Приближение булевых функций к классам Шефера

Е. А. ПОЦЕЛУЕВСКАЯ
Московский государственный университет им. М. В. Ломоносова
e-mail: potseluevskaya@gmail.com

УДК 519.712.2

Ключевые слова: алгоритм, булевы функции, класс Шефера, фиксация, сложность.

Аннотация

В настоящей работе приводится алгоритм перевода булевых функций в классы функций, для которых обобщённая задача выполнимости решается за полиномиальное время (классы Шефера). Для случая, когда исходная функция задана таблицей истинности, доказано, что сложность алгоритма составляет $l^2+l\log_2^2(l)$, где l — длина входа.

Abstract

E. A. Potseluevskaya, Approximation of Boolean functions to Schaefer's classes, Fundamentalnaya i prikladnaya matematika, vol. 16 (2010), no. 7, pp. 197—204.

We consider an algorithm for transferring Boolean functions to function classes for which the generalized satisfiability problem is solvable in polynomial time (Schaefer's classes). For the case where an initial function is represented as a truth-table, it is proved that the complexity of the algorithm is $l^2 + l\log_2^2(l)$, where l is the input length.

1. Введение

Задача выполнимости булевых формул известна математикам уже в течение многих лет, и на сегодняшний день поиск быстрых алгоритмов для решения этой NP-полной задачи имеет значительную практическую ценность. Для обобщённой проблемы выполнимости, называемой F-выполнимостью, Шефером были получены классы задач, решаемых за полиномиальное время. В данной статье описан алгоритм, позволяющий перевести произвольную булеву функцию, не лежащую в классе Шефера, в требуемый класс путём фиксации переменных и таким образом перейти от решения NP-полной проблемы F-выполнимости к решению полиномиальных подзадач для классов Шефера.

2. Основные понятия и утверждения

В работе [2] Шефер выделил следующие классы булевых функций:

- 0-выполнимые функции (обозначим их 0-ВЫП): все функции f, для которых верно $f(0,\ldots,0)=1$;

Фундаментальная и прикладная математика, 2010, том 16, № 7, с. 197—204.

- 1-выполнимые функции (обозначим их 1-ВЫП): все функции f, для которых верно $f(1,\dots,1)=1$;
- слабоотрицательные функции (СЛО): все функции f, для которых существует запись в конъюнктивной нормальной форме, в которой каждая скобка содержит только переменные с отрицаниями и, возможно, одну переменную без отрицания, т. е. формула вида

$$(x_{i_1}^{\alpha}\vee\bar{x}_{i_2}\vee\ldots\vee\bar{x}_{i_k})(x_{j_1}^{\beta}\vee\bar{x}_{j_2}\vee\ldots\vee\bar{x}_{j_l})\ldots(x_{t_1}^{\gamma}\vee\bar{x}_{t_2}\vee\ldots\vee\bar{x}_{t_k}),$$

  где $\alpha,\beta,\dots,\gamma$ — булевы константы;
- слабоположительные функции (СЛП): все функции f, для которых существует запись в конъюнктивной нормальной форме, в которой каждая скобка содержит только переменные без отрицаний и, возможно, одну переменную с отрицанием, т. е. формула вида

$$(x_{i_1}^{\alpha}\vee x_{i_2}\vee\ldots\vee x_{i_k})(x_{j_1}^{\beta}\vee x_{j_2}\vee\ldots\vee x_{j_l})\ldots(x_{t_1}^{\gamma}\vee x_{t_2}\vee\ldots\vee x_{t_k}),$$

  где $\alpha,\beta,\dots,\gamma$ — булевы константы;
- мультиаффинные функции (МАФ): все функции f, которым соответствует формула, представляющая собой конъюнкцию линейных форм, т. е. формула вида

$$(a_1x_1+\ldots+a_nx_n+a_0)(b_1x_1+\ldots+b_nx_n+b_0)\ldots(c_1x_1+\ldots+c_nx_n+c_0),$$

