Алгоритмы решения задачи об F-выполнимости приближением к классам Шефера

Е. А. Поцелуевская

В своей работе *The complexity of satisfiability problems* [1] Шефер выделил 6 классов булевых функций, для которых обобщенная проблема выполнимости (так называемая F-выполнимость) решается за полиномиальное время. Нахождение других классов функций, для которых задача также решалась бы быстро, имеет значительную практическую ценность. В настоящей работе представлены два алгоритма решения задачи об F-выполнимости, которые основаны на приближении булевых функций к классам Шефера, и при определенных ограничениях на исходные функции, имеют полиномиальную сложность.

Ключевые слова: алгоритм, F-выполнимость, классы Шефера, сложность.

1. Основные понятия и утверждения

Шефером были выделены следующие классы булевых функций:

- 0-выполнимые функции: все функции f, для которых верно $f(0,\dots,0)=1$;
- 1-выполнимые функции: 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 (КНФ), в которой каждая скобка содержит только переменные

с отрицаниями кроме, быть может, одной, то есть формула вида: $(x^{\alpha}_{i_1} \vee \bar{x_{i_2}} \vee \cdots \vee \bar{x_{i_k}})(x^{\beta}_{j_1} \vee \bar{x_{j_2}} \vee \cdots \vee \bar{x_{j_l}}) \ldots (x^{\gamma}_{t_1} \vee \bar{x_{t_2}} \vee \cdots \vee \bar{x_{t_k}})$, где $(\alpha, \beta, \ldots, \gamma$ — булевы константы).

- слабоположительные функции (СЛП): все функции f, для которых существует запись в КНФ, в которой каждая скобка содержит только переменные без отрицаний, кроме, быть может, одной, то есть формула вида: $(x^{\alpha}_{i_1} \vee x_{i_2} \vee \cdots \vee x_{i_k})(x^{\beta}_{j_1} \vee x_{j_2} \vee \cdots \vee x_{j_l}) \ldots (x^{\gamma}_{t_1} \vee x_{t_2} \vee \cdots \vee x_{t_k})$, где $(\alpha, \beta, \ldots, \gamma$ — булевы константы).
- мультиаффинные функции (МАФ): все функции f, которым соответствует формула, представляющая собой конъюнкцию линейных форм, то есть 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 $(a_i, b_i, \ldots, c_i$ — булевы константы).
- биюнктивные функции (БИН): все функции f, для которых существует запись в КНФ, где каждая скобка содержит ровно две переменные, то есть формула вида $(x^{\alpha_1}_{i_1} \vee x^{\alpha_2}_{i_2})(x^{\beta_1}_{j_1} \vee x^{\beta_2}_{j_2}) \ldots (x^{\gamma_1}_{t_1} \vee x^{\gamma_2}_{t_2})$, где $(\alpha_i, \beta_i, \ldots, \gamma_i$ — булевы константы).

Сформулируем задачу об F-выполнимости. Пусть дано $F = F_1, \ldots, F_m$ — 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 $x_1, ,x_n$, расставленными некоторым образом. Существует ли набор значений переменных $x_1 = \sigma_1, \ldots, x_n = \sigma_n$, 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 условий:*

- $F_i(0, \ldots, 0) = 1$;
- $F_i(1, \ldots, 1) = 1$;
- F_i — *мультиаффинна;*
- F_i — *биюнктивна;*
- F_i — *слабоположительна;*
- F_i — *слабоотрицательна.*

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

2. Алгоритм решения задачи об F-выполнимости приближением к классам СЛО и СЛП

Пусть в задаче об F-выполнимости все формулы $F_i(\cdot)$ $(i = 1, \ldots, s)$ заданы КНФ. Ниже приведен алгоритм решения задачи об F-выполнимости, основанный на приближении булевых функции к классам СЛО и СЛП. Пусть $X = \{x_1, \ldots, x_n\}$ — множество переменных.

Обозначим

$$D = \{(x_{i_1}^{\alpha_1} \vee x_{i_2}^{\alpha_2} \vee \cdots \vee x_{i_k}^{\alpha_k}) | x_{i_j} \in X, \alpha_j \in \{0,1\}, \\ (x_{i_1}^{\alpha_1} \vee x_{i_2}^{\alpha_2} \vee \cdots \vee x_{i_k}^{\alpha_k}) \& F = F\}$$

— множество дизъюнктов, входящих в запись F-формулы в КНФ. То есть F можно представить в виде $F = \mathop{\&}\limits_{i=1}^{|D|} d_i$, где $d_i \in D$.

Для переменной $x \in X$ будем обозначать $x \in d$, если x входит в соответствующую дизъюнкцию. Кроме того, для литерала x^α будем также обозначать $x^\alpha \in d$, если литерал x^α входит в дизъюнкт d.

Каждому элементу множества D сопоставим следующие числа:

- $N_1(d) = |\{x_{i_j} | x_{i_j} \in d, \alpha_j = 1\}|$ — число переменных, входящих в дизъюнкт без отрицания.
- $N_0(d) = |\{x_{i_j} | x_{i_j} \in d, \alpha_j = 0\}|$ — число переменных, входящих в дизъюнкт с отрицанием.

