А. А. Вороненко[1]***, Н. К. Воронова***[2]***, В. П. Ильютко***[3]

О СУЩЕСТВОВАНИИ УНИВЕРСАЛЬНЫХ ФУНКЦИЙ ДЛЯ КЛАССА ЛИНЕЙНЫХ k-ЗНАЧНЫХ ФУНКЦИЙ ПРИ НЕБОЛЬШИХ k.[*]

Данная статья является продолжением цикла работ, посященных изучению вопроса существования и строения универсальных функций для класса линейных функций k значной логики. Первой работой в этом направлении была статья [1], посвященная изучению универсальных функций для класса линейных булевых функций. Приведем основные определения согласно работе [4]. Пусть K – произвольное множество функций, зависящих от одного множества переменных. Будем говорить, что функция f, зависящая от того же множества переменных, порождает функцию g (при условии $g \in K$), если можно предъявить множество точек X, такое, что $g(x)$ является единственной функцией из удовлетворяющих условию $g \in K$, для которой при любых $x \in X$ выполняется соотношение $f(x) = g(x)$. Если функция f (необязательно всюду определенная) порождает любую функцию g (при условии $g \in K$), то f называется универсальной для класса K. Линейной называется k-значная функция переменных $x_1, \ldots, x_n$, представимая в виде $\alpha + \alpha_1 x_1 + \ldots + \alpha_n x_n$, где сложение и умножение производится по модулю k, а коэффициенты $\alpha, \alpha_1, \ldots, \alpha_n$ принадлежат множеству $\{0, 1, \ldots, k-1\}$.

При решении задач о существовании универсальных функций используется четыре основных утверждения, два из которых являются тривиальными.

Лемма 1. [3] Универсальная функция n переменных для класса линейных k-значных функций определена на не менее чем $k(n+1)$ наборах.

Пусть задана функция $\varphi(x_1, \ldots, x_l)$. Определим для произвольного m функцию $\Phi(x_{11}, \ldots, x_{1l}, \ldots, x_{m1}, \ldots, x_{ml})$. Положим

$$\Phi(0, \ldots, 0, x_{j1}, \ldots, x_{jl}, 0, \ldots, 0) = \varphi(x_{j1}, \ldots, x_{jl})$$

[1]Проф. факультета ВМК МГУ, проф. МФТИ, д.ф.-м.н., e–mail: dm6@cs.msu.ru

[2]Факультет ВМК МГУ, студ., e–mail: voronovank@yandex.ru

[3]Факультет ВМК МГУ, доц., к.ф.-м.н., e–mail: ilyutko@cs.msu.ru

[*]Работа Вороненко А.А. выполнена при поддержке РНФ 16-11-10014.

для всех j и будем считать функцию $\Phi(x_{11},\ldots,x_{1l},\ldots,x_{m1},\ldots,x_{ml})$ не определенной на остальных наборах.

Лемма 2.[3] Если $\varphi(x_1,\ldots,x_l)$ – универсальная функция для класса линейных k-значных функций, то для любого m функция

$$\Phi(x_{11},\ldots,x_{1l},\ldots,x_{m1},\ldots,x_{ml})$$

является универсальной для класса линейных k-значных функций соответствующего множества переменных.

Лемма 3. Если функция $f(\mathbf{x})$ является универсальной для класса линейных функций n переменных, то для любой линейной функции $l(\mathbf{x})$ функция $f(\mathbf{x})+l(\mathbf{x})$ также является универсальной для этого класса.

Доказательство. Докажем, что функция $f(\mathbf{x})+l(\mathbf{x})$ порождает произвольную линейную функцию $g(\mathbf{x})$. По определению универсальной функции $f(\mathbf{x})$ порождает линейную функцию $g(\mathbf{x})-l(\mathbf{x})$. Это значит, что на некотором множестве X функция $h(\mathbf{x})=g(\mathbf{x})-l(\mathbf{x})$ является единственной линейной, для которой всюду выполняется равенство $f(\mathbf{x})=h(\mathbf{x})$. Тогда на множестве X функция $h(\mathbf{x})=g(\mathbf{x})$ является единственной линейной, для которой всюду выполняется равенство $f(\mathbf{x})+l(\mathbf{x})=h(\mathbf{x})$.

