Раздел I.
Дискретные модели информационных систем

А. А. Вороненко[1], *А. А. Щурова*[2]

УНИВЕРСАЛЬНЫЕ ФУНКЦИИ ДВУХ ПЕРЕМЕННЫХ ДЛЯ СПЕЦИАЛЬНЫХ ЗНАЧЕНИЙ k*

Введение

Ранее [1] была поставлена задача нахождения универсальных функций — позволяющих однозначно задать функцию частью своих значений при условии выполнения некоего свойства. Наиболее близкой является классическая задача поиска бент-функций — наибольшим образом уклоняющихся от всех линейных [2]. В настоящей работе заканчивается решение задачи о существовании универсальных функций для класса линейных функций в зависимости от числа переменных и значности.

Основная часть

Пусть $A = \{4, 6, 15, 16, 18, 20, 22\}$.

Напомним основные понятия. Линейная функция — это функция k-значной логики, которая представляется в виде:

$$a_0 + a_1 x_1 + \ldots + a_n x_n, \quad a_i \in \{0, 1, \ldots, k-1\}.$$

Будем говорить, что частичная функция f порождает линейную функцию g, если существует такое множество точек X из области определения функции f, что $g(x)$ является единственной линейной функцией, для которой при любом x из множества X выполняется соотношение $f(x) = g(x)$. Если функция f порождает любую линейную функцию g, то f называется универсальной функцией для класса линейных функций. До настоящей работы было известно следующее

Утверждение 1. *Для $n = 1$ ни при каких k не существует универсальных функций для класса линейных функций. Их также не существует при $k = 2$ и $n = 2, 3$ и при $k = 3$, $n = 2$. Для остальных n и k, кроме $n = 2$, $k \in A$ существуют универсальные функции для класса линейных функций.*

Доказательства несуществования универсальных функций получены при помощи несложных логических рассуждений в работах [1, 3, 5]. Существование булевых универсальных функций конструктивно доказано в работе [1]. В случае простого k в явном виде [3], а в случае

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

[2]Студ. факультета ВМК МГУ, e-mail: an.shchurova011@yandex.ru.

*Работа выполнена при поддержке гранта РНФ (номер проекта 16-11-10014).

составного — градиентным методом [4], было показано существование универсальной функции для $n+1$ переменных в случае, если она имеется при n. Для достаточно больших k (в частности, всех больших чем 336) при помощи градиентного метода удалось доказать существование универсальных функций двух переменных после сведения исходной задачи к задаче покрытия соответствующей матрицы с дополнительными ограничениями. Окончательно утверждение 1 получено в работе [5] при помощи вероятностного метода.

В таблицах 1–11 приводятся универсальные функции двух переменных для всех $k \in A$, кроме $k = 4$ и $k = 22$. Соответствующие таблицы были ранее получены в работе [6], однако для $k = 6, 16, 18$ эти таблицы содержали ошибки. При их исправлении был, в частности, применен метод возможных направлений — выбиралась замена значений, минимизирующая количество пар неотличимых функций.

Для $k = 22$ удалось доказать результат вероятностным методом. Рассмотрим равномерное распределение на множестве всех k-значных функций f двух переменных. Всего существует k^3 линейных функций от двух переменных, и соответственно, $k^6 - k^3$ упорядоченных пар линейных функций. Вероятность того, что не существует точки x такой, что для двух линейных k-значных функций двух переменных g_1 и g_2, различающихся на t наборах таких, что $f(x) = g_1$, но при этом $f(x) \neq g_2$, не превосходит $(1 - 1/k)^t$.

Пусть $g_1 - g_2 = a_0 + a_1 x_1 + a_2 x_2$. Мы рассматриваем ситуацию $k = 22$. Рассмотрим все возможные случаи. Для каждого случая получим верхнюю оценку вероятности того, что найдется пара неразличимых функций g_1 и g_2.

1. НОД$(a_1, a_2) = 1$.
2. НОД$(a_1, a_2) =$ НОД$(a_0, a_1, a_2) = 2$.
3. НОД$(a_1, a_2) =$ НОД$(a_0, a_1, a_2) = 11$.
4. НОД$(a_1, a_2) >$ НОД(a_0, a_1, a_2).

Общее количество разностей функций g_1 и g_2 не превосходит k^3. Из случаев 1, 2, 4 наибольшее число совпадений значений функций g_1 и g_2 во втором — $2k$. Поэтому вероятность наличия каких-то неразличимых функций g_1 и g_2 хотя бы в одном из этих трех случаев не превосходит $k^6(1 - 1/k)^{k(k-2)} < 0{,}15$.

В третьем случае функции g_1 и g_2 совпадают на половине наборов, но соответствующих этому случаю разностей функций g_1 и g_2 всего шесть, поэтому вероятность наличия неразличимых функций g_1 и g_2 в третьем случае не превосходит $6k^3(1 - 1/k)^{k^2/2} < 0{,}83$.

