О распознавании сложности аппроксимации булевых функций[1]

Н. Н. Кузюрин, О. А. Прокопьев

Аннотация. Показано, что задача распознавания существования простой аппроксимации булевой функции алгоритмически трудна.

1. Введение

В данной работе рассматривается задача, связанная с распознаванием схемной сложности булевых функций, заданных своей таблицей истинности. Подобные задачи рассматривалась в прошлом, в частности, в классических работах [2, 5]. Интересна одна из последних работ в этой области [10], в которой рассмотрена следующая задача.

Задача о схеме минимального размера (Minimum Circuit Size Problem, MCSP):

Входные данные: Булева функция f_n: $\{0,1\}^n \to \{0,1\}$ задана своей таблицей истинности размера 2^n и задано натуральное число $s_n \in N$.

Вопрос: Вычислима ли f_n булевой схемой размера не больше, чем s_n?

Отметим, что здесь и далее f_n — некоторая последовательность булевых функций, s_n — последовательность натуральных чисел, ε_n — последовательность вещественных чисел.

В [10] доказано, что при некоторых, достаточно естественных предположениях о существовании псевдослучайных генераторов, задача **MCSP** алгоритмически трудна.

В данной работе рассматривается ее обобщенный вариант, который неформально можно назвать задачей о распознавании существования простой аппроксимации заданной булевой функции. Сформулируем эту задачу.

Задача о ε-схеме минимального размера (Minimum ε-Circuit Size Problem, ε-MCSP):

Пусть задана некоторая последовательность $\varepsilon = \varepsilon_n$ и $0 \le \varepsilon_n \le 1$.

Входные данные: Булева функция f_n: $\{0,1\}^n \to \{0,1\}$ задана своей таблицей истинности размера 2^n, задано натуральное число $s_n \in N$.

[1]Работа выполнена при поддержке РФФИ, проект 04-01-00359.

Вопрос: Существует ли булева схема $G(n)$ размера не больше, чем s_n, вычисляющая некоторую булеву функцию g_n, для которой выполняется

$$Pr_{x\in\{0,1\}^n}\{g_n(x) \neq f_n(x)\} \le \varepsilon_n.$$

Эта запись означает, что доля наборов, на которых g_n не совпадает с f_n, не превосходит ε_n. Отметим, что задача приближения сложной булевой функции другой простой булевой функцией возникает, например, в криптографии [3].

При $\varepsilon \ge 1/2$ задача ε-**MCSP** решается за полиномиальное время. Это почти очевидно. Действительно, рассмотрим таблицу истинности функции f_n. Если на большинстве наборов (т. е. больше, чем 2^{n-1}) f_n принимает значение равное единице, тогда в качестве схемы $G(n)$ можно взять минимальную схему, реализующую 1; в противном случае, $G(n)$ — минимальная схема, реализующая 0. Соответственно, если считать, что размер минимальной схемы реализующей 0 (или 1) равен 2, то при входных данных $s_n \ge 2$, выходной ответ задачи ε-**MCSP** принимает значение «Да», в противном случае — «Нет».

Следующий вопрос — какова сложность задачи ε-**MCSP** для любого другого ε, где $1/2^n < \varepsilon < 1/2$.

Основным результатом настоящей статьи является ответ на этот вопрос, который заключается в том, что задача распознавания существования простой аппроксимации булевой функции — алгоритмически трудна.

А именно, в работе доказано, что при $0 \le \varepsilon_n \le 1/2 - w_n$, где w_n с ростом n стремится к 0 «не очень быстро», задача ε-MCSP трудна (не принадлежит классу $P/poly$), при предположении, что существует сильный псевдослучайный генератор (точная формулировка содержится в теореме 1).

2. Некоторые определения

Напомним некоторые основные определения и понятия, которые понадобятся нам в дальнейшем.

Схема (булева) — это способ вычисления функции $f : \{0,1\}^n \to \{0,1\}^m$. Помимо исходных переменных $x_1, \ldots, x_n$, для которых вычисляется значение f, схема использует некоторое количество вспомогательных переменных $y_1, \ldots, y_s$ и некоторый набор (базис) булевых функций F. Схема S в базисе F определяется последовательностью присваиваний $Y_1, \ldots, Y_s$. Каждое присваивание Y_i имеет вид $y_i = f_j(u_{k_1}, \ldots, u_{k_r})$, где $f_j(\cdot) \in F$, а переменная u_{k_p} $(1 \le p \le r)$ — это либо одна из исходных переменных x_t $(1 \le t \le n)$, либо вспомогательная переменная с меньшим номером y_l $(1 \le l < i)$. Таким образом, для каждого набора значений исходных переменных последова-

тельное выполнение присваиваний, входящих в схему, однозначно определяет значения всех вспомогательных переменных. Результатом вычисления считаются значения последних m вычислений $y_{s-m+1}, \ldots, y_s$.

