Подробнее о симуляторах

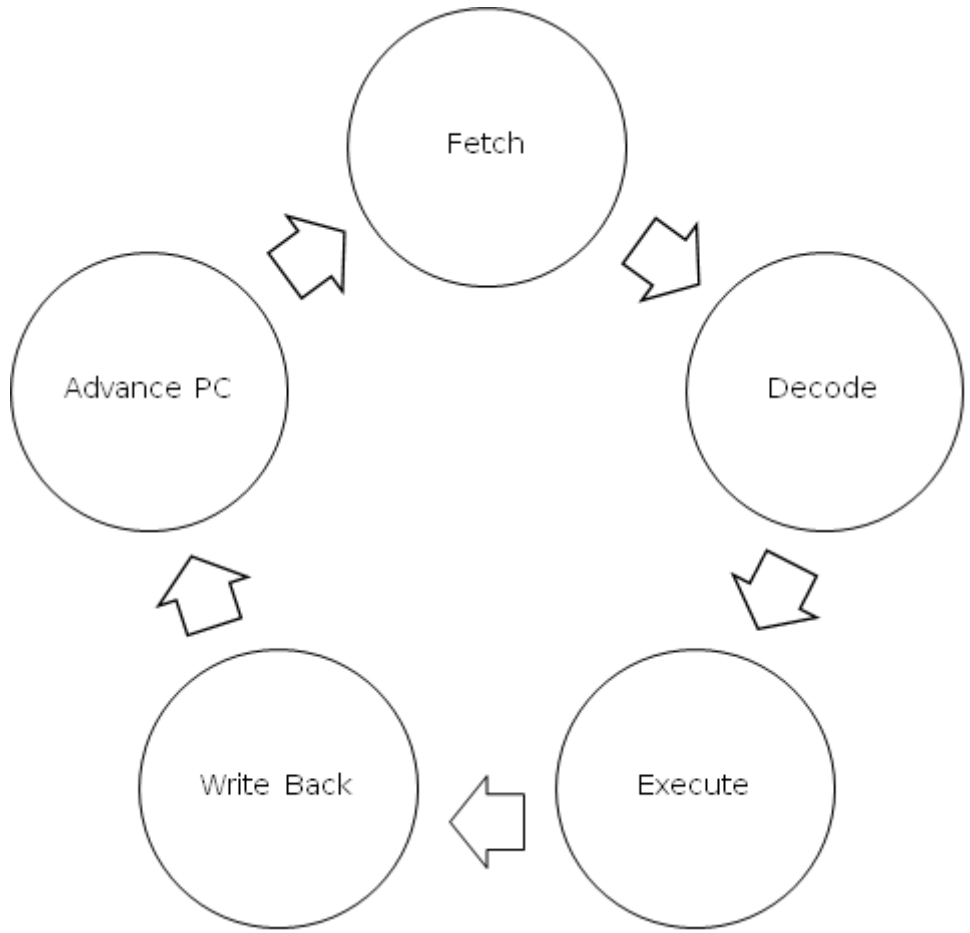
МФТИ
Весна 2024

Виды симуляции

По детальности симуляции

- Функциональный
  - Интерпретация
  - Бинарная трансляция
- Потактовый
- Логический

