Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Периодические свойства многомерного полиномиального генератора над кольцом Гауа. III, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 49–76

DOI: <https://doi.org/10.4213/mvk339>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.237.59.107

26 апреля 2023 г., 13:07:39

Периодические свойства многомерного полиномиального генератора над кольцом Галуа. III

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 15.V.2020

Работа посвящается памяти Виктора Павловича Елизарова

Аннотация. Исследуются многомерные полиномиальные преобразования кольца Галуа R характеристики p^n . Подсчитаны некоторые числовые характеристики циклов и подходов к циклам в орграфах таких преобразований. В некоторых частных случаях строение орграфа преобразования описано по модулю p^2 .

Ключевые слова: полиномиальное преобразование, кольцо Галуа, цикл, подход к циклу, дерево

Periodical properties of multidimensional polynomial generator over Galois ring. III

O. A. Kozlitin

LLC «Sertification Research Center», Moscow

The author devote the paper to the memory of Victor Pavlovich Elizarov

Abstract. Multidimensional polynomial transformations of the Galois ring of characteristics p^n are investigated. Several structural parameters of cycles and paths to cycles in orgraphs of such transforms are computed. For some particular cases the structure of orgraph of transform is described modulo p^2 .

Keywords: polynomial substitution, Galois ring, cycle, path to cycle, tree

1. Введение

Согласно [6] *кольцом Галуа* называется конечное коммутативное локальное кольцо главных идеалов R , нильрадикал (множество нильпотентных элементов) $J(R)$ которого удовлетворяет равенству $J(R) = pR$, где p – простое число. Пусть $\bar{R} = R/J(R)$. Известно, что $\bar{R} = GF(q)$, где $q = p^t$ при некотором $t \in \mathbb{N}$. Если n – индекс нильпотентности идеала $J(R)$, то кольцо Галуа R имеет характеристику p^n . Кольцо Галуа R определяется своей мощностью q^n и характеристикой p^n однозначно, с точностью до изоморфизма. В связи с этим пишут: $R = GR(q^n, p^n)$.

Пусть $R = GR(q^n, p^n)$. Кольцо Галуа R является частным случаем произвольного конечного коммутативного локального кольца главных идеалов (конечного коммутативного *цепного* кольца, кольца *Галуа – Эйзенштейна*). Интерес к изучению генераторов псевдослучайных последовательностей (ПСП) над произвольным кольцом Галуа обусловлен тем, что все конечные поля и все примарные кольца вычетов являются кольцами Галуа. Аппарат колец Галуа позволяет не только рассматривать с общих позиций генераторы над этими простейшими алгебраическими структурами, но и получать новые результаты о генераторах над кольцами вычетов.

Пусть $m \in \mathbb{N}$, $\mathbf{z} = (z_1, z_2, \dots, z_m)$ – строка из m переменных над кольцом R . Рассмотрим последовательность из m многочленов

$$F_1(\mathbf{z}), F_2(\mathbf{z}), \dots, F_m(\mathbf{z}) \in R[\mathbf{z}]$$

и сопоставим этой последовательности многомерное (m -мерное) полиномиальное преобразование F кольца R

$$\forall \mathbf{x} \in R^m : F(\mathbf{x}) = (F_1(\mathbf{x}), F_2(\mathbf{x}), \dots, F_m(\mathbf{x})). \quad (1)$$

Автономный автомат, функция перехода которого задана полиномиальной функцией F вида (1), называют *полиномиальным генератором*. Полиномиальный генератор может быть использован для выработки ПСП с наперед заданными криптографическими характеристиками (периодическими, сложностными и статистическими).

Одномерный полиномиальный генератор (*полиномиальный конгруэнтный генератор*, ПКГ) над кольцом вычетов изучался в статье М.В. Ларина [14]. Аналогичные генераторы над кольцами Галуа и Галуа – Эйзенштейна рассматривались О.А. Козлитиным и Д.М. Ермиловым в [9–11] и [8]. Многомерный полиномиальный генератор над кольцами вычетов и кольцами Галуа обсуждался в [12, 19] и [13]. В этих

статьях исследовались цикловые структуры биективных преобразований вида (1), а также алгоритмы построения подстановок, обладающих циклами максимальной возможной длины.

В перечисленных работах при описании орграфа полиномиального преобразования над локальным кольцом предполагается известным строение соответствующего орграфа над полем вычетов. Ввиду результата Диксона [17] о полиномиальности всякой функции над конечным полем такой орграф является произвольным графом преобразования (или, в биективном случае, произвольным графом подстановки). В то же время для описания орграфа полиномиального преобразования над кольцом необходимо уметь перечислять вершины орграфа, в которых значение производной сравнимо с нулем по модулю радикала. В связи с этим важное значение имеет работа В.Е. Викторенкова [4], в которой комбинаторно-вероятностными методами исследуется раскрашенный в два цвета граф случайной подстановки (можно считать, что первому цвету соответствуют нулевые значения производной, а второму – ее ненулевые значения). Используемый В.Е. Викторенковым математический аппарат тесно связан с введенным В.Н. Сачковым оператором *редуцирования подстановок* (см., например, [15]).

Задача описания орграфа небиективного полиномиального преобразования вида (1) существенно сложнее задачи описания цикловой структуры полиномиальной подстановки. При решении этой задачи необходимо использовать математический аппарат, разработанный В.Е. Викторенковым в [2]. В одномерном случае он применялся в [9, 10] и [3]. Обобщение полученных результатов на m -мерный случай составляет содержание настоящей работы.

Каждый многочлен $F_i(\mathbf{z}) \in R[\mathbf{z}]$ можно представить в виде суммы мономов:

$$F_i(\mathbf{z}) = \omega_1(\mathbf{z}) + \omega_2(\mathbf{z}) + \dots + \omega_l(\mathbf{z}).$$

Определим стандартным образом *частную производную монома*

$$\omega(\mathbf{z}) = a z_1^{\alpha_1} z_2^{\alpha_2} \dots z_m^{\alpha_m}$$

по переменной z_j :

$$\frac{\partial \omega(\mathbf{z})}{\partial z_j} = \alpha_j z_1^{\alpha_1} z_2^{\alpha_2} \dots z_{j-1}^{\alpha_{j-1}} z_j^{\alpha_j-1} z_{j+1}^{\alpha_{j+1}} \dots z_m^{\alpha_m}$$

(если $\alpha_j = 0$, то соответствующая производная считается равной 0). Распространив это определение на все мономы, определим *частную*

производную многочлена $F_i(\mathbf{z})$ по переменной z_j :

$$\frac{\partial F_i(\mathbf{z})}{\partial z_j} = \sum_{s=1}^l \frac{\partial \omega_s(\mathbf{z})}{\partial z_j}.$$

Составим из частных производных матрицу Якоби:

$$J_F(\mathbf{z}) = \begin{pmatrix} \frac{\partial F_1(\mathbf{z})}{\partial z_1} & \frac{\partial F_2(\mathbf{z})}{\partial z_1} & \dots & \frac{\partial F_m(\mathbf{z})}{\partial z_1} \\ \frac{\partial F_1(\mathbf{z})}{\partial z_2} & \frac{\partial F_2(\mathbf{z})}{\partial z_2} & \dots & \frac{\partial F_m(\mathbf{z})}{\partial z_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial F_1(\mathbf{z})}{\partial z_m} & \frac{\partial F_2(\mathbf{z})}{\partial z_m} & \dots & \frac{\partial F_m(\mathbf{z})}{\partial z_m} \end{pmatrix}.$$

Пусть $\mathbf{x}, \mathbf{y} \in R^m$. Имеет место сравнение

$$\forall i \in \{1, 2, \dots, m\} : F_i(\mathbf{x} + p^s \mathbf{y}) \equiv F_i(\mathbf{x}) + p^s \mathbf{y} J_i^\downarrow(\mathbf{x}) \pmod{p^{2s} R},$$

где $J_i^\downarrow(\mathbf{x})$ – i -й столбец матрицы Якоби $J_F(\mathbf{x})$, $\mathbf{y} \in R^m$ – произвольный вектор (здесь и всюду далее запись

$$\mathbf{x} \equiv \mathbf{y} \pmod{I}$$

означает, что каждая координата вектора $\mathbf{x} - \mathbf{y}$ принадлежит идеалу $I \triangleleft R$). Отсюда естественным образом вытекает сравнение

$$F(\mathbf{x} + p^s \mathbf{y}) \equiv F(\mathbf{x}) + p^s \mathbf{y} J_F(\mathbf{x}) \pmod{p^{2s} R}. \quad (2)$$

Обозначим период последовательности

$$\mathbf{x}, F(\mathbf{x}), F(F(\mathbf{x})), \dots,$$

приведенной по модулю $p^s R$, через $\tau(F, s, \mathbf{x})$. В случае когда преобразование F вида (1) и вектор $\mathbf{x} \in R^m$ фиксированы, будем обозначать величину $\tau(F, s, \mathbf{x})$ через τ_s . Выберем и зафиксируем преобразование F вида (1) и вектор $\mathbf{x} \in R^m$. Обозначим через $F^{[k]}$ композиционную степень преобразования F

$$F^{[k]} = F \circ F \circ \dots \circ F \quad (k \text{ раз}).$$

По определению $F^{[0]}$ есть тождественное преобразование модуля R^m . Положим $f_s = F^{[\tau_s]}$. Тогда очевидно, что

$$f_s(\mathbf{x}) \equiv \mathbf{x} \pmod{p^s R}.$$

Напомним аналог формулы производной сложной функции из [12]:

$$J_{F(G)}(\mathbf{z}) = J_G(\mathbf{z})J_F(G(\mathbf{z})). \quad (3)$$

Из этой формулы следует равенство

$$J_{f_1}(\mathbf{z}) = \prod_{s=0}^{\tau_1-1} J_F(F^{[s]}(\mathbf{z})). \quad (4)$$

Факты и определения, приведенные в этом разделе, будут использованы далее при вычислении ряда характеристик подходов к циклам преобразования F . Образ вектора $\mathbf{a} \in R^m$ (многочлена $F_i(\mathbf{z})$, матрицы $J_F(\mathbf{a})$) под действием естественного эпиморфизма $R \rightarrow \bar{R} = R/pR$ обозначим через $\bar{\mathbf{a}}$ (соответственно через $\bar{F}_i(\mathbf{z})$, $\bar{J}_F(\mathbf{a})$). Положим $\bar{F} = (\bar{F}_1, \bar{F}_2, \dots, \bar{F}_m)$. Перечислим основные результаты работы.

