ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 20 МАТЕМАТИКИ Выпуск 5
2013

В. П. Зязин, **М. В. Федюкин** (Москва, МИРЭА, ООО «Линфо»).
О множестве функций, реализуемых полиномами над универсальными алгебрами со случайными сигнатурами псевдомодульных операций.

Пусть $\Omega_{2^n} = \{0, 1, 2, \ldots, 2^n\}$. Для $a = \sum_{i=0}^{n-1} a_i 2^i, a_0, a_1, \ldots, a_{n-1} \in \{0, 1\}$. Будем отождествлять элемент $a \in \Omega_{2^n}$ с вектором $(a_0, a_1, \ldots, a_{n-1})$, а переменную x_j, $j \in \{1, 2, \ldots\}$ с вектором $(x_{j,0}, x_{j,1}, \ldots, x_{j,n-1})$, где $x_{j,i}$ — булевы переменные.

Пусть γ — разбиение множества $\{0, 1, \ldots, n-1\}$ вида $\{0, 1, \ldots, n-1\} = \{0, 1, \ldots, i_1 - 1\}\{i_1, 1, \ldots, i_2 - 1\} \cdots \{i_{t-1}, 1, \ldots, i_t - 1\}$, $i_0 = 0$. Определим псевдомодульную бинарную операцию θ_γ, соответствующую разбиению γ, следующим образом. Для $a = \sum_{i=0}^{n-1} a_i 2^i$, $b = \sum_{i=0}^{n-1} b_i 2^i$, $c = \sum_{i=0}^{n-1} c_i 2^i$, $c = a\theta_\gamma b$, если при всех s, $0 \leqslant s \leqslant t-1$, имеют место равенства

$$\sum_{j=i_s}^{i_{s+1}-1} a_j 2^{j-i_s} + \sum_{j=i_s}^{i_{s+1}-1} b_j 2^{j-i_s} = \sum_{j=i_s}^{i_{s+1}-1} c_j 2^{j-i_s} \left(\mathrm{mod}\, 2^{i_{s+1}-i_s}\right).$$

Обозначим Θ_n множество всех таких операций на Ω_{2^n}, $\mathcal{F}_m(\Theta)$ при $\Theta \subseteq \Theta_n$ — множество всех m-местных функций над универсальной алгеброй с сигнатурой Θ.

Свойства преобразований, получаемых при помощи псевдомодульных операций, изучались в [2, 3]. В частности, в [3] получены условия для равенства $\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)$. Положим $k = |\Theta|$. Равенство может достигаться при $k = n$, а для $m = 1$ — при $k = 2$.

В работе, представленной настоящим докладом, установлены вероятностные оценки для выполнения равенства $\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)$ при случайном и равновероятном выборе операций сигнатуры Θ из множества всех псевдомодульных операций.

Утверждение 1. *Пусть операции сигнатуры Θ выбираются случайно и равновероятно с возвращением из Θ_n, тогда*:

1) $\lim\limits_{n\to\infty} \mathbf{P}\{\mathcal{F}_1(\Theta) = \mathcal{F}_1(\Theta_n)\} = \begin{cases} 1 \text{ при } \lim\limits_{n\to\infty} \dfrac{n}{2^k} = 0; \\ e^{-2\lambda} \text{ при } \lim\limits_{n\to\infty} \dfrac{n}{2^k} = \lambda; \\ 0 \text{ при } \lim\limits_{n\to\infty} \dfrac{n}{2^k} = \infty; \end{cases}$
2) $\lim\limits_{n\to\infty} \mathbf{P}\{\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)\} = 1$ *при* $k = n + \varphi(n)$ *и* $\lim\limits_{n\to\infty} \varphi(n) = \infty$, $m = 2, 3, \ldots$;
3) $\mathbf{P}\{\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)\} = 1$ *при* $k < n$, $m = 2, 3, \ldots$

Утверждение 2. *Пусть операции сигнатуры Θ выбираются случайно и равновероятно без возвращения из Θ_n, тогда*:

1) $\lim\limits_{n\to\infty} \mathbf{P}\{\mathcal{F}_1(\Theta) = \mathcal{F}_1(\Theta_n)\} = \begin{cases} 1 \text{ при } \lim\limits_{n\to\infty} \dfrac{n}{2^k} = 0; \\ 0 \text{ при } \lim\limits_{n\to\infty} \dfrac{n}{2^k} = \infty; \end{cases}$
2) $\lim\limits_{n\to\infty} \mathbf{P}\{\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)\} = 1$ *при* $k = n + \varphi(n)$ *и* $\lim\limits_{n\to\infty} \varphi(n) = \infty$, $m = 2, 3, \ldots$;
3) $\mathbf{P}\{\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)\} = 1$ *при* $k < n$, $m = 2, 3, \ldots$

СПИСОК ЛИТЕРАТУРЫ

1. *Гнеденко Б. В.* Курс теории вероятностей. М.: Едиториал УРСС, 2005, 448 с.
2. *Глухов М. М.* О матрицах переходов разностей при использовании некоторых модулярных групп. — Матем. вопросы криптографии, в печати.
3. *Федюкин М. В.* О функциях, реализуемых полиномами над универсальными алгебрами с псевдомодульными операциями. — В кн.: Труды по дискретной математике. Т. 8. М.: Физматлит, 2004, с. 299–311.
4. *Lausch H.*, *Nöbauer W.* Algebra of Polynomials. Amsterdam: North. Holl., 1973.