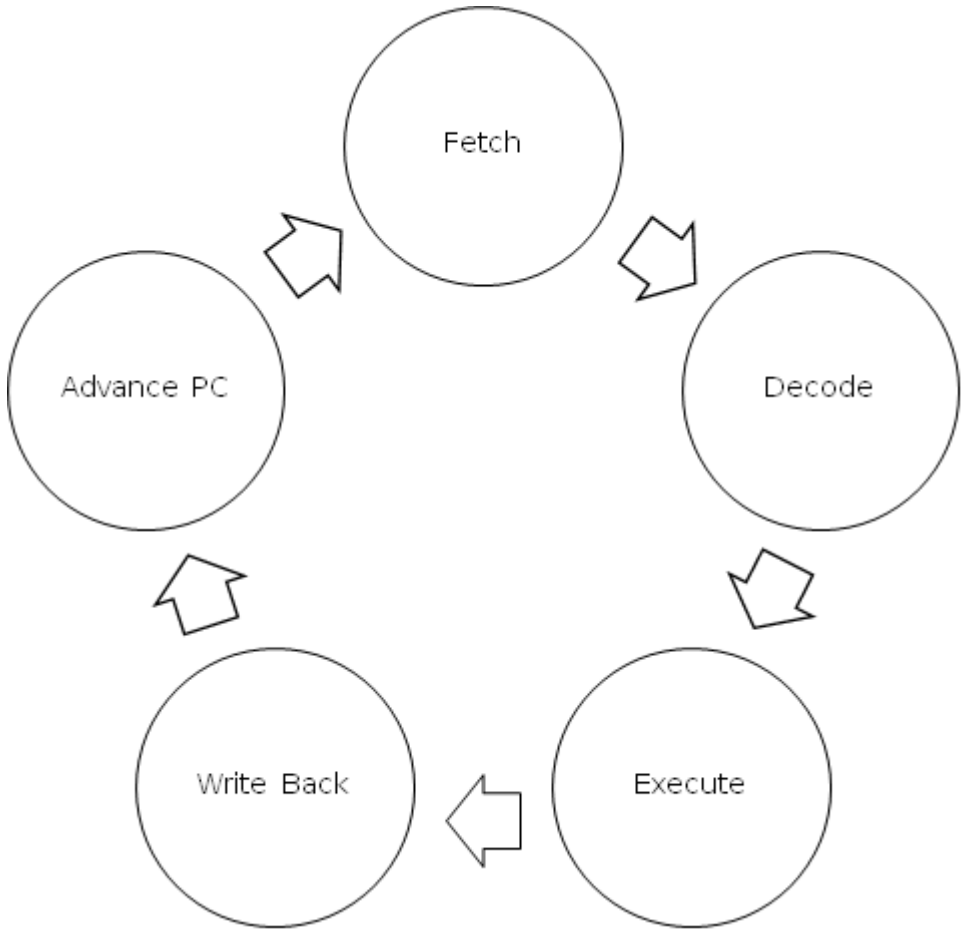
Функциональный симулятор: интерпретация



Функциональный симулятор: интерпретация

Fetch:

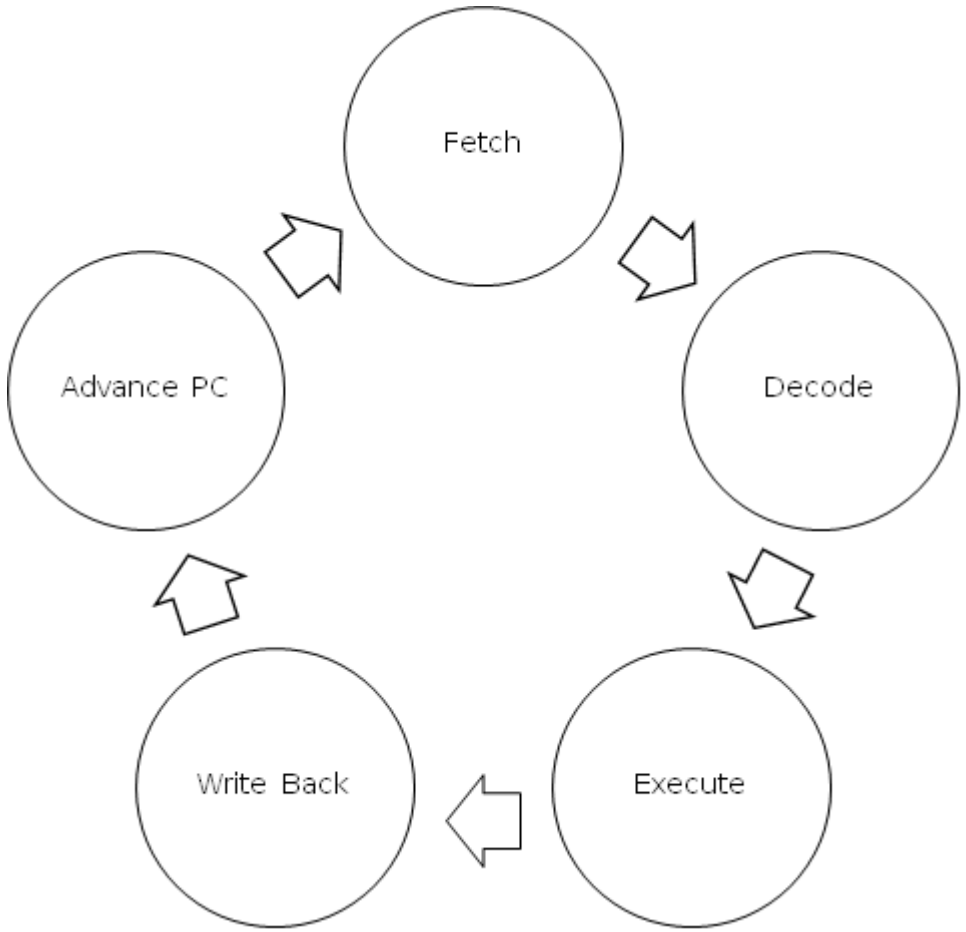
- Загрузка инструкций из памяти



Функциональный симулятор: интерпретация

Decode:

- Декодирование загруженной инструкции



Функциональный симулятор: интерпретация

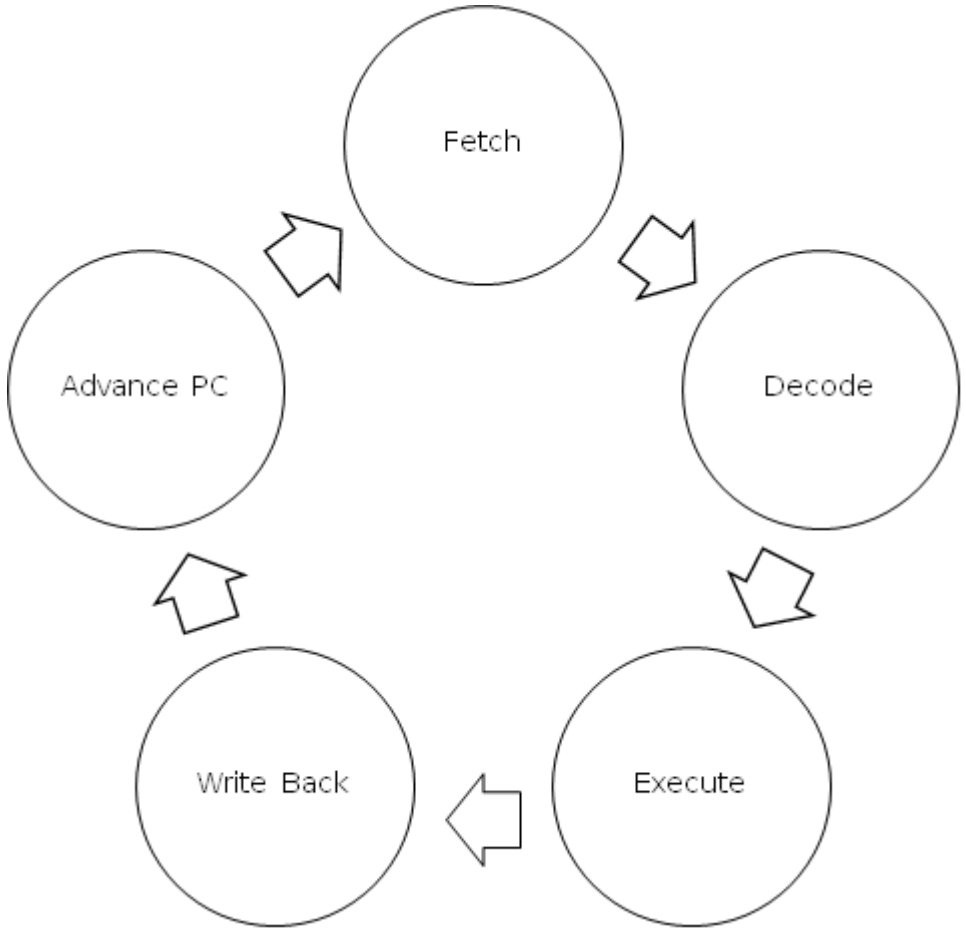
Decode:

- Декодирование загруженной инструкции

Оптимизация:

- Уже декодированные инструкции можно кешировать

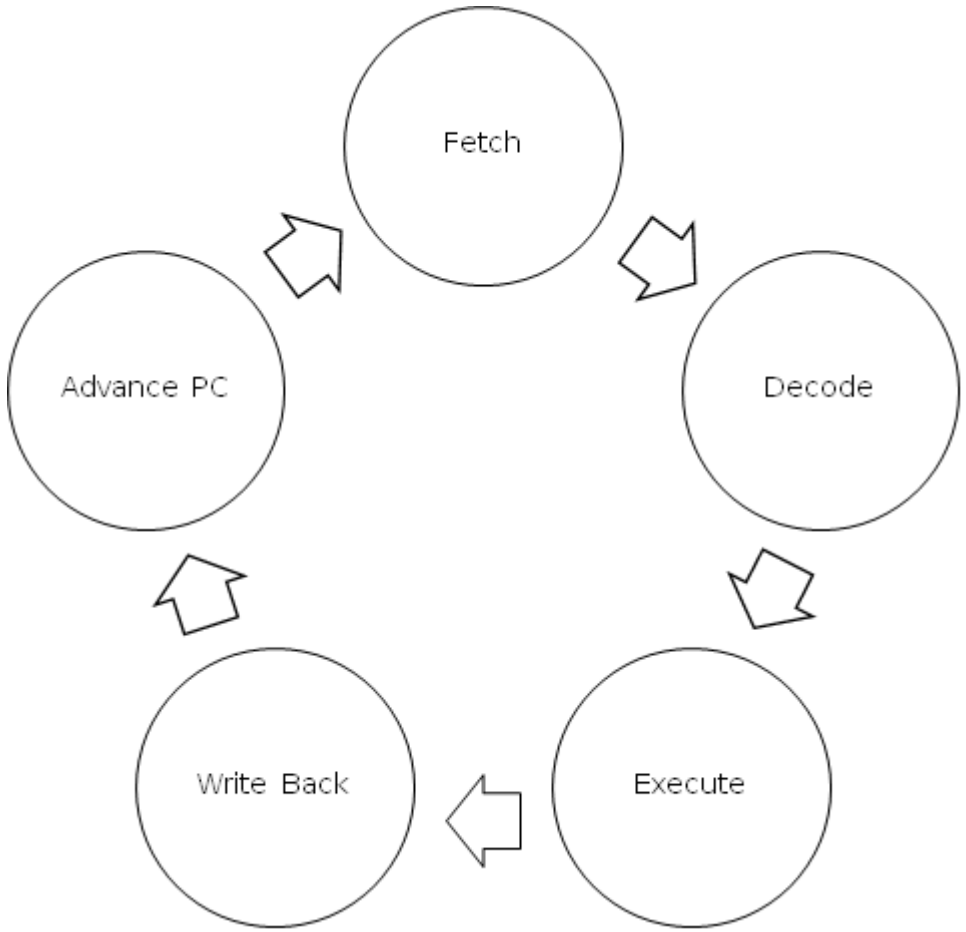
Что делать с самомодифицирующимся кодом?



Функциональный симулятор: интерпретация

Execute:

- Выполнение инструкции



Функциональный симулятор: интерпретация

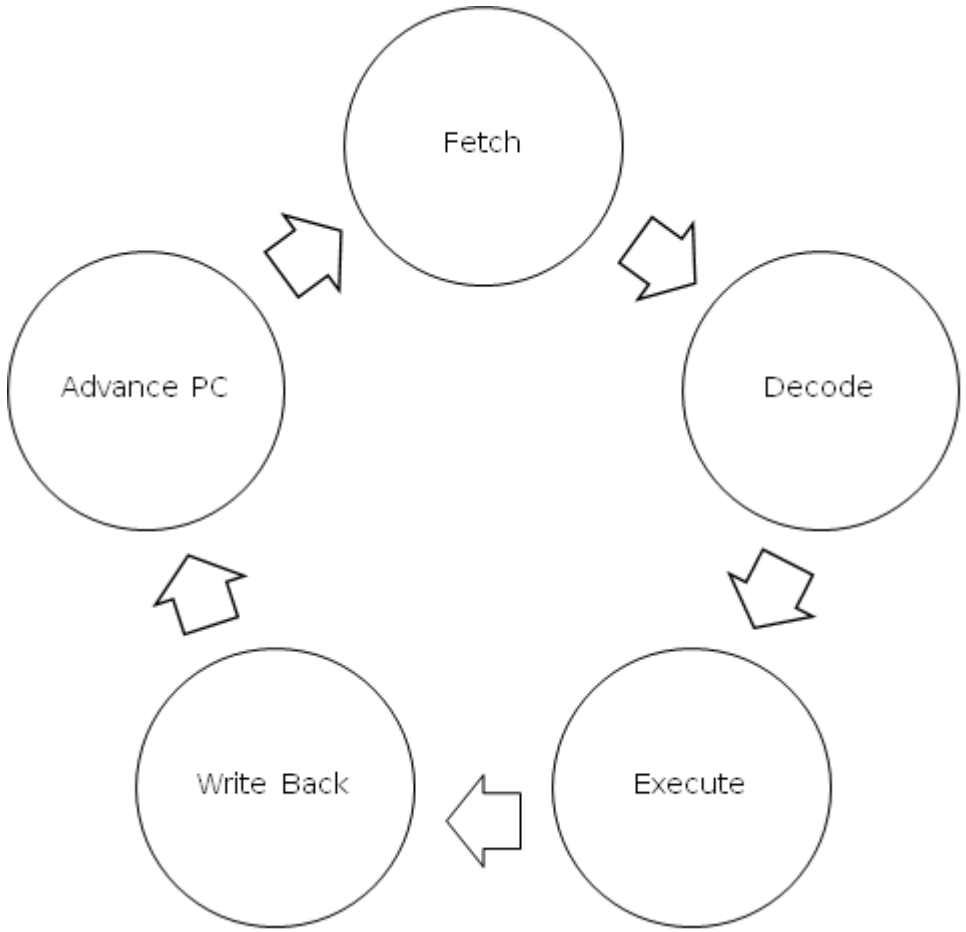
Execute:

- Выполнение инструкции

Оптимизация:

- Заменить switch на таблицу переходов

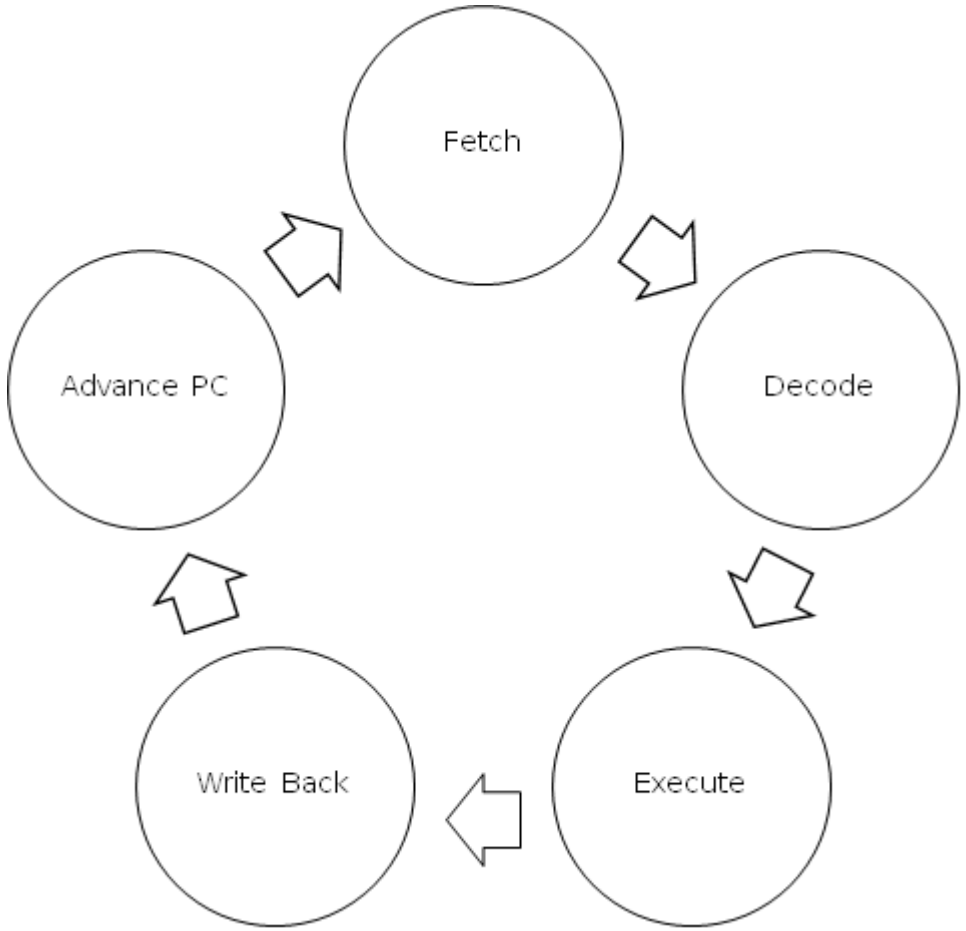
Не ухудшится ли производительность из-за перехода по косвенности?



Функциональный симулятор: интерпретация

Write back:

- Запись результатов выполнения инструкции



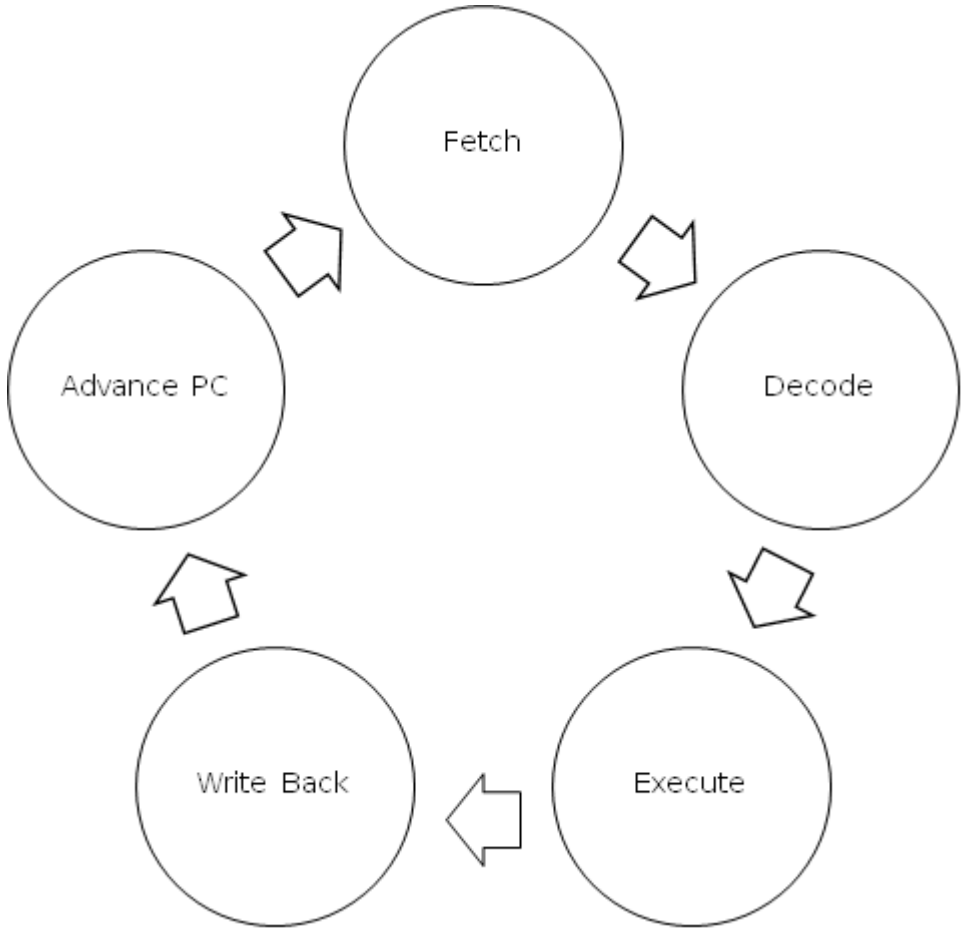
Функциональный симулятор: интерпретация

Write back:

- Запись результатов выполнения инструкции

Оптимизация:

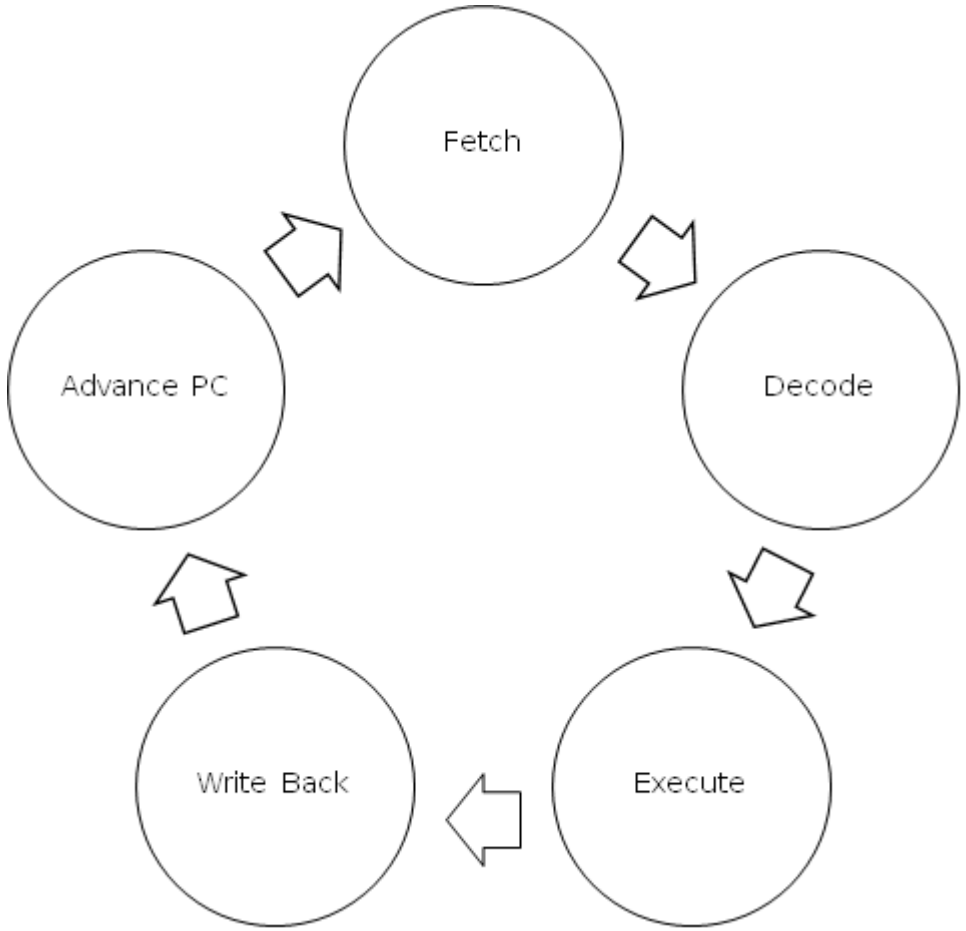
- Кешировать транслированные адреса



Функциональный симулятор: интерпретация

Advance PC:

- Продвижение вперед program counter (регистр-указатель на инструкцию)



Функциональный симулятор: интерпретация

Можем ли мы ускорить симуляцию если интерпретировать не одну инструкцию, а сразу несколько?