Схема вычисляет функцию f, если для любых значений $x_1, \ldots, x_n$ результатом вычисления является $f(x_1, \ldots, x_n)$.

Графически схему можно представлять в виде ориентированного ациклического графа, у которого вершины входной степени 0 (входы) помечены исходными переменными; остальные вершины (функциональные элементы) помечены функциями из базиса F (при этом входная степень вершины должна совпадать с количеством аргументов её пометки); вершины выходной степени 0 (выходы) помечены переменными, описывающими результат работы схемы. Вычисление на графе определяется индуктивно: как только известны значения всех вершин $y_1, \ldots, y_{k_v}$, из которых ведут ребра в данную вершину v, вершина v получает значение $y_v = f_v(y_1, \ldots, y_{k_v})$, где f_v — базисная функция, которой помечена вершина.

Базис называется *полным*, если для любой булевой функции f есть схема в этом базисе, вычисляющая f. Пример полного базиса — $\{\neg, \&, \vee\}$.

Размером схемы называется количество присваиваний в схеме. Минимальный размер схемы в базисе F, вычисляющий функцию f, называется *схемной сложностью* функции f в базисе F.

Пусть L — некоторый язык, $L \subseteq \Sigma^*$. Напомним, что

$$\chi_L(x) = \begin{cases} 1, \ if \ x \in L; \\ 0, \ if \ x \notin L. \end{cases}$$

Класс $P/poly$ [9]. $L \in P/poly$, если существует последовательность булевых схем $\{C_n\}$, для которых выполняются следующие условия:

a) для любого n у схемы C_n ровно n входов и 1 выход;

b) существует полином P такой, что для любого n размер схемы $|C_n| \leq P(n)$ и $C_n(x) = \chi_L(x)$ для всех $x \in \{0,1\}^n$.

Известно, что $P/poly$ содержит любой язык вычислимый эффективным вероятностным алгоритмом (из класса BPP).

Псевдослучайный генератор (pseudorandom generator). Неформально псевдослучайный генератор можно определить как «эффективно вычислимую» функцию, которая преобразует короткую случайную строчку в более длинную псевдослучайную.

Нам потребуется следующее определение.

Определение [11]. **Трудность** (hardness) $H(G_k)$ псевдослучайного генератора $G_k : \{0,1\}^k \to \{0,1\}^{2k}$ определяется как минимальное s, при котором существует схема C размера не больше s для которой выполняется:

$$|Pr_{x \in \{0,1\}^k}[C(G_k(x)) = 1] - Pr_{y \in \{0,1\}^{2k}}[C(y) = 1]| \geq 1/s.$$

Определение [11]. Псевдослучайный генератор G_k называется **сильным**, если $H(G_k) > 2^{k^{\Omega(1)}}$.

Будем говорить, что псевдослучайный генератор $G_k : \{0,1\}^k \to \{0,1\}^{2k}$ принадлежит классу P/poly, если отображение G_k реализуемо булевой схемой полиномиального (от k) размера.

2.1. Естественные свойства

В этом разделе мы приводим краткое изложение некоторых результатов из [11].

Под комбинаторным свойством булевых функций мы будем подразумевать набор булевых функций $\{C_n \subseteq F_n\}$, где F_n обозначает множество всех булевых функций от n переменных. Таким образом булева функция f_n будет обладать свойством C_n тогда и только тогда, когда $f_n \in C_n$. Иногда, удобно давать следующее функциональное определение : $C_n(f_n) = 1$, если $f_n \in C_n$ и $C_n(f_n) = 0$, если $f_n \notin C_n$. Пусть Γ и Λ - некоторые сложностные классы. Комбинаторное свойство **Γ-естественно (Γ-natural) с плотностью** δ_n, если оно содержит подмножество $C_n^* \in C_n$ для которого выполняются два следующих условия:

Конструктивность: Принадлежность f_n классу C_n^* вычислимо за время Γ от размера таблицы значений f_n (напомним, что это число равно 2^n).

Объемность (Largeness): $|C_n^*| \geq \delta_n \cdot |F_n|$.

Комбинаторное свойство C_n называется **полезным против** Λ если оно удовлетворяет следующему условию:

Полезность: Для любой последовательности функций f_n, где $f_n \in C_n$, для бесконечно большого числа значений числа n выполняется $\{f_n\} \notin \Lambda$.

