Разработка декомпилятора языка Java SE 6

Михайлов Дмитрий
СПбГУ, Математико-Механический факультет

Научный руководитель: Шафиров Максим Геннадьевич.

Область применения

- Обратная разработка ПО
- Использование сторонних библиотек
  - Декомпиляция для обеспечения возможности взаимодействия разрешена законом
- Поддержка ПО
  - Рекомпиляция для переноса на другую платформу
  - Поиск багов и уязвимостей
  - Добавление новой функциональности

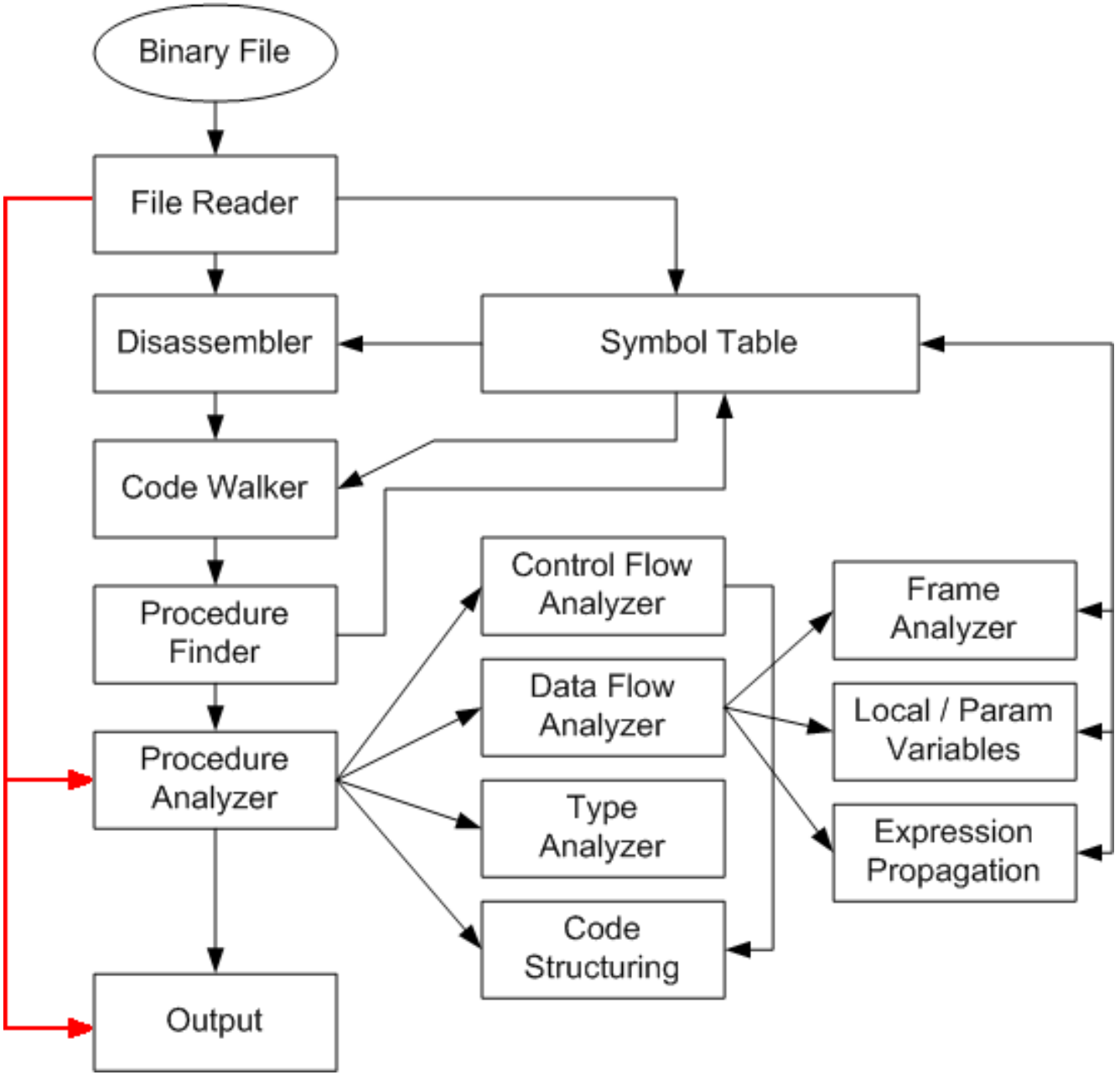
Задачи курсовой

- Разработка декомпилятора языка Java
- Декомпиляция параметризованных типов
  - Способствует взаимодействию со скомпилированными классами
- Декомпиляция аннотаций и их описаний
  - Могут полностью описывать бизнес-логику приложения

Особенности реализации

- ObjectWeb ASM
  - API на основе паттерна Visitor
  - Представление метаданных в виде дерева
  - com.sun.xml.internal.ws.org.objectweb.asm
- Soot Framework
  - Ядро декомпилятора
  - Промежуточное представление методов и генерация кода
- Зависимость алгоритма от метаданных
  - Генерация разного кода из одинаковых промежуточных представлений

Особенности реализации



Результаты

- Разработан Proof-of-Concept прототип декомпилятора
  - Корректное отображение параметризованных типов
  - Разбор и отображение аннотаций классов, полей, методов и их аргументов
  - Декомпиляция пользовательских аннотаций
  - Возможность замены ядра декомпилятора