УДК 519.7

Применение алгоритмов минимизации And-Inverter графов к задаче верификации булевых схем

Уразов Т.А. (Университет ИТМО)

Научный руководитель – к.т.н., доцент Семёнов А.А.

(Университет ИТМО)

Введение. Одна из эквивалентных формулировок известной теоремы Кука-Левина [1, 2] утверждает, что всюду определенную функцию, задаваемую программой машины Тьюринга, которая преобразует слова длины n в слова длины m, можно задать также булевой схемой (Boolean circuit) с n входами и m выходами. Внутренним узлам такой схемы (которые называются гейтами) приписаны элементы некоторого полного базиса. Если данный базис состоит из конъюнкции и отрицания, то соответствующая схема называется And-Inverter графом. Для функций, вычислимых за полиномиальное время сложность перехода от программы, задающей рассматриваемую функцию, к соответствующему And-Inverter графу ограничена полиномом от длины входа. Известны различные программные инструменты, которые по исходному программному описанию функции строят задание этой функции в виде And-Inverter графа. And-Inverter графы в последние годы активно используются в символьной верификации и анализе программ, а также при производстве микросхем для построения наборов тестов, выявляющих ошибки, которые могли возникнуть в ходе изготовления схемы. Одной из центральных в данном контексте является проблема проверки эквивалентности двух схем: требуется выяснить, верно ли что две схемы задают одну и ту же функцию (в случае ответа «да», схемы называются эквивалентными); данная задача известна как LEC (Logical Equivalence Checking). Наиболее часто для решения LEC используются современные программные решатели проблемы булевой выполнимости (SAT). Однако некоторые примеры LEC могут оказаться чрезвычайно сложными для всех известных SAT решателей. Довольно неожиданно, что к такие примеры LEC дают функции, хорошо известные еще из программы средней школы. Речь идет о функциях, задаваемых алгоритмами умножения пар натуральных чисел: известен целый ряд таких алгоритмов (столбик, Дерево Уоллеса [3], умножитель Дадды [4], алгоритм Карацубы [5] и др.). Задачи доказательства эквивалентности схем, реализующих данные алгоритмы, в SAT форме обладают аномальной сложностью и не поддаются на сегодняшний день ни одному из известных SAT решателей.

Основная часть. Ставятся и решаются следующие задачи: 1) исследовать известные инструменты построения и анализа And-Inverter графов – системы ABC [6] и Transalg [7]; 2) разработать алгоритмы подстановки в And-Inverter графы значений гейтов и процедуры распространения ограничений; 3) построить Cube-and-Conquer стратегию декомпозиционного представления And-Inverter графа на семейство подграфов с последующим использованием SAT оракулов; 4) применить разработанные алгоритмы для решения трудных примеров LEC (в отношении умножителей и сортировщиков).

Выводы. Ожидается, что результатом данной работы станут новые алгоритмы решения LEC за счет специализированной Cube-and-Conquer стратегии, показывающие большую эффективность в сравнении с известными на трудных вариантах LEC.

Список использованных источников:

1. Cook S.A. The complexity of theorem-proving procedures. STOC’71. Pp. 151-158.
2. Левин Л.А. Универсальные задачи перебора. Проблемы передачи информации. 1973. Т.9, No 3, С. 265-266.

3. Cormen M., Leiserson C., Rivest R. Introduction to Algorithms. First Edition. 1990. MIT Press and McGraw-Hill.
4. Dadda L. Some schemes for parallel multipliers. Alta Frequenza, vol. 34, no. 5, pp. 349–356, 1965.
5. Knuth D. The Art of Computer Programming, Volume 2: Seminumerical Algorithms (Addison-Wesley Series in Computer Science & Information Processing). Addison-Wesley, 1969.
6. Brayton R., Mishchenko A. ABC: An academic Industrial-Strength Verification Tool. CAV 2010. LNCS. Vol. 6174. Pp. 24-40.
7. https://gitlab.com/transalg/transalg/-/tree/master?ref_type=heads