

Московский Физико-Технический Институт
(государственный университет)
Кафедра Теоретической и Прикладной Информатики

Эмуляция процессора ARM в контексте пользовательского приложения

Выпускная квалификационная работа
студента 311 группы ФРТК
Абрамова С.Э.

Научный руководитель:
Корякин А.Б.

Москва
2017

Содержание

- Цель
- Постановка задачи
- Способ решения
- Загрузчик динамических библиотек
- Эмуляция ARM-v8
- Отладка системы и анализ результатов
- Заключение
- Перспективы

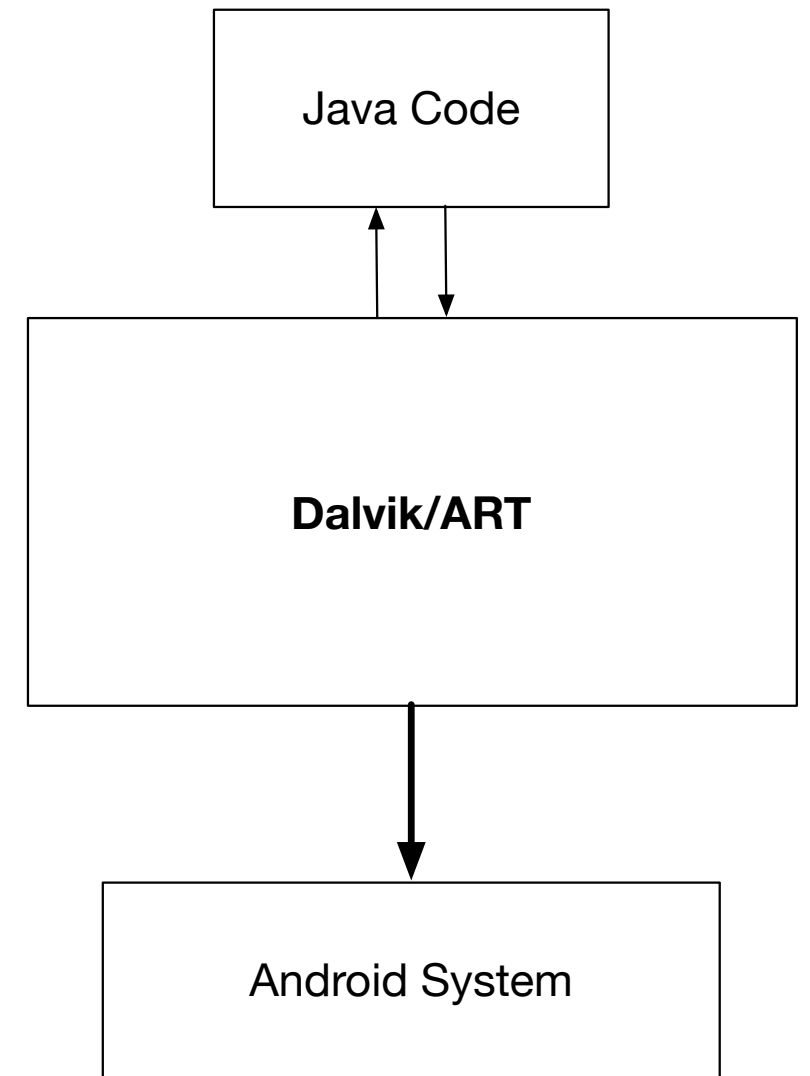
Цель

- Мобильная разработка крайне популярна
- Android - распространенная ОС для мобильной платформы
- ARM - процессорная архитектура подавляющего большинства смартфонов

**Было бы очень полезно и удобно тестировать приложения
без дополнительного аппаратного обеспечения**

Постановка задачи

- Байт-код придает приложениям кроссплатформенность
- **Однако, ...**



Роль Dalvik в Android

Постановка задачи

... android приложения могут использовать нативный код (native code)

Нативный код - бинарный код целевой архитектуры

Следовательно, ...