Рассмотрим также следующие обозначения множеств:

$$D_\alpha = \{d \in D | N_\alpha(d) > 1\}, \text{ где } \alpha \in \{0,1\}.$$

Для переменной x и $\alpha \in \{0,1\}$:

$$D_\alpha(x) = \{d \in D_\alpha | \quad x^\alpha \in d, N_\alpha(d) \leqslant 2\}.$$

Для множества M переменных из X обозначим:

$$D_\alpha(M) = \{d \in D_\alpha | \quad \exists x \in M \quad x^\alpha \in d, \quad |\{x \in M | x^\alpha \in d\}| - N_\alpha(d) \leqslant 1\}.$$

Определение 1. Будем говорить, что множество переменных M *переводит множество дизъюнктов* $D \in D_0$ *в класс СЛП*, если $D \backslash D_0(M) = \oslash$. Множество M *переводит множество дизъюнктов* $D \in D_1$ *в класс СЛО*, если $D \backslash D_1(M) = \oslash$.

Определение 2. Будем говорить, что множество переменных M *α-покрывает* множество переменных $D \in D_\alpha$, если для любого дизъюнкта $d \in D$ существует переменная $x \in M$, такая что $x^\alpha \in d$.

Для множества D_α определим S^α как минимальное по мощности множество переменных, которое переводит D_α в класс СЛП для $\alpha = 0$ или СЛО для $\alpha = 1$: $S = \min\limits_{|M|}\{M\}$, где M — такое, что $D_\alpha \backslash D_\alpha(M) = \oslash$.

Пусть $S = \bigcup S_i$, $S_i \bigcap S_j = \oslash$, $i \neq j$ — разбиение множества S на непересекающиеся подмножества.

Для подмножества $S_i \in S$ и дизъюнкта $d \in D$ будем обозначать $d \in S_i$, если в d входит хотя бы одна переменная из S_i.

Пусть S_i — непересекающиеся по дизъюнкциям подмножества S, то есть в каждое из множеств S_i входят только те переменные S, для которых все переменные, входящие в дизъюнкции с элементами из S_i, не встречаются больше нигде в D. То есть $\forall d \in S_i \quad \forall j \neq i \quad d \notin S_j$.

Алгоритм решения задачи об F-выполнимости путем приближения функций к классам СЛО и СЛП приведен ниже.

Входные данные:

1) Количество функций в F-формуле t.
2) КНФ функций $F_{i_1}(\cdot), F_{i_2}(\cdot), \ldots F_{i_t}(\cdot)$.

Порядок действий:

1) Удаление единичных дизъюнктов и чистых литералов. Если в формуле содержится литерал x_i^α, такой, что его отрицание не входит в формулу, то присваиваем $x_i = \alpha$. Если F содержит дизъюнкт, состоящий из единственного литерала x_i^α, то $x_i = \alpha$. Данный шаг повторяется до тех пор, пока не будет выполнено одно из условий:

- После фиксации переменных был получен 0. Тогда исходная формула невыполнима и алгоритм заканчивает работу.
- После фиксации переменных была получена формула, не содержащая единичных дизъюнктов и чистых литералов. Тогда осуществляется переход к следующему шагу.

2) По КНФ функции F', полученной в результате упрощения $F = F_{i_1}(\cdot), F_{i_2}(\cdot), \dots F_{i_t}(\cdot)$ на предыдущем шаге, строится множество D.
3) Для каждого элемента d множества D вычисляется значение $N_1(d)$ и $N_0(d)$.
4) Если для всех d имеем $N_1(d) \leqslant 1$, то функция слабоотрицательна. Положим в этом случае $\beta = 1$. Если для всех d выполнено $N_0(d) \leqslant 1$, то $\beta = 0$. Далее задача решается для СЛО или СЛП соответственно, как описано на шаге 11 алгоритма.
5) Для всех $d_i \in D$, для которых $N_0(d) > 1$, вычисляется

$$N_0 = \sum_{i=1}^{|D|}(N_0(d_i) - 1).$$

Для всех $d_i \in D$, для которых $N_1(d) > 1$, считаем:

$$N_1 = \sum_{i=1}^{|D|}(N_1(d_i) - 1).$$

6) Вводится вспомогательное множество T следующим образом:
   - Если $N_0 < N_1$, то $T = \{0\}$;
   - Если $N_0 > N_1$, то $T = \{1\}$;
   - Если $N_0 = N_1$, то $T = \{0, 1\}$.
7) Определяются множества M^α переменных, покрывающих дизъюнкты, которые не соответствуют требованиям класса Шефера, следующим образом:
   - Обозначим $D_\alpha = \{d \in D | N_\alpha(d) > 1\}$, где $\alpha \in T$. Для каждого дизъюнкта $d \in D_\alpha$ рассматриваются множества переменных $E^\alpha(d) = \{x \in d | \quad x^\alpha \in d\}$, то есть множество переменных входящих в дизъюнкт с отрицанием (при $T = \{0\}$),

без отрицания (при $T = \{1\}$), либо оба этих множества (при $T = \{0, 1\}$). Обозначим также $E^\alpha = \bigcup\limits_{d \in D_\alpha} E^\alpha(d)$.