- 1) Предложена классификация вершин $\mathbf{a} \in R^m$ орграфа полиномиального преобразования F в зависимости от ранга $r_F(\bar{\mathbf{a}})$ матрицы $\bar{J}_F(\mathbf{a})$. Аналогично случаю $m = 1$ введено понятие *псевдоциклической* вершины, т. е. вершины, циклической по модулю радикала (см., например, [2]). На множестве вершин орграфа введена естественная метрика и доказано, что расстояние от $\mathbf{a}$ до множества псевдоциклических вершин равно расстоянию от $\bar{\mathbf{a}}$ до соответствующего цикла (следствие 2).
- 2) Пусть $\mathbf{a}$ – псевдоциклическая вершина и $C_{\bar{F}}(\bar{\mathbf{a}})$ – цикл преобразования $\bar{F}$, которому принадлежит вершина $\bar{\mathbf{a}}$. Под *псевдоциклом* $C_F^\#(\mathbf{a})$ понимается полный прообраз цикла $C_{\bar{F}}(\bar{\mathbf{a}})$ под действием естественного эпиморфизма $R \rightarrow \bar{R}$. Показано, что псевдоцикл, все вершины $\mathbf{v}$ которого обладают свойством $r_F(\bar{\mathbf{v}}) = m$, состоит из циклов без подходов (теорема 6, п. 1). Если на псевдоцикле есть вершина $\mathbf{v}$ со свойством $r_F(\bar{\mathbf{v}}) = 0$, то такой псевдоцикл состоит из единственного цикла с подходами, причем все элементы цикла попарно различны по модулю радикала (теорема 6, п. 2). В этой последней ситуации псевдоцикл назван *особым*.
- 3) Получены оценки для максимума высот деревьев, являющихся подходами к циклу в особом псевдоцикле (утверждение 8), и числа концевых вершин в орграфе преобразования, биективного по модулю радикала (теорема 17). Псевдоцикл назван *сингулярным*, если хотя бы для одной его вершины $\mathbf{v}$ выполняется неравенство

$r_F(\bar{\mathbf{v}}) < m$. В некоторых частных случаях строение сингулярного псевдоцикла описано по модулю p^2 (теоремы 16 и 18).

Таким образом, в этой статье продолжают исследования, начатые в [12, 13], и обобщается на m -мерный случай ряд результатов из [9, 10].

2. Классификация вершин

Орграф преобразования F вида (1) обозначим через G_{F,R^m} . Назовем вершину $\mathbf{a}$ графа G_{F,R^m} *сингулярной* (*вырожденной*), если выполнено неравенство

$$\text{rank} \overline{J_F(\mathbf{a})} < m.$$

Все вершины, не являющиеся сингулярными, назовем *несингулярными* (*невыврожденными*).

Поскольку кольцо R фиксировано, мы можем обозначить множества циклических вершин орграфов G_{F,R^m} и $G_{\bar{F},\bar{R}^m}$ через C_F и $C_{\bar{F}}$ соответственно. Семейство

$$C_F^\# = C_F + pR^m \quad (5)$$

назовем множеством *псевдоциклических* вершин. Иногда множество $C_F^\#$ будем называть графом, подразумевая подграф графа G_{F,R^m} , порожденный множеством $C_F^\#$ (см., например, [1]). Расстоянием от вершины $\mathbf{a} \in R^m$ до произвольного множества вершин $X \subseteq R^m$ назовем такое минимальное $t \in \mathbb{N}_0$, что $F^{[t]}(\mathbf{a}) \in X$, если такое t существует, и бесконечность – в противном случае. Обозначим указанное расстояние через $\rho(\mathbf{a}, X)$. Сформулируем и докажем ряд вспомогательных утверждений.

Утверждение 1. *Если $\mathbf{a} \in C_F$, то $\bar{\mathbf{a}} \in C_{\bar{F}}$. Если $\bar{\mathbf{a}} \in C_{\bar{F}}$, то существует вектор $\mathbf{b} \in pR^m$ со свойством $\mathbf{a} + \mathbf{b} \in C_F$.*

Доказательство. Первая часть утверждения очевидна. Докажем его вторую часть. Пусть элемент $\mathbf{a} \in R^m$ таков, что $\bar{\mathbf{a}} \in C_{\bar{F}}$. Рассмотрим компоненту связности графа G_F , содержащую вершину $\mathbf{a}$. В этой компоненте связности есть цикл $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{l-1}$. Если элемент $\bar{\mathbf{a}}$ отсутствует в ряду $\bar{\mathbf{c}}_0, \bar{\mathbf{c}}_1, \dots, \bar{\mathbf{c}}_{l-1}$, то он отсутствует и в последовательности $\bar{\mathbf{c}}_0, \bar{F}(\bar{\mathbf{c}}_0), \bar{F}^2(\bar{\mathbf{c}}_0), \dots$, что невозможно в силу цикличности $\bar{\mathbf{a}}$. Следовательно, $\mathbf{a} \equiv \mathbf{c}_i \pmod{pR}$ для подходящего $i \in \{0, 1, \dots, l-1\}$. $\square$

Утверждение 1 является m -мерным аналогом утверждения 1 из [9].

Следствие 2. *Для любого вектора $\mathbf{a} \in R^m$ выполняется равенство*

$$\rho(\mathbf{a}, C_F^\#) = \rho(\bar{\mathbf{a}}, C_{\bar{F}}).$$

Доказательство. Достаточно показать, что

$$\forall t \geq 0 : F^{[t]}(\mathbf{a}) \in C_F^\# \Leftrightarrow \bar{F}^{[t]}(\bar{\mathbf{a}}) \in C_{\bar{F}}.$$

Импликация «слева направо» следует из (5). Импликация «справа налево» следует из утверждения 1. $\square$

Следствие 2 является m -мерным аналогом утверждения 2 из [9].

Пусть $\mathbf{a}$ – псевдоциклическая вершина орграфа G_{F,R^m} , вершина $\bar{\mathbf{a}}$ графа $G_{\bar{F},\bar{R}^m}$ принадлежит циклу длины τ , множество $C_F(\mathbf{a})$ определено равенством

$$C_F(\mathbf{a}) = \{\mathbf{a}, F(\mathbf{a}), F^{[2]}(\mathbf{a}), \dots, F^{[\tau-1]}(\mathbf{a})\}.$$

Множество

$$C_F^\#(\mathbf{a}) = C_F(\mathbf{a}) + pR^m$$

назовем *псевдоциклом, индуцированным вершиной $\mathbf{a}$* или просто *псевдоциклом*. Иногда псевдоцикл $C_F^\#(\mathbf{a})$ будем называть графом, подразумевая подграф графа G_{F,R^m} , порожденный множеством $C_F^\#(\mathbf{a})$ в смысле [1]. Имеет место следующее утверждение.

Утверждение 3. Если в графе $G_{\bar{F},\bar{R}^m}$ ровно k циклов и $\bar{\mathbf{a}}_1, \bar{\mathbf{a}}_2, \dots, \bar{\mathbf{a}}_k$ – их представители, то

$$C_F^\# = \bigsqcup_{i=1}^k C_F^\#(\mathbf{a}_i). \quad (6)$$

Утверждение 3 является m -мерным аналогом утверждения 3 из [9].

Доказательство. Тот факт, что слагаемые в правой части попарно не пересекаются, очевиден. Осталось доказать равенство (6).

Приведением левой и правой частей по модулю радикала легко доказать включение

$$\forall i \in \{1, \dots, k\} : C_F(\mathbf{a}_i) \subseteq C_F^\#.$$

Следовательно, $C_F^\#(\mathbf{a}_i) \subseteq C_F^\#$ для всякого $i \in \{1, 2, \dots, k\}$, и правая часть равенства (6) включается в его левую часть.

Обратно: если $\mathbf{a} \in C_F^\#$, то существует такое $i \in \{1, 2, \dots, k\}$, что $\bar{\mathbf{a}}$ и $\bar{\mathbf{a}}_i$ лежат на одном цикле графа $G_{\bar{F},\bar{R}^m}$. Если длина этого цикла равна τ , то существует число $j \in \{0, 2, \dots, \tau - 1\}$ со свойством $\mathbf{a} \equiv F^{[j]}(\mathbf{a}_i) \pmod{pR}$. Поэтому

$$\mathbf{a} \in C_F(\mathbf{a}_i) + pR^m = C_F^\#(\mathbf{a}_i).$$

Равенство (6) доказано. $\square$

Следующее утверждение доказано в [18]. Доказательство конструктивно; приведем его для удобства дальнейшего изложения.

Утверждение 4. Пусть полиномиальное преобразование $F(\mathbf{z})$ и несингулярная вершина $\mathbf{a} \in R^m$ таковы, что $\bar{F}(\bar{\mathbf{a}}) = 0$. Тогда существует единственный вектор $\mathbf{x} \in R^m$ со свойствами $\bar{\mathbf{a}} = \bar{\mathbf{x}}$ и $F(\mathbf{x}) = 0$.

Доказательство. Используем математическую индукцию по индексу нильпотентности n кольца R . Если $n = 1$, то доказывать нечего. Пусть $n = 2$ и $\mathbf{a}_0$ – нулевая координата вектора $\mathbf{a}$ в разложении Тейхмюллера. Положив $\mathbf{x}_0 = \mathbf{a}_0$, вычислим первую координату $\mathbf{x}_1$ вектора $\mathbf{x}$. Для этого воспользуемся формулой Тейлора (2) при $s = 1$:

$$\begin{aligned} F(\mathbf{x}_0 + p\mathbf{x}_1) &\equiv 0 \pmod{p^2 R}, \\ F(\mathbf{x}_0) + p\mathbf{x}_1 J_F(\mathbf{x}_0) &\equiv 0 \pmod{p^2 R}, \\ \mathbf{x}_1 J_F(\mathbf{x}_0) &\equiv -\frac{F(\mathbf{x}_0)}{p} \pmod{pR}. \end{aligned}$$

Поскольку матрица $J_F(\mathbf{x}_0)$ обратима, то координата $\mathbf{x}_1$ восстанавливается однозначно. База индукции доказана.

Пусть для колец с индексом нильпотентности $n = r$ утверждение верно. Докажем его для колец с индексом нильпотентности $n = r + 1$. Пусть $\mathbf{x}_i$ есть i -я координата в разложении Тейхмюллера вектора $\mathbf{x}$, $i = 0, 1, \dots, r$. По предположению индукции координаты $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{r-1}$ восстанавливаются по F и $\mathbf{a}_0$ однозначно. Покажем, что координата $\mathbf{x}_r$ тоже восстанавливается однозначно. Положим

$$\mathbf{y} = \mathbf{x}_0 + p\mathbf{x}_1 + \dots + p^{r-1}\mathbf{x}_{r-1}.$$

Поскольку $2r \geq r + 1$, применение формулы (2) дает следующий результат:

$$\begin{aligned} F(\mathbf{y} + p^r \mathbf{x}_r) &\equiv 0 \pmod{p^{r+1} R}, \\ F(\mathbf{y}) + p^r \mathbf{x}_r J_F(\mathbf{y}) &\equiv 0 \pmod{p^{r+1} R}, \\ \mathbf{x}_r J_F(\mathbf{y}) &\equiv -\frac{F(\mathbf{y})}{p^r} \pmod{pR}. \end{aligned}$$

Так как $\overline{J_F(\mathbf{a})} = \overline{J_F(\mathbf{y})}$, то матрица $J_F(\mathbf{y})$ обратима. Следовательно, координата $\mathbf{x}_r$ восстанавливается однозначно. $\square$

Утверждение 4 является m -мерным аналогом стандартного алгоритма «подъема корня», использующего лемму Гензеля (см., например [7, теорема 2.7]).