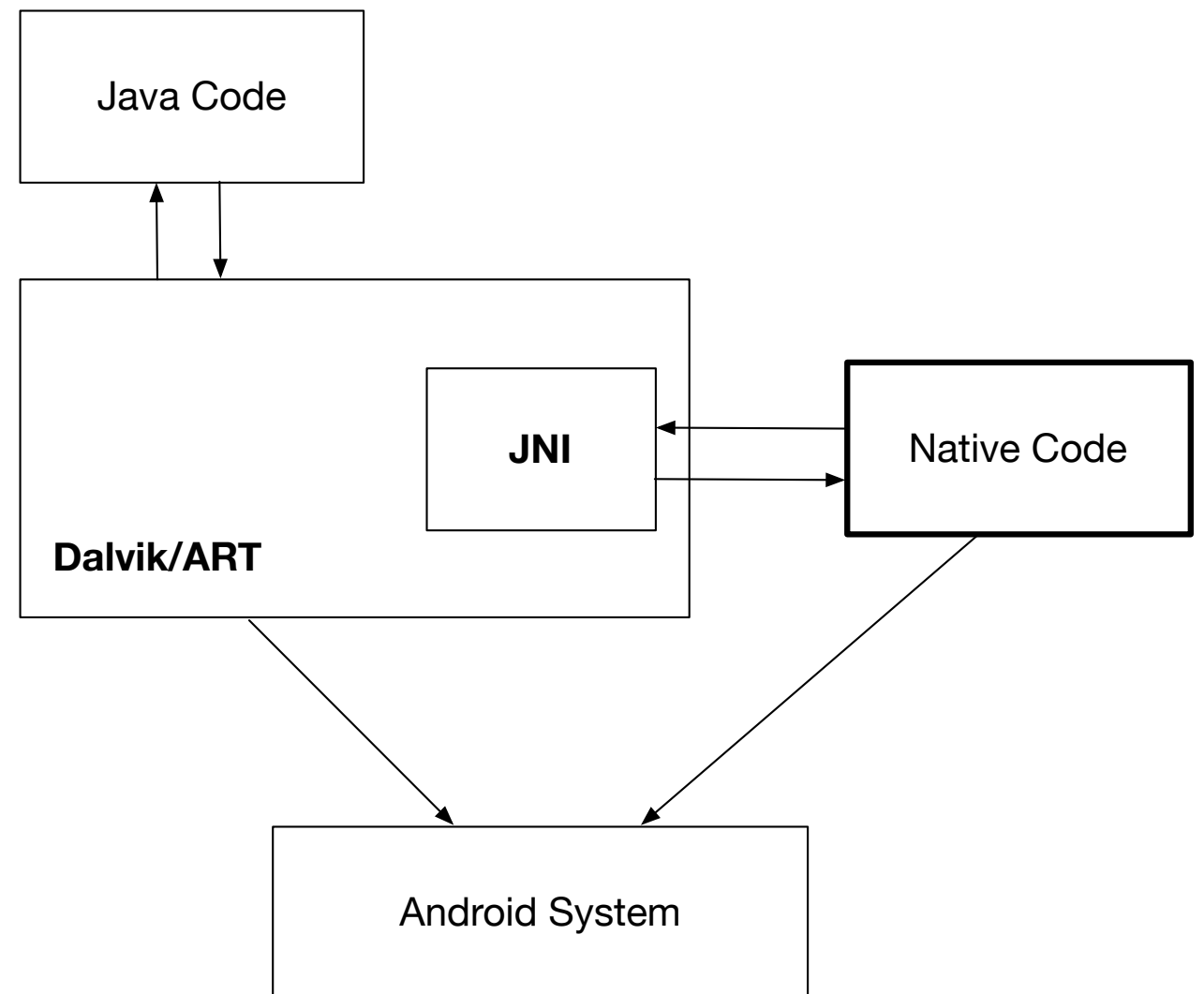


Схема взаимодействия Java и нативного кода

Постановка задачи

**Необходимо реализовать возможность запуска
нативного кода пользовательских приложений
на платформе с процессором архитектуры x86_64**

