DOI 10.1007/s10598-019-09428-z
Computational Mathematics and Modeling, Vol. 30, No. 1, January, 2019

I. DISCRETE MODELS OF INFORMATION SYSTEMS

UNIVERSAL FUNCTIONS OF TWO VARIABLES FOR SPECIAL VALUES OF k

A. V. Voronenko[1] **and A. A. Shchurova**[2]

UDC 519.71

We consider the notion of universal function such that a subset of the function's values defines any function from some set. For the set of linear functions, we consider all the combinations of the number of variables and the number of values, except four-valued functions of two variables.

Keywords: linear function, universal function.

1. Introduction

We have previously considered [1] the problem of finding a universal function that uniquely defines a function of certain properties by a subset of its values. Closest to this is the classical problem of finding a bent function that maximally deviates from all linear functions [2]. In the present article, we conclude the proof of existence of universal functions for a class of linear functions depending on the number of variables and the number of values.

2. The Main Part

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

We start by recalling the main definitions. A linear function is a k-valued logic function representable in the form

$$a_0 + a_1x_1 + \ldots + a_nx_n, \quad a_i \in \{0, 1, \ldots, k-1\}.$$

We say that a partial function f generates the linear function g, if there exists a point set X from the definition domain of f, where $g(x)$ is the unique linear function such that for every x from X we have $f(x) = g(x)$. If f generates every linear function g, then f is a universal function for the class of linear functions. The following proposition is known from earlier work.

Proposition 1. *With $n = 1$ no universal functions exist for the class of linear functions for any k. No such functions exist for $k = 2$ and $n = 2, 3$ or for $k = 3$, $n = 2$. For all other n and k, except $n = 2$, $k \in A$ universal functions exist for the class of linear functions.*

The nonexistence of universal function has been proved by simple logic reasoning in [1, 3, 5]. The existence of Boolean universal functions has been constructively proved in [1]. The existence of a universal function of $n+1$ variables, given that it exists for n variables, has been proved explicitly for prime k [2] and by the gradient method

[1] Faculty of Computational Mathematics and Cybernetics, Moscow State University and MIPT, Russia; e-mail: dm6@cs.msu.ru.
[2] Tinkoff Bank, Moscow, Russia; e-mail: shchurova011@yandex.ru.

Translated from Prikladnaya Matematika i Informatika, No. 58, 2018, pp. 5–11.

Table 1
For $k = 15$

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

Table 2
For $k = 16$

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

for composite k [4]. For sufficiently large k (in particular, for all k greater than 336), the gradient method has been applied to prove the existence of universal functions of two variables after the reduction of the original problem to a covering problem for an appropriate matrix subject to additional constraints. The final proof of Proposition 1 has been obtained in [5] by a probability-theoretical method.

Table 3
For $k = 6$

x_1/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

Table 4
For $k = 18$

x_1/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

Table 5
For $k = 18$

x_1/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

Table 1–11 give the universal functions of two variables for all $k \in A$, except $k = 4$ and $k = 22$. The tables have been previously obtained in [6], but they contained errors for $k = 6, 16, 18$. The errors have been corrected, in particular, by the feasible direction method, selecting a change of variables that minimized the number of pairs of indistinguishable functions.

For $k = 22$, we have managed to prove the result by the probability-theoretical method. Consider a uniform distribution on the set of all k-valued functions f of two variables. There are a total of k^3 linear functions of

Table 6
For $k = 18$

x_1/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

Table 7
For $k = 18$

x_1/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

two variables, and correspondingly $k^6 - k^3$ ordered pairs of linear functions. The probability that there is no point x where two linear k-valued functions of two variables g_1 and g_2 that are not equal on t tuples and such that $f(x) = g_1$ but $f(x) \neq g_2$ is at most $(1 - 1/k)^t$.

Let $g_1 - g_2 = a_0 + a_1x_1 + a_2x_2$. Take $k = 22$ and examine all possible cases. For each case, we derive an upper bound of the probability that a pair of indistinguishable functions g_1 and g_2 exist.

1. $\mathrm{GCD}(a_1, a_2) = 1$.

2. $\mathrm{GCD}(a_1, a_2) = \mathrm{GCD}(a_0, a_1, a_2) = 2$.

3. $\mathrm{GCD}(a_1, a_2) = \mathrm{GCD}(a_0, a_1, a_2) = 11$.

4. $\mathrm{GCD}(a_1, a_2) > \mathrm{GCD}(a_0, a_1, a_2)$.

The total number of differences of the functions g_1 and g_2 is at most k^3. From cases 1, 2, 4, the greatest number of instances when the functions g_1 and g_2 are equal is observed in case 2 when it is $2k$. Therefore, the probability that there are indistinguishable functions g_1 and g_2 in at least one of these three cases is at most $k^6(1 - 1/k)^{k(k-2)} < 0.15$.

Table 8
For $k = 20$

x_1/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

Table 9
For $k = 20$

x_1/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

Table 10
For $k = 20$

x_1/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

Table 11
For $k = 20$

x_1/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

In case 3, the functions g_1 and g_2 are equal on half the tuples, but there are only six differences of g_1 and g_2 corresponding to this case, and therefore the probability of existence of indistinguishable functions g_1 and g_2 case 3 is at most $6k^3(1-1/k)^{k^2/2} < 0.83$.

We have exhausted all the possible cases and $0.15 + 0.83 < 1$. We thus conclude that for $k = 22$ there exists a universal function of two variables for the class of linear k-valued functions.

Theorem 1. *With $n = 1$, no universal functions exist for the class of linear functions for any k. Such universal functions do not exist for $k = 2$ and $n = 2, 3$ and for $k = 3$, $n = 2$ either. For all other n and k, except $n = 2$, $k = 4$, universal functions exist for the class of linear functions.*

The case $n = 2$, $k = 4$ has been examined by computer simulation, but we are still not completely confident in the negative results obtained.

3. Conclusion

The problem of the existence of universal functions for the class of linear functions has been solved almost completely, apart from the final verification of the computer simulation results for one pair of parameters.

Research supported by the Russian Science Foundation grant 16-11-10014.

REFERENCES

1. A. A. Voronenko, "Universal partial functions for the class of linear functions," *Diskr. Mat.*, No. 3, 62–65 (2012).
2. N. N. Tokareva, "Bent functions: results and applications. A survey," *Prikl. Diskr. Matem.*, No. 1(3), 15–37 (2009).
3. A. A. Voronenko, "Generation of false images of linear k-valued functions," *Prikl. Matem. Informat.*, No. 48, 85–92 (2015).
4. A. A. Voronenko, "Generation of false images of linear k-valued functions for composite k with increasing number of variables," *Vestnik MGU, Ser. 15: Vychisl. Matem. Kibernet.*, No. 2, 28–31 (2016).
5. A. A. Voronenko, N. K. Voronova, and V. P. Il'yutko, "The existence of universal functions for the class of linear k-valued functions with moderate k," *Prikl. Matem. Informat.*, No. 51, 100–108 (2016).
6. N. K. Voronova, *Universal Functions of Two Variables* [in Russian], Dissertation (2016).