Поскольку все случаи исчерпаны и $0{,}15 + 0{,}83 < 1$, получаем, что при $k = 22$ существует универсальная функция двух переменных для класса

линейных k-значных функций.

x_1/x_2	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
0	8	11	2	9	0	3	9	2	2	10	9	10	7	7	12
1	12	1	1	8	5	12	14	0	3	6	4	10	2	2	13
2	13	2	10	7	3	2	3	5	5	5	0	14	0	8	13
3	12	5	0	13	5	12	2	11	12	6	2	9	1	3	5
4	14	10	5	1	3	1	4	6	6	1	1	6	7	4	6
5	5	1	3	12	7	8	10	9	4	14	0	14	8	1	11
6	3	8	6	1	9	9	2	5	7	0	6	4	6	5	8
7	5	11	1	8	8	8	2	10	10	13	10	10	4	10	4
8	0	14	12	7	0	6	8	9	4	1	9	10	12	7	1
9	12	12	4	13	6	4	14	0	0	9	5	2	11	10	4
10	0	10	3	4	9	10	3	3	4	7	4	13	9	8	6
11	10	5	10	6	3	1	11	9	1	3	10	7	12	7	2
12	1	14	4	12	4	14	14	7	2	4	6	13	9	0	13
13	7	3	3	3	9	13	4	12	8	13	0	3	12	4	2
14	6	6	2	10	10	6	1	9	5	10	5	3	0	0	3

Табл. 1. При $k = 15$.

x_1/x_2	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	11	14	3	3	8	8	2	1	13	12	15	4	0	12	12	1
1	5	14	0	12	0	3	12	11	3	12	12	9	8	7	11	3
2	5	14	6	13	6	8	14	3	4	13	8	5	9	4	6	12
3	11	5	8	11	9	5	6	12	1	2	5	9	9	0	12	14
4	14	2	12	4	10	10	8	15	8	0	4	1	4	10	13	15
5	15	6	11	8	11	1	4	12	4	9	6	13	9	2	12	7
6	5	8	12	15	2	4	14	10	4	2	12	8	12	9	7	12
7	15	2	4	10	4	9	7	8	2	13	5	12	15	1	3	4
8	9	15	4	12	3	2	6	7	5	2	15	1	12	7	13	11
9	9	2	6	13	11	13	5	13	10	11	9	9	12	13	14	6
10	12	2	2	0	4	8	7	9	11	7	11	7	14	8	2	7
11	10	8	5	5	5	10	3	15	5	12	9	2	9	7	8	6
12	9	10	6	13	2	13	7	13	4	2	4	2	10	7	10	5
13	15	15	10	5	9	13	4	15	10	13	1	3	4	9	9	13
14	3	15	11	5	13	2	3	1	4	7	4	14	14	14	3	14
15	13	14	3	6	11	7	5	5	5	6	9	9	15	2	7	2

Табл. 2. При $k = 16$.

$\mathbf{x}_1/\mathbf{x}_2$	**0**	**1**	**2**	**3**	**4**	**5**
0	5	4	0	4	1	4
1	0	2	5	5	0	0
2	1	5	4	3	5	0
3	0	5	5	1	3	2
4	4	1	2	1	3	1
5	2	4	5	2	4	5

Табл. 3. При $k = 6$.

$\mathbf{x}_1/\mathbf{x}_2$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	2	9	14	–	2	11	2	6	13
1	–	1	0	6	0	16	14	15	4
2	9	2	14	6	5	5	5	4	10
3	16	10	10	10	1	2	7	9	6
4	3	14	10	11	12	0	2	4	11
5	6	12	11	1	11	13	13	17	7
6	9	9	14	11	17	9	5	11	11
7	15	6	7	6	17	4	–	9	5
8	11	13	10	13	0	10	2	6	15

Табл. 4. При $k = 18$.

$\mathbf{x}_1/\mathbf{x}_2$	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
0	5	0	1	–	16	9	15	10	16
1	17	–	7	0	7	14	4	14	–
2	12	3	9	7	11	5	1	6	14
3	1	17	6	15	11	2	8	10	12
4	4	16	15	7	6	3	17	11	15
5	13	14	7	0	13	0	9	0	10
6	–	17	16	4	15	15	1	2	1
7	4	3	6	4	11	0	10	5	17
8	11	11	6	17	15	16	15	4	3

Табл. 5. При $k = 18$.

