Высотой примитивной матрицы A (обозначается $\mathrm{h}(A)$) называется расстояние по Хэммингу между A и ближайшей минимальной примитивной матрицей $M \in P_{\min}(n)$:

$$\mathrm{h}(a) = \min_{M \in P_{\min}(n)} \mathrm{d}(A, M).$$

Величина $\mathrm{h}(A)$ является определённой мерой избыточности при построении связей между элементами входа и выхода преобразований информации.

Алгоритм оценивания $\mathbf{h}(A)$ (метод координатного спуска):

1) последовательно просматривая элементы матрицы A, находим единицы;
2) заменяем найденный единичный элемент в матрице A нулевым и для полученной матрицы A' выполняем:
   - проверяем в A' наличие нулевых строк и столбцов; если таковые есть, возвращаемся к выполнению п. 2 для следующей единицы матрицы A;
   - матрицу A' без нулевых строк и столбцов проверяем на примитивность;
   - если матрица A' не примитивная, возвращаемся к матрице A, восстанавливаем замененную единицу и выполняем п. 2 для следующей единицы матрицы A;
   - примитивную матрицу A' проверяем на минимальность;
   - если A' минимальная, то определяем m — число единиц, заменённых нулями;
   - если A' не минимальная, то переходим к выполнению п. 1 для матрицы A'.

На выходе алгоритма получим минимальную примитивную матрицу M, где

$$\mathrm{h}(A) \leqslant \mathrm{d}(A, M) = m.$$

Сложность алгоритма полиномиальная. Пусть $||A|| = k$, где $n < k \leqslant n^2$ для примитивной матрицы A. Тогда вычислительная сложность алгоритма в битовых операциях в худшем случае не превышает величины $\mathrm{O}(k^2 n^3 \log n)$. Объём памяти требуется порядка $\mathrm{O}(n^2)$ битов. Данный метод можно использовать для поиска минимальных матриц, близких к перемешивающим матрицам раундовых подстановок блочных шифров (DES, ГОСТ 28147-89 и др.).

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.

УДК 519.1:511.2

ЧИСЛА ЭЙЛЕРА НА МНОЖЕСТВАХ ПЕРЕСТАНОВОК И АНАЛОГИ ТЕОРЕМЫ ВИЛЬСОНА

Л. Н. Бондаренко, М. Л. Шарапова

Определяются числа Эйлера на множествах перестановок и с их помощью доказываются аналоги теоремы Вильсона для чисел стандартных полных отображений и чисел стандартных сильных полных отображений.

Ключевые слова: *перестановка, числа Эйлера, полные отображения, теорема Вильсона.*

На симметрической группе S_{n-1} статистика $\mathrm{des}(\sigma) = |\{i{\in}[n{-}1] : \sigma_i{>}\sigma_{i+1}, \sigma_n{=}0\}|$ при фиксированном $n \geqslant 2$ описывает число спусков перестановки $\sigma{=}\sigma_1 \ldots \sigma_{n-1}{\in}S_{n-1}$ над алфавитом $[n{-}1]{=}\{1, \ldots, n{-}1\}$. На множестве перестановок $U \subseteq S_{n-1}$ определим производящий многочлен Эйлера $\sum\limits_{\sigma\in U} t^{\mathrm{des}(\sigma)}$, а его коэффициенты назовём числами Эйлера на U. В частности, этот многочлен на S_{n-1} совпадает с многочленом Эйлера $A_{n-1}(t){=}\sum\limits_{k=1}^{n-1} A_{n-1,k}\, t^k$ степени $n{-}1$, а $A_{n-1,k} = |\{\sigma{\in}S_{n-1} : \mathrm{des}(\sigma) = k\}|$ [1].

Для простого числа p имеем $A_{p-1}(1) = |S_{p-1}| = (p{-}1)! \equiv -1 \pmod p$, что отвечает теореме Вильсона [2], а её усилением служит следующее утверждение.

Теорема 1. $A_{p-1,k} \equiv 1 \pmod p,\ k = 1, \ldots, p{-}1.$

Теорему 1 можно доказать с помощью формул для чисел Эйлера $A_{p-1,k}$, но интереснее получить её прямое доказательство на основе свойств перестановок $\sigma{\in}S_{n-1}$, что позволяет также найти аналоги теоремы Вильсона для чисел, связанных с трудными перечислительными проблемами полных отображений.