  где $a_i,b_i,\dots,c_i$ — булевы константы;
- биюнктивные функции (БИН): все функции f, для которых существует запись в конъюнктивной нормальной форме, где каждая скобка содержит ровно две переменные, т. е. формула вида

$$(x_{i_1}^{\alpha_1}\vee x_{i_2}^{\alpha_2})(x_{j_1}^{\beta_1}\vee x_{j_2}^{\beta_2})\ldots(x_{t_1}^{\gamma_1}\vee x_{t_2}^{\gamma_2}),$$

  где $\alpha_i,\beta_i,\dots,\gamma_i$ — булевы константы.

Сформулируем задачу об F-выполнимости. Пусть дано $F=\{F_1,\dots,F_m\}$ — любое конечное множество формул (функциональных символов). Определим F-формулу как конъюнкцию

$$F_{i_1}(\cdot)F_{i_2}(\cdot)\ldots F_{i_k}(\cdot)$$

с переменными $x_1,\dots,x_n$, расставленными некоторым образом. Существует ли набор значений переменных $x_1=\sigma_1,\dots,x_n=\sigma_n$, обращающий F-формулу в единицу?

Важный результат Шефера состоит в следующем.

Теорема 1. Проблема F-выполнимости полиномиально разрешима, если все функции F_i из множества F одновременно удовлетворяют по крайней мере одному из следующих условий:

- $F_i(0,\dots,0)=1$;
- $F_i(1,\dots,1)=1$;
- F_i мультиаффинна;

- F_i биюнктивна;
- F_i слабоположительна;
- F_i слабоотрицательна.

В противном случае проблема F-выполнимости является NP-полной.

Для классов Шефера СЛО, СЛП, МАФ и БИН С. А. Гизуновым и В. А. Носовым [1] были сформулированы следующие критерии распознавания.

1. $f \in$ СЛО тогда и только тогда, когда для любых $\alpha, \beta \in \{0,1\}^n$

$$\bar{f}(\alpha \wedge \beta) f(\alpha) f(\beta) = 0. \tag{1}$$

2. $f \in$ СЛП тогда и только тогда, когда для любых $\alpha, \beta \in \{0,1\}^n$

$$\bar{f}(\alpha \vee \beta) f(\alpha) f(\beta) = 0. \tag{2}$$

3. $f \in$ МАФ тогда и только тогда, когда для любых $\alpha, \beta, \gamma \in \{0,1\}^n$

$$\bar{f}(\alpha \oplus \beta \oplus \gamma) f(\alpha) f(\beta) f(\gamma) = 0. \tag{3}$$

4. $f \in$ БИН тогда и только тогда, когда для любых $\alpha, \beta, \gamma \in \{0,1\}^n$

$$\bar{f}(\alpha\beta \oplus \beta\gamma \oplus \alpha\gamma) f(\alpha) f(\beta) f(\gamma) = 0. \tag{4}$$

Для данных классов Шефера справедлива также следующая теорема.

Теорема 2. Пусть о функции f известно, что $f \notin M$, где M — это один из классов СЛО, СЛП, МАФ или БИН. Пусть g получена из f фиксацией переменных $(x_1, \ldots, x_k) = (\sigma_1, \ldots, \sigma_k)$. Тогда если среди всевозможных наборов α, β, γ, на которых нарушается условие принадлежности классу Шефера M (одно из условий (1)—(4)) для функции f, есть такие наборы α', β', γ', что

$$\begin{cases} \alpha'_1 = \beta'_1 = \gamma'_1 = \sigma_1, \\ \quad \ldots \\ \alpha'_k = \beta'_k = \gamma'_k = \sigma_k, \end{cases}$$

то $g \notin M$. В противном случае $g \in M$.

3. Алгоритм приближения функций к классам Шефера

Используя теорему 2, можно фиксацией переменных перевести функцию $f \notin M$ в класс Шефера M.

Определение. Будем говорить, что функция f находится *на расстоянии k от класса Шефера M*, если минимальное число переменных, которые нужно зафиксировать для f, чтобы полученная после фиксации функция g принадлежала M, равно k.

