

Можно доказать утверждения, аналогичные утверждениям 2 и 3, которые показывают, какие подстановки из множеств $\Gamma_N(2q + t - 1)$, $\Gamma_N(2q + t)$ принадлежат произведению $\Gamma_N(q) \cdot \Gamma_N(q + t)$.

ЛИТЕРАТУРА

1. Пичкур А. Б. Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек // Прикладная дискретная математика. Приложение. 2011. № 4. С. 16–17.

УДК 519.7

О КОМБИНАТОРНЫХ СВОЙСТВАХ ГРУППЫ, ПОРОЖДЁННОЙ XL -СЛОЯМИ¹

Б. А. Погорелов, М. А. Пудовкина

Алгоритмы блочного шифрования реализуются итеративным применением более простых преобразований, которые должны обеспечивать свойства перемешивания, рассеивания и усложнения. Для получения данных свойств обычно используются слои преобразований трёх типов: наложение ключа (X -слой), преобразования над отдельными частями блока текста (слой s -боксов) и линейное преобразование (линейный слой, или L -слой). Блочные шифрсистемы с таким построением раундовых преобразований и побитным подмешиванием раундового ключа в каждом раунде называют XSL-сетями. Ряд линейных преобразований, используемых в линейном слое в алгоритмах шифрования и обеспечивающих хорошее рассеивание, являются приводимыми. Естественно, приводимыми являются и характеристические многочлены подстановочных матриц, используемых в SP-сетях. Это приводит к импримитивности подгруппы $C(g)$ аффинной группы $AGL_n(2)$, порождённой слоем наложения раундового ключа (т.е. всеми сдвигами) и приводимой невырожденной матрицей $g \in GL_n(2)$. В данной работе рассматриваются свойства графов орбиталов группы $C(g)$.

Пусть $\mathbb{N}$ — множество всех натуральных чисел; V_n — векторное пространство размерности n над $\text{GF}(2)$; $X^\times = X \setminus \{0\}$; $\tilde{g}$ — матрица линейного преобразования g в стандартном базисе $\varepsilon_0, \dots, \varepsilon_{n-1}$, где $\varepsilon_i = (0, \dots, 0, \underbrace{1, 0, \dots, 0}_i) \in V_n$, $i \in \{0, \dots, n-1\}$; GL_n —

полная линейная группа; $\chi_g(x)$ — характеристический многочлен линейного преобразования $g \in GL_n(2)$; $m_{\gamma,g}(x)$ — минимальный многочлен вектора $\gamma \in V_n^\times$ относительно преобразования g .

Напомним, что орбитами группы G , действующей на множестве X , называются орбиты группы G при её действии на множестве X^2 . Действие группы G на множестве X^2 задано как $(\alpha, \beta)^f = (\alpha^f, \beta^f)$ для всех $(\alpha, \beta) \in X^2$ и $f \in G$.

Лемма 1. Для произвольного преобразования $g \in GL_n$ и векторов $\alpha, \beta, \alpha', \beta' \in V_n$, $\alpha \neq \beta$, $\alpha' \neq \beta'$, тогда и только тогда $(\alpha', \beta') \in (\alpha, \beta)^{C(g)}$, когда $\alpha' \oplus \beta' \in (\alpha \oplus \beta)^{\langle g \rangle}$.

Таким образом, различными нетривиальными графами орбиталов группы $C(g)$ являются $\bar{\Gamma}_{(0, \gamma_1)}(g), \dots, \bar{\Gamma}_{(0, \gamma_{d-1})}(g)$, где $\gamma_1^{(g)}, \dots, \gamma_{d-1}^{(g)}$ — попарно различные орбиты группы $\langle g \rangle$ на $V_n^\times$. Среди графов орбиталов группы $C(g)$ могут встречаться изоморфные.

Существует тесная связь между строением характеристического многочлена $\chi_g(x)$ преобразования g , примитивностью (2-транзитивностью) и связностью графов орбиталов группы $C(g)$. Так, группа $C(g)$ примитивна тогда и только тогда, когда много-

¹Работа выполнена при поддержке гранта Президента РФ НШ № 6260.2012.10е

член $\chi_g(x)$ неприводим. Кроме того, группа $C(g)$ 2-транзитивна тогда и только тогда, когда многочлен $\chi_g(x)$ примитивен.