- Для каждой переменной $x \in E^\alpha$ считается суммарное количество вхождений литерала x^α ($\alpha \in T$) в дизъюнкты:

$$k^\alpha(x) = |\{d \in D_\alpha | x^\alpha \in d\}|.$$

- Переменные из E^α упорядочиваются по убыванию функции $k^\alpha(x)$. Без ограничения общности переименуем эти переменные в соответствии с данным порядком: $x_1, x_2, \ldots, x_k$,

$$k^\alpha(x_1) \geqslant k^\alpha(x_2) \geqslant \cdots \geqslant k^\alpha(x_k);$$

- $M^\alpha = \{x_1\}$;
- Пусть $D_\alpha(x_1)$ — множество дизъюнкций D_α, в которые входит литерал x_1^α, при этом $N_\alpha(d) \leqslant 2$. Тогда если $D_\alpha \backslash D_\alpha(x_1) \neq \varnothing$, то для каждой переменной x_j, задействованной в составе литерала x^α в $D_\alpha \backslash D_\alpha(x_1)$ вычисляем величину $k_M^\alpha(x_j) = |\{d \in D_\alpha \backslash D_\alpha(x_1) | x^\alpha \in d\}|$ и добавляем к M^α переменную x_j, для которой k_M^α достигает максимального значения ($k_M^\alpha(x_j) > k_M^\alpha(x_p), p \neq j$). Если максимальных значений несколько ($k_M^\alpha(x_j) \geqslant k_M^\alpha(x_p), p \neq j$), то выбираем среди них такое, для которого $k^\alpha(x_j) > k^\alpha(x_p), p \neq j$. Если и здесь значения совпадают, то в M^α добавляется элемент, имеющий максимальное число вхождений в D_α. Если есть элементы, у которых совпадают и максимальны все три величины, то в M^α добавляется любой из них. Переходим к следующему шагу;
- Рассматриваем множество $D_\alpha(M^\alpha)$. Если $D_\alpha \backslash D_\alpha(M^\alpha) \neq \varnothing$, то рассмотрим переменные из $D_\alpha \backslash D_\alpha(M^\alpha)$. Для них считаем $k_M^\alpha(x_j) = |\{d \in D_\alpha \backslash D_\alpha(M^\alpha) | x_j \in d\}|$ и выбираем x_j для добавления в M^α аналогично предыдущему шагу;
- этот процесс продолжается до тех пор, пока не будет исчерпано множество D_α. Из способа построения M^α видно, что так как D_α конечно, то этот процесс рано или поздно завершится.

8) Множество M^α, фиксация переменных из которого позволяет перевести D_α в класс СЛО или СЛП, не обязательно является наименьшим по мощности. По этому множеству строится множество S следующим образом:
   - $S = \oslash$;
   - для всех элементов D_α вычисляется их «вес» относительно множества M^α: $w_\alpha(d) = |\{x \in M^\alpha | x^\alpha \in d\}|$, то есть, количество элементов из M^α, входящих в данный дизъюнкт в составе литерала x^α;
   - для всех $d \in D_\alpha$, таких что $N_\alpha(d) - w_\alpha(d) = 1$, соответствующие переменные $x \in M^\alpha$, такие что $x\alpha \in d$, добавляется в множество S^α;
   - (*) рассмотрим множество $D_\alpha(S^\alpha)$, тогда если $D_\alpha \backslash D_\alpha(S^\alpha) \neq \oslash$ (то есть множество S^α переводит D_α в СЛО или СЛП), то переходим к следующему шагу;
   - добавляем в S^α переменную из $M^\alpha \backslash S^\alpha$, которая встречается в составе литерала x^α наибольшее количество раз в $D_\alpha \backslash D_\alpha(S^\alpha)$, и переходим к (*);
   - этот процесс продолжается до тех пор, пока не будет исчерпано множество D_α.
   - $S = S^\beta$, где $\beta \in \{0, 1\}$ — такое, что $S^\beta = \min\limits_{|S^\alpha|}\{S^\alpha\}$. Таким образом, после фиксации переменных из множества S полученная формула будет относиться к классу СЛО (при $\beta = 0$) или СЛП (при $\beta = 1$).

9) S разбивается на непересекающиеся по дизъюнкциям подмножества S_i следующим образом:
   - на шаге i: $S_i = \oslash$;
   - выбирается первый элемент из S, не входящий в предыдущие S_j $(j < i)$, (на первом шаге выбирается любой элемент множества S) и добавляется в S_i;
   - для элемента $s_{i_1} \in S_i$ определяется множество
   $$D^i = D(s_{i_1}) = \{d \in D | s_{i_1} \in d\};$$
   - (*) для каждого элемента множества D^i осуществляется проверка, не входят ли туда другие элементы из S. Если

существует $s \in S$, $\forall s_{i_j} \in S_i\, s_{i_j} \neq s$, такое что для какого-то $d \in D^i$ $s \in d$, то в D^i добавляются элементы множества $D(s) = \{d \in D | s \in d\}$, а элемент s добавляется к множеству S_i;

- процесс повторяется до тех пор, пока для всех дизъюнкций $d \in D^i$ не будет выполнено условие $\forall\, x \in d$, таких что $x \in S$, $x \in S_i$ (то есть все элементы S, входящие в D^i, уже учтены в S_i);
- осуществляется проверка, входят ли другие переменные множества D^i в $D \backslash D^i$. Если $\exists d \in D^i, \quad \exists x \in d, \quad x \notin S$, такое что $x \in D \backslash D^i$, то для всех таких x элементы множества $D(x) = \{d \in D_3 | x \in d\}$ добавляем к множеству D^i и переходим к шагу (*);
- если же $\forall d \in D^i, \quad \forall x \in d \quad \nexists d' \in D \backslash D^i$, такого что $x \in d'$, то переходим к шагу i+1;
- процесс формирования множеств S_i продолжается до тех пор, пока не будет исчерпано всё множество S. Так как S конечно, то построение разбиения на каком-то шаге обязательно закончится.

