Верхняя линейная оценка для мощности области определения универсальной функции для пар линейных

А. С. Седова*

Ранее были исследованы задачи существования и оценки мощности области определения универсальных функций для различных классов функций в булевой и k-значной логиках. Для универсальной функции для пар линейных функций было доказано существование начиная с семи переменных. В данной работе, применив обобщения градиентного метода, получена верхняя линейная оценка мощности области определения универсальной функции для пар линейных функций.

Ключевые слова: линейная функция, универсальная функция, градиентный алгоритм, покрытие матрицы.

1. Введение

Понятие универсальной функции было введено в работе [1]. Далее были исследованы задачи о существовании, мощности области определения и представления в простом виде универсальных функций для различных классов. Далее в работе [2] было введено понятие универсальной функции для пар линейных. С помощью вероятностного метода доказано существование таковых для линейных функций, зависящих не менее чем от семи аргументов. В настоящей работе продолжено исследование универсальных функций для пар, и получена оценка мощности области определения.

2. Постановка задачи

Далее, если особо не оговорено, будем считать функции булевыми, зависящими от переменных $x_1, \ldots, x_n$. Далее (см., например, [3]) линейной функцией будем называть такую функцию $f(x_1, \ldots, x_n)$, которая представима в виде

* *Седова Анна Сергеевна* — м.н.с. каф. информационной безопасности ф-та ВМК МГУ, e-mail: okuneva-anna@mail.ru, ORCID: 0009-0009-7424-0043.

Sedova Anna Sergeevna — Junior Researcher, Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, Chair of Information Security.

$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n$, где $a_i \in \{0, 1\}$. Ранее в работе [1] было введено понятие универсальной функции и поставлены основные задачи. Пусть задан некоторый класс функций K. Будем говорить, что функция f, зависящая от того же множества переменных, что и функции из класса K, порождает функцию g (при условии $g \in K$), если можно предъявить множество точек X, на котором $g(x)$ является единственной принадлежащей классу K функцией, такой, что для любого x из множества X выполняется соотношение $f(x) = g(x)$. Функция f называется универсальной для класса K, если она порождает любую функцию из данного класса. Основные задачи при исследовании универсальных функций для различных классов — это задачи существования и нахождения оценки мощности области определения и поиска представления в простой форме. В работе [1] была доказана нижняя оценка $2n + 2$ на мощность области определения универсальной функции для класса линейных функций от n переменных и верхняя, асимптотически равная $\frac{16}{5}n$. Впоследствии эти оценки были улучшены до $\frac{13}{6}n$ и $3n$ соответственно [4].

Для произвольной функции f будем обозначать функцию, принимающую противоположные значения во всех точках, через $\overline{f}$. Заметим, что если g_0 — произвольная булева функция, то для пары функций $(g_0, \overline{g_0})$ не существует точек, на которых они совпадают. Эту пару функций будем называть недопустимой. Остальные пары функций (g_0, g_1) такие, что $g_0 \in L \cap T_0$ и $g_1 \in L \cap \overline{T_0}$, будем называть допустимыми.

Функция $f(x_1, \ldots, x_n)$ порождает допустимую пару линейных функций $(g_0(x_1, \ldots, x_n), g_1(x_1, \ldots, x_n))$, если можно предъявить множество наборов $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$, такое, что (g_0, g_1) является единственной допустимой парой функций, для которой при любых $i \in \{1, \ldots, n\}$ выполнены соотношения $g_0(\mathbf{x}_i) = f(\mathbf{x}_i)$ и $g_1(\mathbf{x}_i) = f(\mathbf{x}_i)$.

Заметим, что если f не порождает пару (g_0, g_1), то для любого множества наборов $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$, на котором для любого $i \in \{1, \ldots, n\}$ выполнено $f(\mathbf{x_i}) = g_0(\mathbf{x_i}) = g_1(\mathbf{x_i})$, найдётся другая пара допустимых функций (g_0', g_1'), для которой при любых $i \in \{1, \ldots, n\}$ выполнено равенство $f(\mathbf{x_i}) = g_0'(\mathbf{x_i}) = g_1'(\mathbf{x_i})$.

