АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧИ О ВЫПОЛНИМОСТИ КНФ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Долгий О.В.

Бибило П.Н.- д.т.н., профессор

К решению задачи выполнимости сводится важная практическая задача верификации (функциональной эквивалентности) комбинационных логических схем, задачи синтеза логических схем, анализа и построения тестов для дискретных устройств. Более того, аппарат логических уравнений является достаточно универсальным, кроме перечисленных задач из области логического проектирования дискретных устройств к решению логических уравнений могут быть сведены и задачи криптоанализа.

Задача выполнимости (SAT) состоит из выяснения, является ли булева функция выполнимой, т.е. существует ли такой набор значений, которые бы давали значение функции, равное «1». Обычно, функция представлена конъюнктивной нормальной формой (КНФ), которая состоит из конъюнкций некоторого числа выражений, представляющих собой дизъюнкции одного или боле литералов. Литералом называется переменная или ее отрицание.

Наиболее известным полным алгоритмом для решения задачи выполнимости является классический алгоритм Дэвиса-Путнама (DP), в котором процесс поиска организован полным перебором всех возможных присвоений значений переменным, и обычно представлен деревом решений. Корень этого дерева решений относится к стартовой точке, когда значения всем переменным не присвоены. Остальные вершины представляют состояния, которые могут быть достигнуты во время процесса поиска. Эти вершины характеризуются соответствующими частичными присвоениями. Если в какой-либо вершине частичное присвоение выполняет функцию, процесс поиска останавливается. В ином случае, поиск должен быть продолжен либо в прямом (если конфликтов не обнаружено), либо в обратном порядке (если конфликт возник).

Пространство поиска задачи выполнимости представлено на рисунке 1.

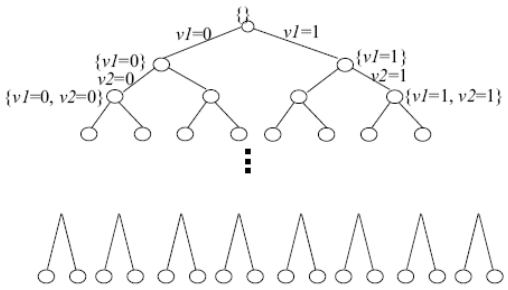

Рис. 1 – Пространство поиска задачи выполнимости

Большинство передовых программных SAT-решателей (GRASP, Relsat, zChaff, BerkMin и т.д.) являются производными DP-алгоритма, расширяя его специальными техниками для уменьшения пространства поиска. Наиболее известными техниками являются техника единичного дизъюнкта и правило литерала одного знака. SAT-соревнование 2011-го года также показало высокую эффективность алгоритмов типа glucose, основанных на правиле склеивания.

Для моделирования исходных VHDL-описаний использовалась систему моделирования ModelSim, для синтеза схем – Xilinx ISE.

Список использованных источников:

9. Davis M., Putnam H. A Computing Procedure for Quantification Theory. Journal of the Association for Computing Machinery, vol. 7, pp. 201-215, 1960.
10. Utkin A.A. Experimental Investigation of Satisfiability Algorithms. Avtomatika i Vichislitelnaya Technika, No. 6, pp.66-74, 1990.
11. Торопов Н. Р. Параллельная проверка ДНФ на тавтологию. // Информатика . – 2005. – № 2. – С. 35-42.