10) В соответствии с разбиением множества S на S_i множество дизъюнкций D оказывается разбито на D^i, такие что каждое D^i зависит от своего набора переменных, которые не встречаются в других множествах разбиения. Далее проверка выполнимости формулы осуществляется независимо для каждого такого подмножества дизъюнкций. Для каждого S_i осуществляется перебор значений переменных, входящих в S_i.

11) При фиксированных значениях переменных из S_i решается задача об F-выполнимости для функций из класса СЛО или СЛП (в зависимости от β) следующим образом. Если в формуле есть дизъюнкты, зависящие только от одной переменной $d \in D^i$, $d = x^\alpha$, для соответствующих переменных фиксируется значение $x = \alpha$. После фиксации переменных этот процесс повторяется до тех пор пока не будет выполнено одно из следующих условий:

- После фиксации переменных был получен 0. Значит формула $\underset{i=1}{\overset{|D^i|}{\&}} d$, где $d \in D^i$, невыполнима.
- После фиксации переменных на данном шаге свободных переменных не осталось, и было получено значение 1. Тогда формула $\underset{i=1}{\overset{|D^i|}{\&}} d$, где $d \in D^i$, выполнима, и зафиксированный набор переменных соответствует части выполняющего набора для всей формулы.
- После фиксации переменных получена формула, в которой каждой дизъюнкт зависит от 2 и более переменных. В этом случае присваиваем значение $\beta \oplus 1$ всем не зафиксированным ранее переменным.

12) Если для какого-то S_i была установлена невыполнимость, то искомая формула невыполнима. Если же для каждого S_i соответствующие формулы выполнимы, то искомая формула выполнима.

Теорема 2. *Для множества S^α, построенного на шаге 8 алгоритма, выполнено $S^\alpha = \min\limits_{|M|}\{M | D_\alpha \backslash D_\alpha(M^\alpha) = \oslash\}$.*

Доказательство. Допустим, что утверждение теоремы не верно и существует множество S', такое что $D_\alpha \backslash D(S') = \oslash$ и $|S'| < |S^\alpha|$. Для каждого из дизъюнктов $d \in D_\alpha$ в множество S^α или S' должно попасть как минимум $N_\alpha(d) - 1$ элементов, так как иначе функция не будет относиться к соответствующему классу Шефера. Введем обозначения для следующих множеств при фиксированном дизъюнкте $d \in D_\alpha$: $S^\alpha(d) = \{x \in S^\alpha | x^\alpha \in d\}$ и $S'(d) = \{x \in S' | x^\alpha \in d\}$ — это множества элементов из S^α (S'), фиксацией которых дизъюнкт переводится в класс СЛО (СЛП). Тогда эти множества имеют как минимум $N(d) - 2$ общих элементов и отличаются максимум одним элементом.

Из соображений размерности ясно, что существует подмножество $D' \subseteq D_\alpha$ и некоторый элемент $x_1 \in S'$, такие что $\forall d \in D' \quad x_1^\alpha \in d$, и D' α-покрыто как минимум двумя элементами S^α, (при этом в дизъ-

юнкты также могут входить другие элементы S^α и S'). Искомый элемент S' не может лежать одновременно и в S^α, так как иначе рассматриваемое множество можно было бы покрыть меньшим количеством элементов S^α, что противоречит предположению.

Введем обозначения для этих элементов: пусть $x_1 \in S'$, $x_2, x_3 \in S^\alpha$, $x_1 \neq x_2$, $x_1 \neq x_3$, $x_2 \neq x_3$.

Так как $x_1 \notin S^\alpha$, то для этой переменной возможны следующие варианты:

- x_1 на шаге 7 алгоритма не попала в исходное множество M^α;
- x_1 на шаге 8 алгоритма не попала в множество S^α.

1) Предположим, элемент $x_1 \in S'$ не попал в M^α. Это значит, что на каком-то шаге алгоритма оказалось, что для D_α литерал x_1^α встречается реже, чем x_2^α (x_3^α), или что x_1^α встречается столько же раз, сколько x_2^α (x_3^α), а элемент M^α был выбран случайным образом. В любом случае, так как в D' встречаются и x_2^α, и x_3^α, то существуют $d_2, d_3 \in D_\alpha \backslash D'$, такие что $x_2^\alpha \in d_2$, $x_3^\alpha \in d_3$.
Обозначим $H_\alpha(x) = \{d \in D_\alpha | \quad x^\alpha \in d\}$ — множество дизъюнктов, в которые входит литерал x^α. Тогда $D' = H_\alpha(x_1)$. Так как S' переводит D_α в СЛО (СЛП), то в дизъюнкты, где встречаются x_2^α и x_3^α (в том числе d_2, d_3), также должны входить элементы из S'. Возможны два случая:
   - для дизъюнктов из множества
   $$H = \Big((H_\alpha(x_2) \bigcup H_\alpha(x_3)\Big) \backslash H_\alpha(x_1)$$
   выполнено
   $$|\bigcup_{d \in H} (S'(d) \backslash S^\alpha(d))| > 1,$$
   то есть для перевода данного множества дизъюнктов в класс Шефера требуется как минимум два элемента из S', не вошедших в $S(d)$. Тогда для того, чтобы перевести одно и то же множество $H_\alpha(x_2) \bigcup H_\alpha(x_3)$ в класс СЛО (СЛП) необходимо зафиксировать общие элементы $S^\alpha \bigcap S'$, а также два элемента множества S^α либо как минимум три элемента множества S';

