Модел. и анализ информ. систем. Т. **17**, № **3** (2010) 58–71

УДК 512.558+512.542.3

Рекуррентные последовательности над почтикольцами

Сбоев А.В.

Ярославский государственный университет им. П. Г. Демидова

e-mail: sboev.andrey@gmail.com

получена 1 июня 2010

Ключевые слова: рекуррентные последовательности, почтикольца, экстраспециальные p-группы, эндоморфизмы групп

Исследуются периоды и статистические свойства линейных рекуррентных последовательностей над почтикольцами, порождёнными эндоморфизмами конечных неабелевых экстраспециальных 2-групп.

1. Введение

Обычно линейная рекуррентная последовательность над полем P задаётся уравнением вида

$$s_i = \sum_{j=1}^{n} f_j s_{i-j}, \tag{1}$$

где $s_j \in P, \quad f_1, \ldots, f_n \in P$.

Как известно, подобная последовательность легко предсказуема: для определения коэффициентов уравнения (1) с помощью алгоритма Берлекэмпа – Мэсси [1] требуется всего лишь $2n$ первых элементов последовательности. Существует также расширение этого алгоритма для работы с последовательностями над кольцами [2].

Естественным образом возникает идея использования для построения линейной рекурренты более сложных алгебраических систем, нежели поля и кольца. В настоящей работе рассматривается подобный подход с использованием почтиколец в качестве альтернативы полям и кольцам традиционной схемы.

Напомним определение почтикольца.

Определение 1. *Пусть R — множество, на котором определены бинарные операции сложение и умножение, обладающие свойствами:*

1. $\langle R, + \rangle$ — *группа (не обязательно абелева);*

2. $\langle R, \cdot \rangle$ — *полугруппа;*

3. $\forall x, y, z \in R$ *выполнено:* $(x + y)z = xz + yz$.

В этом случае R *называется (правым) почтикольцом.*

Опишем важный пример почтикольца. Пусть $\langle G, + \rangle$ — конечная (необязательно абелева) группа, $M(G) = \langle G^G, +, \cdot \rangle$ — множество всех отображений из G в G с операциями поточечного сложения (т.е. $(f + g)(x) = f(x) + g(x)$ для любых двух отображений $f, g \in M(G)$ и любого $x \in G$) и суперпозицией отображений в качестве умножения (т.е. $fg(x) = f(g(x))$ для любых двух отображений $f, g \in M(G)$ и любого $\in G$).

Вообще говоря, в $M(G)$ не выполняется левая дистрибутивность. Нетрудно убедиться, что множество дистрибутивных элементов почтикольца $M(G)$ совпадает с множеством эндоморфизмов $\mathrm{End}(G) \subseteq M(G)$ группы G. При этом $\mathrm{End}(G)$, не образует замкнутой структуры, поскольку известно, что, хотя произведение двух эндоморфизмов есть эндоморфизм, сумма двух эндоморфизмов, не обязательно является эндоморфизмом.

Однако почтикольцо $E(G)$, порождённое множеством $\mathrm{End}(G)$ эндоморфизмов конечной неабелевой экстраспециальной 2-группы G, оказалось весьма интересным для изучения. В [3] в частности определён порядок почтикольца $E(G)$ для группы диедра $G = D_8$ и для группы кватернионов $G = Q_8$. Кроме того, Л.С. Казариным и В.М. Сидельниковым получены теоретические верхние границы периодов рекуррентных последовательностей над $E(G)$.

В настоящей работе использованы данные теоретические результаты и найдено соотношение между периодом рекуррентной последовательности над $E(G)$ и мультипликативным порядком соответствующей сопровождающей матрицы. Также программно смоделированы вычисления в $E(G)$ и реализован линейный регистр сдвига, что позволило получить некоторые опытные данные. Проведённые эксперименты демонстрируют, что верхние границы периодов, предложенные ранее, скорее всего сильно завышены. Однако изучаемые рекуррентные последовательности имеют сложное аналитическое строение, о чём свидетельствуют результаты исследования их профилей линейной сложности.

