Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

РАЗРЯДНО-ИНЪЕКТИВНЫЕ ПРЕОБРАЗОВАНИЯ МОДУЛЯ НАД КОЛЬЦОМ ГАЛУА[1]

А. В. Аборнев

Предлагается новый способ построения большого класса нелинейных подстановок над кольцом Галуа.

Ключевые слова: *разрядно-инъективная матрица, РИ-матрица, подстановка, кольцо Галуа.*

Предлагается способ построения нелинейных подстановок h на модуле ${}_RR^m$, $m \geqslant 1$, над кольцом Галуа $R = \mathrm{GR}(q^2, p^2)$, $q = p^r$, представимых с помощью линейных разрядно-инъективных преобразований этого модуля и соответствующих p-адическому разрядному множеству $P = \Gamma(R) = \{a \in R : a^q = a\}$ кольца R.

Каждый элемент $a \in R$ однозначно представляется в виде [1]

$$a = a_0 + pa_1,\ a_s = \gamma_s(a) \in P,\ s \in \{0, 1\}.$$

Здесь $\gamma_s \colon R \to P$ — *разрядные функции в разрядном множестве* P. Тогда $(P, \oplus, \cdot)$ — поле с операцией $x \oplus y = \gamma_0(x+y)$. Для матриц $A \in R_{m,n}$ также справедливо разложение $A = A_0 + pA_1$, $A_s = \gamma_s(A) \in P_{m,n}$, $s \in \{0, 1\}$.

А. А. Нечаевым предложен следующий способ построения подстановок. Назовём матрицу K размеров $m \times n$ над кольцом Галуа R *разрядно-инъективной* (*РИ-матрицей*), если любая ненулевая строка $\mathbf{a} \in R^m$ однозначно восстанавливается по строке $\gamma_1(\mathbf{a}K) \in P^n$.

Теорема 1. Пусть $G \in P^*_{m,m}$, $U \in R^*_{m,m}$. Тогда матрица

$$K = U(E \mid E + pG)$$

является разрядно-инъективной и отображение $h : R^m \to R^m$, действующее на произвольной строке $\mathbf{x} \in R^m$ по правилу

$$h(\mathbf{x}) = \mathbf{z}, \quad \text{где } \mathbf{z} = \mathbf{z_1} + p\mathbf{z_2} \in R^m, \ \ (\mathbf{z_1} \mid \mathbf{z_2}) = \gamma_1(\mathbf{x}K) \in P^{2m}, \tag{1}$$

является подстановкой.

Для множества подстановок вида $(\Sigma h)^k$, где Σ — регулярное представление группы $(R^m, +)$ в симметрической группе $S(R^m)$, изучаются следующие параметры: показатель 2-транзитивности $d_2(\Sigma h)$ (минимальное k, при котором 2-транзитивно множество $(\Sigma h)^k$) и порождаемая группа [2, 3]. Получены следующие результаты.

[1]Работа выполнена при поддержке Академии криптографии РФ.

Теорема 2. Для любой подстановки h вида (1) верно неравенство $d_2(\Sigma h) \geqslant 4$.

Теорема 3. Пусть $R = \mathrm{GR}(q^2, p^2), m = 1, p > 2$. Тогда если разрядное множество $P = \Gamma(R)$ удовлетворяет условию

$$\{\gamma_1(a+e) \ominus \gamma_1(b+e) : a, b \in P\} = P,$$

то для любой подстановки h вида (1) справедливо равенство $d_2(\Sigma h) = 4$.

Если при этом $R = \mathbb{Z}_{p^2}$, то группа $\langle \Sigma h \rangle$ содержит знакопеременную группу A_{p^2}.

Теорема 4. Пусть $R = \mathrm{GR}(q^2, 4), m > 1$. Тогда если все миноры матрицы U_0 в (1) ненулевые, то для подстановки h из (1) справедливо равенство $d_2(\Sigma h) = 4$.

Автор выражает глубокую благодарность профессору А. А. Нечаеву за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и Логика. 1995. Т. 34. № 2. С. 169–189.
2. *Глухов М. М.* О 2-транзитивности произведения регулярных групп подстановок // Труды по дискретной математике. М.: Физико-математическая литература, 2000. С. 37–52.
3. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т 2. М.: Гелиос АРВ, 2003. 416 с.

УДК 519.1

СВОЙСТВА СТАТИСТИКИ VAR НА ГРУППЕ ПЕРЕСТАНОВОК[1]

Л. Н. Бондаренко

Рассматриваются некоторые свойства статистики var, определяющей число различных символов слова, полученного поэлементным сложением по $\bmod n$ перестановки степени n с фиксированной перестановкой — ключом.

Ключевые слова: *перестановка, статистика, производящий многочлен, перманент, циркулянт.*

Ряд статистик на симметрической группе S_n перестановок σ, где $\sigma = \sigma_1 \dots \sigma_n$ — слово над алфавитом $\{1, \dots, n\}$, рассматривался в [1].

В криптографии применяется биекция $\mathrm{vp} : \sigma \mapsto \tau$ перестановки $\sigma \in S_n$ на слово $\tau = \tau_1 \dots \tau_n \in T_n$, определяемая фиксированным ключом $\varkappa = \varkappa_1 \dots \varkappa_n \in S_n$. Она отображает $\sigma \in S_n$ на слово $\tau \in T_n$ по правилу $\tau = \sigma \oplus \varkappa$, где $\tau_i = \sigma_i + \varkappa_i \,(\bmod n)$, $i = 1, \dots, n$, а τ_i — наименьший положительный вычет, и индуцирует статистику $\mathrm{var}(\sigma, \varkappa) = \mathrm{card}\{\tau_1, \dots, \tau_n\}$ — число различных символов слова $\tau = \mathrm{vp}(\sigma)$.

Так как для любого ключа $\varkappa \in S_n$ статистика var имеет производящий многочлен

$$V_n(t) = \sum_{k=1}^{n} V_{n,k} t^k = \sum_{\sigma \in S_n} t^{\mathrm{var}(\sigma, \varkappa)},$$

то в качестве ключа удобно использовать перестановку $\nu = \nu_1 \dots \nu_n \in S_n$, где $\nu_i = n - i + 1$, $i = 1, \dots, n$. Многочлен $V_n(t)$ не изменяется и при замене перестановок σ на обратные $\sigma^{-1} \in S_n$.

По определению статистики var многочлен $V_n(t)$ имеет коэффициенты $V_{n,k} \geqslant 0$, а их нахождение уже при сравнительно небольших n является трудной задачей. Вычисление даёт $V_1(t) = V_2(t)/2 = t$, $V_3(t)/3 = t + t^3$, $V_4(t)/4 = t + t^2 + 4t^3$, $V_5(t)/5 = t + 20t^3 + 3t^5$.

[1] Работа поддержана грантом РФФИ, проект № 11-01-00212а.