- для дизъюнктов из множества H выполнено

$$|\bigcup_{d\in H}(S'(d)\backslash S^{\alpha}(d))| = 1,$$

то есть данное множество дизъюнктов переводится в класс Шефера одним элементом S' (не считая общих элементов), обозначим этот элемент x_4. Если бы $x_4 \in M^{\alpha}$, то в $D_{\alpha}\backslash D(M^{\alpha})$ литерал x_1^{α} входил бы чаще, чем x_2 и x_3, тогда бы включили x_1 в M^{α}, а это не так по предположению. Значит, $x_4 \notin M^{\alpha}$, а следовательно $x_4 \notin S^{\alpha}$. Итак, x_2 и x_3 встречаются только вместе с x_1 или x_4, значит $|H_{\alpha}(x_1)\bigcup H_{\alpha}(x_4)| \geqslant |H_{\alpha}(x_2)\bigcup H_{\alpha}(x_3)|$. Если $|H_{\alpha}(x_1)\bigcup H_{\alpha}(x_4)| > |H_{\alpha}(x_2)\bigcup H_{\alpha}(x_3)|$, то должны были бы включить x_1 и x_4 в M^{α}, но $x_1, x_4 \notin M^{\alpha}$. Значит, $|H_{\alpha}(x_1)\bigcup H_{\alpha}(x_4)| = |H_{\alpha}(x_2)\bigcup H_{\alpha}(x_3)|$, но тогда одно и то же множество $H_{\alpha}(x_2)\bigcup H_{\alpha}(x_3)$ переводится в класс Шефера фиксацией общих элементов $S^{\alpha}\bigcap S'$, а также двумя элементами S' либо двумя элементами S^{α}.

Таким образом, приходим к противоречию с предположением, что $|S'| < |S^{\alpha}|$. Значит, $x_1 \in M^{\alpha}$.

2) Предположим, что элемент x_1 на шаге 8 алгоритма не включили в S^{α}. Следовательно, x_1 не может входить в дизъюнкции $d \in D_{\alpha}$ с $w_{\alpha}(d) = N_{\alpha}(d) - 1$ (иначе должны были бы включить в S^{α}). Таким образом, для всех $d \in H_{\alpha}(x_1) \quad w(d) = N_{\alpha}(d)$. Выходит, что x_1 могли не включить в S^{α} по следующим причинам:

- все элементы $H_{\alpha}(x_1)$ α-покрываются такими элементами из S^{α}, которые покрывают дизъюнкции с $w_{\alpha}(d) = N_{\alpha}(d) - 1$. То есть, в частности, $x_2^{\alpha}, x_3^{\alpha}$ входят в дизъюнкции с $w_{\alpha}(d) = N_{\alpha}(d) - 1$. Однако эти дизъюнкции должны одновременно покрываться какими-то элементами S', то есть для них должно быть выполнено $N_{\alpha}(d) - 1 \leqslant |\{x \in S' | \; x^{\alpha} \in d\}| \leqslant N_{\alpha}(d)$. Так как в таких дизъюнкциях с весом $N_{\alpha}(d) - 1$ уже есть $N_{\alpha}(d) - 1$ элементов из M^{α} (это элементы, входящие в S^{α}), то существуют элементы S', покрывающие то же множество дизъюнкций, которые не входят в множество M^{α}. Значит, количество элементов S^{α},

α-покрывающих дизъюнкции с весом $N_\alpha(d)-1$, не может превышать количество соответствующих элементов S' (это следует из пункта 1 настоящей теоремы). Таким образом, одно и то же множество $H_\alpha(x_2)\bigcup H_\alpha(x_3)$ переводится в класс Шефера общими элементами $S^\alpha\bigcap S'$, а также двумя элементами множества S^α либо как минимум тремя элементами множества S'.

- множество $H_\alpha(x_1)$ на каком-то шаге оказалось α-покрыто элементами M^α, которые встречаются чаще, чем x_1. После добавления элементов, α-покрывающих дизъюнкции с весом $N_\alpha(d)-1$, в S^α, хотя бы один из элементов x_2 или x_3 должен был остаться в $H_\alpha(x_1)$. Допустим, x_2 входит в $H_\alpha(x_1)$, и остальные элементы $H_\alpha(x_1)$ уже покрыты другими элементами S^α. Тогда либо литерал x_2^α встречается чаще, чем x_1^α, и тогда одно и то же множество $H_\alpha(x_2)$ переводится в класс Шефера множеством из элементов $S^\alpha\bigcap S'$, а также одним элементом S^α или как минимум двумя элементами S'. Либо x_2^α встречается столько же раз, сколько x_1^α, и тогда $H_\alpha(x_2)$ переводится в класс Шефера одинаковым количеством элементов S' и S^α.