Функция $f(x_1, \ldots, x_n)$ называется универсальной функцией для пар линейных функций, если она порождает любую пару допустимых линейных функций.

3. Основные результаты

Теорема 1. *При $n \geqslant 13$ существует универсальная функция для пар линейных, имеющая мощность области определения не более $64n + 1$.*

Доказательство. Будем использовать градиентный алгоритм для решения задачи покрытия матриц (см. напр. [5], с. 136–137).

Построим $(0,1)$-матрицу, содержащую $N = 2^{n+1} - 2$ строк, такую, что каждому набору $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, кроме нулевого, соответствуют две строки для $f(\alpha_1, \ldots, \alpha_n) = 0$ и $f(\alpha_1, \ldots, \alpha_n) = 1$. Строки, соответствующие нулевому набору, в матрице отсутствуют. Столбцы этой матрицы соответствуют упорядоченным парам различных допустимых пар функций $((g_0, g_1), (g_0', g_1'))$. Подмножество строк матрицы, соответствующих набору $P = \{(\tilde{\alpha}_1, f(\tilde{\alpha}_1)), \ldots, (\tilde{\alpha}_k, f(\tilde{\alpha}_k))\}$, является её допустимым покрытием, если в подматрице, образованной этими строками, нет нулевых столбцов и ни при каких $i \in \{1, \ldots, k\}$ пары $(\tilde{\alpha}_i, f(\tilde{\alpha}_i) = 0)$ и $(\tilde{\alpha}_i, f(\tilde{\alpha}_i) = 1)$ не содержатся одновременно в P. Число различных линейных функций с фиксированным значением в нуле равно 2^n, следовательно, число столбцов M не превосходит 2^{4n}. Наличие единицы в позиции на пересечении строки, соответствующей набору $f(\alpha_1, \ldots, \alpha_n) = \beta$, и столбца, соответствующего четвёрке функций $((g_0, g_1), (g_0', g_1'))$, говорит о выполнении условия

$$\left[\begin{array}{l} \begin{cases} g_0(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_0'(\alpha_1, \ldots, \alpha_n) = \overline{\beta} \end{cases} \\ \begin{cases} g_0(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1'(\alpha_1, \ldots, \alpha_n) = \overline{\beta}. \end{cases} \end{array}\right. \tag{1}$$

Таким образом, соответствующий элемент матрицы, равный единице, показывает возможность на наборе отличить пару функций (g_0, g_1) от пары (g_0', g_1'). При этом покрытие матрицы обеспечивает возможность порождения любой допустимой пары линейных функций. Оценим долю единиц в столбце исходной матрицы. Зафиксируем столбец и соответствующую ему пару допустимых пар функций $((g_0, g_1), (g_0', g_1'))$. Условие (1) на наличие единицы в позиции разобьём на две системы

$$\begin{cases} g_0(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_0'(\alpha_1, \ldots, \alpha_n) \oplus 1 = \beta. \end{cases} \tag{2}$$

и

$$\begin{cases} g_0(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1(\alpha_1, \ldots, \alpha_n) = \beta, \\ g_1'(\alpha_1, \ldots, \alpha_n) \oplus 1 = \beta. \end{cases} \tag{3}$$

Оценим снизу число решений $(\alpha_1, \ldots, \alpha_n, \beta)$ совокупности (1) через число решений систем (2) и (3). Заметим, что мощность множества решений системы (1) не менее, чем максимум из мощности множеств, задаваемых одной из систем (2) или (3). Из построения для пары допустимых пар функций должно быть верно хотя бы одно из условий $g_0 \neq g_0'$ и $g_1 \neq g_1'$. Будем считать, что выполнено условие $g_0 \neq g_0'$.