Псевдоциклическая вершина называется *регулярной*, если ее полустепень захода в графе $C_F^\#$ равна 1. Понятия несингулярной вершины и регулярной вершины связывает следующее утверждение.

Утверждение 5. Пусть $\mathbf{a} \in C_F^\#$ и $\mathbf{b} = F(\mathbf{a})$. Тогда вершина $\mathbf{a}$ несингулярна, если и только если вершина $\mathbf{b}$ регулярна.

Доказательство. Рассмотрим систему сравнений относительно $\mathbf{x} \in R^m$:

$$\begin{cases} \mathbf{x} \equiv \mathbf{a} \pmod{pR}, \\ F(\mathbf{x}) = \mathbf{b}. \end{cases}$$

Вершина $\mathbf{b}$ регулярна тогда и только тогда, когда данная система имеет единственное решение. Рассмотрим разложение Тейхмюллера вектора $\mathbf{x}$:

$$\mathbf{x} = \mathbf{x}_0 + p\mathbf{x}_1 + p^2\mathbf{x}_2 + \dots + p^{n-1}\mathbf{x}_{n-1}, \quad (7)$$

где $\mathbf{x}_0 = \mathbf{a}_0$ — нулевая координата в разложении Тейхмюллера вектора $\mathbf{a}$.

Применим к многочлену $F(\mathbf{x}) - \mathbf{b}$ многомерный алгоритм поднятия корня по модулю радикала, восстанавливающий для любого $s \in \{1, 2, \dots, n-1\}$ координату $\mathbf{x}_s$ по координатам $\mathbf{a}_0, \mathbf{x}_1, \dots, \mathbf{x}_{s-1}$. Из доказательства утверждения 4 видно, что это восстановление осуществляется однозначно тогда и только тогда, когда матрица $J_F(\mathbf{a}_0)$ обратима, т. е. когда вершина $\mathbf{a}$ несингулярна. $\square$

Утверждение 5 является m -мерным аналогом утверждения 5 из [9].

Обозначим множество всех сингулярных псевдоциклических вершин орграфа G_{F,R^m} через $SC_F^\#$. Будем называть псевдоцикл *несингулярным*, если он не содержит сингулярных вершин. Согласно утверждению 1 любую псевдоциклическую вершину можно «достроить» до циклической. Следующая теорема дает оценку числа способов, которыми это можно сделать.

Теорема 6. Справедливы следующие утверждения:

1. Компонентами связности всякого несингулярного псевдоцикла являются циклы без подходов.

2. Пусть $\mathbf{a} \in SC_F^\#$, вершина $\bar{\mathbf{a}}$ графа $G_{\bar{F}, \bar{R}^m}$ принадлежит циклу длины τ , $r = \text{rank} J_F(\mathbf{a})$. Тогда существует не менее одного и не более

$$1 + (1 - q^{-r}) \frac{q^{mn} - q^m}{q - 1} \quad (8)$$

векторов $\mathbf{b} \in pR^m$, обладающих свойством $\mathbf{a} + \mathbf{b} \in C_F$. В частности, при $r = 0$ псевдоцикл $C_F^\#(\mathbf{a})$ есть цикл длины τ с подходами.

Доказательство. 1. Рассмотрим несингулярный псевдоцикл $C_F^\#(\mathbf{a})$. Если $\mathbf{x} \in C_F^\#(\mathbf{a})$, то $\bar{\mathbf{x}} = \bar{F}(\bar{\mathbf{b}})$, где вершины $\bar{\mathbf{b}}$ и $\bar{\mathbf{a}}$ принадлежат одному циклу графа $G_{\bar{F}, \bar{R}^m}$. Тогда $\mathbf{b} \in C_F^\#(\mathbf{a})$. Так как вершина $\mathbf{b}$ – несингулярная, вершина $\mathbf{x}$ регулярна (утверждение 5). Таким образом, каждая вершина псевдоцикла $C_F^\#(\mathbf{a})$ регулярна, и псевдоцикл $C_F^\#(\mathbf{a})$ целиком состоит из циклических элементов.

2. Согласно утверждению 1 существует вектор $\mathbf{b} \in pR^m$, обладающий свойством $\mathbf{a} + \mathbf{b} \in C_F$. Выясним, для каких ненулевых векторов $\mathbf{c} \in pR^m$ заведомо не выполняется условие $\mathbf{a} + \mathbf{b} + \mathbf{c} \in C_F$.

Существуют число $s \in \{1, 2, \dots, n-1\}$ и ненулевой по модулю радикала вектор $\mathbf{r} \in R^m$, для которых $\mathbf{c} = p^s \mathbf{r}$. Положим $\mathbf{d} = \mathbf{b} + \mathbf{c} = \mathbf{b} + p^s \mathbf{r}$. Поскольку $2s \geq s + 1$, формула (2) позволяет выписать следующую цепочку равенств и сравнений по модулю $p^{s+1}R$:

$$\begin{aligned} F(\mathbf{a} + \mathbf{d}) - F(\mathbf{a} + \mathbf{b}) &= F(\mathbf{a} + \mathbf{b} + p^s \mathbf{r}) - F(\mathbf{a} + \mathbf{b}) \\ &\equiv p^s \mathbf{r} \cdot J_F(\mathbf{a} + \mathbf{b}) \equiv p^s \mathbf{r} \cdot J_F(\mathbf{a}). \end{aligned}$$

Отсюда вытекает эквивалентность:

$$F(\mathbf{a} + \mathbf{d}) \equiv F(\mathbf{a} + \mathbf{b}) \pmod{p^{s+1}R} \Leftrightarrow \bar{\mathbf{r}} \cdot \overline{J_F(\mathbf{a})} = 0. \quad (9)$$

Если вершина $\mathbf{a} + \mathbf{d}$ – циклическая, то существует такое число $t_1 \in \mathbb{N}$, что $F^{[t_1]}(\mathbf{a} + \mathbf{d}) = \mathbf{a} + \mathbf{d}$. По условию вершина $\mathbf{a} + \mathbf{b}$ – циклическая; пусть она принадлежит циклу длины t_2 . Обозначим через t_0 наименьшее общее кратное чисел t_1 и t_2 : $t_0 = [t_1, t_2]$. Пусть теперь выполнено условие

$$F(\mathbf{a} + \mathbf{d}) \equiv F(\mathbf{a} + \mathbf{b}) \pmod{p^{s+1}R}. \quad (10)$$

Применив к обеим частям (10) преобразование $F^{[t_0-1]}$, получим сравнение

$$\mathbf{a} + \mathbf{d} \equiv \mathbf{a} + \mathbf{b} \pmod{p^{s+1}R},$$

которое, очевидно, невозможно. Ввиду (9) доказана импликация

$$(\mathbf{a} + \mathbf{b} + p^s \mathbf{r} \in C_F) \Rightarrow (\bar{\mathbf{r}} \cdot \overline{J_F(\mathbf{a})} \neq 0). \quad (11)$$

При фиксированном s количество циклических вершин вида $\mathbf{a} + \mathbf{b} + p^s \mathbf{r}$ не превосходит величины

$$(q^m - q^{m-r}) \cdot q^{m(n-s-1)}. \quad (12)$$

Действительно, согласно (11) нулевая координата в разложении Тейхмюллера вектора $\mathbf{r}$ выбирается так, чтобы обеспечить неравенство $\bar{\mathbf{r}} \cdot \overline{J_F(\mathbf{a})} \neq 0$, а остальные $(n - s - 1)$ координат вектора $\mathbf{r}$ выбираются произвольно. Суммируя (12) по всем $s \in \{1, 2, \dots, n - 1\}$ и учитывая вершину $\mathbf{a} + \mathbf{b}$, получим, что число способов, которыми можно достроить псевдоциклическую вершину $\mathbf{a}$ до циклической вершины, не превосходит

$$1 + (q^m - q^{m-r}) \cdot \sum_{i=0}^{n-2} q^{mi}.$$

После очевидных преобразований это выражение превращается в (8).

При $r = 0$ вершина $\mathbf{a}$, очевидно, единственным образом достраивается до циклической. Покажем, что псевдоцикл $C_F^\#(\mathbf{a})$ при этом представляет собой единственный цикл длины τ с подходами.

Покажем сначала, что в псевдоцикле $C_F^\#(\mathbf{a})$ имеется единственный цикл. Рассуждаем от противного: если в этом псевдоцикле есть по крайней мере 2 цикла, то по модулю радикала pR они состоят из одних и тех же элементов. Тогда вершина $\mathbf{a}$ достраивается до циклической по крайней мере двумя способами, т. е. существуют разные $\mathbf{b}_1, \mathbf{b}_2 \in pR^m$, для которых $\mathbf{a} + \mathbf{b}_1 \in C_F$ и $\mathbf{a} + \mathbf{b}_2 \in C_F$. Противоречие с первой частью п. 2.

Теперь покажем, что единственный цикл, являющийся подграфом псевдоцикла $C_F^\#(\mathbf{a})$, имеет длину τ . Поскольку по модулю радикала он имеет длину τ , его длина не может быть меньше τ . Если же его длина больше τ , то на цикле графа $G_{\bar{F}, \bar{R}^m}$, содержащем элемент $\bar{\mathbf{a}}$, есть такой элемент $\bar{\mathbf{d}}$, что вершина $\mathbf{d} \in R^m$ достраивается до циклической по крайней мере двумя способами. Противоречие. $\square$

Теорема 6 обобщает на m -мерный случай теорему 1 из [9] (хотя, в отличие от предыдущих утверждений, не является ее буквальной аналогом). Она является центральным результатом этого раздела.

В случае когда преобразование $\bar{F}$ биективно, утверждение 3 и теорема 6 сводят изучение подходов к циклам графа G_{F, R^m} к изучению *сингулярных* псевдоциклов, т. е. псевдоциклов, на которых имеются сингулярные вершины. Всюду далее будет рассматриваться псевдоцикл

$C_F^\#(\mathbf{a})$, индуцированный сингулярной вершиной $\mathbf{a}$, обладающей свойством

$$J_F(\mathbf{a}) \equiv 0 \pmod{pR}. \quad (13)$$

Всякую вершину $\mathbf{a}$ со свойством (13) и индуцированный ею псевдоцикл $C_F^\#(\mathbf{a})$ будем называть *особой вершиной* и *особым псевдоциклом* соответственно. Согласно п. 2 теоремы 6 при условии (13) особый псевдоцикл $C_F^\#(\mathbf{a})$ связан и представляет собой цикл с подходами, причем длина этого цикла не меняется при приведении по модулю радикала. Выберем и зафиксируем вершину $\mathbf{b} \in C_F^\#(\mathbf{a})$ со свойством

$$\rho(\mathbf{b}, C_F) = \max\{\rho(\mathbf{v}, C_F) \mid \mathbf{v} \in C_F^\#(\mathbf{a})\}.$$

Обозначим длину самого длинного подхода в псевдоцикле $C_F^\#(\mathbf{a})$ через $\lambda(\mathbf{a}, F)$. Вершину $\mathbf{b}$, удовлетворяющую равенству $\lambda(\mathbf{a}, F) = \rho(\mathbf{b}, C_F)$, назовем *максимально удаленной вершиной*.