Таким образом, пришли к противоречию с тем, что $|S'|<|S^\alpha|$ и $x_1\in S^\alpha$, что противоречит предположению.

Значит, действительно, множество S^α, построенное на шаге 8 алгоритма является наименьшим по мощности множеством, переводящим D_α в соответствующий класс Шефера. Теорема доказана.

Утверждение 1. *На шаге 11 алгоритм выдает выполняющий набор для* $\&\limits_{i=1}^{|D^i|} d$, *где* $d\in D^i$, *или ответ, что формула невыполнима.*

Доказательство. Для первых двух случаев утверждение очевидно. Проверим корректность поиска выполняющего набора алгоритмом в случае, когда выполнено третье условие.

Пусть $\beta=1$ и $\&\limits_{i=1}^{|D^i|} d\in$СЛО. Присваиваем всем незафиксированным переменным значение 0. Дизъюнкты, в которые входят толь-

ко переменные с отрицаниями, примут значение 1. Так как каждый дизъюнкт зависит не менее чем от двух переменных, а функция относится к классу СЛО, то в каждом из оставшихся дизъюнктов есть хотя бы одна переменная с отрицанием. А значит, остальные дизъюнкты также принимают значение 1, и формула выполнима. Для класса СЛП доказательство аналогично.

Утверждение 2. *Сложность алгоритма решения задачи об F-выполнимости булевых формул приближением к классам СЛО и СЛП составляет* $\left(1 + \sum\limits_{i=1}^{k} 2^{|S_i|}\right) poly(|x|)$, *где* $|x|$ *— длина входа.*

Доказательство. Если обозначить количество дизъюнктов в КНФ F-формулы за m, то длину входной информации алгоритма можно оценить как $|x| \leqslant Cm$, где $C = \text{const}$. Очевидно, что шаги 1–6 алгоритма выполняются за полиномиальное от m время. Количество переменных D, а значит и D_α, линейно зависит от m, поэтому 7 шаг алгоритма также выполняется за полиномиальное время. Количество элементов множеств M^α и S^α ограничивается общим количеством переменных в D_α, поэтому 8 и 9 шаги алгоритма выполняются за полиномиальное от m время. Перебор значений переменных из S_i занимает $2^{|S_i|}$ шагов, а решение соответствующей подзадачи о выполнимости формулы из СЛО (СЛП) полиномиально.

Следствие 1. *В случае если для всех* $i = 1, \ldots, k$ $|S_i| \leqslant \log_2(poly(m))$ *сложность алгоритма будет полиномиальной величиной.*

3. Алгоритм решения задачи об F-выполнимости приближением к классу МАФ

Пусть в задаче об F-выполнимости все формулы $F_i(\cdot)$ $(i = 1, \ldots, s)$ заданы полиномами Жегалкина. Ниже приведен алгоритм решения задачи об F-выполнимости, основанный на приближении булевых функции к классу МАФ. Пусть $X = \{x_1, \ldots, x_n\}$ — множество переменных.

Обозначим

$$P = \{p = (x_{i_1} \dots x_{i_r} \oplus \dots \oplus x_{j_1} \dots x_{j_t} \oplus x_{l_1} \oplus \dots \oplus x_{l_k} \oplus \sigma) | x_{i_j} \in X, \\ \sigma \in \{0,1\}, \quad p\&F = F\}$$

— множество полиномиальных сомножителей, входящих в запись F-формулы. То есть F можно представить в виде $F = \bigotimes_{i=1}^{|P|} p_i$, где $p_i \in P$.

Для переменной $x \in X$ будем обозначать $x \in p$, если x входит в соответствующий полином. Кроме того, будем обозначать $x \in l(p)$, если x входит в линейную часть полинома p, и $x \in p \oplus l(p)$, если x входит в нелинейную часть полинома p.

Будем обозначать для множества переменных $M = \{x_1, \dots, x_k\}$: $p[M] = p|_{x_1=1,\dots,x_k=1}$ — полином, полученный из p фиксацией всех переменных из M в единичных значениях.

Рассмотрим также следующее обозначение:

$$P' = \{p \in P | deg(p) > 1\}$$

Тогда

$$Q = \{(x_{i_1} \dots x_{i_k}, r) | \exists p \in P' x_{i_1} \dots x_{i_k} \text{ содержится в } p \oplus l(p), \\ r = |\{p \in P' | x_{i_1} \dots x_{i_k} \text{ содержится в } p \oplus l(p)\}|\}$$

— множество нелинейных членов полиномов из P', с учетом кратности. Обозначим также для множества переменных M:

$$Q(M) = \{(q, r) \in Q | \deg q[M] \leqslant 1\}, \\ H(M) = \{(q, r) \in Q | \exists x \in M x \in q\}.$$

Определение 3. Будем говорить, что множество M *покрывает* множество $Q' \in Q$, если $Q' \backslash Q(M) = \oslash$.

Для множества Q определим S как минимальное по мощности множество переменных, которое покрывает Q: $S = \min_{|M|}\{M\}$, где M — такое, что $Q \backslash Q(M) = \oslash$.