Приведём алгоритм, позволяющий найти переменные, которые необходимо зафиксировать, чтобы перевести функцию в класс Шефера, и фиксируемый набор.

Входные данные.

1. Функция $f(x_1, \ldots, x_n) \notin M$, где M — один из классов СЛО, СЛП, МАФ, БИН.
2. Все наборы $\alpha^1, \beta^1, (\gamma^1), \ldots, \alpha^m, \beta^m, (\gamma^m)$, где нарушается условие для соответствующего класса (одно из условий (1)—(4)).

Порядок действий.

1. Для всех наборов $\alpha^1, \beta^1, (\gamma^1), \ldots, \alpha^m, \beta^m, (\gamma^m)$, где нарушаются условия для класса Шефера, составляется матрица A размера $m \times n$, элементы которой принимают следующие значения:
   - $a_{i,j} = 0$, если $\alpha^i_j = \beta^i_j (= \gamma^i_j) = 0$,
   - $a_{i,j} = 1$, если $\alpha^i_j = \beta^i_j (= \gamma^i_j) = 1$,
   - $a_{i,j} = 2$ в противном случае, т. е. если соответствующие элементы пар (троек) наборов не совпадают.
2. Полагается $A^1 = A$.
3. Для всех столбцов a^1_j, $j \in \{1, \ldots, n\}$, матрицы A^1 вычисляются значения
$$N_d(a^1_j) = |\{a^1_{i,j},\ i = 1, \ldots, m \mid a^1_{i,j} = 2\}|,$$
$$N_0(a^1_j) = |\{a^1_{i,j},\ i = 1, \ldots, m \mid a^1_{i,j} = 0\}|,$$
$$N_1(a^1_j) = |\{a^1_{i,j},\ i = 1, \ldots, m \mid a^1_{i,j} = 1\}|.$$
4. Если есть столбец $a^1_{j_1}$, для которого $N_0(a^1_{j_1}) = 0$, то переменной x_{j_1} присваивается значение $x_{j_1} = 0$. Алгоритм заканчивает работу.
5. Если есть столбец $a^t_{j_1}$, для которого $N_1(a^1_{j_1}) = 0$, то переменной x_{j_1} присваивается значение $x_{j_1} = 1$. Алгоритм заканчивает работу.
6. Выбирается столбец матрицы A^1 с максимальным числом различных значений в парах (тройках) $N_d(a^1_{j_1}) = k \geqslant N_d(a^1_j)$, $j \neq j_1$.
7. Рассматривается подматрица
$$A^2 = \{a^2_{i,j} = a^1_{i,j} \mid i \neq i_l,\ \text{где } a^1_{i_l, j_1} = 2\},$$
т. е. матрица, состоящая из строк, для которых в столбце $a^1_{j_1}$ были совпадающие значения. На следующем шаге алгоритма считается, что $t = 2$.
8. Для всех столбцов a^t_j, $j \in \{1, \ldots, n\}$, матрицы A^t вычисляются значения
$$N_d(a^t_j) = |\{a^t_{i,j},\ i = 1, \ldots, m \mid a^t_{i,j} = 2\}|,$$
$$N_0(a^t_j) = |\{a^t_{i,j},\ i = 1, \ldots, m \mid a^t_{i,j} = 0\}|,$$
$$N_1(a^t_j) = |\{a^t_{i,j},\ i = 1, \ldots, m \mid a^t_{i,j} = 1\}|.$$
9. Если есть столбец $a^t_{j_t}$, для которого $N_0(a^t_{j_t}) = 0$, то переменным $x_{j_1}, \ldots, x_{j_{t-1}}$ присваиваются произвольные значения из $\{0, 1\}$, переменной x_{j_t} присваивается значение $x_{j_t} = 0$. Алгоритм заканчивает работу.

