ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 1
2014

В. А. Миронова (Москва, НИУ ВШЭ)**. О структуре спектра Уолша случайной булевой функции.**

Для спектра Уолша булевой функции f от n переменных определяется понятие его структуры и исследуются ее свойства в стохастической постановке, когда функция f случайна и выбирается с равной вероятностью из множества всех булевых функций от n переменных.

Пусть $V_n = \{v_0, v_1, \ldots, v_{2^n-1}\}$ есть n-мерное векторное пространство над полем из двух элементов, векторы которого упорядочены в лексикографическом порядке, $f : V_n \to \{0,1\}$ есть булева функция (б. ф.) от n переменных и $F_n = \{f\}$ — множество всех таких функций.

Преобразование Уолша и *спектр Уолша* (далее просто — спектр) б. ф. f определяются равенствами $w_f(u) = \sum_{x \in V_n} (-1)^{f(x)} (-1)^{(u.x)}$, $u \in V_n$, и, соответственно, $w_n = (w_{n0}, w_{n1}, v_{n,2^n-1})$, $w_{ni} = w_f(v_i)$.

Объектом нашего внимания являются следующие функционалы от спектра (далее $\mathbf{I}\{\cdot\}$ — индикатор): $\mu_r(f) = \sum_{u \in V_n} \mathbf{I}\{w_f(u) = r\}$, $r = 0, \pm 1, \ldots, \pm 2^n$, так что $\mu_r(f)$ есть число *спектральных коэффициентов* $w_f(u)$, имеющих значение r. Совокупность всех этих величин называется *структурой спектра* б. ф. f, а сами величины $\mu_r(f)$ — *элементами структуры*. Эти «сводные» характеристики спектра важны при анализе различных свойств б. ф., используемых в теории информации, кодирования и криптографии [1].

Пусть на множестве $F_n = \{f\}$ задана равномерная мера, в соответствии с которой любая б. ф. f может наблюдаться с вероятностью 2^{-2^n}. Исследование распределений компонентов спектра случайной булевой функции в такой модели проведено в работе [2]. Из результатов этой работы, в частности, следует, что *компоненты спектра случайной булевой функции одинаково распределены и некоррелированны, а при* $n \to \infty$ *они асимптотически нормальны с параметрами* $(0, 2^n)$.

На основе этого факта для элементов структуры случайной булевой функции установлены следующие результаты: если $n \to \infty$ и $r = \alpha 2^{n/2}(1 + o(1))$, $\alpha \leqslant c < \infty$, то $\mathbf{M}\,\mu_{2r}(n) = \sqrt{2/\pi} 2^{n/2} e^{-\alpha}(1 + o(1))$, а при фиксированных l и s выполняется $\operatorname{cov}(\mu_{2l}(n), \mu_{2s}(n)) = (-1)^{l-s} 2^{n+1}/\pi$, для интервальных характеристик структуры вида $\mu_{nk}(a,b) = \sum_{i=0}^{2^k-1} \mathbf{I}\{a < \widehat{w}_{ni} < b\}$ справедливо следующее утверждение.

Теорема. *Пусть при* $n \to \infty$ *разность* $n - k \to \infty$. *Тогда случайная величина* $\mu_{nk}(\alpha 2^{n/2}, \beta 2^{n/2})$, $\alpha < \beta$, *асимптотически имеет биномиальное распределение* $\mathrm{Bi}(2^k, p)$, *где* $p = \Phi(\beta) - \Phi(\alpha)$, Φ — *стандартная нормальная функция распределения. Если дополнительно* $k \to \infty$, *то эта величина асимптотически нормальна с параметрами* $(2^k p, 2^k p(1-p))$.

СПИСОК ЛИТЕРАТУРЫ

1. *Тарaнников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях. — Матем. вопросы киберн., 2002, в. 11, с. 31–148.
2. *Ивченко Г. И.*, *Медведев Ю. И.* Спектр случайной булевой функции и его производящая функция. — Матем. вопросы криптографии, 2011, т. 2, в. 2, с. 41–54.