Очевидно, что фиксация переменных из множества M, для которого выполнено $Q \backslash Q(M) = \oslash$ обеспечивает приближение F-формулы, компоненты которой заданы полиномами Жегалкина, к классу МАФ.

Пусть $S = \bigcup S_i, S_i \bigcap S_j = \oslash, i \neq j$ — разбиение множества S на непересекающиеся подмножества.

Для подмножества $S_i \in S$ и полинома $p \in P$ будем обозначать $p \in S_i$, если в p входит хотя бы одна переменная из S_i.

Пусть S_i — непересекающиеся по полиномам P подмножества S, то есть в каждое из множеств S_i входят только те переменные S, для которых все переменные, входящие в полиномы с элементами из S_i, не встречаются больше нигде в P. То есть $\forall p \in S_i \quad \forall j \neq i \quad p \notin S_j$.

Описание алгоритма решения задачи о выполнимости в случае, когда функции заданы полиномами Жегалкина, приведено ниже.

Входные данные:

1) Количество функций в F-формуле t.
2) Полиномы Жегалкина функций $F_{i_1}(\cdot), F_{i_2}(\cdot), \ldots F_{i_t}(\cdot)$.

Порядок действий:

1) Удаление линейных сомножителей, зависящих от одной переменной. Если F содержит множитель вида $(x_i \oplus \alpha)$, где $\alpha \in \{0, 1\}$, то $x_i = \alpha \oplus 1$. Данный шаг повторяется до тех пор, пока не будет выполнено одно из условий:
   - После фиксации переменных был получен 0. Тогда исходная формула невыполнима и алгоритм заканчивает работу.
   - После фиксации переменных была получена формула, не множителей вида $(x_i \oplus \alpha)$. Тогда осуществляется переход к следующему шагу.
2) По формуле F', полученной в результате упрощения $F = F_{i_1}(\cdot), F_{i_2}(\cdot), \ldots F_{i_t}(\cdot)$ на предыдущем шаге, строятся множества P и Q.
3) Определяется множество M переменных, покрывающих нелинейные части полиномов, следующим образом:

- Обозначим $P' = \{p \in P | deg(p) > 1\}$. Для каждого полинома $p \in P'$ рассматривается множество переменных

$$E(p) = \{x \in p| \quad x \in p \oplus l(p)\},$$

то есть множество переменных входящих в нелинейную часть полинома. Обозначим также $E = \bigcup\limits_{p \in P'} E(p)$.

- Для каждой переменной $x \in E$ считается суммарное количество ее вхождений в нелинейные части полиномов:

$$k(x) = |\{p \in P' | x \in p \oplus l(p)\}|.$$

- Переменные из E упорядочиваются по убыванию функции $k(x)$. Без ограничения общности переименуем эти переменные в соответствии с данным порядком: $x_1, x_2, \ldots, x_k$,

$$k(x_1) \geqslant k(x_2) \geqslant \cdots \geqslant k(x_k);$$

- $M = \{x_1\}$;
- Пусть $Q(x_1)$ — множество нелинейных членов, которые покрываются переменной x_1. Тогда если $Q \backslash Q(x_1) \neq \oslash$, то для каждой переменной x_j, задействованной в $Q \backslash Q(x_1)$ рассматриваем множество вычисляем величину

$$k_M(x_j) = \sum_{(q,r) \in Q \backslash Q(x_1), x_j \in q[M]} r$$

и добавляем к M переменную x_j, для которой k_M достигает максимального значения ($k_M(x_j) > k_M(x_p)$, $p \neq j$). Если максимальных значений несколько ($k_M^{\alpha}(x_j) \geqslant k_M^{\alpha}(x_p)$, $p \neq j$), то выбираем среди них такое, для которого $k(x_j) > k(x_p), p \neq j$. Если и здесь значения совпадают, то в M добавляется элемент, имеющий максимальное число вхождений в P'. Если есть элементы, у которых совпадают и максимальны все три величины, то в M добавляется любой из них. Переходим к следующему шагу;

- Рассматриваем множество $Q(M)$. Если $Q \backslash Q(M) \neq \oslash$, то рассмотрим переменные из $Q \backslash Q(M)$. Для них считаем

$$k_M(x_j) = \sum_{(q,r) \in Q \backslash Q(M), x_j \in q[M]} r$$

  и выбираем x_j для добавления в M аналогично предыдущему шагу;
- этот процесс продолжается до тех пор, пока не будет исчерпано множество Q. Из способа построения M видно, что так как Q конечно, то этот процесс рано или поздно завершится.

4) Множество M, покрывающее нелинейные члены полиномов, не обязательно является наименьшим по мощности. По этому множеству строится множество S следующим образом:
   - $S = \oslash$;
   - для всех элементов $(q, r) \in Q$ вычисляется «вес» соответствующего монома относительно множества M: $w(q) = |\{x \in M | x \in q\}|$, то есть, количество элементов из M, входящих в данное слагаемое.
   - для всех $(q, r) \in Q$, таких что $w(q) = \deg(q) - 1$, соответствующие переменные $x \in M$, такие что $x \in q$, добавляются в множество S;
   - (*) рассмотрим множество $Q(S)$, тогда если $Q \backslash Q(S) \neq \oslash$ (то есть множество S покрывает множество Q), то переходим к следующему шагу;
   - добавляем в S переменную из $M \backslash S$, которая встречается наибольшее количество раз в $Q \backslash Q(S)$, и переходим к (*);
   - этот процесс продолжается до тех пор, пока не будет исчерпано множество Q.
5) S разбивается на непересекающиеся по полиномам подмножества S_i следующим образом:
   - на шаге i: $S_i = \oslash$;
   - выбирается первый элемент из S, не входящий в предыдущие S_j $(j < i)$, (на первом шаге выбирается любой элемент множества S) и добавляется в S_i;