Определим биекцию $\mathbf{c} : S_{n-1} \to S_{n-1}$ с помощью равенств $\mathbf{c}\sigma_i{=}n - \sigma_i$, $i{\in}[n{-}1]$, для символов $\sigma{\in}S_{n-1}$, а дополнение к σ обозначим $\overline{\sigma}{=}\mathbf{c}\sigma$.

В криптографии сложение перестановок $\sigma{\in}S_{n-1}$ часто выполняется посимвольно по $\bmod n$, т. е. на аддитивной группе $\mathbb{Z}_n$, отождествляемой с $\{0, 1, \ldots, n-1\}$, причём это переносится и на умножение $\sigma{\in}S_{n-1}$ на целое число. Будем также использовать формулу $\mathrm{des}(\sigma){=}n^{-1}\sum\limits_{i=0}^{n-1}(\sigma_{i+1}{-}\sigma_i)$, в которой разности берутся по $\bmod n$, а $\sigma_0{=}\sigma_n{=}0$.

Непосредственно из определений следует, что $\mathbf{c}$ есть инволюция, а $\sigma{+}\overline{\sigma} = 0$, причём элементарное равенство $\mathrm{des}(\sigma) + \mathrm{des}(\overline{\sigma}) = n$ влечёт соотношение $t^n A_{n-1}(t^{-1}) = A_{n-1}(t)$.

Определение 1. Перестановки $\sigma, \widetilde{\sigma} \in S_{n-1}$ назовём сопряжёнными относительно $\overline{\varepsilon} \in S_{n-1}$, если $\sigma + \widetilde{\sigma} = \overline{\varepsilon}$, а $\varepsilon \in S_{n-1}$ — единичная перестановка (сопряжённость можно рассматривать относительно любой перестановки $\tau \in S_{n-1}$).

Все $\sigma \in S_{n-1}$, сопряжённые относительно $\varepsilon \in S_{n-1}$, задают множество $CM(\mathbb{Z}_n)$ всех стандартных полных отображений [3], а $|CM(\mathbb{Z}_n)| = |\overline{CM}(\mathbb{Z}_n)|$, $\overline{CM}(\mathbb{Z}_n)$ — множество всех $\sigma \in S_{n-1}$ из определения 1. Множество всех стандартных сильных полных отображений $SCM(\mathbb{Z}_n) = CM(\mathbb{Z}_n) \cap \overline{CM}(\mathbb{Z}_n)$, $|CM(\mathbb{Z}_n)| = 0$ при чётном n и $|SCM(\mathbb{Z}_n)| = 0$ также и при n, кратном трём, а задачи вычисления чисел $|CM(\mathbb{Z}_n)|$ и $|SCM(\mathbb{Z}_n)|$ являются $\#P$-полными [3] ($|CM(\mathbb{Z}_n)|$ при нечётном $n = 1, 3, \ldots, 25$ приведены в [4]).

Свойства чисел Эйлера из теоремы 1 наследуются числами Эйлера $\widetilde{A}_{n-1,k}$ на $CM(\mathbb{Z}_n)$, $\widehat{A}_{n-1,k}$ на $SCM(\mathbb{Z}_n)$ и приводят к аналогам теоремы Вильсона.

Теорема 2. $\widetilde{A}_{p-1,k} \equiv 1 \pmod p,\ k = 1, \ldots, p-2;\ \widetilde{A}_{p-1,p-1} = 0$, что влечёт $|CM(\mathbb{Z}_p)| \equiv -2 \pmod p$.

Теорема 3. $\widehat{A}_{p-1,1} = 0;\ \widehat{A}_{p-1,k} \equiv 1 \pmod p,\ k = 2, \ldots, p-2;\ \widehat{A}_{p-1,p-1} = 0$, что влечёт $|SCM(\mathbb{Z}_p)| \equiv -3 \pmod p$.

Доказательство теорем базируется на следующих вспомогательных утверждениях.

Лемма 1. Пусть $R_n = \{r\varepsilon : r \in [n{-}1], (r, n) = 1, \varepsilon \in S_{n-1}\}$ отвечает приведённой системе вычетов по $\bmod n$. Тогда $\mathrm{des}(r\varepsilon) = r$, а $|R_n| = \varphi(n)$, где при $n = \prod\limits_{p|n} p^{\mathrm{ord}_p(n)}$, $n > 1$, функция Эйлера $\varphi(n) = n\prod\limits_{p|n}(1 - p^{-1})$.

