Отзыв научного руководителя

на диссертацию Батузова Кирилла Андреевича «Исследование и разработка методов оптимизации программ для систем динамической двоичной трансляции», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Динамическая двоичная трансляция лежит в основе эмуляторов и двоичных компиляторов, которые являются сердцевиной множества более сложных технологий – анализа программ в двоичном коде, обратной отладки, восстановления структур данных и алгоритмов, разработки программ для мобильных и встраиваемых систем, обеспечения двоичной переносимости. Производительность эмуляторов во многом определяется качеством кода, сгенерированного в ходе двоичной трансляции. Поэтому целью диссертационной работы К.А. Батузова было ответить на вопрос о том, как выстраивать оптимизационную часть динамического двоичного транслятора для самого общего случая – различных исходной и целевой архитектур транслируемого кода, разработать соответствующие методы оптимизации и апробировать их на эмуляторе QEMU, единственном промышленном эмуляторе с открытым исходным кодом.

Актуальность и сложность задачи непосредственно следует из особенностей динамической трансляции и подвергаемого оптимизациям двоичного кода. Так, при оценке динамических оптимизаций нужно сравнивать затраты на выполнение оптимизационных проходов с выигрышем в скорости получаемого кода. Вдобавок двоичный код, из которого строится оптимизируемое внутреннее представление транслятора, как правило, уже получен в результате работы агрессивных оптимизаций компилятора с языка высокого уровня.

Диссертант рассмотрел весь спектр возможных методов оптимизации и предложил свое решение для каждого класса методов в поставленных в работе ограничениях. В случае машинно-независимых оптимизаций им предложено использовать классические итерационные методы продвижения констант и копий, а также разработан и теоретически обоснован алгоритм обхода региона трансляции, который гарантирует сходимость этих методов за одну итерацию. Для машинно-зависимых оптимизаций разработаны однопроходные алгоритмы локального и глобального распределения регистров, получаемого за счет учета локальным алгоритмом распределения необходимых условий по распределению перемен-

ных на регистры на границах базовых блоков. Доказываются теоремы о корректности построенных граничных условий и об оптимальности алгоритма генерации обеспечивающего эти условия кода внутреннего представления. Наконец, рассматривается вопрос поддержки выполнения векторных инструкций исходной архитектуры путем трансляции их также в векторные инструкции целевой архитектуры. Автором были предложены соответствующие структуры данных, учитывающие совершенно обычным образом возникающие перекрытия векторных регистров, разработаны алгоритмы анализа времени жизни переменных и анализа указателей, необходимые для корректной генерации векторных инструкций и распределения векторных регистров.

Все предложенные алгоритмы К.А. Батузов реализовал в эмуляторе QEMU, в результате чего было получено ускорение для машинно-независимых оптимизаций в пределах 1-2%, для алгоритма распределения регистров – до 30%, для векторных инструкций – до трех раз. Машинно-независимые алгоритмы уже включены в основные исходные коды QEMU. В ходе работы над диссертацией автор стал активным участником сообщества разработчиков QEMU, а возглавляемая им группа исследователей выполнила множество работ по оптимизации и улучшению инфраструктуры QEMU, что позволило с успехом использовать этот эмулятор в проектах ИСП РАН по анализу двоичного кода программ. Инструменты, полученные в этих проектах, внедрены и промышленно используются у заказчиков как в России, так и за рубежом.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а ее автор, Батузов Кирилл Андреевич, безусловно заслуживает присуждения ему ученой степени кандидата физико-математических наук по указанной специальности.

Научный руководитель:
в.н.с. ИСП РАН, к. ф.-м. н. А.А. Белеванцев
«20» января 2018 г.

Подпись Белеванцева А.А. удостоверяю:

Директор ИСП РАН А.И. Аветисян