- для элемента $s_{i_1} \in S_i$ определяется множество

$$P^i = P(s_{i_1}) = \{p \in P | s_{i_1} \in p\};$$

- (*) для каждого элемента множества P^i осуществляется проверка, не входят ли туда другие элементы из S. Если существует $s \in S$, $\forall s_{i_j} \in S_i\, s_{i_j} \neq s$, такое что для какого-то $p \in P^i$ $s \in d$, то в P^i добавляются элементы множества $P'(s) = \{p \in P | s \in p\}$, а элемент s добавляется к множеству S_i;
- процесс повторяется до тех пор, пока для всех полиномов $p \in P^i$ не будет выполнено условие $\forall\, x \in p$, таких что $x \in S$, $x \in S_i$ (то есть все элементы S, входящие в P^i, уже учтены в S_i);
- осуществляется проверка, входят ли другие переменные множества P^i в $P \backslash P^i$. Если $\exists p \in P^i \exists x \in p$, $x \notin S$, такое что $x \in P \backslash D^i$, то для всех таких x элементы множества $P'(x) = \{p \in P | x \in p\}$ добавляем к множеству P^i и переходим к шагу (*);
- если же $\forall p \in P^i\, \forall x \in p \quad \nexists p' \in P \backslash P^i$, такого что $x \in p'$, то переходим к шагу i+1;
- процесс формирования множеств S_i продолжается до тех пор, пока не будет исчерпано всё множество S. Так как S конечно, то построение разбиения на каком-то шаге обязательно закончится.

6) В соответствии с разбиением множества S на S_i множество полиномов P оказывается разбито на P^i, такие что каждое P^i зависит от своего набора переменных, которые не встречаются в других множествах разбиения. Далее проверка выполнимости формулы осуществляется независимо для каждого такого подмножества полиномов. Для каждого S_i осуществляется перебор значений переменных, входящих в S_i.

7) При фиксированных значениях переменных из S_i решается задача об F-выполнимости для функций из класса МАФ путем решения системы линейных уравнений.

8) Если для какого-то S_i была установлена невыполнимость, то искомая формула невыполнима. Если же для каждого S_i соответствующие формулы выполнимы, то искомая формула выполнима.

Теорема 3. *Для множества S, построенного на шаге 4 алгоритма, выполнено* $S = \min\limits_{|M|}\{M|Q\backslash Q(M) = \oslash\}$.

Доказательство аналогично теореме 2.

Утверждение 3. *Сложность алгоритма решения задачи об F-выполнимости булевых формул приближением к классу МАФ составляет* $\left(1 + \sum\limits_{i=1}^{k} 2^{|S_i|}\right) poly(|x|)$, *где $|x|$ — длина входа.*

Доказательство. Если обозначить количество полиномов в записи F-формулы за m, то длину входной информации алгоритма можно оценить как $|x| \leqslant Cm$, где $C = \text{const}$. Очевидно, что шаги 1 и 2 алгоритма выполняются за полиномиальное от m время. Количество переменных P, линейно зависит от m, поэтому шаг 3 алгоритма также выполняется за полиномиальное время. Количество элементов множеств M и S ограничивается общим количеством переменных в P, поэтому 4 и 5 шаги алгоритма выполняются за полиномиальное от m время. Перебор значений переменных из S_i занимает $2^{|S_i|}$ шагов, а решение соответствующей подзадачи о выполнимости формулы из МАФ полиномиально.

Следствие 2. *В случае если для всех $i = 1, \ldots, k$ $|S_i| \leqslant \log_2(poly(m))$ сложность алгоритма будет полиномиальной величиной.*

4. Заключение

В соответствии с разработанными алгоритмами были написаны программы на языке C, позволяющие по заданному множеству булевых функций определить, выполнима ли F-формула, являющаяся конъюнкцией от этих функций, и в случае выполнимости выдающая

выполняющий набор. С помощью данных программ были получены практические результаты, полностью отвечающие доказанным теоретическим оценкам.

В работе [2] приведен алгоритм решения задачи об F-выполнимости булевых функций от 3 переменных, который основан на приближении функций к классу БИН. Таким образом, в зависимости от исходного задания функций в задаче об F-выполнимости, можно решать задачу выполнимости путем приближения функций к одному из классов Шефера (БИН, СЛО, СЛП или МАФ). При этом в случае выполнения соответствующих условий для функций, задача решается за полиномиальное время, что подтверждается практическими результатами.

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

Список литературы

[1] Schaefer T. J. The complexity of satisfiability problems // Proceedings of the 10th ACM Symposium on Theory of Computing. 1978. P. 216–226.

[2] Поцелуевская Е. А. Полиномиальные случаи решения задачи об F-выполнимости булевых формул // Интеллектуальные системы. Т. 12, вып. 1–4. 2008. С. 351–362.