软件分析考点列表

软件分析概述

1. 静态分析（Static Analysis）和动态测试（Dynamic Testing）的区别是什么？
2. 完全性（Soundness）、正确性（Completeness）、假积极（False Positives）和假消极（False Negatives）分别是什么含义？
3. 为什么静态分析通常需要尽可能保证完全性？
4. 如何理解抽象（Abstraction）和过近似（Over-Approximation）？

程序的中间表示

1. 编译器（Compiler）和静态分析器（Static Analyzer）的关系是什么？
2. 三地址码（3-Address Code，3AC）是什么，它的常用形式有哪些？
3. 如何在中间表示（Intermediate Representation，IR）的基础上构建基块（Basic Block，BB）？
4. 如何在基块的基础上构建控制流图（Control Flow Graph，CFG）？

数据流分析

1. 定义可达性（Reaching Definitions）分析、活跃变量（Live Variables）分析和可用表达式（Avaliable Expressions）分析分别是什么含义？
2. 上述三种数据流分析（Data Flow Analysis）有哪些不同点？又有什么相似的地方？
3. 如何理解数据流分析的迭代算法？数据流分析的迭代算法为什么最后能够终止？
4. 如何从函数的角度来看待数据流分析的迭代算法？
5. 格和全格的定义是什么？
6. 如何理解不动点定理？
7. 怎样使用格来总结可能性分析与必然性分析？
8. 迭代算法提供的解决方案与 MOP 相比而言精确度如何？

9. 什么是常量传播（Constant Propagation）分析？
10. 数据流分析的工作表算法（Worklist Algorithm）是什么？

过程间分析

1. 如何通过类层级结构分析（Class Hierarchy Analysis，CHA）来构建调用图（Call Graph）？
2. 如何理解过程间控制流图（Interprocedural Control-Flow Graph，ICFG）的概念？
3. 如何理解过程间数据流分析（Interprocedural Data-Flow Analysis，IDFA）的概念？
4. 如何进行过程间常量传播（Interprocedural Constant Propagation）分析？

指针分析

1. 什么是指针分析（Pointer Analysis）？
2. 如何理解指针分析的关键因素（Key Factors）？
3. 我们在指针分析的过程中具体都分析些什么？
4. 指针分析的规则（Pointer Analysis Rules）是什么？
5. 如何理解指针流图（Pointer Flow Graph）？
6. 指针分析算法（Pointer Analysis Algorithms）的基本过程是什么？
7. 如何理解方法调用（Method Call）中指针分析的规则？
8. 怎样理解过程间的指针分析算法（Inter-procedural Pointer Analysis Algorithm）？
9. 即时调用图构建（On-the-fly Call Graph Construction）的含义是什么？
10. 上下文敏感（Context Sensitivity，C.S.）是什么？
11. 上下文敏感堆（C.S. Heap）是什么？
12. 为什么 C.S. 和 C.S. Heap 能够提高分析精度？
13. 上下文敏感的指针分析有哪些规则？
14. 如何理解上下文敏感的指针分析算法（Algorithm for Context-sensitive Pointer Analysis）？
15. 常见的上下文敏感性变体（Context Sensitivity Variants）有哪些？

16. 常见的几种上下文变体之间的差别和联系是什么？

静态分析与安全

1. 信息流安全（Information Flow Security）的概念是什么？
2. 如何理解机密性（Confidentiality）与完整性（Integrity）？
3. 什么是显式流（Explicit）和隐蔽信道（Covert Channels）？
4. 如何使用污点分析（Taint Analysis）来检测不想要的信息流？

基于 Datalog 的程序分析

1. Datalog 语言的基本语法和语义是什么？
2. 如何用 Datalog 来实现指针分析？
3. 如何用 Datalog 来实现污点分析？

CFL 可达与 IFDS

1. 什么是 CFL 可达（CFL-Reachability）？
2. IFDS（Interprocedural Finite Distributive Subset Problem）的基本想法是什么？
3. 怎样的问题可以用 IFDS 来解决？

完全性与近似完全性

1. 近似完全性（Soundiness）的动机和概念是什么？
2. 为什么 Java 反射（Reflection）和原生代码是难分析的？