Далее по умолчанию будем считать $\delta_n = 2^{-cn}$, где c — некоторая константа. Для случая $\Lambda = P/poly$ свойство **полезности** формулируется следующим образом:

Полезность: Размер минимальных схем любой последовательности функций $f_1, f_2, ..., f_n, ...$, где $f_n \in C_n$, суперполиномиален, то есть для любой константы k и для достаточно больших значений n, размер схемы f_n больше, чем n^k.

Имеет место следующий факт:

Теорема (Разборов-Рудих) [11]: Если существует *$P/poly$-естественное свойство полезное против $P/poly$*, тогда не существует *сильного псевдослучайного генератора* в $P/poly$.

Другими словами существование $P/poly$-свойства, полезного против $P/poly$, означает существование «эффективного» алгоритма, при помощи которого можно взламывать любой псевдослучайный генератор.

2.2. Задача MCSP

Как уже было сказано выше в работе Кабанец-Каи [10] рассматривается **Задача о схеме минимального размера (Minimum Circuit Size Problem, MCSP)**:

Входные данные: Булева функция f_n: $\{0,1\}^n \to \{0,1\}$ задана своей таблицей истинности размера 2^n и задано натуральное число $s_n \in N$.

Вопрос: Вычислима ли f_n булевой схемой размера не больше, чем s_n?

В [10] показано следующее:

Теорема(Кабанец-Каи) [10]: Если задача **MCSP** принадлежит классу $P/poly$, тогда не существует сильного псевдослучайного генератора в $P/poly$.

3. Задача ε-MCSP

Рассмотрим задачу ε-**MCSP**:

Пусть задана последовательность $\varepsilon = \varepsilon_n$, $0 \le \varepsilon \le 1$.

Входные данные: Булева функция f_n: $\{0,1\}^n \to \{0,1\}$ задана своей таблицей истинности размера 2^n, задано натуральное число $s_n \in N$.

Вопрос: Существует ли булева схема $G(n)$ размера не больше, чем s_n, вычисляющая некоторую функцию g_n, для которой выполняется

$$Pr_{x\in\{0,1\}^n}\{g_n(x) \neq f_n(x)\} \le \varepsilon_n. \quad (1)$$

Свойство (1) означает, что g_n «достаточно близка» к f_n — то есть отличается от значений f_n не более, чем на ε_n доле наборов значений.

Очевидно, что для $\varepsilon < 1/2^n$ выполняется **Теорема (Кабанец-Каи)**. Нас интересует насколько сложна задача ε-**MSCP** для остальных значений ε.

Напомним, что функция $h(n)$ — суперполиномиальна, если для любой константы k существует достаточно большое число N такое, что для всех $n > N$ выполняется $h(n) > n^k$. Основной результат работы содержится в следующей теореме.

Теорема 1: Пусть $\varepsilon \le 1/2 - w_n$, $h(n)$ — суперполиномиальная функция и пусть выполняются следующие условия: $0 < w_n < 1/2$, $h(n) = o(\frac{2^n}{n})$ и

$$w_n \ge 5 \cdot \frac{\sqrt{h(n)\log h(n)}}{2^{\frac{n}{2}}}.$$

Если ε-**MCSP** принадлежит $P/poly$, то не существует сильного псевдослучайного генератора в $P/poly$.

3.1. Доказательство теоремы 1

Для доказательства этой теоремы воспользуемся **теоремой Разборова-Рудиха** [11]. Предположив, что ε-**MCSP** принадлежит классу $P/poly$, построим $P/poly$-естественное свойство полезное против $P/poly$. Пусть $s_n = h(n)$, где $h(n)$ — некоторая суперполиномиальная функция, для которой выполняется условие $h(n) = o(\frac{2^n}{n})$.

Определим комбинаторное свойство C_n следующим образом:

$f_n \in C_n$, если не существует булевой схемы $G(n)$ размера меньше, чем $h(n)$, вычисляющей некоторую функцию g_n, для которой выполняется

$$Pr_{x\in\{0,1\}^n}\{g_n(x) \neq f_n(x)\} \le \varepsilon_n. \quad (2)$$

Возьмем в качестве подмножества C_n^* само множество C_n (согласно выше приведенному определению комбинаторного свойства).

Теперь необходимо доказать, что это свойство *естественно*. То есть надо показать, что C_n удовлетворяет двум необходимым условиям: *Конструктивность* и *Объемность*.

Что касается первого условия — оно выполняется в силу предположения нашей теоремы (задача ε-**MCSP** принадлежит $P/poly$).

Покажем, что также выполняется требование *Объемности*, то есть

$$|C_n| \ge 2^{-cn} \cdot 2^{2^n}, \quad (3)$$

где c — некоторая положительная константа.

