

В. С. Домрачев (Москва, РТУ МИРЭА). **О получении оценок значности логики k для гарантированного наличия равновероятных функций в классах k -значных функций определенного вида.**

УДК 004.421.5

DOI https://doi.org/10.52513/08698325_2023_30_1_1

Резюме: Предложен способ получения оценки значности k логики для гарантированного наличия равновероятных функций в классе k -значных функций. Сформулировано и доказано утверждение, с помощью которого возможно получить оценку значности логики исходя из количества вершин и ребер в графе связности исходной булевой функции в случае задания определенного вида. Приведена таблица полученных с помощью данного утверждения значений значности k логики для всех графов связности.

Ключевые слова: k -значная логика, метод растяжения, равновероятная функция.

В работе [1] исследовался вопрос о нахождении такого значения, начиная с которого класс k -значных функций, полученный из произвольной исходной булевой функции методом растяжения ([2]), будет содержать хотя бы одну равновероятную функцию. Метод растяжения заключается в действии на систему линейных неравенств, задающих исходную булеву функцию, линейным преобразованием растяжения $x \rightarrow (k-1)x$, фактически домножая обе части неравенств на коэффициент $(k-1)$. Для нахождения такого значения k оценивается объем, в который попадает значение α (обозначим его V_α) и другой объем, в который попадает значение β (обозначим его V_β). Тогда k должно удовлетворять системе условий:

$$\begin{cases} V_\alpha \geq k^{n-1}, \\ V_\beta \geq k^{n-1}. \end{cases}$$

(в случае равновероятной функции от 3-х переменных будет ровно k^2 значений аргументов, на которых она принимает одинаковые значения). Однако предложенная система условий не учитывает возможное пересечение объемов V_α и V_β , а потому дает неточную оценку.

Для анализа класса функции k -значной логики на наличие в нем равновероятных функций в данных тезисах предлагается следующий порядок действий:

1. Расчет V_α , V_β , $V_\cap = V_\alpha \cap V_\beta$.
2. Вычисление

$$V' = \min(V_\alpha, V_\beta) - \frac{1}{2}V_\cap. \quad (1)$$

3. Получение оценки k из неравенства $V' \geq k^2$.

В данных тезисах ограничимся рассмотрением только булевых функций от 3-х переменных, заданных сокращенной ДНФ, в которой все элементарные конъюнкции

имеют длину 3, и полученных из них методом растяжения классов ([2]). Воспользуемся классификацией всех булевых функций от 3-х переменных, введенной в [3] и связанной с графом связности функции:

Вес функции f	Граф связности функции f	Номер графа связности функции f	Вес функции \bar{f}	Граф связности функции \bar{f}	Номер графа связности функции \bar{f}
0		0.1	8		8.1
1		1.1	7		7.1
2		2.1	6		6.1
		2.2			6.2
		2.3			6.3
3		3.1	5		5.1
		3.2			5.2
		3.3			5.3
4		4.1	4		4.1
		4.2			4.2
		4.3			4.3
		4.4			4.4
		4.5			4.5
		4.6			4.6

Основным результатом доклада является утверждение 1, позволяющее получить оценку значности логики k исходя из количества вершин и ребер в графе связности исходной булевой функции с учетом вида ее задания.

Утверждение 1. Пусть v — количество вершин, а e — количество ребер в графе связности исходной булевой функции от 3-х переменных, заданной сокращенной ДНФ, в которой все элементарные конъюнкции имеют длину 3. Оценка значности логики k для гарантированного наличия равновероятных функций в классе, полученном из исходной функции с номером графа связности функции 1.1–4.6 методом растяжения, находится из неравенства:

$$\frac{v + e + 2}{24} \geq \frac{k^2}{(k - 1)^3}.$$

Таким образом, в условиях утверждения 1 получены следующие оценки значности логики k :

Вес функции f	Граф связности функции f	Номер графа связности функции f	$\frac{v+e+2}{24}$	k
1		1.1	0,125	≥ 11
2		2.1	0,208333	≥ 8
		2.2	0,166667	≥ 9
		2.3	0,166667	≥ 9
3		3.1	0,291667	≥ 6
		3.2	0,25	≥ 7
		3.3	0,208333	≥ 8
4		4.1	0,416667	≥ 5
		4.2	0,375	≥ 6
		4.3	0,375	≥ 6
		4.4	0,333333	≥ 6
		4.5	0,333333	≥ 6
		4.6	0,25	≥ 7

СПИСОК ЛИТЕРАТУРЫ

1. Никонов Н. В. Метод растяжения в построении классов равновероятных k -значных функций с запретом. — Обозрение. прикл. и промышл. матем., 2006, т. 13, в. 6, с. 961–974. // *Nikonov N. V.* An extension method in the construction of classes of equiprobable k -valued functions with interdiction. — *OPPM Surv. Appl. Ind. Math.*, Moscow, 2006, v. 3, is. 6, p. 961–974. (In Russian)
2. Никонов Н. В. Полиэдральные классы функций k -значной логики с обобщенными запретами и полузапретами. — Математические вопросы криптографии. 2012, т. 3, в. 1, с. 53–69. // *Nikonov N. V.* Polyhedral classes of k -valued logic functions with generalized filter taboo and semitaboo. — *Mathematical Aspects of Cryptography*, Moscow, 2012, v. 3, is. 1, p. 53–69 (In Russian)
3. Никонов Н. В. О классификации всех булевых функций от 3-х переменных с обобщенными запретами. — Ж. Вестник МГУЛ «Лесной вестник», 2004, №5 (36), с. 177–188. // *Nikonov N. V.* Classification of all Boolean functions in 3 variables with generalized taboo tuples. — *Forestry Bulletin*, 2004, v. 5 (36), p. 177–188 (In Russian)

Поступила в редакцию
3.X.2023

UDC 004.421.5

Domrachev V. S. (Moscow, RTU MIREA). **On obtaining estimates of logic values k for the guaranteed presence of balanced functions in the classes of k -valued functions of a certain type.**

Abstract: The article proposes a method for obtaining an estimate of logic value k for the guaranteed presence of balanced functions in the class of k -valued functions. The author has formulated and proved a statement by which it is possible to obtain an estimate of logic value k based on the number of vertices and edges in the connectivity graph of the original boolean function in the case of a certain type of assignment. In addition, the study provides a table of logic values k for all types of connectivity graphs obtained using this statement.

Keywords: k -valued logic, extension method, balanced function.