

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА**

**ТРУДЫ
IX МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ
«ДИСКРЕТНЫЕ МОДЕЛИ
В ТЕОРИИ
УПРАВЛЯЮЩИХ СИСТЕМ»**

Москва и Подмосковье

20–22 мая 2015 г.

МОСКВА

2015

СПИСОК ЛИТЕРАТУРЫ

- [1] Фаулер М. Рефакторинг. Улучшение существующего кода. — М.: Символ-Плюс, 2008. — 432 с.
- [2] Иткин В. Э. Логико-термальная эквивалентность схем программ // Кибернетика. — 1972. — № 1. — С. 5–27.
- [3] Новикова Т. А., Захаров В. А. Полиномиальный по времени алгоритм проверки логико-термальной эквивалентности программ // Труды института системного программирования РАН. — 2012. — Т. 22 — С. 435–455.
- [4] Костылев Е. В., Захаров В. А. О сложности задачи антиунификации // Дискретная математика. — 2008. — Т. 20, № 5. — С. 131–144.

Оценки периода полиномиальной рекуррентной последовательности

Парватов Николай Георгиевич¹, Алексеева Дарья Владимировна²

¹ Томский государственный университет, e-mail: parvatov@mail.tsu.ru

² Томский государственный университет, e-mail: alekseevad@gmail.com

Рассматриваются полиномиальные рекуррентные последовательности над конечными алгебраическими структурами. Приводятся верхние оценки периода для полиномиальных рекуррентных последовательностей над примарным кольцом классов вычетов.

Рекуррентные последовательности

Пусть m — целое положительное число, p — простое и $f_1, \dots, f_n$ — целочисленные многочлены от n переменных. Обозначим через $s(f, m, x)$ рекуррентную последовательность

$$f^0(x) + p^m Z^n, f^1(x) + p^m Z^n, f^2(x) + p^m Z^n, \dots,$$

где Z — кольцо целых чисел, $x \in Z^n$, $f(x) = (f_1(x), \dots, f_n(x))$, $f^0(x) = x$ и $f^k(x) = f(f^{k-1}(x))$ для $k > 0$.

Пусть $d > 0$. Последовательность называется *периодической с периодом d* , если выполняется равенство $f^0(x) = f^d(x)$; обозначим $\tau(f, m, x)$ наименьший период в этом случае. Функцию f назовём *периодической по модулю p^m* , если указанная последовательность периодична при любом выборе x (и тогда функция f определяет подстановку по модулю p^m).

Полиномиальные подстановки рассматривались в ряде работ [1,2,3]. В том числе в [1] установлены условия периодичности. В [1,2] описаны транзитивные (одноцикловые) полиномиальные подстановки, существующие только при $n = 1$. В [3] найдены возможные длины периодов полиномов одной переменной над кольцом Галуа. Этот результат обобщается далее для полиномиальных вектор-функций от n переменных над примарным кольцом классов вычетов.

Именно, устанавливается верхняя оценка длины периода $\tau(f, m, x)$ при условии, что последовательность $s(f, m, y)$ периодична для любого набора y из смежного класса $x + pZ^n$.

Условия периодичности и оценка периода

Обозначим через M_n кольцо целочисленных квадратных матриц размера n с единичной матрицей E , через $\det(A)$ — определитель матрицы A и через $\text{ord}_p(A)$ — порядок обратимой матрицы по модулю p , то есть наименьшее положительное k , при котором $A^k \equiv E \pmod{pM_n}$, существующее, если $\det(A) \not\equiv 0 \pmod{pZ}$. Положим

$$D_f(x) = \begin{pmatrix} \frac{df_1}{dx_1}(x) & \cdots & \frac{df_n}{dx_1}(x) \\ \vdots & & \vdots \\ \frac{df_1}{dx_n}(x) & \cdots & \frac{df_n}{dx_n}(x) \end{pmatrix}$$

и $D_f^\tau(x) = D_f(f^0(x)) \cdots D_f(f^{\tau-1}(x))$ для любого положительного τ . Матрица $D_f(x)$ называется *матрицей Якоби* функции f в точке x .

Следующая теорема даёт условия периодичности и верхние оценки для периода полиномиальной рекуррентной последовательности.

Теорема. Пусть последовательность $s(f, 1, x)$ периодична с наименьшим периодом $\tau_1 = \tau(f, 1, x)$ и $m > 1$.

Имеют место следующие свойства.

1. Последовательность $s(f, m, y)$ периодична для любого набора y из смежного класса $x + pZ^n$ тогда и только тогда, когда $\det_p(D_f^{\tau_1}(x)) \pmod{pZ} \neq 0$.
2. Пусть $\det_p(D_f^{\tau_1}(x)) \pmod{pZ} \neq 0$. Тогда для любого набора y из $x + pZ^n$ имеет место следующее соотношение для периода:

$$\tau(f, m, y) | \tau_1 \cdot p^{m-1} \cdot \text{ord}_p(D_f^{\tau_1}(x)).$$

3. Если ещё и $\det_p(D_f^{\tau_1}(x) - E) \pmod{pZ} \neq 0$, то для любого y из $x + pZ^n$ выполняется соотношение:

$$\tau(f, m, y) | \tau_1 \cdot p^{m-2} \cdot \text{ord}_p(D_f^{\tau_1}(x)).$$

Свойства, сформулированные выше для последовательностей над кольцом классов вычетов по приматрному модулю, допускают обобщение на случай произвольного конечного коммутативного кольца с единицей.

СПИСОК ЛИТЕРАТУРЫ

- [1] Анашин В. С. Равномерно распределенные последовательности целых p -адических чисел. Дискретная математика. — 2002. — Т. 14, № 4. — С. 3–64.
- [2] Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов. Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 20–32.
- [3] Ермилов Д. М., Козлитин О. А., Цикловая структура полиномиального генератора над кольцом Галуа. Математические вопросы криптографии. — 2013 — Т. 4, № 1. — С. 27–57.