Рассмотрим множество всех «плохих» (не удовлетворяющих свойству C_n) функций S, то есть функций, для которых в их ε-окрестности есть хотя бы одна функция, реализуемая схемой, размер которой меньше, чем $h(n)$.

Пусть M_t — это число схем размера t в базисе $\{\neg, \vee, \&\}$ и пусть $F_{\varepsilon N}$ — это число различных функций в шаре радиуса $r = \varepsilon \cdot N$.

Очевидно, что для мощности этого множества S выполняется следующее неравенство:

$|S| \le M_{h(n)} \cdot F_{\varepsilon N}$, где $N = 2^n$.

Остается оценить сверху $M_{h(n)}$ и $F_{\varepsilon N}$.

Лемма 1. Выполняется следующая оценка

$$M_t \le t^{4t}. \quad (4)$$

Доказательство. Для доказательства можно например воспользоваться оценками из [4]. Дадим здесь простое доказательство оценки (4). M_t можно оценить сверху как число ориентированных графов с t вершинами со следующим свойством — в каждую вершину входит не более, чем два ребра. Пронумеровав все вершины графа от 1 до t, такой граф можно задать например матрицей $A = \{a_{ij}\}$, где $a_{ij} = 1$, если $i \neq j$ и из вершины j исходит ребро в вершину i, и $a_{ij} = 0$ в противном случае. В силу выше определенного свойства графа в каждой строчке матрицы может быть не более двух единиц. Число различных таких матриц не превосходит

$$(\binom{t}{2} + \binom{t}{1} + \binom{t}{0})^t.$$

При этом каждой вершине может быть сопоставлена одна из трех базисных функций: $\{\&, \vee, \neg\}$.

Следовательно, для любого $t \geq 2$ значение M_t можно оценить сверху, как

$$M_t \leq 3^t \cdot (\binom{t}{2} + \binom{t}{1} + \binom{t}{0})^t \leq 3^t \cdot (t^2/2 + t + 1)^t \leq (\frac{3t^2}{2} + 3t + 3)^t \leq t^{4t}.$$

Доказательство леммы закончено.

Для $t = h(n)$ получаем

$$M_{h(n)} \leq h(n)^{4h(n)} \leq 2^{4h(n)\log h(n)}. \quad (5)$$

Нам понадобится следующая лемма (см. [6]).

Лемма 2. Пусть X — сумма N независимых случайных величин, каждая из которых принимает значение 1 с вероятностью $1/2$ и 0 с вероятностью $1/2$. Тогда для любого $\delta > 0$

$$Pr\{|X - N/2| > \delta N/2\} \leq 2\ \exp\{-(\delta^2/3) \cdot N/2\}. \quad (6)$$

Лемма 3. Для числа $F_{\varepsilon N}$ различных булевых функций в шаре радиуса $r = \varepsilon \cdot N$ справедлива оценка

$$F_{\varepsilon N} \leq 2^{N+1} \cdot \exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\}. \quad (7)$$

Доказательство. Справедлива следующая оценка

$$F_{\varepsilon N} \leq \sum_{i=0}^{\varepsilon N} C_N^i \leq 2^N \cdot Pr\{|x_1 + \cdots + x_N - N/2| > (1/2-\varepsilon)N\}, \quad (8)$$

где $x_1 + \cdots + x_n$ — сумма независимых случайных величин, каждая из которых принимает значение 1 с вероятностью $1/2$ и значение 0 — также с вероятностью $1/2$.

Согласно *Лемме 2* из (9) получаем следующую оценку

$$F_{\varepsilon N} \leq 2^N \cdot Pr\{|x_1 + \cdots + x_N - N/2| > (1/2-\varepsilon)N\} \leq$$

$$2^N \cdot 2 \cdot \exp\{-1/6(1/2-\varepsilon)^2 \cdot N\},$$

и, наконец, искомое неравенство

$$F_{\varepsilon N} \leq 2^{N+1} \cdot \exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\}.$$

Лемма доказана.