Лемма 4. Не существует универсальных функций для класса линейных k-значных при $k=2,n=3$ и при $k=3,n=2$.

Доказательство. Пусть существует универсальная булева функция трех переменных $f(x_1,x_2,x_3)$. По лемме 1 она определена на восьми, то есть на всех, наборах. По лемме 3 функция f', задаваемая соотношением

$$f'(x_1,x_2,x_3)=f(x_1,x_2,x_3)\oplus f(1,0,0)\cdot x_1\oplus f(0,1,0)\cdot x_2\oplus$$

$$\oplus f(0,0,1)\cdot x_3\oplus f(0,0,0)\cdot(1\oplus x_1\oplus x_2\oplus x_3),$$

также является универсальной. Но функция $f'(x_1,x_2,x_3)$ – медиана и совпадает с линейной функцией $x_1\oplus x_2\oplus x_3$ всего лишь на двух наборах – нулевом и единичном, а, следовательно, не порождает ее и не является универсальной.

Потенциальная универсальная функция двух переменных для линейных трехзначных функций по лемме 1 должна иметь по три точки с каждым значением. В силу леммы 3 можно считать, что $f(0,0)=f(0,1)=f(1,0)=0$. Тогда рассмотрим функцию $g(x_1,x_2)=x_1+1$ и функцию $2g$. Обе эти функции не совпадают с $f(x_1,x_2)$ на ее нулях и друг с другом в точках, где они не равны нулю. На оставшихся шести наборах функция f не имеет нулей, а g и $2g$ имеют три общих

нуля. Одновременное порождение f обеих этих функций невозможно, поэтому универсальных функций для класса линейных трехзначных функций двух переменных не существует.

Лемма 5. 1. Если существует универсальная функция n переменных для класса линейных k-значных функций, то существует универсальная функция $n+1$ переменных для класса линейных k-значных функций.

2. Для простых k универсальные функции для класса линейных существуют, начиная с $n = 4$ – для булевых, начиная с $n = 3$ – для трехзначных и, начиная с $n = 2$ при $k \geq 5$.

3. При составных $k \geq 336$ существуют универсальные функции двух переменных для класса линейных.

Доказательство. 1. Для простых k, $k \geq 5$, доказано в работе [3], для всех составных – в [4]. Случай $k = 3$ рассматривается ниже.

2. Случай $k = 2$ рассмотрен в статье [1]. Результат для произвольного простого k, $k \geq 7$, получен в статье [3]. Пример двуместной универсальной функции для $k = 5$ приведен в таблице 2.

3. Доказано в работе [4] с использованием градиентного метода.

Для $k = 3$ универсальной является функция следующей таблицы.

Таблица 1.
Универсальная функция $f_3(x_1, x_2, x_3)$.

$x_1 \backslash x_2x_3$	00	01	02	10	11	12	20	21	22
0	0	0	0	0	2	1	0	1	2
1	0	2	1	2	2	2	1	2	1
2	0	1	2	1	2	1	2	1	-

При этом, если $n > 3$, а $f_{n-1}(x_1, \ldots, x_{n-1})$ – универсальная функция $n-1$ переменной для класса линейных трехзначных, то любая частичная функция $f_n(x_1, \ldots, x_n)$, задаваемая системой

$$\begin{cases} f_n(x_1, x_2, \ldots, x_{n-1}, 0) = f_{n-1}(x_1, x_2, \ldots, x_{n-1}), \\ f_n(0, x_2, x_3, 0, \ldots, 0, 1) = f_3(0, x_2, x_3), \\ f_n(1, x_2, x_3, 0, \ldots, 0, 1) = f_3(1, x_2, x_3) + 1, \\ f_n(0, x_2, x_3, 0, \ldots, 0, 2) = f_3(0, x_2, x_3) + 1, \end{cases}$$

является универсальной функцией n переменных для класса линейных трехзначных.

Таблица 2.

$x_1 \backslash x_2$	0	1	2	3	4
0	0	0	0	0	0
1	0	4	3	2	1
2	0	-	-	-	2
3	0	2	4	1	3
4	0	1	2	3	4

Нерешенным до конца вопросом является существование универсальных функций для класса линейных функций при фиксированных k и n, а именно, при $n = 2$.

Докажем более сильное, чем п.3 леммы 5, утверждение вероятностным методом.