Функциональный симулятор: трансляция

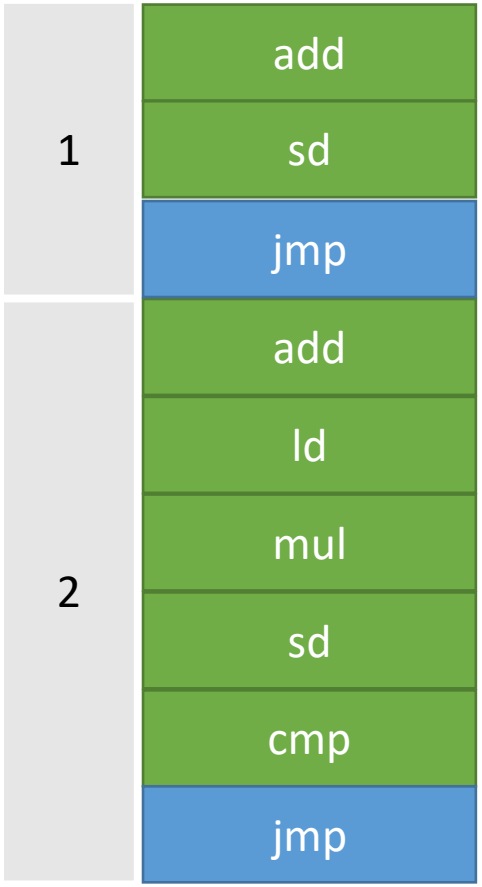
Можем ли мы ускорить симуляцию если интерпретировать не одну инструкцию, а сразу несколько?

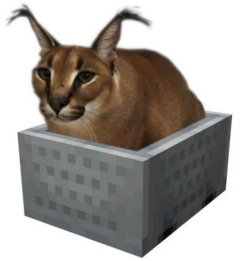
Да, делать бинарную трансляцию

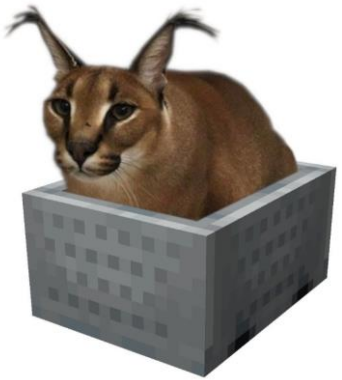
Функциональный симулятор: трансляция

1. Разбиваем последовательность инструкций на *базовые блоки*

Базовый блок – последовательность инструкций или кода, имеющую одну точку входа и одну точку