Согласно Лемме 1 и Лемме 3 для мощности множества всех «плохих» (не удовлетворяющих свойству C_n) функций S справедлива следующая оценка

$$|S| \leq 2^{4h(n)\log h(n)} \cdot 2^{N+1} \cdot \exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\}.$$

Или

$$|S| \leq 2^{N+1} \cdot \exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\ +\ 4\ h(n)\log h(n)\}.$$

Для выполнения свойства **Объемности** нам достаточно, чтобы

$$2^N - |S| \geq 2^{-c\log N} \cdot 2^N,$$

то есть необходимо выполнение следующего условия

$$2^{N+1} \cdot \exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\ +\ 4\ h(n)\log h(n)\} \leq (1 - 2^{-c\log N}) \cdot 2^N.$$

Далее получаем

$$\exp\{\frac{-(1/2-\varepsilon)^2}{6} \cdot N\ +\ 4\ h(n)\log h(n)\} \leq 1/2 - 2^{-c\log N}.$$

Обозначив $w = 1/2 - \varepsilon$ и учитывая, что $N = 2^n$, получаем, что для выполнения этого неравенства достаточно выбрать $w(n)$ так, чтобы

$$\frac{w^2}{6} N > 4\ h(n)\log h(n) + 2,$$

а для этого, в свою очередь, достаточно выполнения

$$w \geq 5 \cdot \frac{\sqrt{h(n)\log h(n)}}{2^{\frac{n}{2}}}. \qquad (9)$$

Условие $h(n) = o(\frac{2^n}{n})$ гарантирует, что существует $0 < w < 1/2$, удовлетворяющее (9). Доказательство выполнения свойства *Объемности* закончено.

Выполнение последнего условия — *полезности против P/poly* — следует из суперполиномиальности функции $h(n)$ и определения комбинаторного свойства C_n. Доказательство теоремы закончено.

3.2. Оптимальные оценки аппроксимации.

Доказав **Теорему 1** мы получили следующий результат:
При $\varepsilon \leq 1/2 - w$,

$$w \geq 5 \cdot \frac{\sqrt{h(n)\log h(n)}}{2^{\frac{n}{2}}},$$

где $h(n)$ — суперполиномиальная функция, $0 < w < 1/2$, $h(n) = o(\frac{2^n}{n})$, задача ε-**MCSP** не имеет «эффективного» алгоритма решения (конечно же в предположении, что существует сильный псевдослучайный генератор).

Интересно исследовать, что происходит при больших значениях ε — то есть, когда значение ε стремится к $1/2$ «быстрее», чем (9).

В работе [7] показано, что для функции Шеннона $L(n, w)$, которая описывает зависимость между схемной сложностью функции и степенью аппроксимации w (напомним, что $w = 1/2 - \varepsilon$ в наших обозначениях) справедливо

$$L(n, w) = O\left(\frac{2^n w^2}{\log(2 + 2^n w^2)}\right) + O(n).$$

Как следствие, для степени аппроксимации, которая может быть достигнута схемой полиномиального размера для любой булевой функции справедливо

$$n^k = O\left(\frac{2^n w^2}{n}\right),$$

откуда вытекает, что

$$w = O\left(\frac{\sqrt{n^{k+1}}}{2^{\frac{n}{2}}}\right). \qquad (10)$$

Сравнив (10) и (9), можно заметить, что отличие заключается только в том, что если k стремится к $+\infty$ с ростом n, то мы получаем (9) и аппроксимация «трудна». Если $k = const$, то аппроксимация при условии (10) всегда возможна схемой полиномиального размера.

Литература

[1] Гэри М., Джонсон Д., Вычислительные машины и труднорешаемые задачи: Пер. с англ.- М.: Мир, 1982.

[2] Лупанов О.Б., Об одном подходе к синтезу управляющих систем — принципе локального кодирования, Проблемы кибернетики, вып. 14, М., Наука, 1965, С. 31-110.

[3] Сидельников В.М., Криптография и теория кодирования, Московский университет и развитие криптографии в России. Материалы конференции в МГУ 17-18 октября 2002 г. - М.: МЦНМО, 2003, С. 49–84.

[4] Яблонский С. В., Введение в дискретную математику, М.: Наука, 1979.

[5] Яблонский С. В., О невозможности элиминации перебора при решении некоторых задач теории схем, ДАН СССР, 1959, т. 124, N 1, С. 44-47.

[6] Alon N., Spencer J., The Probabilistic Method, Wiley, 1992.

[7] Andreev A., Clementi A., Rolim J., Optimal Bounds for the Approximation of Boolean Functions and Some Applications, ECCC, TR95-041, 1995.

[8] Cook S., The complexity of theorem proving procedures, Proc. Third Annual ACM Symp. on Theory of Computing, Association for Computing Machinery, New York, 1971, pp. 151-158.

[9] Goldreich O., Introduction to Complexity Theory, Lecture Notes for a Two-Semester course [1999], http://www.wisdom.weizmann.ac.il/mathusers/oded/cc99.html

[10] Kabanets V., Cai J., Circuit Minimization Problem, Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pages 73-79, 2000.

[11] Razborov A., Rudich S., Natural Proofs, Journal of Computer and System Sciences, 49:149-167, 1994.