2. Рекуррентные последовательности над почтикольцами

2.1 Проблемы арифметики почтиколец

В данном разделе представлены некоторые простые следствия строения, а также некоммутативности и недистрибутивности почтикольца $\mathrm{E}(G)$.

Как в доказательстве теоремы 1 из [3], будем использовать следующее обозначение: $J \leqslant E(G)$ — идеал почтикольца $E(G)$, порождённый эндоморфизмами, переводящими каждый элемент группы G в $Z(G)$.

Лемма 1. *Пусть имеется множество элементов* $X = \{x_{ij} \in E(G),\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m\}$. *Справедливо равенство*

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = \sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij} + \delta, \quad \delta \in J, \delta = \sum_{1\leqslant l<s\leqslant m}\ \sum_{1\leqslant i<j\leqslant n} [x_{is},\ x_{jl}].$$

Доказательство. Мы должны перегруппировать слагаемые двойной суммы:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = (x_{11}+x_{12}+\ldots+x_{1m})+(x_{21}+\ldots+x_{22}+\ldots+x_{2m})+\ldots\ldots+(x_{n1}+\ldots+x_{nm}).$$

Основываясь на тех фактах, что

1. $u+v \ = \ v+u \ -u-v \ + \ u+v \ = \ v+u \ + \ [v,u] \quad \forall u, v \in \mathrm{E(G)}$, и
2. $a+\eta = \eta+a \quad \forall a \in \mathrm{E(G)},\ \eta \in J$,

будем проводить что-то вроде сортировки методом вставок, расплачиваясь за каждый обмен позициями соседних элементов суммы дополнительным слагаемым-коммутатором.

Сгруппируем слагаемые вида x_{i1} и вычислим полученный при этом штраф δ_{i1}. Сначала переместим на нужное место x_{21} с добавочным слагаемым δ_{21} :

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = x_{11} + \underbrace{\boldsymbol{x_{12}} + \ldots + x_{1m}}_{m-1} + \boldsymbol{x_{21}} + \ldots$$

$$\delta_{21} = \sum_{r=2}^{m} [x_{1r},\ x_{21}].$$

Здесь согласно утверждению (2) порядок суммирования произволен.

Теперь возьмёмся за x_{31} :

$$x_{11} + x_{21} + \underbrace{\boldsymbol{x_{12}} + \ldots + x_{1m} + x_{22} + \ldots + x_{2m}}_{2(m-1)} + \boldsymbol{x_{31}} + \ldots$$

$$\delta_{31} + \delta_{32} = \sum_{r=2}^{m} [x_{1r},\ x_{31}] + \sum_{r=1}^{m} [x_{2r},\ x_{31}].$$

Резюмируем

$$\delta_{i1} = \sum_{r=2}^{n}\sum_{t=1}^{r-1}\sum_{s=2}^{m} [x_{ts},\ x_{r1}]$$

Аналогично перемещаем x_{i2}, x_{i3}, и так далее. В итоге получим

$$\delta = \sum_{l=1}^{m-1} \delta_{il} = \sum_{l=1}^{m-1}\sum_{r=2}^{n}\sum_{t=1}^{r-1}\sum_{s=2}^{m} [x_{ts},\ x_{rl}]$$

Упрощаем индексы и выписываем требуемое утверждение

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n} x_{ij} + \sum_{1\leqslant l<s\leqslant m}\ \sum_{1\leqslant i<j\leqslant n} [x_{is},\ x_{jl}].$$

Лемма доказана. □

Лемму 1 мы в дальнейшем будем активно использовать. Поэтому введём для элемента δ единообразную запись с параметрами.

Определение 2. *Пусть имеется множество элементов* $X = \{x_{ij} \in E(G),\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m\}$. *Элемент* $\delta = \delta(X, i, j)$ *такой, что* $\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} = \sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij} + \delta$, *назовём коммутатором суммирования.*

Основное "неудобство" в работе с почтикольцом $\mathrm{E}(G)$ вносит отсутствие левой дистрибутивности. Рассмотрим подробнее, какой ценой даётся "раскрытие скобок".

