Алгоритм проверки минимальности веса биюнктивной функции, не имеющей аффинных имплицент

Ю. В. Таранников*, Н. М. Трубицин‡

В работе рассматривается задача проверки минимальности веса биюнктивной функции, существенно зависящей от всех своих переменных и не имеющей аффинных имплицент. Приведён алгоритм её решения для минимальной 2-КНФ за полиномиальное время.

Ключевые слова: биюнктивная функция, существенная переменная, аффинная имплицента, минимальная 2-КНФ.

1. Постановка задачи

В работе [1] для биюнктивной функции (т. е. представимой в виде 2-КНФ), существенно зависящей от всех своих переменных и не имеющей аффинных имплицент, определена глубина — характеристика, не зависящая от вида её 2-КНФ. В ней также приведены достижимые верхняя оценка веса произвольной биюнктивной функции и нижняя оценка веса одновременно слабо положительной и слабо отрицательной функции через их глубину.

Идеи статьи [1] получили развитие в работе [2]: в ней указаны все биюнктивные функции заданной глубины максимального веса, вычислен минимальный вес биюнктивной функции, не имеющей аффинных имплицент, и доказана его инвариантность относительно глубины.

Однако в статье [2] не описаны все биюнктивные функции, не имеющие аффинных имплицент и обладающие наименьшим весом. Поэтому на данный момент актуальна задача проверки минимальности веса биюнктивной функции, не имеющей аффинных имплицент, за полиномиальное время. Её решение и предложено в данной работе.

* *Таранников Юрий Валерьевич* — д.ф.-м.н., каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: yutarann@gmail.com.

Tarannikov Yuri Valeryevich — Doctor of Physical and Mathematical Sciences, Department of Discrete Mathematics, Faculty of Mechanics and Mathematics, Moscow State University.

‡ *Трубицин Никита Михайлович* — Московский центр фундаментальной и прикладной математики, e-mail: trubitsin.nik@mail.ru.

Trubitsin Nikita Mikhailovich — Moscow Center for Fundamental and Applied Mathematics.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

2. Используемые понятия и обозначения

Всюду далее в работе будем использовать систему понятий и обозначений, введённую в статье [2]. В частности, аффинными имплицентами биюнктивной функции $f(x_1, \ldots, x_n)$ будем называть имплиценты вида x_k, $\overline{x}_k$ и $x_i \oplus x_j \oplus a$, $a \in \{0, 1\}$, $k \in \overline{1, n}$, $1 \leqslant i < j \leqslant n$, а множество биюнктивных функций от n переменных, существенно зависящих от всех своих переменных и не имеющих аффинных имплицент, обозначим через Bi''_n.

Определение 1. Литералы x и $\overline{x}$ называются *комплементарными*. Множество литералов называется *противоречивым*, если в нём есть комплементарные литералы, и *непротиворечивым* — в противном случае.

Для произвольного литерала $x \in \{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$ и некоторой 2-КНФ F функции $f(x_1, \ldots, x_n) \in Bi''_n$ обозначим через $T(x)$ множество литералов, достижимых в ориентированном графе (графе импликаций) 2-КНФ F из литерала x. Тогда имеет место следующее определение.

Определение 2. *Полным распространением вынужденных литералов* для заданной 2-КНФ F и множества литералов s, считающихся истинными, называется множество $S = \bigcup\limits_{x \in s} T(x)$. Результатом полного распространения вынужденных литералов называется *редуцированная 2-КНФ* F', полученная из 2-КНФ F удалением элементарных дизъюнкций, содержащих литералы из множества S, и вычёркиванием литералов, комплементарных к литералам из множества S. Переменные, входящие в множество S, называются *зафиксированными*, а остальные переменные формулы F' называются *незафиксированными*. Незафиксированные переменные называются *активными*, если они входят в 2-КНФ F'.

Замечание 1. Полное распространение вынужденных литералов противоречиво тогда и только тогда, когда полученная редуцированная 2-КНФ невыполнима. Для класса Bi''_n такая ситуация невозможна.

Обозначим количество активных переменных через a. Если множество S непротиворечиво, то $0 \leqslant a \leqslant n - |S|$.

Замечание 2. Полное распространение вынужденных литералов является полиномиальной процедурой (лежит в основе алгоритма Крома проверки выполнимости 2-КНФ [3]) и гарантирует, что в редуцированной формуле нет литералов, значение которых однозначно определено текущим присваиванием.

