Таким образом, пробегая по всем биективным функциям, можно предложенным способом получить все транзитивные функции.

Итак, для генерации последовательностей больших периодов биективные дифференцируемые по модулю p^n функции могут быть использованы как сопрягающие для транзитивных функций. Представляют интерес также статистические свойства таких последовательностей. Поэтому группа дифференцируемых по модулю p^n функций заслуживает внимания. Однако пока не описано представление, позволяющее эффективно вычислять данные функции, их реальное использование не практично. Поэтому в дальнейшем стоит задача поиска эффективного представления для функций из класса дифференцируемых по модулю p^n функций или из его подклассов. Предполагается, что данное представление можно получить для этих функций по модулю 2^n, используя элементарные операции, такие, как AND, XOR, RIGHT_SHIFT.

ЛИТЕРАТУРА

1. *Ивачев А. С.* Исследование класса дифференцируемых функций в кольцах классов вычетов по примарному модулю // Прикладная дискретная математика. Приложение. 2014. № 7. С. 19–22.

УДК 512.543.72 DOI 10.17223/2226308X/8/11

ОБРАЩЕНИЕ ДИФФЕРЕНЦИРУЕМЫХ ПЕРЕСТАНОВОК НАД ГРУППОЙ

А. В. Карпов

Вводится понятие дифференцируемой функции над группой с нормальным рядом, обобщающее понятие полиномиальной функции. Для абелевых, нильпотентных и разрешимых групп доказывается формула для нахождения обратной в смысле композиции перестановки к заданной дифференцируемой перестановке.

Ключевые слова: *перестановка, полином над группой, дифференцируемая функция.*

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Через Ψ обозначим множество функций, отображающих $\mathbb{G}$ в себя, которые действуют на факторах H_k/H_{k+1} ($k \in \{0, \ldots, n-1\}$) как эндоморфизмы.

Определение 1. Функция $f : \mathbb{G} \to \mathbb{G}$ называется *дифференцируемой* в точке $a \in \mathbb{G}$ относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, если существует функция $\psi_{f,a} \in \Psi$, такая, что для любого члена нормального ряда H_k и любого элемента $h \in H_k$ выполняется равенство

$$f(a+h) \equiv f(a) + \psi_{f,a}(h) \pmod{H_{k+1}}.$$

Функция называется дифференцируемой, если она дифференцируема в каждой точке группы $\mathbb{G}$. Функция $\psi_{f,a}$ называется производной функции f в точке a.

В качестве примеров дифференцируемых функций можно привести следующие: полиномиальные функции над примарным кольцом вычетов $\mathbb{Z}_{p^n}$, где в качестве $\mathbb{G}$ выступает $(\mathbb{Z}_{p^n}, +)$, $H_k = p^k\mathbb{Z}_{p^n}$, $\psi_{f,a} = f'(a)$ и $\psi_{f,a}(h) = h * f'(a)$; полиномиальные вектор-функции, т. е. системы из m полиномов от m переменных с коэффициентами из $\mathbb{Z}_{p^n}$, где $\mathbb{G} = (\mathbb{Z}_{p^n}^m, +)$, $\psi_{f,a}$ совпадает с матрицей частных производных, вычисленных в точке a;

полиномы над разрешимой группой вида $u(x) = g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \dots g_k x^{\varepsilon_1}$ с $\psi_{u,a}(h) = h^{\sum\limits_{i=1}^{k} \varepsilon_i}$ в случае центрального ряда.

Следующая теорема обобщает критерий биективности из [1] на случай дифференцируемой функции.

Теорема 1. Пусть $u : \mathbb{G} \to \mathbb{G}$ — дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = e$ функция. Тогда u биективна на $\mathbb{G}$, если и только если выполняются следующие два условия:

1) u биективна по модулю H_1;
2) для всех $x \in \mathbb{G}$ производная $\psi_{u,x}$ является автоморфизмом на всех факторах ряда.

Естественно называть дифференцируемую биективную функцию *дифференцируемой перестановкой*. Будем говорить, что v — *обратная* (*по модулю* H_k) к u дифференцируемая перестановка, если для всех $x \in \mathbb{G}$ выполняется

$$v(u(x)) = x \quad (v(u(x)) \equiv x \pmod{H_k}).$$

В работе решается задача нахождения обратной дифференцируемой перестановки к заданной. Нормальный ряд в группе $\mathbb{G}$ задаёт структуру, аналогичную последовательности модулей $p,\ p^2, \dots, p^n$ в случае примарного кольца, что даёт возможность применять схожие с [2] методы обращения перестановок. Основная идея заключается в сведении задачи обращения над всей группой к обращению над «маленькой» фактор-группой с последующим подъёмом решения. Это удаётся сделать, если группа $\mathbb{G}$ разрешима и известно промежуточное решение по модулю некоторой подгруппы из нормального ряда.