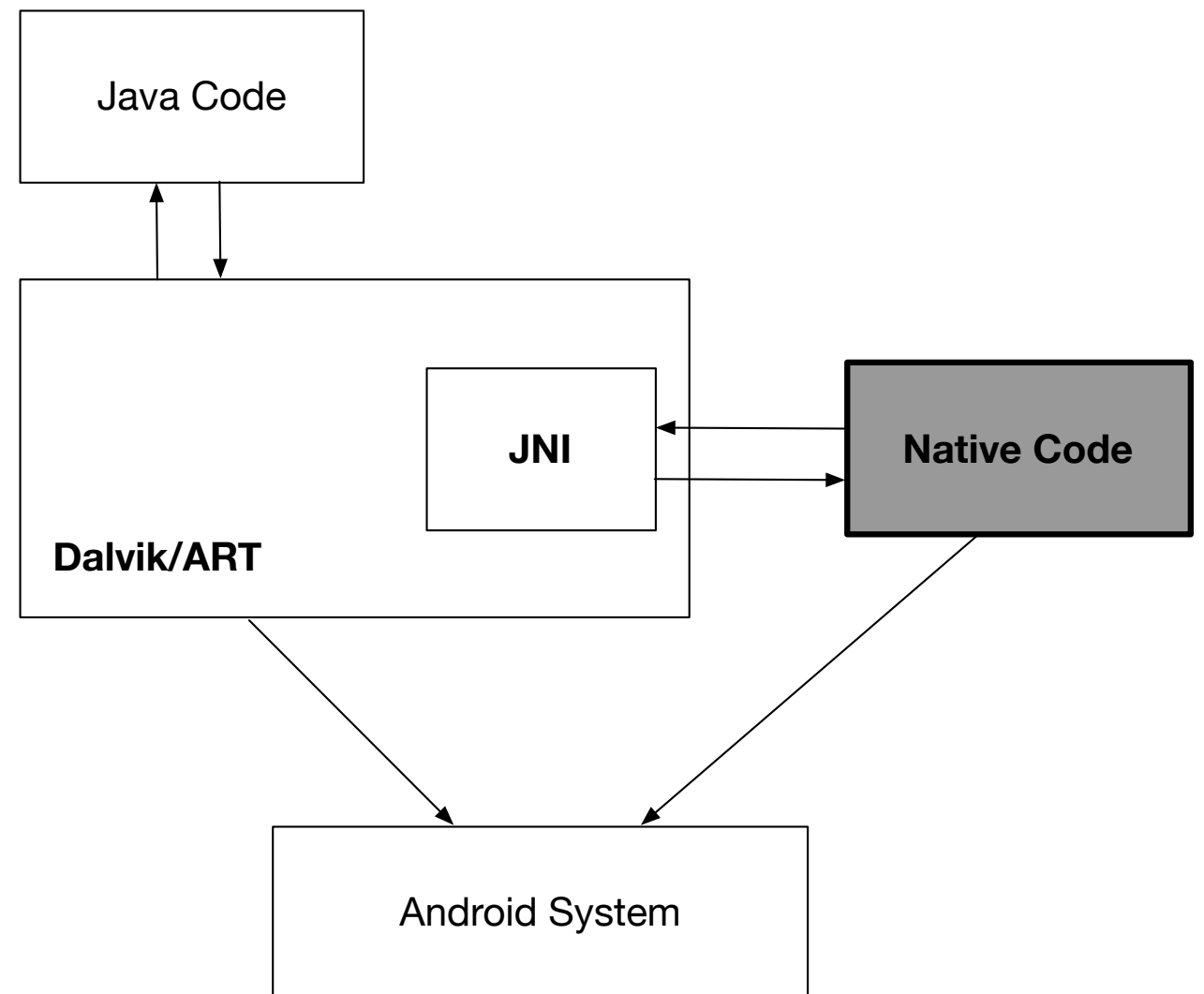


Схема взаимодействия Java и нативного кода

Способ решения

Эмуляция архитектуры ARM-v8,
необходимая для запуска нативного кода

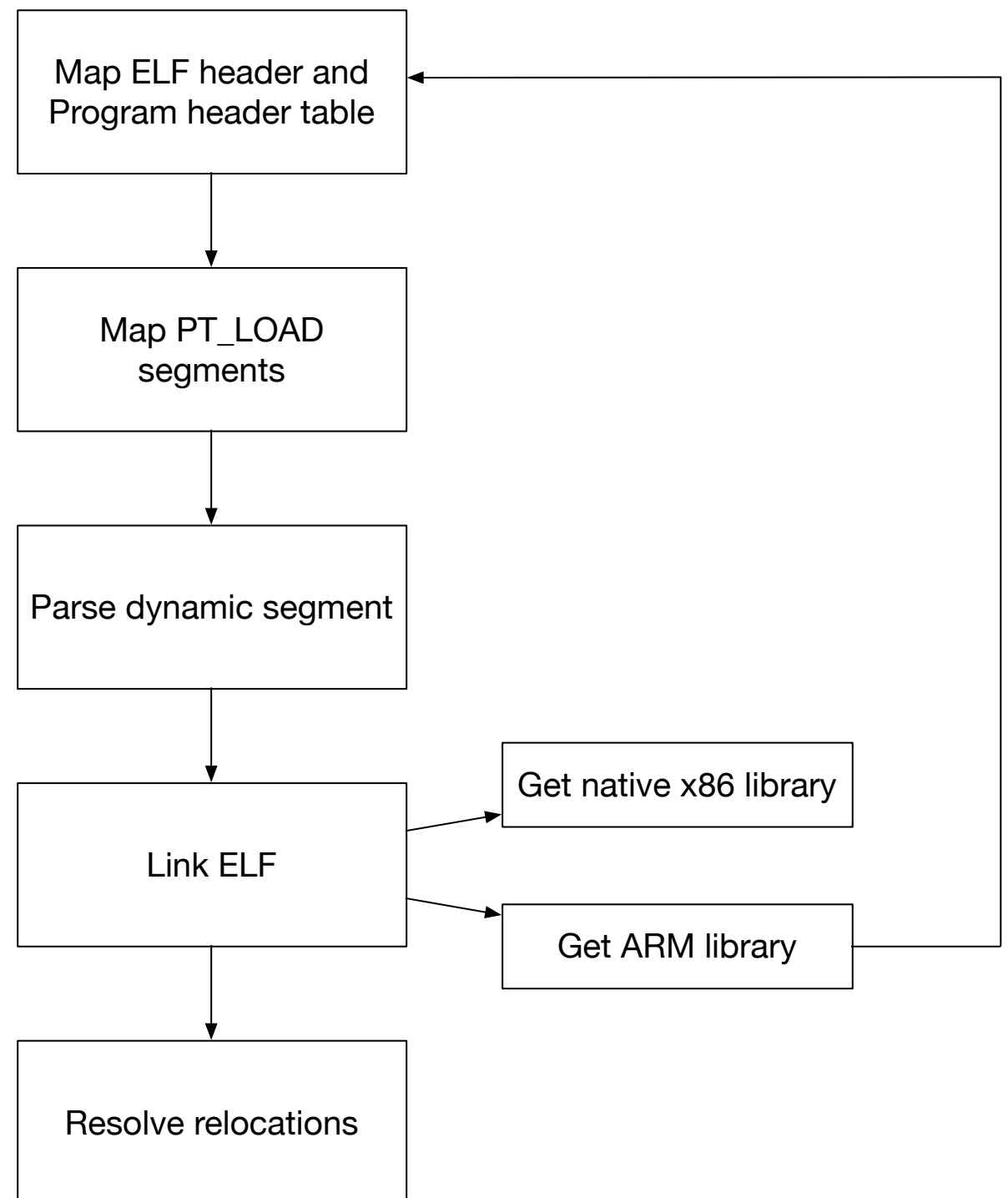
ARM®



Загрузчик динамических библиотек

Методы Java вызывают нативный код,