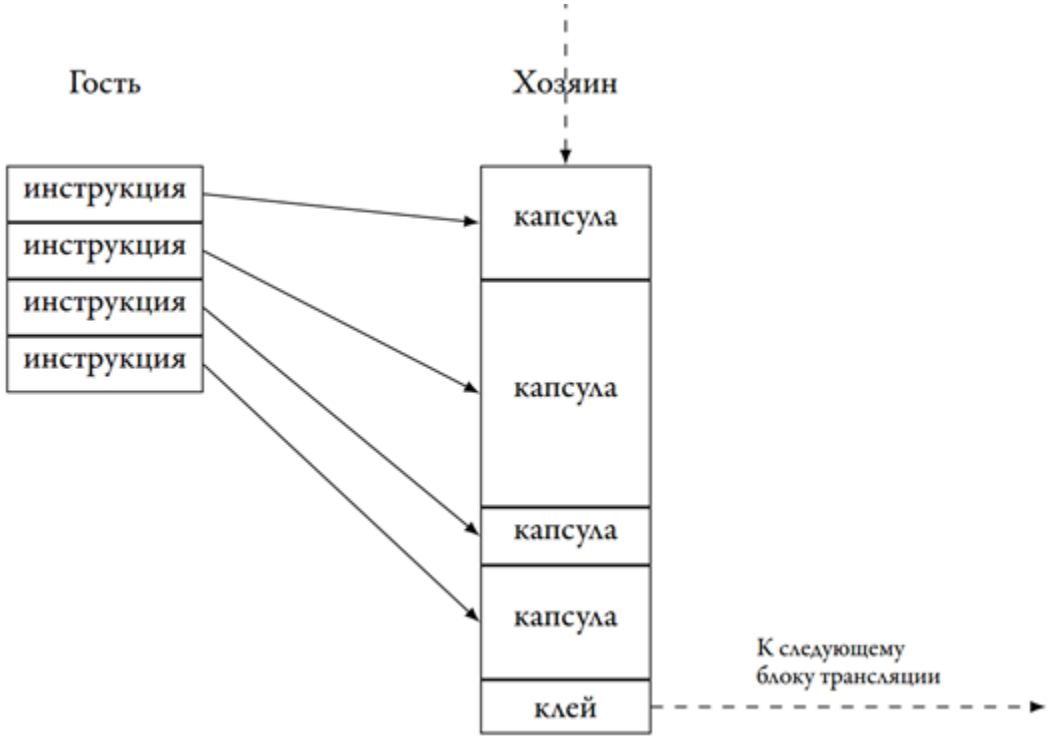






Функциональный симулятор: трансляция

2. Транслируем базовый блок гостевой архитектуры в базовый блок архитектуры хоста



Функциональный симулятор: трансляция

Что еще на ваш взгляд можно добавить для улучшения эффективности бинарной трансляции?

Функциональный симулятор: трансляция

Что еще на ваш взгляд можно добавить для улучшения эффективности бинарной трансляции?

- Оптимизация базовых блоков:
  - Пропуск nop инструкций
  - Объединение инструкций

Функциональный симулятор: трансляция

Какие проблемы вы видите у бинарной трансляции?

Функциональный симулятор: трансляция

Какие проблемы вы видите у бинарной трансляции?

- Самомодифицирующийся код
- Изменение адресов для jump и branch инструкций
- Ограниченность оптимизаций

Готов или не готов?

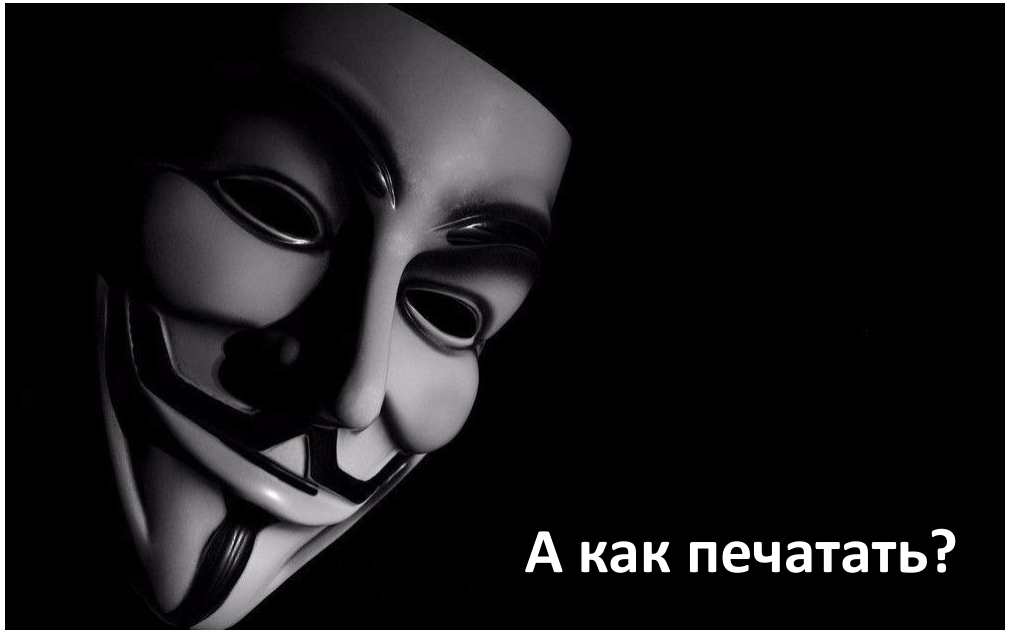
RISC-V Architecture Test – фреймворк архитектурных тестов

Референсные модели: SAIL и SPIKE

А как печатать?

`print` – одна из первых функций при изучении языков программирования, но далеко не первая при создании новой платформы

Почему?



Пытаемся выводить

Печать – операция ввода/вывода, т.е. работа с периферией

Как бы вы это реализовали в процессоре?

Пытаемся выводить

Печать – операция ввода/вывода, т.е. работа с периферией

Как бы вы это реализовали в процессоре?

- Специальная инструкция
- Memory-mapped IO
- Что-то среднее

Задание: пишем симулятор

Реализуйте симулятор rv32i процессора без привилегированных инструкций

`ecall` – semihosting

`ebreak` – остановка

fence.i – nop

Входной формат: образ памяти и адрес _start

To be continued …

На следующем занятии

- Узнаем как отличается производительность разных симуляторов
- Познакомимся с LLVM-based тестовым генератором