Лемма 1 следует из свойств des, а её применение при нечётном $n > 1$ с определением 1 даёт $|(R_n \cap \overline{CM}(\mathbb{Z}_n))| = n\prod\limits_{p|n}(1-2p^{-1})$ и $|(R_n \cap SCM(\mathbb{Z}_n))| = n\prod\limits_{p|n}(1-3p^{-1})$.

Лемма 2. Если $\sigma \in \overline{CM}(\mathbb{Z}_n)$, то $\mathrm{des}(\sigma) + \mathrm{des}(\widetilde{\sigma}) = n-1$.

Применение формулы вычисления статистики des к перестановкам из определения 1 даёт требуемое. Так как $\deg \widetilde{A}_{n-1}(t) = n-2$, то по лемме 2 имеем $t^{n-1}\widetilde{A}_{n-1}(t^{-1}) = \widetilde{A}_{n-1}(t)$, а также $\deg \widehat{A}_{n-1}(t) = n-2$, $\widehat{A}_{n-1,1} = 0$ и $t^n\widehat{A}_{n-1}(t^{-1}) = \widehat{A}_{n-1}(t)$.

Определение 2. $\tau = \tau_1 \dots \tau_{n-1} \in S_{n-1}$, $\tau = \mathbf{d}\sigma$ назовём смещением $\sigma \in S_{n-1}$, если биекция $\mathbf{d} : S_{n-1} \to S_{n-1}$ задана выражениями $\tau_i = \sigma_{i+1} - \sigma_i \pmod n$, $i = 1, \dots, n-2$, и $\tau_{n-1} = n - \sigma_1$, а порядком $d = d(\sigma)$ назовём наименьшее $k \in \mathbb{Z}^+$, для которого $\mathbf{d}^k\sigma = \sigma$.

Лемма 3. Если $\sigma \in S_{n-1}$, то $\mathrm{des}(\mathbf{d}\sigma) = \mathrm{des}(\sigma)$ и $d|n$.

Равенство $\mathrm{des}(\mathbf{d}\sigma) = \mathrm{des}(\sigma)$ получается из свойств des, а делимость $d|n$ следует из определения 2, так как повторное применение $\mathbf{d}$ разбивает S_{n-1} на классы эквивалентности (так, $\mathbf{d}r\varepsilon = r\varepsilon$, $r\varepsilon \in R_n$, т. е. $d = 1$). При $n > 4$ в словах $\mathbf{d}^k\sigma \in S_{n-1}$, $k = 0, \dots, d-1$, имеется $n/d - 1$ неподвижных символов σ_i, кратных d, с индексом i, кратным d.

Теоремы 1–3 доказываются с помощью лемм 1, 2 и леммы 3, справедливой также на $\overline{CM}(\mathbb{Z}_n)$ и $SCM(\mathbb{Z}_n)$, причём применяемый метод дополнительно даёт следующие сравнения: $|CM(\mathbb{Z}_n)| \equiv 1 \pmod 2$ при нечётном n и $|SCM(\mathbb{Z}_n)| \equiv 0 \pmod 2$ при $n > 1$.

ЛИТЕРАТУРА

1. *Стенли Р.* Перечислительная комбинаторика. Т. 1. М.: Мир, 1990.
2. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.
3. *Hsiang J., Hsu D. F., and Shieh Y. P.* On the hardness of counting problems of complete mappings // Discr. Math. 2004. V. 277. P. 87–100.
4. `http://oeis.org/A003111` — Sloane N. J. A. The on-line encyclopedia of integer sequences.

УДК 519.7

О НЕКОТОРЫХ ОТКРЫТЫХ ВОПРОСАХ В ОБЛАСТИ APN-ФУНКЦИЙ

В. А. Виткуп

Приведены открытые вопросы в области APN-функций, связанные с их построением. Перечислены некоторые известные результаты в данном направлении. Доказано необходимое и достаточное условие того, что сумма двух APN-функций является APN-функцией.

Ключевые слова: *векторная булева функция, APN-функция.*

Работа К. Ньюберг [1] положила начало новому направлению в исследовании векторных булевых функций — изучению совершенно и почти совершенно нелинейных векторных булевых функций, обладающих наилучшей стойкостью к дифференциальному криптоанализу.

Векторная булева функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называется *APN-функцией* (Almost Perfect Nonlinear), если уравнение $F(x \oplus a) \oplus F(x) = b$ имеет не более двух решений для любых $a \in \mathbb{F}_2^n \setminus \{0\}$, $b \in \mathbb{F}_2^n$. В настоящее время APN-функции активно изучаются, но