УДК 004.23

ЭВОЛЮЦИОННЫЕ АЛГОРИТМЫ ПОСТРОЕНИЯ ДЕКОМПОЗИЦИОННЫХ МНОЖЕСТВ ДЛЯ ТРУДНЫХ ВАРИАНТОВ ЗАДАЧ О БУЛЕВОЙ ВЫПОЛНИМОСТИ, ПОЗВОЛЯЮЩИХ ДОСТИЧЬ СВЕРХЛИНЕЙНОГО УСКОРЕНИЯ ПРИ РЕШЕНИИ

Павленко А.Л. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель – к.т.н., доцент факультета ИТиП Ульянцев В.И.
(Университет ИТМО, г. Санкт-Петербург)

Задача о выполнимости булевых формул (SAT – Boolean Satisfiability problem) является важной для теории вычислительной сложности алгоритмической задачей. Для их решения могут быть использованы специальные программные средства – SAT-решатели. Современные SAT-решатели позволяют решать многие SAT-задачи за разумное время, но далеко не все. Эволюционные методы, предлагаемые в этой работе, позволяют строить особые декомпозиционные множества, которые позволяют достигать сверхлинейного ускорения при параллельном решении SAT-задач.

Введение. Декомпозиционные множества (или Backdoors) позволяют упростить задачу, путем её декомпозиции на более простые подзадачи. Однако, чтобы решить исходную задачу, необходимо решить все множество подзадач, полученных путем декомпозиции. Также существует еще такое понятие как Strong Backdoor, подстановка значений переменных из которого позволяет решать подзадачи, используя полиномиальный алгоритм. Но такие множества обычно содержат большое количество переменных, а число задач, которые необходимо решить, экспоненциально от их числа. Поэтому в данной работе мы рассмотрим Non-Deterministic Oracle Backdoor Set (NOBS).

Основная часть. В данной работе применяются эволюционные алгоритмы для построения особых декомпозицонных множеств для SAT-задач, позволяющих достичь сверхлинейного ускорения при решении. В статье «On cryptographic attacks using backdoors for SAT» было введено понятие NOBS для описания таких множеств. Оно звучит следующим образом:

> Пусть A – некоторый полный алгоритм, C - произвольная КНФ формула над множеством переменных V. Тогда непустое множество B: $B \subseteq V$, является Non-Deterministic Oracle Backdoor Set (NOBS), если время решения задачи C алгоритмом A больше, чем суммарное время решения всех задач $C[\beta/B]$ для всех β таких, что $\beta \in (0,1)^{|B|}$.

Поскольку множество переменных V в большинстве случаев имеет большую мощность в интересующих нас задачах, предполагается, что для задачи известно такое множество $V_{in} \subset V$, что его переменные являются особо значимыми для данной задачи. Например, для задач обращения криптографических функций таким множеством переменных V_{in} является множество переменных секретного ключа. Для построения декомпозиционного множества B посредством эволюционных вычислений представим это множество в виде битового вектора, такого что если i-ый бит равен единице, то $i \in B$. В качестве инициализирующего вектора положим вектор из единиц размера $|V_{in}|$. Для оценки декомпозиционных множеств будем использовать метод Guess-and-Determine. Если множество слишком большое, то вычислять оценочное значение будем с помощью метода Монте-Карло. Пусть N – размер оценочной выборки, от которого зависит точность получаемой оценки. Тогда для вычисления оценки формируем N подзадач $C[\beta_1/B]$, $C[\beta_2/B], \dots, C[\beta_N/B]$ со случайными подстановками β_1, $\beta_2, \dots, \beta_N$ из множества B, а затем замеряем времена их решения $t_1, t_2, \dots, t_N$ с помощью SAT-решателя A. После решения всех подзадач, оценочное значение будет находиться как среднее арифметическое всех значений времени $t_1, t_2, \dots, t_N$ домноженное на $2^{|B|}$. Если же количество

всевозможных подзадач, получаемых в результате декомпозиции, меньше или равно чем N, тогда оценка будет равна сумме всех значений времени, затраченных на решения этих подзадач.
Используя описанный выше алгоритм, было проведено экспериментальное исследование для класса SAT-задач, которые доказывают эквивалентность двух разных алгоритмов сортировки. В качестве V_{in} использовалось множество переменных, отвечающие за биты начального вектора чисел для сортировки. В ходе экспериментов были построены декомпозицонные множества для исследуемого класса задач, которые позволяют достигать сверхлинейное ускорение при параллельном решении *независимых* подзадач, получаемых в результате декомпозициии.

Выводы. Были разработаны и реализованы эволюционные алгоритмы построения NOBS. Было проведено экспериментальное исследование для класса SAT-задач, которые доказывают эквивалентность двух разных алгоритмов сортировки с использованием разработанных алгоритмов, а также были получены экспериментальные данные, которые подтверждают возможность достижения сверхлинейного ускорения при решении.

Павленко А.Л. (автор)

Ульянцев В.И. (научный руководитель)