Лемма 2. *Пусть* $a \in E(G),\ b_j \in E(G),\ 1 \leqslant j \leqslant n,\ a = \sum_{i=1}^{m_a} \alpha_i$, *где* $\alpha_i \in End(G),\ 1 \leqslant i \leqslant m_a$, *тогда*

$$a(\sum_{j=1}^{n} b_j) = \sum_{j=1}^{n} ab_j + \xi,$$

где $\xi = \delta\left(\{\alpha_i b_j\},\ i,\ j\right) \in J$

Доказательство.

$$a(\sum_{j=1}^{n} b_j) = (\sum_{i=1}^{m_a} \alpha_i) \cdot (\sum_{j=1}^{n} b_j).$$

У нас в распоряжении есть правая дистрибутивность, поэтому можно раскрыть скобки:

$$(\sum_{i=1}^{m_a} \alpha_i) \cdot (\sum_{j=1}^{n} b_j) = (\sum_{i=1}^{m_a} \alpha_i \cdot (\sum_{j=1}^{n} b_j))$$

А так как все эндоморфизмы дистрибутивны, мы можем еще m_a раз раскрыть скобки:

$$\sum_{i=1}^{m_a} \alpha_i \cdot (\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m_a}\sum_{j=1}^{n} \alpha_i b_j.$$

Применяем лемму 1 и меняем местами знаки суммы:

$$\sum_{i=1}^{m_a}\sum_{j=1}^{n} \alpha_i b_j = \sum_{j=1}^{n}\sum_{i=1}^{m_a} \alpha_i b_j + \delta\left(\{\alpha_i b_j\},\ i,\ j\right),$$

Снова обращаемся к правой дистрибутивности и получаем

$$\sum_{i=1}^{m_a} \alpha_i b_j = ab_j$$

В итоге

$$a(\sum_{i=1}^{n} b_i) = \sum_{i=1}^{n} ab_i + \delta\left(\{\alpha_i b_j\},\ i,\ j\right)$$

Лемма доказана. □

Функция $\delta\left(\{\alpha_i b_j\},\ i,\ j\right)$ из леммы 2 также будет востребована в следующих разделах. Для неё тоже введём

Определение 3. *Пусть* $a \in E(G)$, $b_j \in E(G)$, $1 \leqslant j \leqslant n$, $a = \sum_{i=1}^{m_a} \alpha_i$, *где* $\alpha_i \in End(G)$, $1 \leqslant i \leqslant m_a$, *тогда элемент* $\xi = \xi(a, \{b_j\})$ *такой, что*

$$a(\sum_{j=1}^{n} b_j) = \sum_{j=1}^{n} ab_j + \xi,$$

назовём искажением недистрибутивности элемента a по множеству $\{b_j\}$.

2.2 Арифметика матриц над почтикольцом $E(G)$

Условимся обозначать через $\mathfrak{M}_n(R)$ множество квадратных матриц размера $n \times n$ с элементами из почтикольца $R = E(G)$. На этом множестве обычным образом определяются операции сложения и умножения. Также обозначим через $\mathfrak{J}$ подмножество множества $\mathfrak{M}_n(R)$, состоящее из матриц с элементами из идеала J почтикольца $R = E(G)$.

Рекуррентную последовательность (1) удобно задать с помощью начального вектора $x = (x_1, x_2, \ldots, x_n)$ и сопровождающей матрицы A размера $n \times n$, определяемой коэффициентами f_i :

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ f_1 & f_2 & f_3 & \ldots & f_n \end{pmatrix} \tag{2}$$

Тогда очередное состояние рекурренты рассчитывается по формуле

$$x_i = Ax_{i-1}. \tag{3}$$

Нас интересует прежде всего, как соотносятся периоды последовательностей и мультипликативные порядки соответствующих сопровождающих матриц. Поэтому важно получить выражение для i-го состояния в терминах степеней сопровождающей матрицы.