Определение 3. КНФ называется *пустой*, если она не содержит ни одной элементарной дизъюнкции.

3. Основной результат

Поскольку ориентированный граф (граф импликаций) минимальной 2-КНФ биюнктивной функции, не имеющей аффинных имплицент, не содержит ориентированных циклов (см. [2]), в нём найдётся хотя бы одна начальная вершина (то есть вершина с нулевой полустепенью захода). Это значит, что в минимальной 2-КНФ рассматриваемой функции хотя бы одна переменная входит только в одной степени. В силу данного свойства корректна работа следующего алгоритма.

Алгоритм 1.

Вход: минимальная 2-КНФ F, задающая функцию $f \in Bi''_n$.

Выход: ответ «да», если вес функции f минимален среди функций из класса Bi''_n, и «нет» — в противном случае.

Этап 1. Полагаем $G := F$ и создаём счётчик a количества активных переменных формулы G. Инициализируем его значением $a := n$.

Этап 2. Пока формула G непуста, выполняем следующие действия:

1. Выбираем любую переменную, входящую в 2-КНФ G только в одной степени. Пусть, без ограничения общности, это переменная x, и она входит в 2-КНФ G только в отрицательной степени. В противном случае меняем ролями литералы x и $\overline{x}$.
2. Строим подформулы G_1 и G_0, полученные из 2-КНФ G в результате присваиваний $x = 1$ и $x = 0$ соответственно и последующих полных распространений вынужденных литералов.
3. Проверяем подформулу G_1: если она непуста или имеет незафиксированные переменные, алгоритм завершается с ответом «нет».
4. Анализируем подформулу G_0. Для этого обозначим через a_0 число переменных, не зафиксированных после её построения.
   - Если формула G_0 непуста, в неё входят все a_0 незафиксированных переменных и при этом $a_0 = a - 1$, полагаем $G := G_0$, $a := a_0$ и переходим к следующей итерации шага 1.
   - Если формула G_0 пуста и $a_0 = 1$, то она имеет в точности $2^{a_0} = 2$ решения, и в этом случае алгоритм завершается с ответом «да».
   - В остальных случаях алгоритм завершается с ответом «нет».

Некоторые характеристики алгоритма 1. Алгоритм 1 не нуждается в хранении очереди подзадач: на каждом шаге достаточно хранить единственную текущую 2-КНФ G и счётчик a количества её активных переменных. Требуемая память ограничена $O(n^2)$ бит, а общее время работы полиномиально зависит от n.

Список литературы

[1] Тарасов А. В., "Булевы биюнктивные функции, графы 2-КНФ и их порядковые функции. Оценки веса биюнктивной функции с заданным числом слоев", *Математические вопросы криптографии*, **12**:1 (2021), 83–95. DOI: 10.4213/mvk349.

[2] Трубицин Н. М., "Биюнктивные функции заданной глубины экстремального веса", *Дискретная математика*, **38**:2 (2026), 96–131. DOI: 10.4213/dm1854.

[3] Krom M. R., "The Decision Problem for a Class of First-Order Formulas in Which all Disjunctions are Binary", *Mathematical Logic Quarterly*, **13**:1–2 (1967), 15–20. DOI: 10.1002/malq.19670130104.

Статья поступила 27 сентября 2026 г.

An algorithm for checking the minimality of the weight of a bijunctive function that does not have affine implicits

Y. V. Tarannikov, N. M. Trubitsin

This paper addresses the problem of verifying the weight minimality of a bijunctive function that depends essentially on all its variables and has no affine implicits. A polynomial-time algorithm is presented for solving this problem in the case of a minimal 2-CNF.

Keywords: bijunctive function, essential variable, affine implicant, minimal 2-CNF.

References

[1] Tarasov A. V., "Bijunctive Boolean functions, 2-CNF graphs and their order functions. Weight estimates of a bijunctive function with a given number of layers", *Mathematical Issues of Cryptography*, **12**:1 (2021), 83–95.

[2] Trubitsin N. M., "Bijunctive functions of given depth of extreme weight", *Discrete Mathematics*, **38**:2 (2026), 96–131.

[3] Krom M. R., "The Decision Problem for a Class of First-Order Formulas in Which all Disjunctions are Binary", *Mathematical Logic Quarterly*, **13**:1–2 (1967), 15–20.

Received on September 27, 2026