Утверждение 1. Для произвольных вектора $\gamma \in V_n^\times$, преобразования $g \in GL_n$ с характеристическим многочленом $\chi_g(x)$ граф $\bar{\Gamma}_{(0,\gamma)}(g)$ связан для всех векторов $\gamma \in V_n^\times$ тогда и только тогда, когда характеристический многочлен $\chi_g(x)$ неприводим.

Утверждение 2. Для вектора $\gamma \in V_n^\times$ граф $\bar{\Gamma}_{(0,\gamma)}(g)$ связан тогда и только тогда, когда $m_{\gamma,g}(x) = \chi_g(x)$. Если группа $C(g)$ примитивна, то все её графы орбиталов изоморфны.

В алгебраической теории графов наибольший интерес представляют следующие классы графов: вершинно-транзитивные, рёберно-транзитивные, дистанционно-регулярные, дистанционно-транзитивные [1].

Утверждение 3. Пусть $n \geq 2$, $i \in \{1, \dots, d-1\}$, $\bar{\Gamma}_{(0,\gamma_i)}(g)$ — нетривиальный связный граф диаметра $b \geq 2$. Тогда: а) $\bar{\Gamma}_{(0,\gamma_i)}(g)$ — рёберно-транзитивный граф; б) если $\gamma_i^{(g)}$ является базисом V_n , то граф $\bar{\Gamma}_{(0,\gamma_i)}(g)$ является дистанционно-транзитивным и $\text{Aut} \bar{\Gamma}_{(0,\gamma_i)}(g) \approx S_2 \uparrow S_n$.

Графом Хемминга на V_n будем называть граф с множеством вершин V_n и множеством рёбер $\{(\alpha, \beta) \in V_n^2 : \chi_n(\alpha, \beta) = 1\}$. Очевидно, что если граф изоморфен графу Хемминга, то его метрика изоморфна метрике Хемминга. Отметим, если множество $\gamma_i^{(g)}$ является базисом V_n , то граф $\bar{\Gamma}_{(0,\gamma_i)}(g)$ изоморфен графу Хемминга и является дистанционно-регулярным.

Теорема 1. Пусть $n \geq 2$, преобразование $g \in GL_n$ и вектор $\gamma \in V_n$ такие, что

$$m_{\gamma,g}(x) = x^{r(q-1)} \oplus x^{r(q-2)} \oplus \dots \oplus x^r \oplus 1 = \frac{(x^r)^q - 1}{x^r - 1},$$

где $rq = m = |\gamma^{(g)}|$. Граф $\bar{\Gamma}_{(0,\gamma)}(g)$ дистанционно-регулярный тогда и только тогда, когда выполняется одно из условий: а) $r = 1$; б) $r \geq 2$ и $q = 3$.

ЛИТЕРАТУРА

1. *Godsil C. and Royle G. Algebraic Graph Theory.* Springer Verlag, 2001.

УДК 519.14

О БУЛЕВЫХ ФУНКЦИЯХ, ПОЧТИ УРАВНОВЕШЕННЫХ В ГРАНЯХ¹

В. Н. Потапов

Обозначим через E^n множество упорядоченных двоичных наборов (вершин) длины n . Введём операцию $[x, y] = (x_1y_1, \dots, x_ny_n)$ для наборов $x, y \in E^n$. Количество единиц в наборе $y \in E^n$ называется *весом набора* и обозначается через $\text{wt}(y)$. Множество вершин чётного веса будем обозначать через E_0^n (нечётного — через E_1^n). *Гранью размерности* $(n - \text{wt}(y))$ называется множество $E_y^n(z) = \{x \in E^n : [x, y] = [z, y]\}$.

Пусть $S \subset E^n$; через χ^S будем обозначать характеристическую функцию множества S . Функция χ^S называется *корреляционно-иммунной порядка* $(n - m)$, если для любой грани $E_y^n(z)$ размерности m пересечения $E_y^n(z) \cap S$ имеют одинаковую мощность.

¹Работа выполнена при поддержке РФФИ (проекты 11-01-997, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0362).