Л.С. Казариным и В.М. Сидельниковым были описаны некоторые свойства операций над матрицами из $\mathfrak{M}_n(R)$. Было замечено, что умножение матриц ассоциативно и дистрибутивно лишь с точностью до дополнительного слагаемого из $\mathfrak{J}$.

Например, пусть x_0 — начальный вектор рекуррентной последовательности. Согласно (3) $x_i = A(Ax_{i-2}) = A^2x_{i-2}+U$, где $U \in \mathfrak{J}$. Тогда $x_{i+1} = Ax_i = A(A^2x_{i-2}+U) =$

$A(A^2)x_{i-2} + V + AU = A^3x_{i-2} + U' + V + AU$, где $U', V \in \mathfrak{J}$. Следующие векторы будут выглядеть ещё сложнее, поскольку приведение $A \cdot AU$ к A^2U даст очередное добавочное слагаемое, и так далее.

Однако при некоторых условиях возможно и небольшое упрощение.

Лемма 3. *Пусть* $A, B, C \in \mathfrak{M}_n(R)$, *и* $B \in \mathfrak{J}$. *Тогда*

$$C(A + B) = CA + CB \tag{4}$$

$$(A + B)C = AC + BC \tag{5}$$

Доказательство. Пусть $A = \{a_{ij}\}$, $B = \{b_{ij}\}$, $C = \{c_{ij}\}$, $1 \leqslant i, j \leqslant n$.

Запишем формулу элемента матрицы $C(A + B)$:

$$x_{ij} = \sum_{k=1}^{n} c_{ik}(a_{kj} + b_{kj}).$$

Отсюда по лемме 2

$$x_{ij} = \sum_{k=1}^{n} \big(c_{ik}a_{kj} + c_{ik}b_{kj} + \xi(c_{ik}, \{a_{kj}, b_{kj}\})\big) = \sum_{k=1}^{n}(c_{ik}a_{kj} + c_{ik}b_{kj}) + \sum_{k=1}^{n} \xi_k.$$

Второе равенство выполняется, поскольку $\xi_k \in J$.

Теперь, воспользовавшись леммой 1, перегруппируем слагаемые суммы ценой дополнительного слагаемого из J:

$$\sum_{k=1}^{n}(c_{ik}a_{kj} + c_{ik}b_{kj}) = \sum_{k=1}^{n} c_{ik}a_{kj} + \sum_{k=1}^{n} c_{ik}b_{kj} + \delta.$$

В данном случае для применения упомянутой леммы вместо второго знака суммы у нас два слагаемых — с умножением соответственно на a_{kj} и b_{kj}. Так как $b_{kj} \in J$ $\forall k$ и j, то $\xi(c_{ik}, \{a_{kj}, b_{kj}\}) = 0$ и $\delta = 0$, откуда следует равенство (4).

Далее переходим к матрице $(A+B)C$. Выпишем выражение для её коэффициента

$$x_{ij} = \sum_{k=1}^{n}(a_{kj} + b_{kj})c_{ik}.$$

Поскольку по определению почтикольца всегда выполняется правая дистрибутивность, то мы можем раскрыть скобки:

$$x_{ij} = \sum_{k=1}^{n}(a_{kj}c_{ik} + b_{kj}c_{ik}).$$

Теперь, аналогично, используя лемму 1, перегруппируем слагаемые суммы ценой дополнительного слагаемого из J:

$$x_{ij} = \sum_{k=1}^{n} a_{kj}c_{ik} + \sum_{k=1}^{n} b_{kj}c_{ik} + \delta.$$

Так же, как и в первом случае, заключаем, что $\delta = 0$, и равенство (5) доказано.

