ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 31 МАТЕМАТИКИ Выпуск 1
2024

А. И. Зобов, **С. Ю. Катышев** (Москва, ФСРБИТ; Москва, РТУ МИРЭА). **Методы приближения k-значных отображений.**

УДК 519.233.33 DOI https://doi.org/10.52513/08698325_2024_31_1_1

Резюме: В работе предлагаются новые характреристики близости k-значных отображений и изучается их взаимосвязь.

Ключевые слова: k-значное отображение, характеристики близости.

В задачах оценки стойкости криптографических алгоритмов зачастую возникает необходимость замены функции на «близкую» к ней, но более простого вида, например, на линейные. Если в булевом случае основной и, по существу, единственной характеристикой близости функций является расстояние Хэмминга между векторами значений, то в k-значном случае можно предложить целый ряд различных подходов к заданию таких характеристик.

Как правило, ранее в качестве меры близости k-значных отображений использовалось обобщенное расстояние Хэмминга, соответствующее количеству входных наборов, на которых функции принимают разные значения. Если на множестве входных наборов $\vec{x} \in \mathbb{Z}_k^n$ функций задать равномерное распределение, то обобщенное расстояние Хэмминга между функциями $f_1(x)$, $f_2(x)$ соответствует первой координате вектора распределения случайной величины соответствующий разности функций:

$$f_1(x) - f_2(x).$$

Перспективным для практического применения представляется использование для определения «близости» функций всего вектора распределения разности функций. В рамках данной работы предлагается сделать первые шаги в указанном направлении, а именно исследовать начальные моменты указанного распределения.

Введем *степенную характеристику близости* между функциями $f_1(x)$, $f_2(x)$ вида:

$$\xi_m(f_1(x), f_2(x)) = \frac{1}{k^n} \sum_{x \in \mathbb{Z}_k^n} (f_1(x) - f_2(x))^m.$$

Точное значение математического ожидания значения введенной характеристики для случайных функций вычислено в следующей теореме.

Теорема 1. *Пусть $f_1, f_2 \in F_k(n)$ — независимо и равномерно распределены на множестве $F_k(n)$. Тогда математическое ожидание степенной характеристики равно*

$$M\xi_m(f_1, f_2) = \begin{cases} \dfrac{2}{k^2} \sum\limits_{t=l}^{2l} (-1)^t \dfrac{(2l)!}{(2l-t)!t!} + \dfrac{1}{k^2}(-1)^l \dfrac{(2l)!}{(l!)^2} \left(\sum\limits_{s=0}^{k-1} s^l \right)^2, & m = 2l; \\ 0, & m = 2l-1, \quad l \in \mathbb{N}. \end{cases}$$

Интерес представляет еще одна характеристика — мультипликативная:

$$\xi_*^{(l)}(f_1, \ldots, f_l) = \frac{1}{k_n} \sum_{x \in \mathbb{Z}_k^n} (f_1(x) \cdot \ldots \cdot f_l(x)).$$

Точное значение математического ожидания значения мультипликативной характеристики для случайных функций вычислено в следующей теореме.

Теорема 2. *Пусть* $f_1, \ldots, f_l \in F_k(n)$ *— независимо и равномерно распределены на множестве* $F_k(n)$. *Тогда математическое ожидание мультипликативной характеристики равно*

$$M\xi_*^{(l)}(f_1, \ldots, f_l) = \frac{(k-1)^l}{2^l};$$

Далее можно обобщить понятие статистического аналога функций в k-значном случае, относительно введенных характеристик. Функция $f_1 \in F_k(n)$ называется *статистическим аналогом функции* $f_2 \in F_k(n)$ *относительно мультипликативной характеристики*, если выполнено:

$$\xi_*^{(2)}(f_1, f_2) \neq \frac{(k-1)^2}{4}.$$

Аналогично могут быть введены понятия статистических аналогов относительно квадратичной, степенной характеристики или всего вектора распределения разности в целом.

Связь между наличием статистических аналогов относительно мультипликативной $\xi_*^{(2)}$ и квадратичной характеристики ξ_2 показывает следующая теорема:

Теорема 3. *Пусть* $f_1, f_2 \in F_k(n)$ *— сбалансированные функции. Тогда* f_1 *не является статистическим аналогом* f_2 *относительно* ξ_2 *тогда и только тогда, когда* f_1 *не является статистическим аналогом* f_2 *относительно* ξ_*.

Полученные результаты позволяют расширить в k-значном случае область применения таких криптографических методов, как, например, корреляционный.

СПИСОК ЛИТЕРАТУРЫ

1. *Никонов В. Г.*, *Зобов А. И.* Характеристики близости функций k-значной логики и их взаимосвязь. — Computational nanotechnology, 2019, № 2.
2. *Логачев О. А.*, *Федоров С. Н.*, *Ященко В. В.* Булевы функции как точки на гиперсфере в евклидовом пространстве. — Дискретная математика, 2018, т. 30, № 1, с. 39–55.
3. *Яблонский С. В.* Введение в дискретную математику: Учеб. пособие для вузов. 2-е изд., перераб. и доп. М.: Наука, Гл. ред. физ.-мат. лит., 1986, 384 с.

Поступила в редакцию
13.XII.2024

UDC 519.233.33 DOI https://doi.org/10.52513/08698325_2024_31_1_1

A. I. Zobov, ***S. Yu. Katyshev*** (Moscow, FSRBIT; Moscow, RTU MIREA).

Approximation Methods of k-Valued Functions.

Abstract: This paper proposes new proximity characteristics of k-valued function and studies their interrelation.

Keywords: k-valued function, total deviation.