Лемма 6. При $k \geq 48$ всегда существует универсальная функция двух переменных для класса линейных k-значных.

Доказательство. Всего имеется k^3 линейных функций двух переменных. При этом существует $k^6 - k^3$ упорядоченных пар различных линейных функций. Любые две линейные функции отличаются не менее чем на половине наборов [4]. Рассмотрим равномерное распределение на множестве всех k-значных функций f двух переменных. Вероятность того, что для двух линейных функций g_1 и g_2 не найдется точки $\mathbf{x}$, такой, что $f(\mathbf{x}) = g_1(\mathbf{x})$, но $f(\mathbf{x}) \neq g_2(\mathbf{x})$, не превосходит

$$\left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}}.$$

При этом вероятность того, что функция f не является универсальной, не превосходит

$$\left(k^6 - k^3\right) \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}} \qquad (1).$$

Найдем, при каких k последняя величина меньше единицы. Оценивая сверху ее логарифм, получим неравенство

$$6 \ln k + \frac{k^2}{2} \cdot \ln\left(1 - \frac{1}{k}\right) < 0.$$

Взяв два первых члена разложения функции $\ln(1 - \frac{1}{k})$, получим более сильное неравенство

$$6 \ln k - \frac{k}{2} + \frac{1}{4} < 0.$$

Выражение в левой части последнего неравенства убывает при $k > 12$. При $k = 48$ оно равно $6\ln 48 - 23.75 < 0$. Последнее доказывает существование универсальных функций при $k \geq 48$.

Замечание 1. Если рассмотреть функции трех переменных, то выражение (1) преобразуется к виду $\left(k^8 - k^4\right) \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^3}{2}}$ и будет меньше единицы при $k \geq 6$. Таким образом, для всех составных $k \geq 6$ существуют универсальные функции трех переменных.

Докажем теперь усиленный вариант леммы 6.

Лемма 7. При $k \geq 32$ всегда существует универсальная функция двух переменных для класса линейных k-значных.

Доказательство. Заметим, что только при четном k имеются линейные функции, совпадающие в половине точек. Для каждой линейной функции g с ней на половине точек совпадают ровно шесть функций вида

$$g + \sigma\frac{k}{2} + \sigma_1\frac{k}{2}x_1 + \sigma_2\frac{k}{2}x_2,$$

где $\sigma, \sigma_1, \sigma_2 \in \{0, 1\}$ и $\sigma_1 + \sigma_2 > 0$. Совпадения с оставшимися функциями для g возможны не чаще каждой третьей точки. Таким образом, вероятность (1) точнее оценивается сверху выражением

$$\left(k^6 - 7k^3\right) \cdot \left(1 - \frac{1}{k}\right)^{\frac{2k^2}{3}} + 6k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}} \qquad (2).$$

Потребуем одновременного выполнения неравенств

$$\left(k^6 - 7k^3\right) \cdot \left(1 - \frac{1}{k}\right)^{\frac{2k^2}{3}} \leq \frac{1}{\sqrt{\mathrm{e}}} \qquad (3).$$

и

$$6k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}} \leq \frac{1}{\mathrm{e}} \qquad (4).$$

Тогда в силу неравенства $\frac{1}{\mathrm{e}} + \frac{1}{\sqrt{\mathrm{e}}} < 1$ выражение (2) будет меньше единицы.

Оценивая сверху левые части неравенств (3)-(4) и переходя к логарифму, получим неравенства

$$6\ln k + \frac{2k^2}{3} \cdot \ln\left(1 - \frac{1}{k}\right) \leq -\frac{1}{2}$$

и

$$\ln 6 + 3\ln k + \frac{k^2}{2} \cdot \ln\left(1 - \frac{1}{k}\right) \leq -1.$$

Взяв два первых члена разложения функции $\ln(1-\frac{1}{k})$, получим более сильные неравенства

$$6\ln k - \frac{2k}{3} + \frac{1}{3} \le -\frac{1}{2}$$

и

$$\ln 6 + 3\ln k - \frac{k}{2} + \frac{1}{4} \le -1.$$

Левые части обоих неравенств убывают при $k \ge 9$. При $k = 32$ неравенства выполнены.