Всякой вершине $\mathbf{v} \in R^m$ сопоставим ее *проекцию*

$$\pi(\mathbf{v}) = F^{[\rho(\bar{\mathbf{v}}, C_{\bar{F}})]}(\bar{\mathbf{v}})$$

на множество $C_F^\#$ псевдоциклических вершин графа G_{F, R^m} . По следствию 2 вершина $\pi(\mathbf{v})$ есть ближайшая к $\mathbf{v}$ псевдоциклическая вершина графа G_{F, R^m} . Верно следующее утверждение.

Утверждение 7. Пусть $\mathbf{a}$ – особая вершина графа G_{F, R^m} и $\pi(\mathbf{v}) \in C_F^\#(\mathbf{a})$. Если $D(\mathbf{v}), T(\mathbf{v}), D(\bar{\mathbf{v}}), T(\bar{\mathbf{v}})$ – длины подходов и периоды последовательностей

$$(\mathbf{v}, F(\mathbf{v}), F^{[2]}(\mathbf{v}), \dots) \quad \text{и} \quad (\bar{\mathbf{v}}, \bar{F}(\bar{\mathbf{v}}), \bar{F}^{[2]}(\bar{\mathbf{v}}), \dots)$$

соответственно, то

$$D(\bar{\mathbf{v}}) + T(\bar{\mathbf{v}}) \leq D(\mathbf{v}) + T(\mathbf{v}) \leq D(\bar{\mathbf{v}}) + T(\bar{\mathbf{v}}) + \lambda(\mathbf{a}, F). \quad (14)$$

Доказательство. По следствию 2 имеем: $D(\bar{\mathbf{v}}) = \rho(\mathbf{v}, C_F^\#)$, и согласно п. 2 теоремы 6 справедливо равенство $T(\mathbf{v}) = T(\bar{\mathbf{v}})$. Дальнейшее очевидно. $\square$

Чтобы сделать оценку (14) содержательной, необходимо оценить сверху величину $\lambda(\mathbf{a}, F)$ для произвольной особой вершины $\mathbf{a}$. Нормой элемента $r \in R$ назовем такое максимальное $k \in \{0, 1, \dots, n\}$, что $r \in p^k R$ (обозначение: $\|r\|$). Имеет место следующее утверждение.

Утверждение 8. Если $\mathbf{a}$ – особая псевдоциклическая вершина, удовлетворяющая равенству $\tau(F, 1, \mathbf{a}) = \tau$, то

$$\lambda(\mathbf{a}, F) \leq \tau \cdot \left\lceil \frac{n-1}{N_F(\mathbf{a})} \right\rceil, \quad (15)$$

где $N_F(\mathbf{a})$ – количество особых вершин в множестве

$$C_F(\mathbf{a}) = \{\mathbf{a}, F(\mathbf{a}), F^{[2]}(\mathbf{a}), \dots, F^{[\tau-1]}(\mathbf{a})\}.$$

Доказательство. Пусть $b \in C_F^\#(\mathbf{a})$ – максимально удаленная вершина. Ввиду (13) и теоремы 6 псевдоцикл $C_F^\#(\mathbf{a})$ состоит из одного цикла с подходами. Пусть $\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{\tau-1}$ – вершины этого цикла, занумерованные так, что

$$\mathbf{b} \equiv \mathbf{a}_0 \pmod{pR}, \quad \forall s \geq 0 : \quad \mathbf{a}_{s+1} = F(\mathbf{a}_s)$$

(в последнем равенстве суммирование в нижнем индексе осуществляется по модулю τ). Определим $\mathbf{a}_s$ для любого $s \in \mathbb{N}_0$: $\mathbf{a}_s = \mathbf{a}_{r_\tau(s)}$, где $r_\tau(s)$ – остаток от деления s на τ . Обозначим

$$\nu_s = \|J_F(\mathbf{a}_s)\|, \quad J_F(\mathbf{a}_s) = p^{\nu_s} J_s(\mathbf{a}_s), \quad J_s(\mathbf{a}_s) \in R_{m \times m},$$

где норма матрицы $J_F(\mathbf{a}_s)$ определена равенством

$$\|J_F(\mathbf{a}_s)\| = \min_{i,j} \|J_F(\mathbf{a}_s)_{i,j}\|,$$

т. е. равна минимуму норм элементов матрицы $J_F(\mathbf{a}_s)$.

Положим

$$n_0 = 1, \quad \forall s \geq 0 : \quad n_{s+1} = \min\{2n_s, n_s + \nu_s\}.$$

Покажем индукцией по s , что

$$\forall s \geq 0 : \quad F^{[s]}(\mathbf{b}) \equiv \mathbf{a}_s \pmod{p^{n_s}R}.$$

При $s = 0$ все следует из определения вершины $\mathbf{b}$. Осуществим индуктивный переход от s к $s + 1$. По предположению индукции существует такой вектор $\mathbf{r}_s \in R^m$, что

$$F^{[s]}(\mathbf{b}) = \mathbf{a}_s + p^{n_s} \mathbf{r}_s.$$

Тогда по формуле (2) имеем следующую цепочку равенств и сравнений по модулю $p^{2n_s}R$:

$$F^{[s+1]}(\mathbf{b}) = F(F^{[s]}(\mathbf{b})) = F(\mathbf{a}_s + p^{n_s} \mathbf{r}_s) \equiv \mathbf{a}_{s+1} + p^{n_s + \nu_s} \mathbf{r}_s J_s(\mathbf{a}_s).$$

Отсюда получаем сравнение

$$F^{[s+1]}(\mathbf{b}) \equiv \mathbf{a}_{s+1} \pmod{p^{n_{s+1}} R}.$$

Индуктивный переход завершен.

Заметим, что

$$\begin{aligned} \lambda(\mathbf{a}, F) &= \min\{s \geq 0 : F^{[s]}(\mathbf{b}) \in \{\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{\tau-1}\}\} \\ &\leq \min\{s \geq 0 : F^{[s]}(\mathbf{b}) = \mathbf{a}_s\} \leq \min\{s \geq 0 : n_s \geq n\}. \end{aligned}$$

Оценим последнюю величину. Понятно, что вершина $\mathbf{a}_i$ является особой тогда и только тогда, когда $\nu_i > 0$, $i = 0, 1, \dots, \tau - 1$. Имеем:

$$\forall s \geq 0 : n_{s+l} \geq n_s + |\{i \in \{0, 1, \dots, \tau - 1\} : \nu_i > 0\}| = n_s + N_F(\mathbf{a}).$$

В частности, для любого натурального k

$$n_{k\tau} \geq n_0 + k \cdot N_F(\mathbf{a}) = 1 + k \cdot N_F(\mathbf{a}).$$

Тогда

$$\min\{s \geq 0 : n_s \geq n\} \leq \tau \cdot \min\{k : 1 + k \cdot N_F(\mathbf{a}) \geq n\} = \tau \cdot \left\lceil \frac{n-1}{N_F(\mathbf{a})} \right\rceil.$$

□

Утверждение 8 обобщает на m -мерный случай теорему 9 из [10]. Отметим, что аналогичный результат для $m = 1$ и произвольного конечного коммутативного локального кольца R , вообще говоря, не являющегося кольцом главных идеалов, получен В.Е. Викторенковым в [3].

Поскольку вершина $\mathbf{a}$ – особая, $N_F(\mathbf{a}) \geq 1$, и из (15) следует неравенство

$$\lambda(\mathbf{a}, F) \leq \tau(F, 1, \mathbf{a}) \cdot (n - 1),$$

а тогда из (14) вытекает оценка

$$D(\mathbf{v}) + T(\mathbf{v}) \leq D(\bar{\mathbf{v}}) + T(\bar{\mathbf{v}}) \cdot n. \quad (16)$$

Если F – полиномиальное регистровое преобразование и $\mathbf{v}$ – начальный вектор соответствующей полиномиальной рекуррентной последовательности v , то в условиях утверждения 7 последовательность v обладает «достаточно коротким» отрезком аперидичности

$$v(0), v(1), \dots, v(D(v) + T(v) - 1).$$

Следовательно, при использовании полиномиальных регистров сдвига в качестве генераторов ПСП следует гарантировать отсутствие особых состояний.

3. Строение особого псевдоцикла

В этом разделе $n \geq 2$, $\mathbf{a}$ – особая псевдоциклическая вершина и псевдоцикл $C_F^\#(\mathbf{a})$ является циклом длины $\tau(F, 1, \mathbf{a})$ с подходами. Будем считать, что рассматриваемый псевдоцикл удовлетворяет условию: для любой вершины $\mathbf{b}$ орграфа $C_F^\#(\mathbf{a})$

$$\text{либо } J_F(\mathbf{b}) \in R_{m,m}^*, \quad \text{либо } J_F(\mathbf{b}) \in pR_{m,m}. \quad (17)$$

Условие (17) выполняется, например, при $m = 1$, а также для любого полиномиального преобразования вида $F(\mathbf{z}^p)$, где $\mathbf{z}^p = (z_1^p, z_2^p, \dots, z_m^p)$.

Рассмотрим строение подходов в орграфе $C_F^\#(\mathbf{a})$.

Пусть $\mathbf{b}$ – вершина псевдоцикла $C_F^\#(\mathbf{a})$. Рассмотрим полустепень захода вершины $F(\mathbf{b})$ в орграфе $C_F^\#(\mathbf{a})$. Если вершина $\mathbf{b}$ несингулярна, то согласно утверждению 5 полустепень захода вершины $F(\mathbf{b})$ равна 1. Случай сингулярной вершины $\mathbf{b}$ рассмотрен в следующей лемме.

