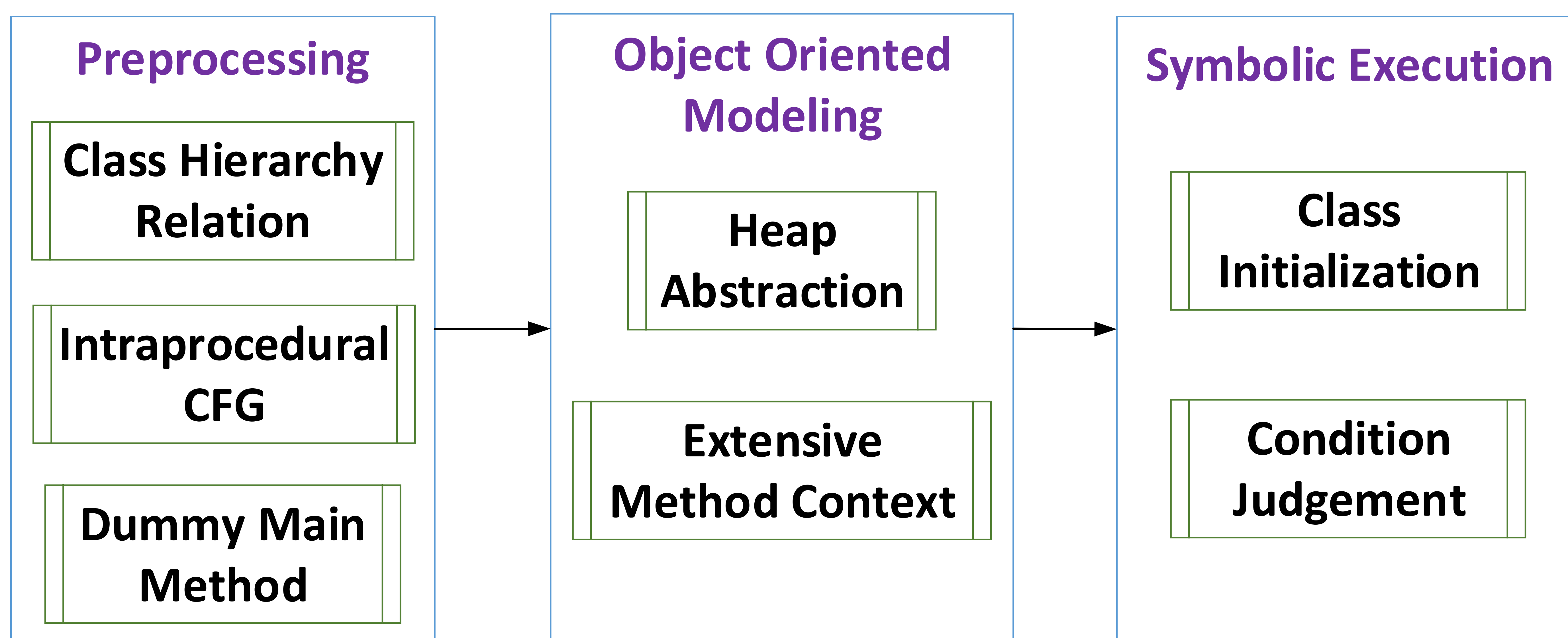
潘临杰 严俊

题目: Androlic: An Extensible Flow, Context, Object, Field, and Path-sensitive Static Analysis Framework for Android

会议: Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, 394-397, July15-19, 2019

联系方式: 潘临杰 15210968812 panlj@ios.ac.cn
严俊 15810566092 yanjun@ios.ac.cn

静态分析技术被广泛应用于安卓应用的错误检测。目前已有的分析工具大多针对特定的问题并且精度差别很大,导致工具的复用性和扩展性较差。有鉴于此,我们开发了流,上下文,对象,数据成员以及路径敏感的高精度程序分析框架Androlic。通过Androlic提供的配置项和接口,开发人员可以轻松地对框架进行扩展以处理特定的程序分析问题。我们在20个真实应用上对框架进行了测评,实验结果证实了Androlic的高精度。



•配置项

- 最大路径数量(40000)
- 最大递归层数 (0)
- 最大上下文层数 (1)
- 入口方法 (dummy main)
-

•接口

- ISymbolicEngineInstrumenter
- ILibraryInvocationProcessor
- INewExprProcessor
- INewArrayExprProcessor

Github地址: <https://github.com/pangeneral/Androlic>