# Декомпиляция выражений по байт-коду JVM

Поздин Дмитрий 344 гр.

Научный руководитель: Булычев Д. Ю.

# Общая постановка задачи

- Дано: байт-код JVM
- Требуется получить его представление на различных целевых языках

# Цели

- Создание декомпилятора выражений по байт-коду JVM в промежуточное представление в случае линейного кода
- Исследование выражений JVM в случае нелинейного кода

# Верификация

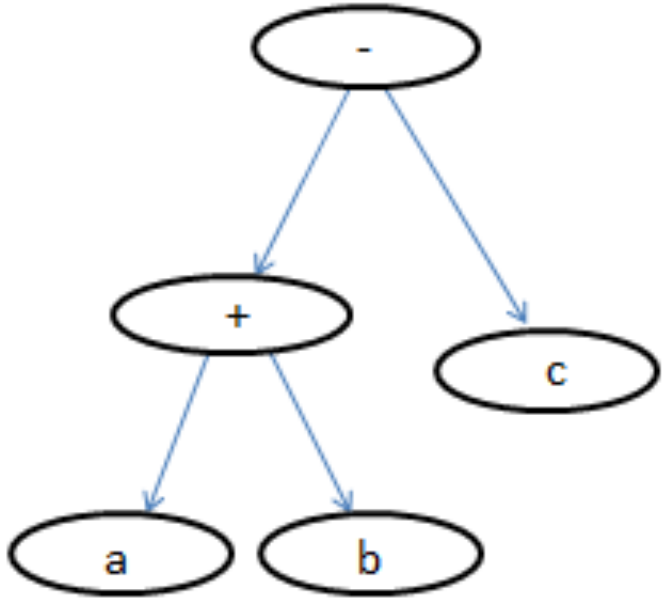
Проверяется:

- формат класс-файла
- формат команд байт-кода
- аргументы и индексы
- семантика команд
- размер стека операндов

Основное условие: на параллельных участках стек обрабатывается одинаково

# Пример выражения без переходов

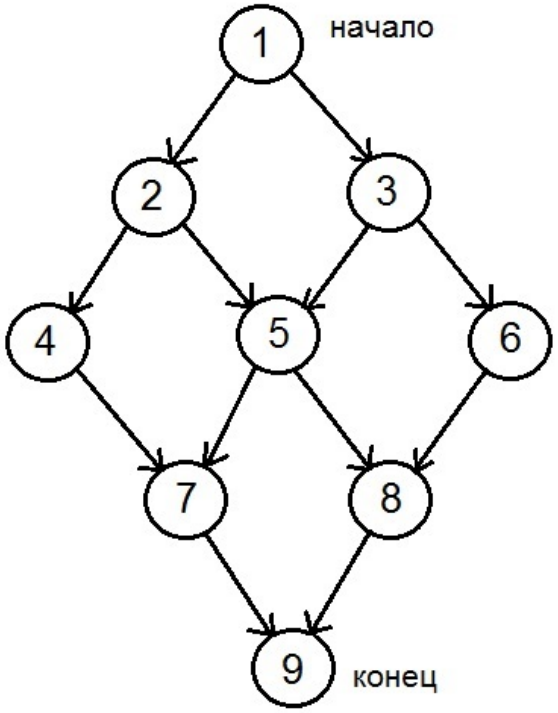
- 0: iload_1
- 1: iload_2
- 2: iadd
- 3: iload_3
- 4: isub




- Пример простого выражения: (a+ b)-c

# Пример выражения с переходами

- Часть графа потока управления
- Узлы - линейный код
- Ребра - переходы
- Глубина стека одинаковая в ребрах, идущих в одну вершину



# Использованные технологии

- ASM – многофункциональная библиотека чтения и модификации JVM-классов.
- Jasmin - ассемблер для JVM

# Результаты

Реализовано построение JVM-дерева выражений для большинства основных операций линейного кода:

- арифметические операции;
- загрузка, выгрузка на стек;
- вызов метода, добавление константы.

Исследован случай выражений с переходами.