Запишем систему (2) линейных уравнений относительно $(\alpha_1, \ldots \alpha_n, \beta)$.

$$\begin{cases} c_{0,1}\alpha_1 \oplus c_{0,2}\alpha_2 \oplus \ldots \oplus c_{0,n}\alpha_n \oplus c_{0,0} = \beta, \\ c_{1,1}\alpha_1 \oplus c_{1,2}\alpha_2 \oplus \ldots \oplus c_{1,n}\alpha_n \oplus c_{1,0} = \beta, \\ c'_{0,1}\alpha_1 \oplus c'_{0,2}\alpha_2 \oplus \ldots \oplus c'_{0,n}\alpha_n \oplus c'_{0,0} \oplus 1 = \beta. \end{cases}$$

По построению, $c_{0,0} = 0, c'_{0,0} = 0, c_{1,0} = 1$.

$$\begin{cases} c_{0,1}\alpha_1 \oplus c_{0,2}\alpha_2 \oplus \ldots \oplus c_{0,n}\alpha_n = \beta, \\ c_{1,1}\alpha_1 \oplus c_{1,2}\alpha_2 \oplus \ldots \oplus c_{1,n}\alpha_n \oplus 1 = \beta, \\ c'_{0,1}\alpha_1 \oplus c'_{0,2}\alpha_2 \oplus \ldots \oplus c'_{0,n}\alpha_n \oplus 1 = \beta. \end{cases} \tag{4}$$

Получим систему с $n+1$ неизвестной и тремя линейно независимыми уравнениями. Следовательно, мощность множества решений системы (4) не менее, чем 2^{n-2}. Причём среди этих решений нет решения, соответствующего $(\alpha_1, \ldots, \alpha_n) = (0, \ldots, 0)$, так как подобная подстановка приводит к противоречию

$$\begin{cases} 0 = \beta, \\ 1 = \beta, \\ 0 = \beta. \end{cases}$$

Аналогичные рассуждения верны, если выполнено условие $g_1 \neq g_1'$. Так как число строк матрицы равно $2^{n+1} - 2$, то доля единиц в столбце не менее чем $\frac{1}{8}$.

Задача построения универсальной функции при этом сводится к задаче о покрытии матрицы с дополнительным ограничением: нельзя взять и строку, соответствующую $f(\alpha_1, \ldots, \alpha_n) = 0$, и строку, соответствующую $f(\alpha_1, \ldots, \alpha_n) = 1$.

Пусть в каждом столбце на каждом шаге доля единиц не меньше, чем γ' . Тогда в матрице не менее $\gamma' \cdot M_t \cdot N_t$ единиц, где N_t, M_t — число строк и столбцов на шаге t соответственно. Существует строка с не менее чем $\gamma' \cdot M_t$ единиц. Поэтому на каждом шаге число столбцов уменьшается, по крайней мере, с мультипликативной константой $(1 - \gamma')$.

При этом за t шагов при

$$(1 - \gamma')^t \leqslant \frac{1}{M} \tag{5}$$

градиентный алгоритм строит покрытие матрицы не более чем за $(t + 1)$ шагов.

Пусть сделано t шагов, тогда число единиц в столбце не менее чем $\frac{N}{8} - t$, так как на каждом шаге из непокрытых столбцов может быть удалено не более одной единицы, после удаления строки, соответствующей значению функции $f(\alpha_1, \ldots, \alpha_n)$, противоположному взятому. При этом число строк после t шагов равно $N - 2t$, а значит, доля единиц в столбцах не менее $\frac{\frac{N}{8} - t}{N - 2t}$. Потребуем дополнительное ограничение на долю единиц в столбце после t шагов, положив $\gamma' = 1 - 2^{-\frac{1}{16}}$. Величину $(1 - \gamma')$ удобно логарифмировать. Получим неравенство

$$\frac{\frac{N}{8} - t}{N - 2t} \geqslant 1 - 2^{-\frac{1}{16}}. \tag{6}$$

С учётом ограничения на число столбцов из неравенства (5) получим систему

$$\begin{cases} \frac{\frac{N}{8} - t}{N - 2t} \geqslant 1 - 2^{-\frac{1}{16}}, \\ (1 - \gamma')^t \leqslant \frac{1}{2^{4n}}. \end{cases}$$