Замечание 2. Для $k = 4$ и случая трех переменных выделение пар функций, совпадающих на половине наборов, дает верхнюю оценку вероятности отсутствия универсальных функций

$$14k^4 \cdot \left(1-\frac{1}{k}\right)^{\frac{k^3}{2}} + \left(k^8 - 15k^4\right) \cdot \left(1-\frac{1}{k}\right)^{\frac{3k^3}{4}}.$$

Последняя величина меньше единицы, поэтому четырехзначные трехместные функции также существуют. Технику леммы 7 можно успешно использовать для доказательства существования универсальных функций при некоторых k меньших тридцати двух, но не делящихся одновременнно на два и три. Соответствующие (2) выражения для верхних оценок вероятностей отсутствия универсальных функций имеют вид:

$$\begin{aligned}
&\left(k^6 - 7k^3\right) \cdot \left(1-\tfrac{1}{k}\right)^{\frac{3k^2}{4}} + 6k^3 \cdot \left(1-\tfrac{1}{k}\right)^{\frac{k^2}{2}}, && k = 28;\\
&\left(k^6 - 25k^3\right) \cdot \left(1-\tfrac{1}{k}\right)^{\frac{8k^2}{9}} + 24k^3 \cdot \left(1-\tfrac{1}{k}\right)^{\frac{2k^2}{3}}, && k = 27,\\
&\left(k^6 - 7k^3\right) \cdot \left(1-\tfrac{1}{k}\right)^{\frac{12k^2}{13}} + 6k^3 \cdot \left(1-\tfrac{1}{k}\right)^{\frac{k^2}{2}}, && k = 26,\\
&\left(k^6 - 120k^3\right) \cdot \left(1-\tfrac{1}{k}\right)^{\frac{24k^2}{25}} + 120k^3 \cdot \left(1-\tfrac{1}{k}\right)^{\frac{4k^2}{5}}, && k = 25.
\end{aligned}$$

Значения всех этих выражений меньше единицы, поэтому универсальные функции двух переменных для класса линейных функций существуют при $k = 25, 26, 27, 28$.

Замечание 3. При рассмотрении $k = 21$ приходится выписывать сумму трех слагаемых, соответствующих разностям функций, кратным семи, трем и всем остальным. Получается верхняя оценка вероятности несуществования универсалных функций

$$24k^3 \cdot \left(1-\frac{1}{k}\right)^{\frac{2k^2}{3}} + 336\left(1-\frac{1}{k}\right)^{\frac{6k^2}{7}} + \left(k^6 - 360k^3\right) \cdot \left(1-\frac{1}{k}\right)^{\frac{20k^2}{21}}$$

Логарифмированием легко доказать, что первое и третье слагаемые в этом выражении меньше $\frac{1}{\mathrm{e}}$, второе – меньше $\frac{1}{\mathrm{e}^2}$. Из неравенства $\frac{2}{\mathrm{e}} + \frac{1}{\mathrm{e}^2} < 1$ вытекает существование универсальной функции для класса двуместных линейных функций при $k = 21$.

Для $k = 30$, выделив отдельные слагаемые, соответствующие парам линейных функций, совпадающим в каждой второй, третьей и пятой точках и оценив оставшиеся как все, совпадающие в каждой шестой, получим верхнюю оценку вероятности несуществования универсалных функций

$$6k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}} + 24k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{2k^2}{3}} + 120k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{4k^2}{5}} + k^6 \cdot \left(1 - \frac{1}{k}\right)^{\frac{5k^2}{6}}.$$

Логарифмированием легко доказать, что все слагаемые в этом выражении меньше $\frac{1}{\mathrm{e}^2}$. Из неравенства $\frac{4}{\mathrm{e}^2} < 1$ вытекает существование универсальной функции для класса двуместных линейных функций при $k = 30$.

В случае $k = 24$ слагаемое $6k^3 \cdot \left(1 - \frac{1}{k}\right)^{\frac{k^2}{2}}$, соответствующее парам функций, совпадающих на каждом втором наборе, оценивается сверху как $\mathrm{e}^{-0.4}$, все слагаемые для пар, совпадающих на каждом третьем, четвертом, шестом, восьмом и двенадцатом наборах – через e^{-4}, а слагаемое, соответствующее всем оставшимся парам – через e^{-3}. Из неравенства $\frac{5}{\mathrm{e}^4} + \frac{1}{\mathrm{e}^3} + \frac{1}{\mathrm{e}^{0.4}} < 1$ вытекает существование универсальной функции для класса двуместных линейных функций при $k = 24$.