собранный в динамические библиотеки

Необходимо реализовать загрузчик библиотек



Структурная схема загрузчика

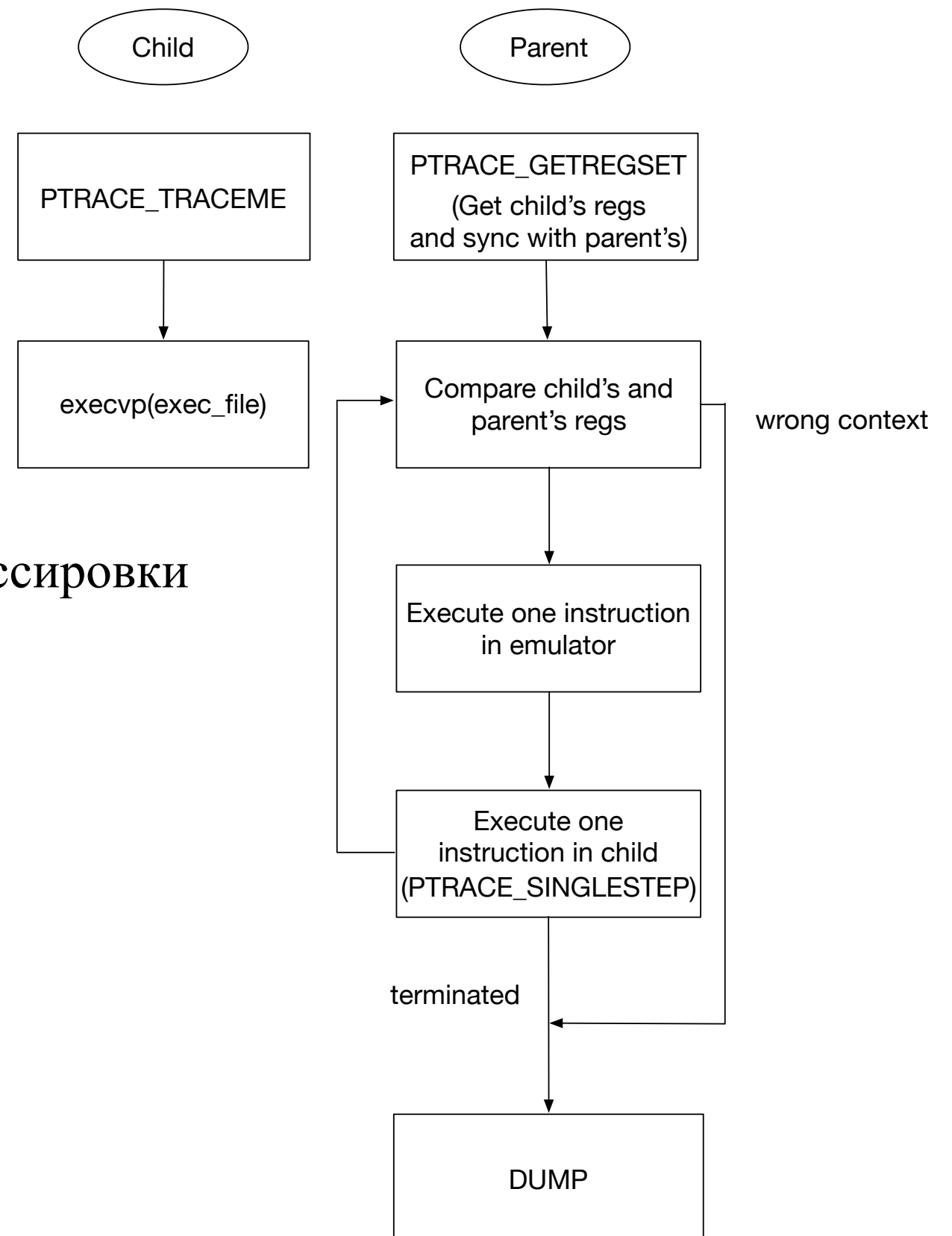
Эмуляция процессора архитектуры ARM-v8

ARM-v8 - современная 64-битная архитектура

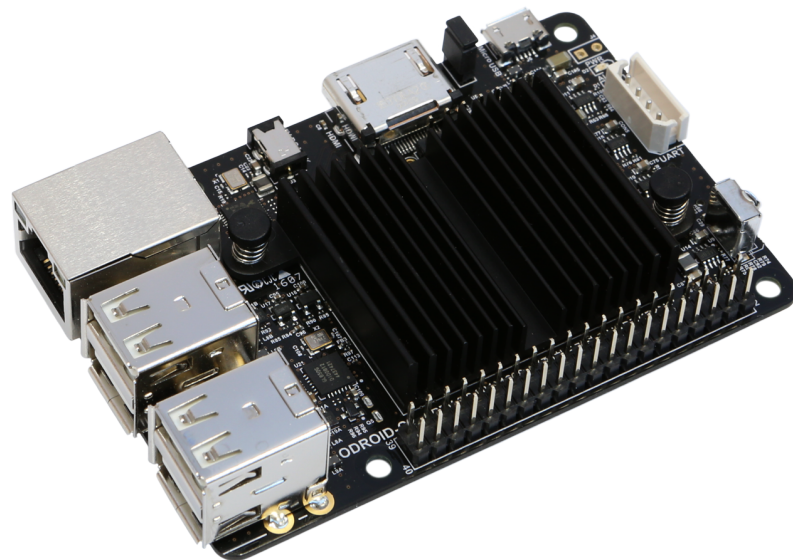
Для решения задачи необходимо осуществить:

- Реализацию общей структуры функционирования процессора, необходимой для исполнения нативного кода
- Реализацию набора команд процессора (A64)
- Возможность исполнения кода загруженных библиотек (интеграцию самого эмулятора и загрузчика)