$\mathbf{x}_1/\mathbf{x}_2$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
9	4	8	14	7	2	0	0	15	5
10	–	11	12	12	7	4	8	15	6
11	12	3	7	10	6	6	3	16	9
12	11	0	4	17	14	12	–	16	17
13	7	6	1	16	–	–	17	9	12
14	15	14	6	17	2	6	9	7	8
15	14	–	15	17	1	15	2	13	4
16	4	1	5	17	5	11	10	1	5
17	4	15	15	10	–	–	14	17	16

Табл. 6. При $k = 18$.

$\mathbf{x}_1/\mathbf{x}_2$	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
9	15	11	7	9	3	6	11	4	9
10	9	–	10	12	11	17	7	17	2
11	9	12	5	13	13	8	17	–	17
12	–	12	2	1	13	12	13	11	1
13	8	7	14	12	6	7	16	2	13
14	12	7	1	17	9	7	4	2	12
15	–	2	–	2	12	2	1	13	2
16	7	9	13	10	7	13	13	–	–
17	–	0	8	6	1	12	7	8	14

Табл. 7. При $k = 18$.

$\mathbf{x}_1/\mathbf{x}_2$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	10	12	7	3	14	18	3	12	10	3
1	7	14	6	18	18	8	6	16	2	0
2	19	17	16	15	5	6	16	13	16	18
3	12	10	10	17	9	11	8	17	7	3
4	12	15	2	17	6	16	12	17	9	4
5	14	1	1	19	5	6	17	16	0	0
6	1	14	17	0	0	7	19	16	18	16
7	12	7	8	19	13	1	13	7	18	5
8	0	12	1	9	5	16	4	17	8	8
9	2	10	17	14	10	1	17	10	4	9

Табл. 8. При $k = 20$.

$\mathbf{x}_1/\mathbf{x}_2$	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0	14	10	16	15	18	9	8	9	2	19
1	19	5	4	6	0	11	16	4	3	6
2	12	15	5	11	14	3	11	0	11	13
3	4	18	13	12	5	18	19	1	11	7
4	3	1	6	13	10	7	4	10	5	3
5	3	4	15	6	13	14	14	5	11	3
6	0	4	17	13	3	15	12	12	11	4
7	3	12	11	0	12	3	19	3	0	17
8	1	0	15	1	0	8	14	5	7	13
9	19	4	1	13	14	7	9	10	16	10

Табл. 9. При $k = 20$.

$\mathbf{x}_1/\mathbf{x}_2$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
10	18	10	10	13	11	2	13	6	0	1
11	7	7	10	9	12	4	8	2	14	16
12	5	19	3	0	7	12	6	8	18	14
13	3	12	19	1	19	17	11	0	13	19
14	12	11	16	6	14	2	12	14	1	13
15	12	1	12	3	6	3	0	14	1	10
16	16	1	12	14	12	10	2	1	3	3
17	1	2	9	14	11	0	1	6	15	15
18	15	9	8	0	16	6	2	7	17	11
19	13	18	12	1	13	2	14	3	14	8

Табл. 10. При $k = 20$.

$\mathbf{x}_1/\mathbf{x}_2$	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
10	11	2	3	8	16	6	9	6	8	13
11	4	13	6	14	18	10	9	4	16	9
12	13	17	2	3	6	14	7	6	8	14
13	1	18	10	4	11	17	16	17	17	6
14	8	16	5	19	17	16	8	1	8	2
15	13	5	1	9	11	7	3	3	1	4
16	3	15	4	7	18	2	11	11	17	4
17	3	12	8	15	18	1	17	12	14	0
18	11	10	13	12	4	16	12	6	3	8
19	15	10	17	3	10	14	10	4	13	19

Табл. 11. При $k = 20$.

Теорема 2. *Для $n = 1$ ни при каких k не существует универсальных функций для класса линейных функций. Их также не существует при $k = 2$ и $n = 2, 3$ и при $k = 3$, $n = 2$. Для остальных n и k, кроме $n = 2$, $k = 4$ существуют универсальные функции для класса линейных функций.*

Случай $n = 2$, $k = 4$ рассматривался при помощи ЭВМ, однако стопроцентной уверенности в полученных отрицательных результатах пока нет.

Заключение

Таким образом, задача о существовании универсальных функций для класса линейных решена почти полностью — с точностью до окончательного доверия результатам машинного эксперимента для одной пары параметров.

Литература

1. *Вороненко А. А.* Об универсальных частичных функциях для класса линейных функций // Дискретная математика. 2012. Т. 24, № 3. С. 62–65.
2. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика, 2009. № 1(3). С. 15–37.
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 // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2016. №2. С. 28–31.
5. *Вороненко А. А., Воронова Н. К., Ильютко В. П.* О существовании универсальных функций для класса линейных k-значных функций при небольших k // Прикладная математика и информатика. М.:МАКС Пресс, 2016. №51. С. 100–108.
6. *Воронова Н. К.* Универсальные функции двух переменных. Выпускная квалификационная работа. 2016.