10. Если есть столбец $a^t_{j_t}$, для которого $N_1(a^t_{j_t}) = 0$, то переменным $x_{j_1}, \ldots, x_{j_{t-1}}$ присваиваются произвольные значения из $\{0,1\}$, переменной x_{j_t} присваивается значение $x_{j_t} = 1$. Алгоритм заканчивает работу.
11. Выбирается столбец матрицы A^t с максимальным числом различных значений в парах (тройках) $N_d(a^t_{j_t}) = k \geqslant N_d(a^t_j)$, $j \neq j_t$. При этом если столбцов, удовлетворяющих этому условию, несколько, выбирается тот, для которого число различных наборов
$$p = |S| = |\{(a^t_{i,j_1}, a^t_{i,j_2}, \ldots, a^t_{i,j_t}) \mid a^t_{i,j_l} \neq 2\}|$$
наименьшее. При этом $p \leqslant 2^t$.
12. Если $p < 2^t$, то выбирается любой такой набор σ, что $\sigma \notin S$, и переменным присваиваются соответствующие значения, чтобы получить функцию g:
$$x_{j_1} = \sigma_1, \ldots, \quad x_{j_t} = \sigma_t.$$
На этом шаге алгоритм заканчивает свою работу.
13. Если $p = 2^t$, то рассматривается подматрица
$$A^{t+1} = \{a^{t+1}_{i,j} = a^t_{i,j} \mid i \neq i_l, \text{ где } a^t_{i_l,j_t} = 2\},$$
т. е. матрица, состоящая из строк, для которых в столбце $a^t_{j_t}$ были совпадающие значения, и переходим к шагу 8 алгоритма.

Теорема 3. Алгоритм заканчивает работу за конечное число шагов.

Доказательство. Если бы алгоритм зацикливался, это означало бы, что для любого t на шаге 13 алгоритма мы имеем $p = 2^t$. Это должно быть верно и для $t = n$. Но это значит, что в матрице A задействованы все возможные наборы из 0 и 1 длины n и, в частности, в ней есть строки $(0, \ldots, 0)$ и $(1, \ldots, 1)$. Но элементы A равны 0 или 1, когда соответствующие элементы пар (троек) $\alpha, \beta, (\gamma)$ совпадают и равны 0 или 1 соответственно. Это значит, что условие для класса Шефера M нарушается для пары (тройки) наборов, которые полностью совпадают: $\alpha = \beta (= \gamma) = \sigma$. Но это невозможно, так как для СЛО
$$\bar{f}(\alpha \wedge \beta) f(\alpha) f(\beta) = \bar{f}(\sigma) f(\sigma) = 0,$$
для СЛП
$$\bar{f}(\alpha \vee \beta) f(\alpha) f(\beta) = \bar{f}(\sigma) f(\sigma) = 0,$$
для МАФ
$$\bar{f}(\alpha \oplus \beta \oplus \gamma) f(\alpha) f(\beta) f(\gamma) = \bar{f}(\sigma) f(\sigma) = 0,$$
для БИН
$$\bar{f}(\alpha\beta \oplus \beta\gamma \oplus \alpha\gamma) f(\alpha) f(\beta) f(\gamma) = \bar{f}(\sigma) f(\sigma) = 0.$$
Таким образом, таких наборов, а значит и строк в матрице, быть не может, и на каком-то шаге $t < n$ алгоритм остановится. □

Теорема 4. При фиксации переменных функции f, полученной в результате работы алгоритма, новая функция g принадлежит M.

Доказательство. Рассмотрим различные варианты остановки алгоритма.

Пусть алгоритм заканчивает работу на шаге 4 или 5. Тогда имеем $N_0(a^1_{j_1}) = 0$ или $N_1(a^1_{j_1}) = 0$. Но это значит, что не существует таких наборов $\alpha, \beta, (\gamma)$, на которых нарушается условие для M, что $\alpha_{j_1} = \beta_{j_1} (= \gamma_{j_1}) = 0$ (или $\alpha_{j_1} = \beta_{j_1} (= \gamma_{j_1}) = 1$ соответственно). Значит, зафиксировав соответствующее значение x_{j_1}, по теореме 2 получим, что $g \in M$.