Лемма 9. *Если выполнено условие (17), $\mathbf{b}$ – сингулярная вершина графа $C_F^\#(\mathbf{a})$, $\nu = \|J_F(\mathbf{b})\|$ и $k = \min\{\lceil \frac{n}{2} \rceil, \nu\}$, то полустепень захода вершины $F(\mathbf{b})$ в орграфе $C_F^\#(\mathbf{a})$ не меньше q^{mk} .*

Доказательство. Ввиду условия (17) имеем: $\nu \geq 1$. Пусть J^* – ненулевая по модулю радикала матрица со свойством $J_F(\mathbf{b}) = p^\nu J^*$. По формуле (2) для всякого $s \geq \lceil \frac{n}{2} \rceil$ и любого вектора $\mathbf{r} \in R^m$ верна цепочка равенств

$$F(\mathbf{b} + p^s \mathbf{r}) = F(\mathbf{b}) + p^s \mathbf{r} J_F(\mathbf{b}) = F(\mathbf{b}) + p^{s+\nu} \mathbf{r} J^*. \quad (18)$$

Положим в формуле (18) $s = \max\{\lceil \frac{n}{2} \rceil, n - \nu\}$. Заметим, что $n - s = k$. Если $s + \nu \geq n$, то существует не меньше $q^{m(n-s)} = q^{mk}$ попарно разных по модулю $p^{n-s}R$ векторов $\mathbf{r}$ со свойством $F(\mathbf{b} + p^s \mathbf{r}) = F(\mathbf{b})$. Если же $s + \nu < n$, то будем выбирать вектор $\mathbf{r}$ из множества $p^{n-s-\nu}R^m$. Для любых двух векторов $\mathbf{r}_1 = p^{n-s-\nu} \mathbf{c}_1$ и $\mathbf{r}_2 = p^{n-s-\nu} \mathbf{c}_2$ имеет место цепочка эквивалентностей:

$$p^s \mathbf{r}_1 \neq p^s \mathbf{r}_2 \Leftrightarrow p^{n-\nu}(\mathbf{c}_1 - \mathbf{c}_2) \neq 0 \Leftrightarrow \mathbf{c}_1 \not\equiv \mathbf{c}_2 \pmod{p^\nu R}.$$

Поскольку число смежных классов группы $(R^m, +)$ по подгруппе $(p^\nu R^m, +)$ равно $q^{m\nu}$ и $q^{m\nu} \geq q^{mk}$, получаем, что и в этом случае полустепень захода вершины $F(\mathbf{b})$ в орграфе $C_F^\#(\mathbf{a})$ не меньше q^{mk} . $\square$

Лемма 9 является m -мерным аналогом леммы 1 из [10].

Для всякого $s \in \{1, 2, \dots, n\}$ обозначим через φ_s естественный эпиморфизм $R \rightarrow R_s = R/p^s R$. Для краткости будем обозначать через G_n оргграф $C_F^\#(\mathbf{a})$, через V_n – множество вершин оргграфа G_n , а через V_s – множество $\varphi_s(V_n)$, $s = 1, 2, \dots, n$. Оргграф преобразования $\varphi_s(F)$ множества V_s обозначим через G_s , $s = 1, 2, \dots, n$. Вершину оргграфа G_s , $s = 1, 2, \dots, n$, назовем *концевой*, если ее полустепень захода равна 0. Обозначим через $K(G_s)$ множество концевых вершин оргграфа G_s , $s = 1, 2, \dots, n$. Оценим снизу число $|K(G_n)|$ концевых вершин оргграфа G_n .

Если $\mathbf{v} \in V_2$ – концевая вершина оргграфа G_2 , то все вершины из полного прообраза $\varphi_2^{-1}(\mathbf{v}) \subseteq V_n$ также являются концевыми. Поэтому верно неравенство

$$|K(G_n)| \geq q^{m(n-2)} \cdot |K(G_2)|, \quad (19)$$

и вопрос сведен к подсчету концевых вершин в оргграфе G_2 . Поскольку G_2 – псевдоцикл, индуцированный особой вершиной $\varphi_2(\mathbf{a})$, по п. 2 теоремы 6 оргграф G_2 есть цикл с подходами. Обозначим цикл оргграфа G_2 через C_2 . На этом цикле имеется по крайней мере одна особая вершина (например, та, которая сравнима с $\varphi_2(\mathbf{a})$ по модулю радикала). Рассмотрим участок цикла C_2 , заключенный между соседними особыми вершинами (начало и конец участка могут совпадать):

$$\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_s, \mathbf{c}_{s+1},$$

где $s \geq 0$, $\mathbf{c}_1$ и $\mathbf{c}_{s+1}$ – особые вершины, $\mathbf{c}_2, \mathbf{c}_3, \dots, \mathbf{c}_s$ – несингулярные вершины. По утверждению 5 вершины $\mathbf{c}_3, \mathbf{c}_4, \dots, \mathbf{c}_{s+1}$ имеют полустепень захода 1.

Пусть $\tilde{F}$ – образ F под действием эпиморфизма φ_2 . Опишем строение подхода к вершине $\mathbf{c}_{s+2} = \tilde{F}(\mathbf{c}_{s+1})$, т. е. подграфа $T = T(\mathbf{c}_{s+2})$ графа G_2 , порожденного множеством вершин

$$\{\mathbf{v} \in V_2 \setminus \{\mathbf{c}_{s+1}\} : \exists t \geq 0 : \tilde{F}^{[t]}(\mathbf{v}) = \mathbf{c}_{s+2}\}.$$

Оргграф T является деревом. Напомним (см. раздел 1), что через $\rho(\mathbf{u}, \mathbf{v})$ обозначена длина кратчайшего пути из вершины $\mathbf{u}$ в вершину $\mathbf{v}$. Опишем строение дерева T .

Утверждение 10. При условии (17) дерево $T = T(\mathbf{c}_{s+2})$ имеет $s(q^m - 1) + 1$ вершин. Вершина $\mathbf{c}_{s+2}$ имеет полустепень захода $q^m - 1$ и полустепень исхода 0, а остальные неконцевые вершины имеют полустепень захода 1 и полустепень исхода 1. Число концевых вершин

равно $q^m - 1$, каждая из них имеет полустепень исхода 1, и для любой концевой вершины $\mathbf{u}$ верно равенство $\rho(\mathbf{u}, \mathbf{c}_{s+2}) = s$.

Доказательство. Дуги дерева T направлены от листьев к корню $\mathbf{c}_{s+2}$. Поэтому полустепени исхода всех вершин, кроме корня, равны 1, а полустепень исхода корня равна 0.

Покажем, что в орграфе G_2 полустепень захода любой вершины $\mathbf{v}$ не превосходит q^m . Пусть $\mathbf{v}$ – не концевая вершина: $\mathbf{v} = \tilde{F}(\mathbf{w})$. Если $\mathbf{x} \in \tilde{F}^{-1}(\mathbf{v})$, то $\bar{\mathbf{x}} = \bar{\mathbf{w}}$ (по модулю радикала все вершины орграфа G_2 принадлежат одному циклу). Поскольку индекс нильпотентности кольца R_2 равен 2, число $\tilde{F}$ -прообразов вершины $\mathbf{v}$ не превосходит q^m .

Поскольку $\mathbf{c}_{s+1}$ – особая вершина, в соответствии с леммой 9 полустепень захода вершины $\mathbf{c}_{s+2}$ в орграфе G_2 не меньше q^m . Тогда полустепень захода вершины $\mathbf{c}_{s+2}$ в орграфе G_2 равна q^m , а в дереве T равна $(q^m - 1)$. Рассмотрим $\mathbf{v}_1$ – один из $\tilde{F}$ -прообразов вершины $\mathbf{c}_{s+2}$ в дереве T . Так как $\bar{\mathbf{v}}_1 = \bar{\mathbf{c}}_{s+1}$ и вершина $\mathbf{c}_s$ несингулярна, существует единственный вектор $\mathbf{r}_1 \in R_2^m$ со свойством

$$\tilde{F}(\mathbf{c}_s + p\mathbf{r}_1) = \mathbf{c}_{s+1} + p\mathbf{r}_1 J_{\tilde{F}}(\mathbf{c}_s) = \mathbf{v}_1.$$

Это означает, что у вершины $\mathbf{v}_1$ полустепень захода равна 1 и ее единственный $\tilde{F}$ -прообраз равен $\mathbf{c}_s + p\mathbf{r}_1$.

Положим $\mathbf{v}_2 = \mathbf{c}_s + p\mathbf{r}_1$. Аналогично, поскольку вершина $\mathbf{c}_{s-1}$ несингулярна, существует единственный вектор $\mathbf{r}_2 \in R_2^m$ со свойством

$$\tilde{F}(\mathbf{c}_{s-1} + p\mathbf{r}_2) = \mathbf{c}_s + p\mathbf{r}_2 J_{\tilde{F}}(\mathbf{c}_{s-1}) = \mathbf{v}_2.$$

Следовательно, у вершины $\mathbf{v}_2$ есть единственный $\tilde{F}$ -прообраз, равный $\mathbf{c}_{s-1} + p\mathbf{r}_2$. Обозначим $\mathbf{v}_3 = \mathbf{c}_{s-1} + p\mathbf{r}_2$. Продолжая этот процесс далее, получим, что в дереве T есть ориентированная цепь

$$\mathbf{v}_s \rightarrow \mathbf{v}_{s-1} \rightarrow \dots \rightarrow \mathbf{v}_2 \rightarrow \mathbf{v}_1, \quad (20)$$

в которой полустепени захода всех вершин, кроме $\mathbf{v}_s$, равны 1, и $\bar{\mathbf{v}}_s = \bar{\mathbf{c}}_2$. Покажем, что $\mathbf{v}_s$ – концевая вершина дерева T .

Так как $\mathbf{c}_2 = \tilde{F}(\mathbf{c}_1)$ и $\mathbf{c}_1$ – особая вершина, то по лемме 9 число $\tilde{F}$ -прообразов вершины $\mathbf{c}_2$ равно q^m . Это означает, что любой вектор вида $\mathbf{c}_1 + p\mathbf{r}$ является $\tilde{F}$ -прообразом вершины $\mathbf{c}_2$ и не является $\tilde{F}$ -прообразом вершины $\mathbf{v}_s$. Поэтому $\mathbf{v}_s$ – концевая вершина дерева T .

Итак, дерево T состоит из $(q^m - 1)$ попарно не пересекающихся по вершинам цепей вида (20), вершины $\mathbf{c}_{s+2}$ и дуг, соединяющих конечные вершины цепей вида (20) с вершиной $\mathbf{c}_{s+2}$. Всего в дереве T имеется

$(q^m - 1)s + 1$ вершин, и расстояние от любой концевой вершины дерева T до корня $\mathbf{c}_{s+2}$ равно s . $\square$

Утверждение 10 является m -мерным аналогом утверждения 11 из [10]. Следующая теорема – центральный результат этого раздела.

Теорема 11. Пусть $\bar{F}$ – подстановка и выполнено условие (17). Если $N_{\bar{F}}$ – количество особых вершин в орграфе $G_{\bar{F}, R^m}$ и $K(G_{F, R^m})$ – множество концевых вершин орграфа G_{F, R^m} , то

$$|K(G_{F, R^m})| \geq q^{m(n-2)}(q^m - 1)N_{\bar{F}}.$$

Доказательство. По утверждению 10 число $|K(G_2)|$ концевых вершин в орграфе G_2 в $(q^m - 1)$ раз больше, чем число $N_F(\mathbf{a})$ особых вершин на цикле C_2 (и на цикле псевдоцикла $C_F^\#(\mathbf{a})$). Отсюда согласно (19) имеем:

$$|K(C_F^\#(\mathbf{a}))| \geq q^{m(n-2)}(q^m - 1)N_F(\mathbf{a}).$$

Поскольку $\bar{F}$ – подстановка, все вершины орграфа G_{F, R^m} являются псевдоциклическими, и согласно (6)

$$\begin{aligned} |K(G_{F, R^m})| &= \sum_{i=1}^k |K(C_F^\#(\mathbf{a}_i))| \geq q^{m(n-2)}(q^m - 1) \sum_{i=1}^k N_F(\mathbf{a}_i) \\ &= q^{m(n-2)}(q^m - 1)N_{\bar{F}}, \end{aligned}$$

где $\bar{\mathbf{a}}_1, \bar{\mathbf{a}}_2, \dots, \bar{\mathbf{a}}_k$ – представители всех циклов орграфа $G_{\bar{F}, R^m}$ (по одному представителю каждого цикла). $\square$

Будем говорить, что некоторое свойство выполняется *почти для всех* вершин орграфа G_{F, R^m} , если доля от общего числа вершин, для которых это свойство не выполняется, есть $o(1)$ при $m \rightarrow \infty$.

