Прямое исполнение

Курс «Программное моделирование вычислительных систем»

Григорий Речистов
grigory.rechistov@phystech.edu

5 марта 2015 г.

На прошлой лекции

- Интерпретаторы — медленная шутка
- Двоичная трансляция быстрее, потому что вычисляет «меньше»

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО?

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО? Декомпиляция.

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО? Декомпиляция.
- А ЯВО $\rightarrow$ ЯВО?

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО? Декомпиляция.
- А ЯВО $\rightarrow$ ЯВО?Source-level компилятор

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО? Декомпиляция.
- А ЯВО $\rightarrow$ ЯВО?Source-level компилятор
- В каких случаях ДТ будет медленнее интерпретации на одной и той же гостевой программе?

Вопросы

- ЯВО $\rightarrow$ маш. код — компиляция. Маш. код $\rightarrow$ маш. код — ДТ. А что такое маш. код $\rightarrow$ ЯВО? Декомпиляция.
- А ЯВО $\rightarrow$ ЯВО?Source-level компилятор
- В каких случаях ДТ будет медленнее интерпретации на одной и той же гостевой программе? Если программа полна SMC.

Когда применимо прямое исполнение

- Когда гостевая ISA совпадает с хозяйской
- Ну или почти совпадает

Алгоритм

- BB

Почему это не будет работать

- Не полностью совпадающие ISA
- Различное положение внешних ресурсов (устройств и памяти)
- Привилегированность инструкций
- Необходимость изоляции симулятора от обнаружения и разрушения гостем

Почему это не будет работать

add %r1, %r2
mul $10, %r3
div %r4, %r5 Отсутствующая в хозяине инструкция
ld (0xa000), %r10 Другое расположение в памяти
st %r10, (%r11)
sub %r11, %r1
mov $16, %r13
mov %r13, %cr0 Привилегированные инструкции
trap $32

Предпросмотр кода

Заплатки и заглушки

Двоичная инструментация

- Общее название методики исследования и модификации приложений Pin http://pintool.org DynamoRIO http://dynamorio.org/

Сложности DEX

•••••Необходимость предпросмотра негативно влияет на производительность симуляции Необходимость контролировать SMC Переменная длина инструкций усложняет stubbing/patching Необходимо контролировать время исполнения гостя • А как это делается в многозадачных вытесняющих ОС? Для DEX оптимально иметь аппаратную поддержку на хозяине

Спектр симуляционных подходов

Коробка передач

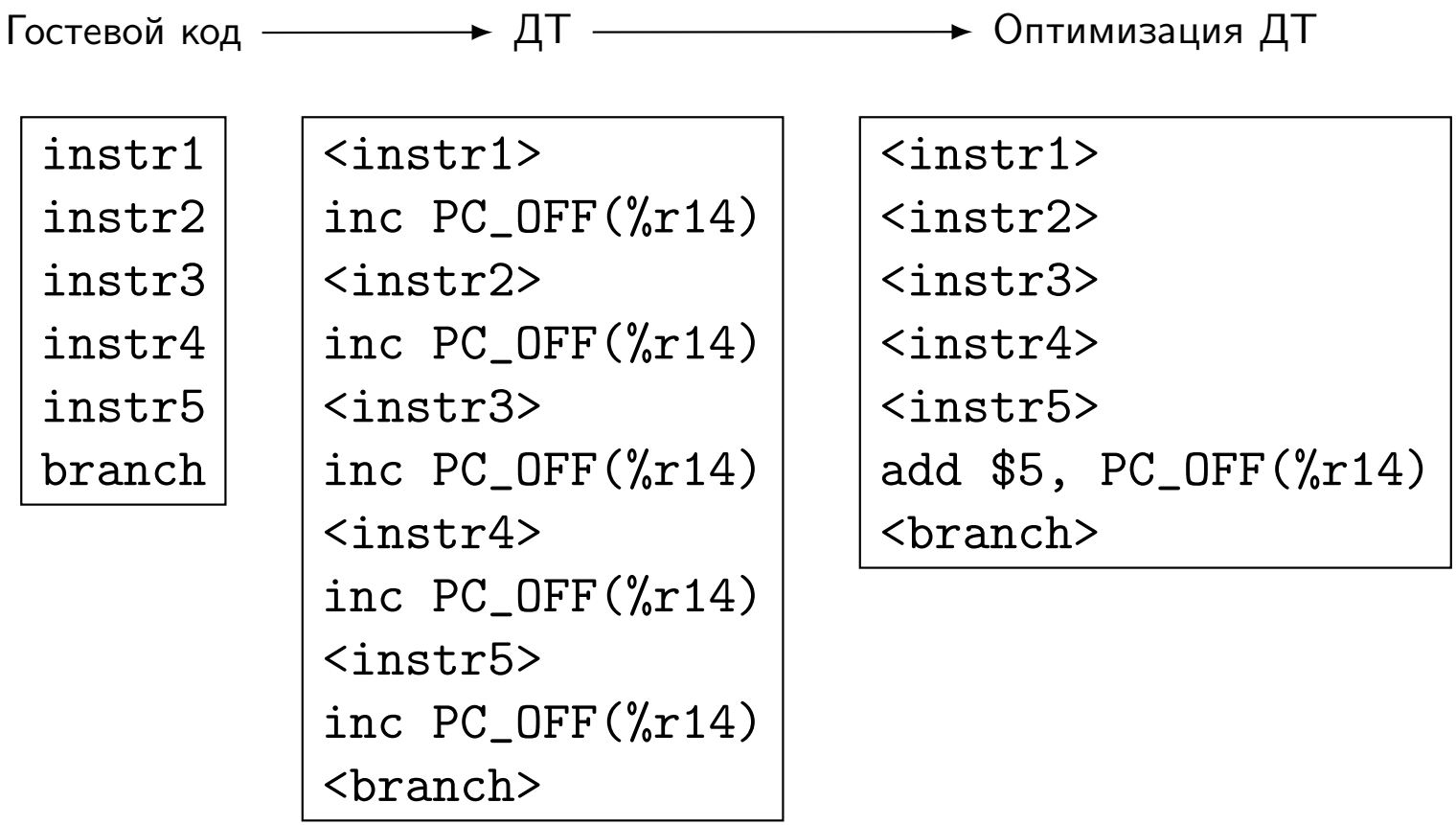
Динамическое переключение режимов

+Оптимальное использование лучших сторон каждого из подходов - Необходимость разработки фактически нескольких симуляторов

Итоги

Наивное прямое исполнение Заплатки и заглушки DEX с аппаратной поддержкой Переключение режимов симуляции • Условия на переходы

Оптимизации



Итоги

- Наивное прямое исполнение
- Заплатки и заглушки
- DEX с аппаратной поддержкой
- Переключение режимов симуляции
- Условия на переходы

Литература I

F. Leung, G. Neiger, D. Rodgers, A. Santoni, R. Uhlig. Intel® Virtualization Technology // Intel Technology Journal No10 (03 Aug 2006). http://www.intel.com/technology/itj/2006/v10i3/

Matias Zabaljauregui. Hardware Assisted Virtualization Intel Virtualization Technology. 2008. http://lib.mipt.ru/book/283035/

На следующей лекции

Симуляция периферийных устройств и полной платформы

Спасибо за внимание!

Слайды и материалы курса доступны по адресу
http://is.gd/ivuboc

Замечание: все торговые марки и логотипы, использованные в данном материале, являются собственностью их владельцев. Представленная здесь точка зрения отражает личное мнение автора, не выступающего от лица какой-либо организации.