Пусть алгоритм заканчивает работу на шаге 9 или 10 и зафиксировано значение $(x_{j_1}, \ldots, x_{j_{t-1}}, x_{j_t}) = (\sigma_1, \ldots, \sigma_{t-1}, \delta)$ (где $\delta = 0$, если алгоритм заканчивает работу на шаге 9, и $\delta = 1$ иначе). Тогда всем строкам матрицы A, для которых $a_{i,j_l} = 2$ для некоторого $l = 1, \ldots, t$, соответствуют пары (тройки) наборов, для которых не выполнено

$$\begin{cases} \alpha_{j_i} = \beta_{j_i} (= \gamma_{j_i}) = \sigma_i, \quad i = 0, \ldots, t-1, \\ \alpha_{j_t} = \beta_{j_t} (= \gamma_{j_t}) = \delta. \end{cases}$$

Для остальных строк матрицы нарушается равенство $\alpha_{j_1} = \beta_{j_1} (= \gamma_{j_1}) = \delta$. Таким образом, по теореме 2 имеем, что $g \in M$.

Пусть алгоритм заканчивает работу на шаге 12. Тогда зафиксирован некий набор $\sigma \notin S$. Всем строкам матрицы A, для которых $a_{i,j_l} = 2$ для некоторого $l = 1, \ldots, t$, соответствуют пары (тройки) наборов, для которых не выполнено

$$\alpha_{j_i} = \beta_{j_i} (= \gamma_{j_i}) = \sigma_i, \quad i = 0, \ldots, t-1.$$

Для остальных строк матрицы A значения переменных в парах (тройках) наборах также не совпадут с зафиксированным набором σ в силу выбора этого набора. Тогда по теореме 2 имеем, что $g \in M$. □

Теорема 5. Количество переменных, которые фиксируются для функции f в результате работы алгоритма, минимально.

Доказательство. Докажем теорему индукцией по минимальному числу фиксируемых переменных.

База индукции. Пусть минимальное количество переменных $k = 1$. Если матрица A такая, что есть столбец $a^1_{j_1}$, для которого $N_0(a^1_{j_1}) = 0$ или $N_0(a^1_{j_1}) = 1$, то на шаге 4 или 5 алгоритма будет зафиксирована одна переменная и алгоритм остановится. Это минимальное значение. Если же такого столбца в матрице A нет, то для любого столбца a_j имеем $N_0(a^1_j) > 0$ и $N_1(a^1_j) > 0$. Если зафиксировать только одну переменную $x_j = \delta$, для любого столбца найдётся строка с соответствующим значением переменной. Это значит, что найдётся пара (тройка) $\alpha, \beta, (\gamma)$, где $\alpha_j = \beta_j (= \gamma_j) = \delta$, и по теореме 2 получаем, что $g \notin M$. Значит, минимальное число переменных k, которые необходимо зафиксировать для функции f, не меньше двух.

Индуктивный переход. Пусть теорема доказана для $k \leqslant t-1$. Докажем её для $k = t$. Пусть для подматрицы A^t существует столбец $a^t_{j_t}$, для которого $N_0(a^t_{j_t}) = 0$ или $N_1(a^t_{j_t}) = 0$. Тогда в результате работы алгоритма будет зафиксировано t переменных, т. е. минимально возможное количество.

Если для матрицы A^t есть столбец a_{j_t}, для которого $p < 2^t$, то в результате работы алгоритма фиксируется набор из t переменных, что также соответствует минимальному количеству.