Следствие 12. Пусть $\bar{F}$ – подстановка, $\Phi(\mathbf{z}) = F(\mathbf{z}^p)$, C_Φ – множество циклических вершин графа G_{Φ, R^m} , подстановка $\Psi = \Phi \mid C_\Phi$ есть ограничение преобразования Φ на множество C_Φ . Тогда:

- а) цикловые структуры постановок Ψ и $\bar{\Phi}$ совпадают ($[\Psi] = [\bar{\Phi}]$),
- б) почти все вершины орграфа G_{Φ, R^m} являются концевыми.

Доказательство. Преобразование $\bar{\Phi}$ – подстановка как суперпозиция подстановок $\bar{F}$ и $\mathbf{z} \mapsto \mathbf{z}^p$. Непосредственно проверяется, что все вершины орграфа G_{Φ, R^m} являются особыми. В соответствии с п. 2 теоремы 6 длины циклов подстановки $\Psi = \Phi \mid C_\Phi$ не изменяются при

приведении по модулю радикала, т. е. верен п. а). П. б) следует из теоремы 11:

$$|K(G_{\Phi, R^m})| \geq q^{m(n-2)}(q^m - 1)q^m, \quad \frac{|K(G_{\Phi, R^m})|}{q^{mn}} = 1 - q^{-m}.$$

□

Преобразования вида $F(\mathbf{z}^p)$, где $\bar{F}$ – подстановка, в определенном смысле противоположны МДЦ-преобразованиям из работ [12, 13]: у них самые маленькие циклы и самые «ветвистые» подходы. Векторные последовательности, вырабатываемые соответствующим полиномиальным генератором, обладают короткими отрезками апериодичности (утверждение 8).

Во всех утверждениях этого раздела предполагалось, что выполнено условие (17). В следующем разделе будет показано, что условие (17) выполняется для всякого особого псевдоцикла.

4. Строение сингулярного псевдоцикла

Всюду в этом разделе $\mathbf{a} \in SC_F^\#$, $G_{\mathbf{a}} = C_F^\#(\mathbf{a})$, $\tau = \tau(F, 1, \mathbf{a})$, $f = F^{[\tau]}$. Всякой вершине $\mathbf{b}$ орграфа $G_{\mathbf{a}}$ сопоставим характеристический многочлен $\chi_{\mathbf{b}}(x) \in \bar{R}[x]$ матрицы $\overline{J_f(\mathbf{b})}$. Ввиду (4) для любых двух вершин $\mathbf{b}_1$ и $\mathbf{b}_2$ орграфа $G_{\mathbf{a}}$ матрицы $\overline{J_f(\mathbf{b}_1)}$ и $\overline{J_f(\mathbf{b}_2)}$ отличаются лишь «циклическим сдвигом сомножителей»:

$$\overline{J_f(\mathbf{b}_1)} = \prod_{s=0}^{\tau-1} \overline{J_F(F^{[s]}(\mathbf{b}_1))}, \quad \overline{J_f(\mathbf{b}_2)} = \prod_{s=l}^{\tau-1} \overline{J_F(F^{[s]}(\mathbf{b}_1))} \times \prod_{s=0}^{l-1} \overline{J_F(F^{[s]}(\mathbf{b}_1))},$$

где $0 \leq l \leq \tau$. Хорошо известно (см., например, [16, задача 40.12]), что для любых квадратных матриц A и B над полем характеристические многочлены матриц AB и BA совпадают. Поэтому $\chi_{\mathbf{b}_1}(x) = \chi_{\mathbf{b}_2}(x)$, и можно говорить о *характеристическом многочлене $\chi(x)$ псевдоцикла $G_{\mathbf{a}}$* .

Дефектом $\delta(G_{\mathbf{a}})$ псевдоцикла $G_{\mathbf{a}}$ назовем длину подхода характеристического многочлена $\chi(x)$ (см., например, [5]). Пусть $\mathbf{b}$ – произвольная вершина орграфа $G_{\mathbf{a}}$, $GL_{\mathbf{b}}$ – орграф линейного преобразования пространства строк $\bar{R}^m$, заданного матрицей $\overline{J_f(\mathbf{b})}$. Поскольку характеристический многочлен матрицы $\overline{J_f(\mathbf{b})}$ равен $\chi(x)$, количество циклических вершин орграфа $GL_{\mathbf{b}}$ равно $q^{\delta(G_{\mathbf{a}})}$. Обозначим через $\delta_{\mathbf{b}}$ дефект матрицы $\overline{J_f(\mathbf{b})}$.

Лемма 13. Для любой вершины $\mathbf{b}$ орграфа $G_{\mathbf{a}}$ следующие утверждения эквивалентны:

- 1) $\delta(G_{\mathbf{a}}) = \delta_{\mathbf{b}}$,
- 2) 0 не является кратным корнем минимального многочлена матрицы $\overline{J_f(\mathbf{b})}$,
- 3) в орграфе $GL_{\mathbf{b}}$ расстояние от всякой концевой вершины до соответствующего цикла равно 1.

Доказательство. 1) $\Rightarrow$ 2). От противного: пусть минимальный многочлен матрицы $\overline{J_f(\mathbf{b})}$ кратен x^2 . Это означает, что во второй нормальной форме N_2 матрицы $\overline{J_f(\mathbf{b})}$ есть клетка вида $S(x^k)$, где $k \geq 2$. Поскольку $\delta(G_{\mathbf{a}})$ есть сумма размеров необратимых сопровождающих клеток в матрице N_2 и $\text{rank} S(x^k) \geq 1$, имеем: $\delta_{\mathbf{b}} < \delta(G_{\mathbf{a}})$, что противоречит условию 1).

2) $\Rightarrow$ 3). В силу п. 2) вторая нормальная форма N_2 матрицы $\overline{J_f(\mathbf{b})}$ имеет следующий квазидиагональный вид:

$$N_2 = \text{Diag}(S(\psi_1), S(\psi_2), \dots, S(\psi_t), 0, \dots, 0), \quad (21)$$

где $\psi_1, \dots, \psi_t$ — унитарные реверсивные многочлены над $\bar{R}$ степеней $m_1, \dots, m_t$ соответственно. Пусть $T \in \bar{R}_{m,m}$ — трансформирующая матрица:

$$T^{-1} \cdot \overline{J_f(\mathbf{b})} \cdot T = N_2. \quad (22)$$

Ввиду (21) циклическими являются те и только те вершины $\alpha \in \bar{R}^m$, которые удовлетворяют равенству

$$\alpha \cdot T = (a_1, a_2, \dots, a_r, 0, \dots, 0),$$

где $r = m_1 + m_2 + \dots + m_t$, $a_i \in \bar{R}$, $i = 1, 2, \dots, r$. Отсюда, из (21) и (22) следует, что для любого вектора $\beta \in \bar{R}^m$ вершина $\beta \cdot \overline{J_f(\mathbf{b})}$ является циклической, т. е. выполняется п. 3).

3) $\Rightarrow$ 1). Из п. 3) следует, что многочлен x^2 не делит минимальный многочлен матрицы $\overline{J_f(\mathbf{b})}$. Это означает, что вторая нормальная форма N_2 матрицы $\overline{J_f(\mathbf{b})}$ имеет вид (21), и ранг $r_f(\bar{\mathbf{b}})$ матрицы $\overline{J_f(\mathbf{b})}$ удовлетворяет равенствам

$$r_f(\bar{\mathbf{b}}) = m_1 + m_2 + \dots + m_t = m - \delta(G_{\mathbf{a}}).$$

Отсюда вытекает 1). □

Напомним (см. раздел 3), что G_2 есть образ псевдоцикла G_a под действием естественного эпиморфизма φ_2 . Цель этого раздела – описать строение орграфа G_2 при условии, что для любой вершины $\mathbf{b}$ псевдоцикла G_a выполняется условие 2) леммы 13.

Пусть VG_2 – множество вершин орграфа G_2 , $\tilde{f} = \tilde{F}^{[\tau]}$. Всякой вершине $\mathbf{b} \in VG_2$ сопоставим орграф $GL_{\mathbf{b}}$ линейного преобразования пространства $\bar{R}^m$, заданного матрицей $J_{\tilde{f}}(\bar{\mathbf{b}})$.

Лемма 14. *Если $\mathbf{b}$ – циклическая вершина орграфа G_2 , то для всякого вектора $\mathbf{x} \in R_2^m$ следующие утверждения эквивалентны:*

- 1) $\mathbf{b} + p\mathbf{x}$ – циклическая вершина орграфа G_2 ,
- 2) $\bar{\mathbf{x}}$ – циклическая вершина орграфа $GL_{\mathbf{b}}$.

Доказательство. В силу (2) для всякого вектора $\mathbf{x} \in R_2^m$ верно равенство

$$\tilde{f}(\mathbf{b} + p\mathbf{x}) = \tilde{f}(\mathbf{b}) + p\mathbf{x}J_{\tilde{f}}(\mathbf{b}). \quad (23)$$

Длины всех циклов орграфа G_2 кратны τ . Следовательно, существует такое $t \in \mathbb{N}$, что $\tilde{f}^{[t]}(\mathbf{b}) = \mathbf{b}$. Тогда из (23) следует равенство

$$\tilde{f}^{[t]}(\mathbf{b} + p\mathbf{x}) = \mathbf{b} + p\mathbf{x}J_{\tilde{f}}(\mathbf{b})^t,$$

и, следовательно,

$$\forall s \geq 1 : \quad \tilde{f}^{[ts]}(\mathbf{b} + p\mathbf{x}) = \mathbf{b} + p\mathbf{x}J_{\tilde{f}}(\mathbf{b})^{ts}. \quad (24)$$

Если $\mathbf{b} + p\mathbf{x}$ – циклическая вершина, то существует такое $d \geq 1$, что

$$\tilde{f}^{[d]}(\mathbf{b} + p\mathbf{x}) = \tilde{F}^{[\tau d]}(\mathbf{b} + p\mathbf{x}) = \mathbf{b} + p\mathbf{x}.$$

Тогда согласно (24) имеем:

$$\mathbf{b} + p\mathbf{x} = \tilde{f}^{[td]}(\mathbf{b} + p\mathbf{x}) = \mathbf{b} + p\mathbf{x}J_{\tilde{f}}(\mathbf{b})^{td}.$$

Следовательно, $\bar{\mathbf{x}} = \bar{\mathbf{x}} \cdot J_{\tilde{f}}(\bar{\mathbf{b}})^{td}$, и $\bar{\mathbf{x}}$ – циклическая вершина орграфа $GL_{\mathbf{b}}$.

