О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Т о м 21 М А Т Е М А Т И К И В ы п у с к 2
2014

В. П. З я з и н, М. В. Ф е д ю к и н (Москва, МГТУ МИРЭА, ООО «Линфо»). **Об одном обобщении 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.

Обозначим символом γ разбиение множества $\{0, 1, \ldots, n-1\}$ вида

$$\{0, 1, \ldots, n-1\} = \Delta_0 \cup \Delta_1 \cup \cdots \cup \Delta_{t-1},$$

где блоком разбиения является $\Delta s = \{j_{s,0}, j_{s,1}, \ldots, j_{s,r_s}\}$, $s = 0, 1, \ldots, t-1$, $t = 1, 2, \ldots, n$.

Определим обобщенную псевдомодульную бинарную операцию θ_γ на множестве Ω_{2^n}, соответствующую разбиению γ, следующим образом: $c = \sum_{i=0}^{n-1} c_i 2^i = a\theta_\gamma b$, если для $a = \sum_{i=0}^{n-1} a_i 2^i$, $b = \sum_{i=0}^{n-1} b_i 2^i$ при всех s,

$0 \leqslant s \leqslant t_1$, имеют место равенства:

$$\sum_{u=0}^{r_s} a_{j_{s,u}} 2^u + \sum_{u=0}^{r_s} b_{j_{s,u}} 2^u = \sum_{u=0}^{r_s} c_{j_{s,u}} 2^u (\mod 2^{r_s+1}).$$

Обозначим множество всех таких операций на Ω_{2^n} символом $\widetilde{\Theta}_n$, а множество всех таких m-местных функций над универсальной алгеброй с сигнатурой Θ, что $\Theta \subseteq \widetilde{\Theta}_n$ обозначим символом $\widetilde{F}_m(\Theta)$.

Известно, что мощность множества операций $\widetilde{\Theta}_n$ равна числу Бэлла $\mathcal{B}_n$.

Операции называются псевдомодульными операциями, если каждый блок разбиения Δ_s, $s = 0, 1, \ldots, t-1$ имеет вид:

$$\Delta_s = \{i_s + 1, i_s + 2, \ldots, i_{s+1} - 1\}.$$

Обозначим Θ_n множество всех таких операций на Ω_{2^n}. Очевидно, что мощность множества операций Θ_n равна 2^{n-1}.

Свойства преобразований, получаемых с помощью псевдомодульных операций, изучались в ряде работ, в том числе, в [2], [3], [6]. Отметим, в частности, что М. В. Федюкиным был установлен критерий совпадения группы трансляций алгебры на $\Omega_{2^n}(\Theta_n)$ с силовской 2-подгруппой симметрической группы, состоящей из треугольных подстановок (подробное описание этой 2-группы приведено в [5]). В работе [3] получены достаточные условия для выполнения равенства $\mathcal{F}_m(\Theta) = \mathcal{F}_m(\Theta_n)$.

Так как множество операций $\widetilde{\Theta}_n$ содержит множествто Θ_n, то можно предполагать возможность более простой реализации функций с их помощью.

Далее приведем результаты изучения возможности распространения отмеченных результатов, полученных для операций из множества Θ_n, на операции из множества $\widetilde{\Theta}_n$.

Напомним, что группы трансляций алгебр $\Omega_{2^n}(\Theta_n)$ и $\Omega_{2^n}(\Theta)$ совпадают тогда и только тогда, когда в множестве операций $\Theta, \Theta \subseteq \Theta_n$, содержатся операции, соответствующие разбиению, у которого первый блок имеет вид $\{0, 1, \dots, s\}$ при любом $s = 0, 1, \dots, n-1$.

Следующий пример показывает, что для множества операций $\widetilde{\Theta}_n$ такое утверждение не верно.

Пусть $n = 3$, множество операций $\Theta \subseteq \widetilde{\Theta}_n$ содержит операции $\theta_1, \theta_2, \theta_3$, соответствующие, соответственно, разбиениям $\{0, 1, 2\}, \{0, 1\} \cup \{2\}$, $\{0, 2\} \cup \{1\}$. Непосредственной проверкой можно убедиться, что порядок группы трансляций алгебры с этими операциями равен 128 и совпадает с порядком силовской 2-подгруппы группы S_8. Однако, сигнатура этой алгебры не содержит операции, соответствующей разбиению, имеющему в качестве первого блока множество $\{0\}$.

Тем не менее, для одноместных функций полученные для операций Θ_n результаты на множество операций $\widetilde{\Theta}_n$ удается распространить.

Очевидно, что $\mathcal{F}_1(\Theta_n) = \mathcal{F}_1(\widetilde{\Theta}_n)$.

Утверждение. *Пусть* $\Theta \subseteq \widetilde{\Theta}_n$. *Тогда равенство*

$$\mathcal{F}_1(\Theta) = \mathcal{F}_1(\Theta_n)$$

имеет место тогда и только тогда, когда для любого $i \in \{0, 1, \dots, n-1\}$ *в множестве* Θ *существуют такие операция* θ_1, *соответствующая разбиению* $\gamma_{\theta_1} = \Delta_1 \cup \Delta_2 \cup \dots \cup \Delta_{t_{\theta_1}}$, *и операция* θ_2, *соответствующая разбиению* $\gamma_{\theta_2} = B_1 \cup B_2 \cup \dots \cup B_{t_{\theta_2}}$, *что множество* $\{i, i+1\}$ *содержится в множестве* Δ_j *при некотором* $j \in \{1, 2, \dots, t_{\theta_1}\}$, *и при любом* $j \in \{1, 2, \dots, t_{\theta_2}\}$, *множество* $\{i, i+1\}$ *не содержится в множестве* B_j.

СПИСОК ЛИТЕРАТУРЫ

1. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978, 287 с.
2. *Глухов М. М.* О матрицах переходов разностей при использовании некоторых модулярных групп. — Матем. вопросы криптографии, 2013, т. 4, в. 3, с. 27–47.
3. *Федюкин М. В.* О функциях, реализуемых полиномами над универсальными алгебрами с псевдомодульными операциями. — В сб.: Труды по дискретной математике. Т. 8, М.: Фазис, 2004, с. 299–311.
4. *Lausch H., Nöbauer W.* Algebra of Polynomials. Amsterdam: North. Holland, 1973.
5. *Сущанський В. I., Сікора В. С.* Операції на групах підстановок. — Теорія та застосування, Чернівці, 2003, «Рута», 255 с.
6. *Зязин В. П., Федюкин М. В.* О множестве функций, реализуемых полиномами над универсальными алгебрами со случайными сигнатурами псевдомодульных операций. — Обозрение прикл. и промышл. матем., 2013, т. 20, в. 5. (В печати.)