

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

5–15

Аборнев А. В. Подстановки, индуцированные разрядно-инъективными преобразованиями модуля над кольцом Галуа // ПДМ. 2013. № 4(22). С. 5–15.

16–21

Карпов А. В. Перестановочные многочлены над примарными кольцами // ПДМ. 2013. № 4(22). С. 16–21.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

22–40

Девянин П. Н. Администрирование системы в рамках мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux // ПДМ. 2013. № 4(22). С. 22–40.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

41–46

Величко И. Г., Зинченко А. И. V-графы и их связь с задачами размещения фигур на плоскости // ПДМ. 2013. № 4(22). С. 41–46.

47–55

Гавриков А. В. Т-неприводимые расширения объединений некоторых типов орграфов // ПДМ. 2013. № 4(22). С. 47–55.

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

56–66

Быкова В. В. Об асимптотике решений рекуррентных соотношений специального вида и технике Кульмана — Люкхардта // ПДМ. 2013. № 4(22). С. 56–66.

67–72

Гоцуленко В. В. Комбинаторные числа для подсчёта разбиений конечных мультимножеств // ПДМ. 2013. № 4(22). С. 67–72.

73–81

Костюк Ю. Л. Задача коммивояжёра: улучшенная нижняя граница в методе ветвей и границ // ПДМ. 2013. № 4(22). С. 73–81.

82–95

Рыжов А. С. О реализации основных этапов блочного алгоритма Видемана — Копперсмита для двоичных систем линейных уравнений на вычислителях кластерного типа // ПДМ. 2013. № 4(22). С. 82–95.

96–102

Шангин Р. Э. Алгоритм точного решения дискретной задачи Вебера для простого цикла // ПДМ. 2013. № 4(22). С. 96–102.

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

103–113

Назаров М. Н. Моделирование роста ткани с учётом возможности внешнего воздействия на её форму // ПДМ. 2013. № 4(22). С. 103–113.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7

ПОДСТАНОВКИ, ИНДУЦИРОВАННЫЕ РАЗРЯДНО- ИНЪЕКТИВНЫМИ ПРЕОБРАЗОВАНИЯМИ МОДУЛЯ НАД КОЛЬЦОМ ГАЛУА

А. В. Аборнев

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: abconf.c@gmail.com

Для произвольного кольца Галуа $R = \text{GR}(q^2, p^2)$, $q = p^r$, построен большой класс $m \times 2m$ -матриц над R , называемых разрядно-инъективными (РИ-матрицами), которым соответствует нелинейная подстановка π на модуле R^m . В качестве криптографической характеристики таких подстановок изучаются свойства множества $\Sigma\pi$, где Σ — регулярное представление группы $(R^m, +)$ в симметрической группе $S(R^m)$. В случаях $R = \text{GR}(q^2, p^2)$, $p > 2$, $m = 1$ и $R = \text{GR}(q^2, 4)$, $m > 1$ описаны классы разрядно-инъективных матриц с минимально возможным показателем 2-транзитивности множества подстановок $\Sigma\pi$ равным 4. В случае $R = \mathbb{Z}_{p^2}$, $m = 1$ показано также, что группа, порождённая множеством $\Sigma\pi$, содержит знакопеременную группу подстановок.

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

Введение

Пусть $R = \text{GR}(q^2, p^2)$ — кольцо Галуа с полем вычетов $\bar{R} = R/pR = \text{GF}(q)$, $q = p^r$. В частности, при $r = 1$ имеем $R = \mathbb{Z}_{p^2}$. Подмножество $P = \Gamma(R) = \{a \in R : a^q = a\}$ называют *p-адическим координатным множеством* или *координатным множеством Тейхмюллера* кольца R . Будем называть его также *разрядным* множеством.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1, \quad a_i \in P, \quad i \in \{0, 1\},$$

называемом *p-адическим разложением элемента a*. Отображения

$$\gamma_i: R \rightarrow P, \quad \gamma_i(a) = a_i, \quad i \in \{0, 1\},$$

будем называть *разрядными функциями в разрядном множестве P*, а элементы $a_i = \gamma_i(a)$ — *p-адическими разрядами элемента a*. Алгебра (P, \oplus, \cdot) с операцией сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in P$, является полем.

Понятия *p-адического разложения* и значения функции γ_i естественным образом (поэлементно) распространяются на матрицы $A \in R_{m \times m}$, при этом используется обозначение $A_i = \gamma_i(A)$. Так же естественным образом операции \oplus и \cdot распространяются на матрицы и векторы над полем P , при этом операция умножения матриц обозначается через \odot .