Теорема 2. Пусть u — перестановка элементов разрешимой группы $\mathbb{G}$, дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = e$, v_k — обратная перестановка к u по модулю H_k. Тогда обратной к u по модулю H_{k+1} является перестановка

$$v_{k+1}(x) = v_k(x) - \psi^{-1}_{u,v_k(x)}(-x + u(v_k(x))),$$

где $\psi^{-1}_{u,v_k(x)}$ — обратный к $\psi_{u,v_k(x)}$ автоморфизм в $\mathrm{Aut}(H_k/H_{k+1})$. Если дополнительно $\psi_{u,v_k(x)}$ и $\psi_{v_k,x}$ — взаимно обратные автоморфизмы фактора H_k/H_{k+1}, то

$$v_{k+1}(x) = v_k(x) - v_k(u(v_k(x))) + v_k(x).$$

Возможно также обращение дифференцируемой перестановки, если известно обращение другой дифференцируемой перестановки, отличающейся от заданной на определённую добавку.

Теорема 3. Пусть u и v — взаимно обратные по модулю H_k дифференцируемые перестановки и для всех $x \in \mathbb{G}$ дифференцируемая функция u_0 удовлетворяет следующим условиям:

1) $u_0(x) \in H_{k-1}$;
2) $\psi_{u_0,x} : H_{k-1} \to H_k$.

Тогда обратной к $u^*(x) = u(x) + u_0(x)$ по модулю H_k является перестановка $v^*(x) = v(x) - \psi_{v,x}(u_0(v(x)))$.

В качестве примера рассмотрим $\mathbb{G} = T_3(\mathbb{Z}_7)$ с разрешимым рядом $\mathbb{G} = T_3(\mathbb{Z}_7) \trianglerighteq \trianglerighteq UT_3(\mathbb{Z}_7) \trianglerighteq UT_3^2(\mathbb{Z}_7) \trianglerighteq UT_3^3(\mathbb{Z}_7) = e$, где $UT_3^i(\mathbb{Z}_7)$ — подгруппа, состоящая из унитреугольных матриц с $(i-1)$ нулевыми диагоналями над главной.

Введём функцию $u(x) = \begin{pmatrix} 2 & 4 & 3 \\ 0 & 3 & 5 \\ 0 & 0 & 6 \end{pmatrix} x \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} x^{-1} \begin{pmatrix} 1 & 6 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x$. Сначала обратим $u(x)$ в первом факторе $T_3(\mathbb{Z}_7)/UT_4(\mathbb{Z}_7) \simeq \mathbb{Z}_7^* \otimes \mathbb{Z}_7^* \otimes \mathbb{Z}_7^*$:

$$v_1(x) = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 6 \end{pmatrix} x,\ v_1\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & \mathbf{0} & \mathbf{4} \\ 0 & 2 & \mathbf{6} \\ 0 & 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} (\bmod\ UT_3(\mathbb{Z}_7)).$$

Так как производная $\psi_{u,x}$ — тождественный автоморфизм, по теореме 2 получаем

$$v_2(x) = v_1(x)(x^{-1}u(v_1(x)))^{-1},\quad v_3 = v_2(x)(x^{-1}u(v_2(x)))^{-1},$$

$$v_2\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & \mathbf{6} \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} (\bmod\ UT_3^2(\mathbb{Z}_7)),$$

$$v_3\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Умножим справа $u(x)$ на добавку $u_0(x)$, удовлетворяющую условиям 1 и 2 теоремы 3:

$$u_0(x) = x^{-1} \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} x,\quad u^*(x) = u(x)u_0(x).$$

Построенная ранее $v_3(x)$ не обращает $u^*(x)$:

$$v_3\left(u^*\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & \mathbf{5} \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Построим обратную к $u^*(x)$ функцию:

$$v^*(x) = v_3(x)(\psi_{v_3,x}(u_0(v_3(x))))^{-1} = v_3(x)(u_0(v_3(x)))^{-1},$$

$$v^*\left(u^*\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Таким образом, задача обращения дифференцируемой перестановки над разрешимой группой сводится к обращению над фактор-группой с последующим подъёмом решения. Если известна обратная перестановка по модулю H_k, то можно строить другие пары взаимно обратных перестановок по модулю H_k, используя теорему 3.

ЛИТЕРАТУРА

1. *Anashin V. S.* Noncommutative algebraic dynamics: ergodic theory for profinite groups // Proc. Steklov Institute of Math. 2009. V. 265. P. 30–58.
2. *Карпов А. В.* Перестановочные многочлены над примарными кольцами // Прикладная дискретная математика. 2013. № 4(22). С. 16–21.