Ниже приведены таблицы универсальных функций двух переменных для $k = 8, 9, 10, 12, 14$, полученные градиентным методом при помощи компьютера.

Таблица 3.

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7
0	0	0	1	1	2	2	3	3
1	0	5	1	6	2	7	3	4
2	1	2	2	1	2	3	6	4
3	2	3	3	1	3	4	-	-
4	3	6	0	3	5	0	-	-
5	1	4	4	3	-	2	7	1
6	4	7	-	7	3	-	0	0
7	-	2	4	-	5	1	0	-

Таблица 4.

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8
0	0	0	0	1	1	2	2	2	1
1	8	1	7	4	2	5	6	0	6
2	8	0	-	7	-	7	-	7	3
3	0	3	4	1	-	8	-	8	5
4	8	8	4	-	7	7	4	3	1
5	2	4	1	-	-	-	-	6	3
6	-	8	6	5	-	7	5	1	0
7	0	7	6	-	7	8	-	6	6
8	0	-	-	-	8	-	-	-	-

Таблица 5.

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8	9
0	0	4	1	5	8	1	7	0	8	9
1	0	0	0	9	-	7	1	0	0	0
2	1	1	6	4	2	4	5	0	-	-
3	6	5	1	4	-	0	-	1	-	1
4	4	5	8	-	-	-	3	0	-	7
5	2	6	3	8	0	3	3	2	1	7
6	1	8	6	-	-	-	1	3	-	-
7	8	-	-	-	1	2	7	-	0	9
8	8	-	-	-	-	9	9	0	-	-
9	1	-	-	-	-	5	1	6	-	-

Таблица 6.

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	11	9	10	11	8	5	11	3	-	3	1
2	0	10	9	1	7	-	1	0	5	11	11	2
3	0	9	7	2	-	2	10	-	2	8	1	3
4	0	8	11	1	6	-	-	-	-	11	10	4
5	0	7	-	8	-	10	4	11	-	1	-	5
6	0	6	-	11	2	-	-	-	-	3	10	6
7	0	5	-	1	-	-	8	-	1	-	7	7
8	0	4	9	-	9	-	5	2	7	9	-	8
9	0	3	5	-	-	10	-	-	10	4	11	9
10	0	2	-	7	-	-	-	-	-	9	-	10
11	0	1	2	3	4	5	6	7	8	9	10	11

Таблица 7.

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	11	-	5	6	3	-	9	10	11	10	-	1
2	0	11	8	9	-	10	-	-	-	13	5	-	7	2
3	0	-	9	12	5	12	-	-	5	-	1	13	9	3
4	0	5	-	5	9	-	-	9	-	-	9	-	-	4
5	0	6	10	12	-	8	13	-	-	-	-	-	-	5
6	0	3	-	-	-	13	-	-	11	-	8	-	3	6
7	0	-	-	-	9	-	-	4	7	-	-	6	-	7
8	0	9	-	5	-	-	11	7	1	-	7	-	-	8
9	0	10	13	-	-	-	-	-	-	8	-	-	-	9
10	0	11	5	1	9	-	8	-	7	-	11	-	-	10
11	0	10	-	13	-	-	-	6	-	-	-	-	-	11
12	0	-	7	9	-	-	3	-	-	-	-	-	-	12
13	0	1	2	3	4	5	6	7	8	9	10	11	12	13

Остаются нерассмотренными случаи $k = 4, 6$, а также $15, 16$, $18, 20, 22$.

Литература

1. *Вороненко А. А.* Об универсальных частичных функциях для класса линейных функций // Дискретная математика. 2012. **24**. № 3. С. 62–65.

2. *Вороненко А. А., Кафтан Д. В.* О порождении ложных образов линейных булевых функций // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. 2014. № 4. С. 70–73.

3. *Вороненко А. А.* О порождении ложных образов линейных k-значных функций // Прикладная математика и информатика. № 48. М. Макс Пресс, 2015. С. 85–92.

4. *Вороненко А. А.* О порождении ложных образов линейных k-значных функций для составных k при растущем числе переменных // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. 2016. № 2. С. 28–31.

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