Обратно, пусть $\bar{\mathbf{x}}$ – циклическая вершина орграфа $GL_{\mathbf{b}}$. Существует такое $k \geq 1$, что $\bar{\mathbf{x}} = \bar{\mathbf{x}} \cdot J_{\tilde{f}}(\bar{\mathbf{b}})^k$. Из (24) следует цепочка равенств

$$\tilde{f}^{[tk]}(\mathbf{b} + p\mathbf{x}) = \mathbf{b} + p\mathbf{x}J_{\tilde{f}}(\mathbf{b})^{tk} = \mathbf{b} + p\mathbf{x},$$

и, следовательно, вершина $\mathbf{b} + p\mathbf{x}$ – циклическая. $\square$

Лемма 15. Если e – единица поля $\bar{R}$ и $\chi(e) \neq 0$, то в орграфе G_a имеется единственный цикл длины τ .

Доказательство. Дословно так же, как при доказательстве утверждения 1 из [12], можно показать, что при условии $\chi(e) \neq 0$ для всякой вершины $\mathbf{b}$ орграфа G_a существует единственная циклическая вершина $\mathbf{b}^*$ этого орграфа со свойствами $\bar{\mathbf{b}}^* = \bar{\mathbf{b}}$ и $\tau = \tau(F, 1, \mathbf{b}^*) = \tau(F, n, \mathbf{b}^*)$. Отсюда вытекают существование и единственность цикла длины τ в орграфе G_a . $\square$

Пусть CG_2 – подграф орграфа G_2 , порожденный множеством циклических вершин орграфа G_2 (см., например, [1]), а CGL_a – подграф орграфа GL_a , порожденный множеством циклических вершин орграфа GL_a . Обозначим: $Z_2(y)$ – цикловой тип орграфа CG_2 , $Z_a(y)$ – цикловой тип орграфа CGL_a (см. [5]). Следующая теорема описывает «циклическую составляющую» орграфа G_2 .

Теорема 16. Пусть $\mathbf{a} \in SC_F^\#$, $\chi(e) \neq 0$, $G_a = C_F^\#(\mathbf{a})$, G_2 – образ орграфа G_a под действием естественного эпиморфизма φ_2 . Тогда $Z_2(y) = Z_a(y^\tau)$.

Доказательство. Пусть $\mathbf{a}^*$ – вершина орграфа G_2 со свойствами $\bar{\mathbf{a}}^* = \bar{\mathbf{a}}$ и $\tau = \tau(F, 1, \mathbf{a}^*) = \tau(F, 2, \mathbf{a}^*)$ (см. доказательство леммы 15), $\tilde{\mathbf{a}} = \varphi_2(\mathbf{a})$. Тогда $\tilde{f}(\mathbf{a}^*) = \mathbf{a}^*$ и

$$J_{\tilde{f}}(\mathbf{a}^*) \equiv J_{\tilde{f}}(\tilde{\mathbf{a}}) \pmod{pR}. \quad (25)$$

Установим взаимно однозначное соответствие ψ между циклами орграфов CG_2 и CGL_a так, чтобы длины $l(C)$ и $l(\psi(C))$ циклов C и $\psi(C)$ были связаны соотношением

$$l(C) = \tau \cdot l(\psi(C)). \quad (26)$$

Пусть C – цикл орграфа CG_2 . Поскольку вершина $\bar{\mathbf{a}}$ принадлежит циклу $\bar{C}$, существует такой вектор $\mathbf{x} \in R_2^m$, что вершина $\mathbf{a}^* + p\mathbf{x}$ принадлежит циклу C . Обозначим через $\psi(C)$ тот цикл орграфа GL_a , которому принадлежит вершина $\bar{\mathbf{x}}$. Докажем корректность, инъективность и сюръективность ψ .

1. Корректность и инъективность. Будем говорить, что две циклические вершины $\mathbf{u}$ и $\mathbf{v}$ эквивалентны (обозначение: $\mathbf{u} \sim \mathbf{v}$), если они принадлежат одному циклу. В силу (25) имеет место цепочка эквивалентностей:

$$(\mathbf{a}^* + p\mathbf{x} \sim \mathbf{a}^* + p\mathbf{y}) \Leftrightarrow (\exists t \geq 0 : \tilde{F}^{[t]}(\mathbf{a}^* + p\mathbf{x}) = \mathbf{a}^* + p\mathbf{y}) \Leftrightarrow$$

$$\Leftrightarrow (\exists k \geq 0 : \tilde{f}^{[k]}(\mathbf{a}^* + p\mathbf{x}) = \mathbf{a}^* + p\mathbf{y}) \Leftrightarrow (\exists k \geq 0 : \mathbf{x}J_{\tilde{f}}(\tilde{\mathbf{a}})^k \equiv \mathbf{y} \pmod{pR}).$$

Последнее условие равносильно тому, что $\bar{\mathbf{x}} \sim \bar{\mathbf{y}}$ в орграфе $GL_{\mathbf{a}}$. Отсюда следуют корректность и инъективность отображения ψ .

2. Сюръективность. Пусть C' – цикл орграфа $GL_{\mathbf{a}}$, $\bar{\mathbf{x}}$ – вершина, принадлежащая циклу C' . Поскольку вершина $\bar{\mathbf{x}}$ – циклическая, то по лемме 14 и вершина $\mathbf{a}^* + p\mathbf{x}$ – циклическая. Обозначим через C тот цикл орграфа CG_2 , которому принадлежит вершина $\mathbf{a}^* + p\mathbf{x}$. Тогда $\psi(C) = C'$.

Осталось доказать (26). Во-первых, заметим, что $l(C) \mid l(\psi(C)) \cdot \tau$. Действительно, пусть вектор $\mathbf{x} \in R_2^m$ таков, что вершина $\mathbf{a}^* + p\mathbf{x}$ принадлежит циклу C . Тогда

$$\tilde{F}^{[l(\psi(C)) \cdot \tau]}(\mathbf{a}^* + p\mathbf{x}) = \tilde{f}^{[l(\psi(C))]}(\mathbf{a}^* + p\mathbf{x}) = \mathbf{a}^* + p\mathbf{x}J_{\tilde{f}}(\tilde{\mathbf{a}})^{l(\psi(C))} = \mathbf{a}^* + p\mathbf{x}.$$

Чтобы доказать соотношение $l(\psi(C)) \cdot \tau \mid l(C)$, рассмотрим равенство

$$l(\psi(C)) = \min\{t \geq 1 : \bar{\mathbf{x}}J_{\tilde{f}}(\tilde{\mathbf{a}})^t = \bar{\mathbf{x}}\}. \quad (27)$$

Поскольку

$$\forall t \geq 1 : \tilde{f}^{[t]}(\mathbf{a}^* + p\mathbf{x}) = \mathbf{a}^* + p\mathbf{x}J_{\tilde{f}}(\tilde{\mathbf{a}})^t,$$

из (27) получаем, что $l(\psi(C))$ есть период последовательности

$$\mathbf{a}^* + p\mathbf{x}, \tilde{f}(\mathbf{a}^* + p\mathbf{x}), \tilde{f}^{[2]}(\mathbf{a}^* + p\mathbf{x}), \dots,$$

т. е. $l(\psi(C))$ совпадает с периодом регулярной $(0, \tau)$ -выборки из последовательности

$$\mathbf{a}^* + p\mathbf{x}, \tilde{F}(\mathbf{a}^* + p\mathbf{x}), \tilde{F}^{[2]}(\mathbf{a}^* + p\mathbf{x}), \dots \quad (28)$$

Период последовательности (28) равен $l(C)$. Так как $l(\bar{C}) = \tau$, верно соотношение $\tau \mid l(C)$. Наименьшее общее кратное периодов всех τ -выборок из последовательности (28) равно $l(C)/\tau$, поэтому $l(\psi(C)) \cdot \tau \mid l(C)$. $\square$

Всюду далее будем считать, что $\chi(e) \neq 0$ и для любой вершины $\mathbf{b}$ орграфа $G_{\mathbf{a}}$ значение 0 не является кратным корнем минимального многочлена матрицы $J_f(\mathbf{b})$. Рассмотрим последовательность циклических вершин $\mathbf{c}_0, \mathbf{c}_1, \dots \in VG_2$, удовлетворяющую соотношению

$$\forall i \geq 0 : \mathbf{c}_{i+1} = \tilde{F}(\mathbf{c}_i).$$

Тогда $\bar{\mathbf{c}}_0, \bar{\mathbf{c}}_1, \dots, \bar{\mathbf{c}}_{\tau-1}$ – цикл в орграфе $G_{\bar{F}, \bar{R}^m}$. Для всякого $i \in \{0, 1, \dots, \tau-1\}$ обозначим через δ_i дефект матрицы $J_{\bar{F}}(\bar{\mathbf{c}}_i)$. Напомним (см. начало раздела), что $\delta_{\mathbf{c}}$ есть дефект матрицы $J_{\bar{F}}(\bar{\mathbf{c}})$, а $\delta(G_2)$ – дефект многочлена $\chi(x)$. Согласно п. 1 леммы 13

$$\forall i \in \{0, 1, \dots, \tau-1\} : \quad \delta_i \leq \delta_{\mathbf{c}_i} = \delta(G_2). \quad (29)$$

Введем обозначения $\delta = \delta(G_2)$, $r = m - \delta$. По п. 3 леммы 13 в орграфе $GL_{\mathbf{c}_i}$ все подходы к циклам имеют длину 1 и существует ровно $q^m - q^r$ концевых вершин.