Если же для любого столбца a_j имеем $p = 2^t$, то после фиксации любого набора из t переменных $(x_{l_1}, \ldots, x_{l_t}) = (\delta_1, \ldots, \delta_t)$ получим, что найдётся пара (тройка) $\alpha, \beta, (\gamma)$, где

$$\begin{cases} \alpha_{l_1} = \beta_{l_1} \, (= \gamma_{l_1}) = \delta_1, \\ \quad \ldots \\ \alpha_{l_t} = \beta_{l_t} \, (= \gamma_{l_t}) = \delta_t, \end{cases}$$

и по теореме 2 получаем, что $g \notin M$. Значит, в этом случае фиксации t переменных недостаточно и $k \geqslant t + 1$. □

4. Сложность алгоритма

Теорема 6. Пусть функция f задана таблицей истинности, l — длина входа алгоритма. Тогда алгоритм заканчивает работу менее чем за $l^2 + l \log_2^2(l)$ шагов.

Доказательство. Длина входа алгоритма представляется в виде

$$l = 2^n + kmn,$$

где $n \geqslant 2$ — число переменных, $m \geqslant 1$ — число наборов, где нарушаются условия для класса Шефера, $k \in \{2, 3\}$ — число элементов в комбинации (пары или тройки в зависимости от рассматриваемого класса Шефера). Таким образом, $l \geqslant 8$.

На первом шаге работы алгоритма для составления матрицы требуется kmn шагов. На третьем шаге осуществляется перебор всех элементов матрицы, на что затрачивается mn операций. Для поиска максимального элемента на шаге 6 требуется не более n операций.

На этапе 8 при $t = 2$ осуществляется работа с матрицей, из которой вычеркнули как минимум $[m/n]$ строк. Действительно, каждая пара (тройка) элементов, где не выполнено условие для класса Шефера, содержит хотя бы один разряд, где наборы отличаются, так как в противном случае элементы пары (тройки) совпадали бы и было бы выполнено условие принадлежности к классу Шефера. Таким образом, в любой строке матрицы есть хотя бы один элемент, равный 2. Так как матрица имеет размер $m \times n$, то максимальное число элементов 2 в одном столбце не менее $[m/n] \geqslant 1$. Далее, для всех t из матрицы вычёркивается как минимум одна строка и для вычисления значений $N_d(a^t_{j_t})$, $N_0(a^t_{j_t})$, $N_1(a^t_{j_t})$ требуется максимум $(m - t + 1)n$ операций.

На шаге 11 на поиск максимального значения среди n столбцов затрачивается не более n операций, на поиск наименьшего числа наборов p — не более $n2^t$ операций.

Таким образом, имеем следующее ограничение на число шагов алгоритма:

$$kmn + mn + n + \sum_{t=2}^{n-1}\bigl((m-t+1)n + n + n2^t\bigr) =$$

$$= n\biggl(km + 1 + m(n-2) + 2(n-2) + \sum_{t=2}^{n-1}(2^t - t)\biggr) <$$

$$< (k+1)mn + 3m^2n^2 + n^2 2^n.$$

Так как $n < \log_2(l)$ и $l^2 = 2^{2n} + 2^{n+1}kmn + k^2m^2n^2$, то

$$(k+1)mn + 3m^2n^2 + n^2 2^n < l^2 + l\log_2^2(l). \qquad \square$$

5. Заключение

Из результатов, описанных в данной статье, следует, что любую ненулевую булеву функцию можно перевести в заданный класс Шефера фиксацией некоторых переменных за конечное число шагов. Таким образом, если на входе алгоритма решения задачи об F-выполнимости задан набор булевых функций, а также известны наборы, на которых нарушаются условия для классов Шефера, то в случае, если удастся перевести фиксацией переменных все функции в один класс Шефера, при каждом заданном наборе значений переменных задачу можно будет решить за полиномиальное время по теореме Шефера.

Автор работы выражает признательность В. А. Носову за научное руководство.

Литература

[1] Гизунов С. А., Носов В. А. Сложность распознавания классов Шефера // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 1996. — № 4. — С. 7—12.

[2] Schaefer T. J. The complexity of satisfiability problems // Proc. of the 10th Symp. on Theory of Computing (STOC'78), San Diego (California, USA), 1978. — New York: ACM Press, 1978. — P. 216—226.