

$= \sum_{i,j \in \{0,1\}} c_{ij}^a \cdot w(g(i, j, z))$. Следовательно, функция h статистически не зависит от переменных в x . ■

Следующее утверждение характеризует условия статистической независимости от переменных в x суммы двух функций в частном случае — когда одна из функций зависит только от x .

Утверждение 3. Пусть x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно и функция $f(x, y)$ статистически не зависит от переменных в x . Тогда функция $f(x, y) \oplus g(x)$, где g — любая функция от n переменных, статистически не зависит от переменных в x , если и только если f уравновешена или $g = \text{const}$.

Доказательство. По условию $w(f(a, y)) = w(f)/2^n$ для всех $a \in \{0, 1\}^n$; следовательно, $w(f(a, y) \oplus g(a))$ не зависит от a , если и только если $g = \text{const}$ или $w(f)/2^n = 2^m - w(f)/2^n$; последнее равенство равносильно уравновешенности f . ■

ЛИТЕРАТУРА

1. Агibalов Г. П., Панкратова И. А. Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.
2. Колчева О. Л., Панкратова И. А. О статистической независимости суперпозиции булевых функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 11–12.

УДК 519.712.2

ОБ ОДНОЙ ЗАДАЧЕ КОМБИНАТОРНОЙ ОПТИМИЗАЦИИ¹

А. С. Кузнецова, К. В. Сафонов

Пусть есть n стульев, каждый из которых имеет уникальный порядковый номер $i = 1, 2, \dots, n$. Стулья расставлены по окружности. На стулья произвольным образом садятся n человек так, что на каждом стуле оказывается по одному человеку. Каждый человек имеет уникальный порядковый номер $j = 1, 2, \dots, n$. Посадка называется правильной, если у всех стульев порядковые номера совпадают с номерами сидящих на них людей, в противном случае посадка называется неправильной. Будем называть перестановкой перемену мест двух сидящих рядом людей. Требуется вычислить наименьшее число перестановок d , которые позволят получить правильную посадку из произвольной начальной посадки.

Перестановки (p, q) , указанные в условии задачи, порождают симметрическую группу S_n степени n . Запишем данную группу через порождающие элементы и определяющие соотношения. Пусть $x_1 = (1, 2)$, $x_2 = (2, 3)$, $\dots$, $x_{n-1} = (n-1, n)$, $x_n = (1, n)$ — порождающие элементы группы S_n . Теперь запишем определяющие соотношения R для S_n :

$$R = \begin{cases} x_i^2 = e, & i = 1, 2, \dots, n, \\ (x_i x_j)^2 = e, & \text{если } 1 < |j - i| < n - 1, \\ (x_i x_j)^3 = e, & \text{если } |j - i| = 1 \text{ или } |j - i| = n - 1, \\ x_1 x_2 \dots x_{n-2} x_{n-1} x_{n-2} \dots x_2 x_1 = x_n. \end{cases}$$

Таким образом,

$$S_n = \langle x_1, x_2, \dots, x_n \mid R \rangle.$$

¹Работа поддержана грантом РФФИ, проект № 10-01-00509-а.

Построим группу S_n в формате минимальных слов по алгоритму из [1]. В итоге максимальная длина минимальных слов группы S_n является решением задачи.

Ниже в таблице приведены решения для $n = 2, 3, \dots, 12$, полученные при помощи компьютерных вычислений.

n	2	3	4	5	6	7	8	9	10	11	12
d	1	2	4	6	9	12	16	20	25	30	36

Аналогичные задачи встречаются на практике, например при проектировании компьютерных вычислительных сетей [2]. Сеть процессоров может быть представлена как неориентированный граф, в котором процессоры являются вершинами, а две вершины графа соединены ребром, если имеется прямое соединение между соответствующими процессорами. С одной стороны, желательно, чтобы между процессорами было как можно меньше соединений, а с другой — обмен данными между процессорами предпочтительно производить с наименьшим числом посредников. Очевидно, эти два критерия противоречат друг другу. На теоретико-групповом языке диаметр графа вычислительной сети равен максимальной длине минимальных слов соответствующей графу группы.

ЛИТЕРАТУРА

1. Кузнецов А. А., Антамошкин А. Н., Шлёпкин А. К. Моделирование периодических групп // Системы управления и информационные технологии. 2008. № 2. С. 4–8.
2. Halt D., Eick B., and O'Brien E. Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005.

УДК 519.6

СТРУКТУРНЫЕ СВОЙСТВА ПРИМИТИВНЫХ НАБОРОВ НАТУРАЛЬНЫХ ЧИСЕЛ

С. Н. Кяжин, В. М. Фомичев

При исследовании перемешивающих свойств композиции преобразований конечно-го множества возникает задача распознавания примитивности квадратной неотрицательной матрицы M и определения её экспонента $[1, 2]$, то есть наименьшего натурального числа γ , при котором $M^\gamma > 0$.

При изучении указанных свойств матрица $M = (m_{ij})$ обладает ровно теми же свойствами, что и её носитель, то есть матрица $\nu(M) = (\nu m_{ij})$, где

$$\nu m_{ij} = \begin{cases} 1, & \text{если } m_{ij} > 0, \\ 0, & \text{если } m_{ij} = 0. \end{cases}$$

Вместо матрицы M можно равносильным образом исследовать примитивность и экспонент орграфа Γ , матрица смежности вершин которого совпадает с $\nu(M)$. Заметим, что множество 0,1-матриц порядка n образует полугруппу G_n относительно операции $*$, где $A * B = \nu(AB)$.

Критерий примитивности орграфа определяется длинами его простых контуров [1]. Если $C_1, \dots, C_k$ — все простые контуры орграфа Γ длин $l_1, \dots, l_k$ соответственно, то орграф Γ примитивный, если и только если наибольший общий делитель $\gcd(l_1, \dots, l_k) = 1$. Таким образом, один из способов распознавания примитивности