Откуда

$$(2^{-\frac{1}{16}})^t \leqslant \frac{1}{2^{4n}},$$

следовательно,

$$2^{-\frac{t}{16}} \leqslant 2^{-4n}.$$

Логарифмируя последнее неравенство, получим

$$\frac{t}{16} \geqslant 4n.$$

Таким образом, градиентный алгоритм при

$$t \geqslant 64n$$

строит покрытие матрицы при выполнении условия (6).

Для доказательства выполнения неравенства (6) воспользуемся промежуточным соотношением $0,05 \geqslant 1 - 2^{-\frac{1}{16}}$. При $\frac{N}{t} \geqslant 12$ выполняется неравенство $\frac{\frac{N}{8}-t}{N-2t} \geqslant 0,05$, из которого вытекает неравенство (6).

Так как $N = 2^{n+1} - 2$, при $t \leqslant 64n + 1$ справедливо $\frac{N}{t} \geqslant \frac{2^{n+1}-2}{64n+1}$. При этом $\frac{2^{n+1}-2}{64n+1} \geqslant 12$ при $n \geqslant 13$.

Следовательно, при $n \geqslant 13$ функция f является универсальной для пар линейных функций.

□

Список литературы

[1] Вороненко А. А., "Об универсальных частичных функциях для класса линейных функций", *Дискретная математика*, **24**:3 (2012. DOI: 10.4213/dm1197), 62–65.

[2] Седова А.С., "Универсальные функции для пар линейных", Проблемы теоретической кибернетики (Москва, 05–08 декабря 2024 года), 2024, 120–121.

[3] Алексеев В.Б., *Дискретная математика*, М.: ИНФРА-М, 2021.

[4] Вороненко, А.А., Вялый М.Н., "Нижняя оценка мощности области определения универсальных функций для класса линейных булевых функций", *Дискретная математика*, **28**:4 (2016. DOI: 10.4213/dm1392), 50–57.

[5] *Дискретная математика и математические вопросы кибернетики*, М.: Наука, **1**, ред. С.В. Яблонский, О.Б. Лупанов., 1974.

Статья поступила 30 апреля 2026 г.

Upper Linear Bound for the Cardinality of the Domain of a Universal Function for Pairs of linear

A. S. Sedova

Previously, the problems of existence and cardinality estimation of the domain of universal functions for various classes of functions in Boolean and k-valued logics were investigated. For the universal

function for pairs of linear functions, existence was proven starting from seven variables. We obtained an upper linear bound on the cardinality of the domain of the universal function for pairs of linear functions by applying generalizations of the gradient method.

Keywords: linear function, universal function, gradient algorithm, matrix covering.

References

[1] Voronenko A.A., *Discrete Mathematics and Applications*, **22**:4 (2012. DOI: 10.1515/dma-2012-028), 421–425.

[2] Sedova A.S., "Universal functions for pairs of linear functions", Problems of Theoretical Cybernetics (Moscow, 05–08 December), 2024, 120–121 (In Russian).

[3] Alekseev V.B., *Discrete mathematics*, M.: INFRA-M, 2021 (In Russian).

[4] Voronenko A. A., Vyalyi M. N., "Lower estimate for the cardinality of the domain of universal functions for the class of linear Boolean functions", *Discrete Mathematics and Applications*, **27**:5 (2017. DOI: 10.1515/dma-2017-0033), 319–324.

[5] *Discrete Mathematics and Mathematical Issues of Cybernetics*, M.: Nauka, **1**, eds. S.V. Yablonsky, O.B. Lupanov., 1974 (In Russian).

Received on April 30, 2026