Для всякой сингулярной циклической вершины $\mathbf{b}$ орграфа G_2 обозначим через $s(\mathbf{b})$ расстояние от ближайшей к $\mathbf{b}$ сингулярной циклической вершины до $\mathbf{b}$:

$$s(\mathbf{b}) = \min_{\mathbf{c} \in SG_2 \setminus \{\mathbf{b}\}} \{\rho(\mathbf{c}, \mathbf{b})\},$$

где SG_2 – множество сингулярных циклических вершин орграфа G_2 . Рассмотрим участок $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\tau-1}$ цикла орграфа G_2 . По утверждению 5 если $\mathbf{c}_i$ несингулярна, то вершина $\mathbf{c}_{i \oplus 1}$ регулярна (здесь $\oplus$ – сложение по модулю τ). Пусть вершина $\mathbf{c}_i$ сингулярна. Ввиду вытекающего из (2) соотношения

$$\forall \mathbf{x} \in R_2^m : \quad \tilde{F}(\mathbf{c}_i + p\mathbf{x}) = \mathbf{c}_{i+1} + p\mathbf{x}J_{\bar{F}}(\mathbf{c}_i)$$

полустепень захода вершины $\mathbf{c}_{i+1}$ равна q^{δ_i} . В силу (29) количество циклических вершин в орграфе $GL_{\mathbf{c}_i}$ равно q^r , и сумма Σ_2 полустепеней захода в циклические вершины орграфа G_2 вычисляется по формуле

$$\Sigma_2 = q^r \cdot (q^{\delta_0} + q^{\delta_1} + \dots + q^{\delta_{\tau-1}}). \quad (30)$$

Выберем и зафиксируем такое $i \in \{0, 1, \dots, \tau-1\}$, что $\mathbf{c}_i$ – сингулярная вершина. Согласно лемме 14 каждая из $q^m - q^r$ концевых вершин орграфа $GL_{\mathbf{c}_i}$ является ациклической вершиной орграфа G_2 . Пусть $\mathbf{b}$ – произвольная концевая вершина орграфа $GL_{\mathbf{c}_i}$. Так как $\bar{\mathbf{b}} = \bar{\mathbf{c}}_i$, вершина $\mathbf{b}$ является сингулярной, и в орграфе G_2 существует цепь вида (20):

$$\mathbf{b} \leftarrow \mathbf{v}_1 \leftarrow \mathbf{v}_2 \leftarrow \dots \leftarrow \mathbf{v}_{s(\mathbf{c}_i)-1}, \quad (31)$$

где $\bar{\mathbf{v}}_j = \bar{\mathbf{c}}_{i \ominus j}$, $j = 1, 2, \dots, s(\mathbf{c}_i) - 1$, $\ominus$ – вычитание по модулю τ . Все вершины $\mathbf{v}_j$ несингулярны, $j = 1, 2, \dots, s(\mathbf{c}_i) - 1$. В этой ситуации будем говорить, что вершина $\mathbf{b}$ порождает цепь (31). Пусть $K(GL_{\mathbf{c}_i})$ – множество концевых вершин орграфа $GL_{\mathbf{c}_i}$,

$$I = \{i \in \{0, 1, \dots, \tau-1\} : \mathbf{c}_i \in SG_2\}.$$

По утверждению 5 ввиду несингулярности всех вершин $\mathbf{v}_j$ вершины

$$\mathbf{b}, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{s(\mathbf{c}_i)-2}$$

регулярны. Поэтому разные вершины $\mathbf{b}$ из множества

$$\bigcup_{i \in I} K(GL_{\mathbf{c}_i})$$

порождают не пересекающиеся по вершинам цепи (31).

Вычислим суммарное количество K_2 ациклических вершин орграфа G_2 , содержащихся в цепях (31). Пусть $i \in I$. Суммарная длина цепей (31), для которых $\mathbf{b} \in K(GL_{\mathbf{c}_i})$, равна $(q^m - q^r)s(\mathbf{c}_i)$. Поэтому

$$K_2 = (q^m - q^r) \cdot \sum_{i \in I} s(\mathbf{c}_i) = (q^m - q^r) \cdot \tau. \quad (32)$$

В силу теоремы 16 орграф G_2 имеет ровно $q^r \tau$ циклических вершин. Поскольку $|VG_2| = q^m \tau$, из (32) следует, что все ациклические вершины орграфа G_2 принадлежат цепям (31). Поэтому величина Σ_2 может быть вычислена по формуле

$$\Sigma_2 = q^r \tau + (q^m - q^r) \cdot |I|.$$

Рассматривая это равенство совместно с (30), получаем:

$$(q^m - q^r) \cdot |I| = q^r \cdot \sum_{i \in I} (q^{\delta_i} - 1). \quad (33)$$

Из (33) вытекает цепочка неравенств

$$(q^m - q^r) \cdot |I| = q^r \cdot \sum_{i \in I} (q^{\delta_i} - 1) \leq q^r \cdot |I| \cdot (q^\delta - 1) = (q^m - q^r) \cdot |I|.$$

Отсюда

$$\forall i \in I : \quad \delta_i = \delta. \quad (34)$$

В частности, из равенства (34) следует, что для всякого особого псевдоцикла $C_F^\#(\mathbf{a})$ выполняется условие (17). Этот факт позволяет существенно усилить результаты раздела 3.

Все сингулярные вершины особого псевдоцикла являются особыми. Как показано при доказательстве теоремы 11, если $\bar{F}$ – подстановка, то число $|K(C_F^\#(\mathbf{a}))|$ концевых вершин особого псевдоцикла $C_F^\#(\mathbf{a})$ удовлетворяет неравенству

$$|K(C_F^\#(\mathbf{a}))| \geq q^{m(n-2)}(q^m - 1)N_F(\mathbf{a}),$$

где $N_F(\mathbf{a})$ – число особых вершин в множестве $C_F(\mathbf{a})$ (см. утверждение 8). Дословно повторяя доказательство теоремы 11, получаем следующее утверждение.

Теорема 17. *Если $\bar{F}$ – подстановка, $N_{\bar{F}}$ – количество особых вершин в орграфе $G_{\bar{F}, R^m}$ и $K(G_{F, R^m})$ – множество концевых вершин орграфа G_{F, R^m} , то*

$$|K(G_{F, R^m})| \geq q^{m(n-2)}(q^m - 1)N_{\bar{F}}.$$

Теорема 17 обобщает теорему 11, поскольку не требует выполнения условия (17). Она является m -мерным аналогом следствия 6 из [10]. Аналогичный результат для $m = 1$ и произвольного конечного коммутативного локального кольца R , вообще говоря, не являющегося кольцом главных идеалов, получен В.Е. Викторенковым в [3].

Пусть $\mathbf{a}$ – сингулярная псевдоциклическая вершина орграфа G_{F, R^m} , $G_{\mathbf{a}}$ – соответствующий сингулярный псевдоцикл. Напомним (см. начало раздела), что через $\delta(G_{\mathbf{a}})$ обозначена длина подхода (дефект) характеристического многочлена χ псевдоцикла $G_{\mathbf{a}}$. Учитывая, что минимальный многочлен матрицы над полем делит ее характеристический многочлен, а любой неприводимый делитель характеристического многочлена является делителем минимального многочлена, легко показать, что в случае $\delta(G_{\mathbf{a}}) \in \{0, 1, m\}$ для любой вершины $\mathbf{b}$ орграфа $G_{\mathbf{a}}$ значение 0 не является кратным корнем минимального многочлена матрицы $\bar{J}_f(\mathbf{b})$. При этом если $\delta(G_{\mathbf{a}}) = 0$, то псевдоцикл $G_{\mathbf{a}}$ – несингулярный, а если $\delta(G_{\mathbf{a}}) = m$, то псевдоцикл $G_{\mathbf{a}}$ – особый. Из (34) вытекает следующая теорема.

Теорема 18. *Пусть во введенных обозначениях $\delta(G_{\mathbf{a}}) \in \{0, 1, m\}$, $\chi(e) \neq 0$, $\oplus$ – сложение по модулю τ . Для всякого $i \in \{0, 1, \dots, \tau - 1\}$ выполняются следующие утверждения:*

- 1) *если вершина $\mathbf{c}_i$ несингулярна, то $\mathbf{c}_{i \oplus 1}$ – циклическая вершина без подхода,*
- 2) *если вершина $\mathbf{c}_i$ сингулярна, то подход к циклической вершине $\mathbf{c}_{i \oplus 1}$ состоит из $(q^\delta - 1)$ цепей (31), каждая из которых соединена дугой с вершиной $\mathbf{c}_{i \oplus 1}$.*

Осталось показать, что ситуация $\delta(G_{\mathbf{a}}) = 1$, $\chi(e) \neq 0$ возможна. Пусть

$$(F_1(z_1, z_2, \dots, z_{m-1}), F_2(z_1, z_2, \dots, z_{m-1}), \dots, F_{m-1}(z_1, z_2, \dots, z_{m-1}))$$

есть МДЦ-подстановка на модуле R^{m-1} (см. [12, 13]), и преобразование F определено равенством

$$F(\mathbf{z}) = (F_1(z_1, z_2, \dots, z_{m-1}), F_2(z_1, z_2, \dots, z_{m-1}), \dots, F_{m-1}(z_1, z_2, \dots, z_{m-1}), z_m^p).$$

Очевидно, $\bar{F}$ – биекция. Из результатов работ [12, 13] следует, что для всякой вершины $\mathbf{a} \in R^m$ характеристический многочлен $\chi(x)$ псевдоцикла $G_{\mathbf{a}}$ имеет вид $xg(x)$, где $g(e) \neq 0$ и $g(0) \neq 0$. Таким образом, $\delta(G_{\mathbf{a}}) = 1$ и $\chi(e) \neq 0$.

Список литературы

- [1] Асанов М.О., Баранский В.А., Расин В.В., *Дискретная математика: графы, матроиды, алгоритмы. 2-е изд., испр. и доп.*, Санкт-Петербург-Москва-Краснодар: Лань, 2010, 368 с.
- [2] Викторенков В.Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозр. прикл. и промышл. матем.*, **7**:2 (2000), 327.
- [3] Викторенков В.Е., “О строении орграфов полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29**:3 (2017), 3–23.
- [4] Викторенков В.Е., “Цикловая структура случайных подстановок на множестве двухцветных элементов, Γ ”, *Математические вопросы криптографии*, **10**:3 (2019), 9–32.
- [5] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра. Учебник. 2-е изд., испр. и доп.*, Санкт-Петербург-Москва-Краснодар: Лань, 2015, 608 с.
- [6] Елизаров В.П., *Конечные кольца. Основы теории*, М.: Гелиос-АРВ, 2006, 304 с.
- [7] Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В., *Введение в теоретико-числовые методы криптографии*, Санкт-Петербург-Москва-Краснодар: Лань, 2011, 394 с.
- [8] Ермилов Д.М., “Количество полиномиальных преобразований максимального периода над кольцами Галуа нечетной характеристики”, *Математические вопросы криптографии*, **9**:4 (2018), 85–100.
- [9] Ермилов Д.М., Козлитин О.А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4**:1 (2013), 27–57.
- [10] Ермилов Д.М., Козлитин О.А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **6**:3 (2015), 47–73.
- [11] Козлитин О.А., “Оценка длины максимального цикла в графе полиномиального преобразования кольца Галуа–Эйзенштейна”, *Дискретная математика*, **29**:4 (2017), 41–58.
- [12] Козлитин О.А., “Периодические свойства многомерного полиномиального генератора над кольцом Галуа. Γ ”, *Математические вопросы криптографии*, **9**:3 (2018), 61–98.
- [13] Козлитин О.А., “Периодические свойства многомерного полиномиального генератора над кольцом Галуа. Γ^p ”, *Математические вопросы криптографии*, **11**:1 (2020), 63–100.
- [14] Ларин М.В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14**:2 (2002), 20–32.
- [15] Сачков В.Н., “Оператор редуцирования, Γ ”, *Труды по дискретной математике*, **2** (1998), 282–295.

- [16] *Сборник задач по алгебре*, ред. А.И. Кострикин, М.: Факториал, 1995.
- [17] Dickson L.E., “General theory of modular invariants”, *Trans. Amer. Math. Soc.*, **10**:2 (1909), 123–158.
- [18] Fisher B., “A note on Hensel’s lemma in several variables”, *Proc. Amer. Math. Soc.*, **125** (1997).
- [19] Parvatov N.G., “On the period length of vector sequences generated by polynomials modulo prime powers”, *Прикл. дискрет. матем.*, **1 (31)** (2016), 57–61.