

Н. В. Ф о м и ч е в (Москва, МИФИ). **Признаки π -конгруэнтности в группах подстановок.**

Наличие у преобразований свойства совершенности [2] затрудняет применение методов типа последовательного опробования. Множество таких несовершенных преобразований, как треугольные или треугольно-ступенчатые, образует наследственный признак в группах подстановок [3] и полугруппах преобразований множества X^n , где X — конечное множество. В работе, представленной данным сообщением, изучено обобщение свойства треугольно-ступенчатости.

Пусть $\text{Part}(X)$ — множество всех разбиений множества X на непустые блоки и $\pi = (X_0, \dots, X_{m-1}) \in \text{Part}(X)$, где $X_0, \dots, X_{m-1}$ — блоки разбиения.

Пусть подстановка g множества X имеет цикловую структуру $C(g) = (l_1[q_1], \dots, l_m[q_m])$, где $l_i[q_i]$ при $i = 1, \dots, m$ означает, что в g имеется q_i циклов длины l_i . Подстановка g есть унарная операция на X . Относительно g некоторые разбиения из $\text{Part}(X)$ являются конгруэнциями. Принадлежность элементов x и x' множества X одному блоку разбиения π обозначим $x \stackrel{\pi}{\cong} x'$. Разбиение π назовем g -конгруэнцией, а подстановку g π -конгруэнтной, если из $x \stackrel{\pi}{\cong} x'$ следует $g(x) \stackrel{\pi}{\cong} g(x')$.

Актуальной задачей криптографического анализа является изучение таких несовершенных преобразований в наследственных признаках полугрупп, как треугольные и треугольно-ступенчатые преобразования. Треугольно-ступенчатые преобразования являются π -конгруэнтными, где разбиение π имеет специальный вид.

Укажем условия, при которых подстановка g является π -конгруэнтной. Пусть Ω — конечное множество, Ω^* — множество слов в алфавите Ω , $l \in N$, и слово $\omega = (\omega_0, \omega_1, \dots, \omega_{l-1}) \in \Omega^l$. Длиной периода слова ω назовем такой наименьший делитель τ числа l , что $\tau < l$ и $\omega_i = \omega_{i+\tau}$ для $i = 0, 1, \dots, l - \tau - 1$, если такой существует. В противном случае длиной периода слова ω полагается l . Слова ω и ω' из Ω^* циклически эквивалентны, если они совпадают с точностью до циклического сдвига. Будем говорить, что слово ω имеет бесповторный период, если период слова ω есть бесповторная выборка из алфавита Ω . Слова ω и ω' называются совместимыми, если они имеют такие бесповторные периоды, которые либо циклически эквивалентны, либо не содержат общих элементов. Множество из двух и более слов совместимо, если любые два слова множества совместимы, а множество из одного слова с бесповторным периодом полагается совместимым.

Пусть $\pi = (X_0, \dots, X_{m-1}) \in \text{Part}(X)$ и g_c — разбиение $\pi_c(g) = (C_1, \dots, C_r)$, где длина цикла C_j равна l_j , $j = 1, \dots, r$. Рассмотрим отображение $\omega_\pi: X \rightarrow Z/m$, где $\omega_\pi(x) = i$, $x \in X_i$. Отображение ω_π индуцирует отображение $\omega_\pi^*: X^* \rightarrow Z/m^*$, где $\omega_\pi^*(x_1, x_2, \dots) = (\omega_\pi(x_1), \omega_\pi(x_2), \dots)$. Таким образом, $\omega_\pi^*(C_j)$ есть слово длины l_j в алфавите Z/m , $j \in \{1, \dots, r\}$.

Теорема. Подстановка g является π -конгруэнтной тогда и только тогда, когда совместимо множество слов $\omega_\pi^*(C_j)$, $j = 1, \dots, r$.

Данный критерий позволяет получить ряд необходимых условий π -конгруэнтности подстановки g , выраженных через характеристики цикловой структуры подстановки g и блочной структуры разбиения π . Проверка невыполнения этих условий для многих подстановок и разбиений требует существенно меньше вычислений, чем проверка условий критерия.

Пусть $R(i_1, \dots, i_s) = \{B_{\alpha_1, \dots, \alpha_s}^{i_1, \dots, i_s}, (\alpha_1, \dots, \alpha_s) \in X^s\} \in \text{Part}(X^n)$ есть разбиение, где $B_{\alpha_1, \dots, \alpha_s}^{i_1, \dots, i_s}$ — множество всех наборов из X^n , у которых значение компонент с номерами $i_1, \dots, i_s$ фиксированно и равно $\alpha_1, \dots, \alpha_s$, соответственно.

Обозначим $T_\Delta(s, n)$ множество преобразований пространства X^n , у которых координатные функции $f_1, \dots, f_s$ зависят от $x_1, \dots, x_s$, а $f_{s+1}, \dots, f_n$ — от $x_1, \dots, x_n$. Треугольно-ступенчатые преобразования с несколькими ступенями принадлежат пересечению нескольких множеств вида $T_\Delta(s, n)$ с различными значениями s .

Утверждение. Подстановка g множества X^n принадлежит $T_\Delta(s, n)$ тогда

и только тогда, когда g является $R(1, \dots, s)$ -конгруэнтной.

СПИСОК ЛИТЕРАТУРЫ

1. Биркгоф Г. Теория решеток. М.: Наука, 1984, 567 с.
2. Фомичев В. М. Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003, 400 с.
3. Фомичев В. М. Исследование признаков в конечных группах и в группах подстановок. — В сб.: Математические вопросы кибернетики. В. 14. М.: Физматлит, 2005, с. 161–260.