Отладка системы и анализ результатов

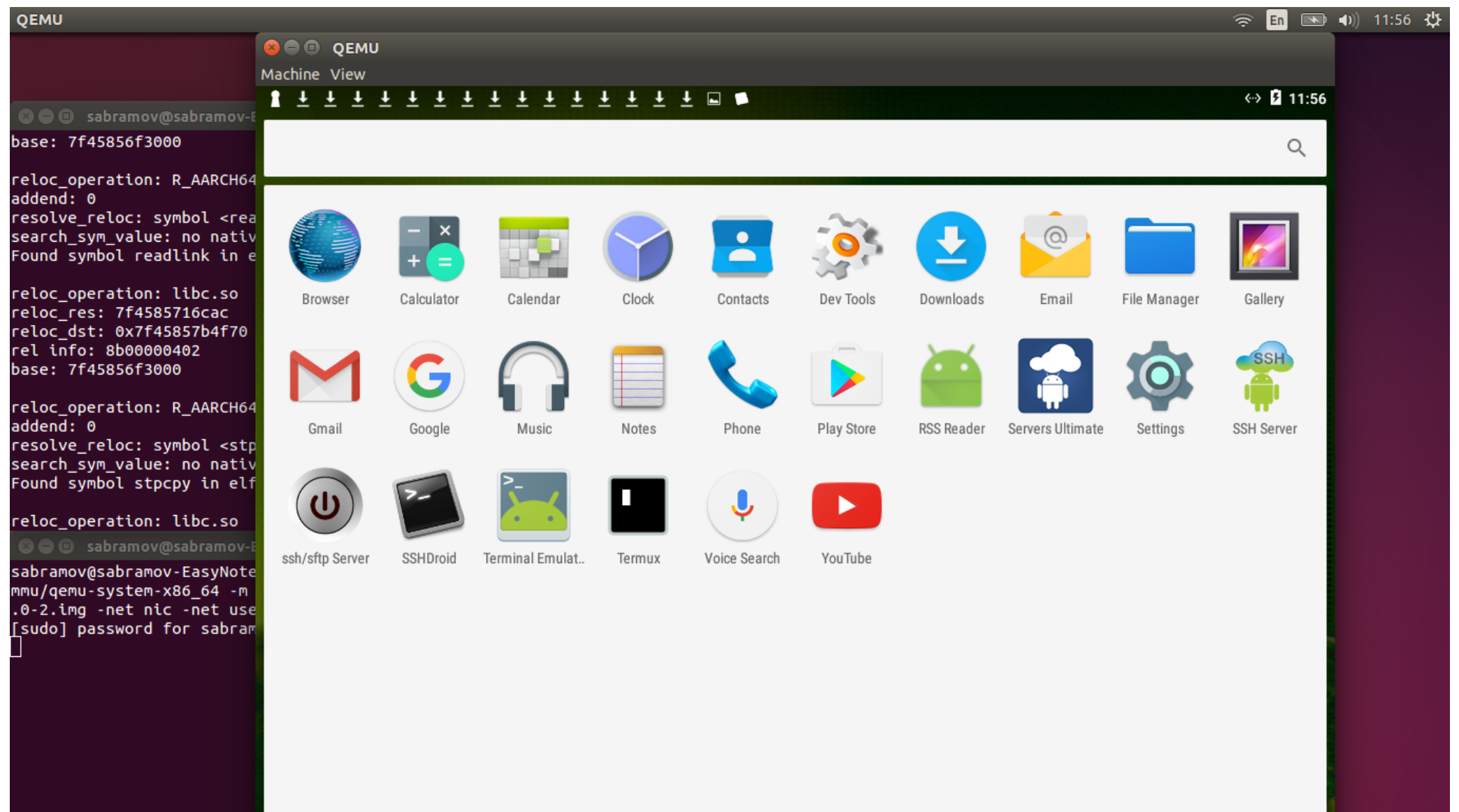


Отладка набора команд A64 методом трассировки (Odroid-C2)



Отладка системы и анализ результатов

Проверка функционирования системы
в гостевом окружении Android-x86_64 6.0



Заключение

Построен механизм для исполнения нативного ARM кода пользовательских приложений в Android-x86_64

В рамках работы:

- Реализован загрузчик динамических библиотек
- Реализована эмуляция ARM-v8, необходимая в рамках задачи
- Осуществлена отладка системы в окружении Android-x86_64 6.0

Результаты отладки:

- Реализованные механизмы и оптимизации работают корректно (загрузка пользовательских и стандартных библиотек; исполнение ARM кода; оптимизация: вызовы функций из нативных x86_64 библиотек вместо эмуляции функций ARM кода)

Перспективы

Эмуляция - базовый механизм для дальнейших оптимизаций:

- Интеграция с ART (Android RunTime)
- Бинарная трансляция

Спасибо за внимание!