Лемма доказана. □

Лемма 4. *Пусть* $A, B, C \in \mathfrak{M}_n(R)$, *и* $A = \{a_{ij}\}$, $B = \{b_{ij}\}$, $C = \{c_{ij}\}$, $1 \leqslant i, j \leqslant n$. *Тогда выполнено:*

1. $(AB)C = A(BC) + \Gamma, \qquad \Gamma \in \mathfrak{J}.$
2. *Если* $a_{ij} \in End(G) \quad \forall i, j$ *и по крайней мере одна из матриц* A, B *или* C *принадлежит* $\mathfrak{J}$, *то* $\Gamma = 0$.
3. *Если* B *или* C *принадлежит* $\mathfrak{J}$, *то* $\Gamma = 0$.

Доказательство. Введём обозначения

$$W = ABC, \quad W = \{w_{ij}\},\ 1 \leqslant i, j \leqslant n;$$

$$a_{ij} = \sum_{k=1}^{m_{ij}} \alpha_k^{(ij)},\ \alpha_k^{(ij)} \in \mathrm{End}(G);$$

$$w_{ij} = \sum_{k=1}^{n}((\sum_{l=1}^{n} a_{il}b_{lk})c_{kj});$$

$$w_{ij} = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{il}b_{lk}c_{kj}.$$

Применим лемму 1

$$w_{ij} = \sum_{l=1}^{n}\sum_{k=1}^{n} a_{il}b_{lk}c_{kj} + \delta_{ij}, \quad \delta_{ij} \in J,$$

где δ_{ij} — коммутатор суммирования по k и l.

Теперь нам мешает отсутствие левой дистрибутивности. Но на помощь приходит лемма 2

$$\sum_{k=1}^{n} a_{il}b_{lk}c_{kj} = a_{il}\sum_{k=1}^{n} b_{lk}c_{kj} + \xi_{ij}^{(l)},$$

где $\xi_{ij}^{(l)} = \xi(a_{il}, \{b_{lk}c_{kj} \mid 1 \leqslant k \leqslant n\})$ — искажение недистрибутивности элемента a_{il} по множеству $\{b_{lk}c_{kj} \mid 1 \leqslant k \leqslant n\}$.

Таким образом,

$$w_{ij} = \sum_{l=1}^{n}\left(a_{il}\sum_{k=1}^{n} b_{lk}c_{kj} \ + \ \xi_{ij}^{(l)}\right) + \delta_{ij}, \quad \xi_{ij}^{(l)},\ \delta_{ij} \in J.$$

Обозначим $\xi_{ij} = \sum_{l=1}^{n} \xi_{ij}^{(l)}$. В итоге получим

$$w_{ij} = \sum_{l=1}^{n} a_{il}\sum_{k=1}^{n} b_{lk}c_{kj} \ + \ \xi_{ij} \ + \ \delta_{ij}. \tag{6}$$

Это означает, что

$$W = (AB)C = A(BC) + \Xi_{ABC} + \Delta_{ABC}, \tag{7}$$

где $\Xi_{ABC}, \Delta_{ABC} \in \mathfrak{J}$

Из (6) и (7) сразу следуют требуемые утверждения. □

Замечание 1. *Здесь обнаруживается существенное различие между левым* (3) *и правым умножениями при построении рекуррентной последовательности. А именно, левое умножение матриц на вектор из* $\mathfrak{J}$ *ассоциативно, то есть* $A(AU) = A^2U$. *Но* $(UA)A = UA^2 + U'$, *где* $U, U' \in \mathfrak{J}$.

2.3 Левое умножение

Выше мы выяснили, что применение левого умножения приводит к "упрощению" рекуррентных последовательностей. Рассмотрим этот вариант подробнее.

Пусть x_0 — начальный вектор последовательности, A — её сопровождающая матрица. Обозначим мультипликативный порядок матрицы A буквой q, а период последовательности — p. Также примем ещё одно обозначение

$$\underbrace{A \cdot (A \cdot (\ldots \cdot (A}_{r} x) \ldots)) = A^{(r)}x.$$

Согласно леммам 4 и 3 $\forall \gamma \in \mathfrak{J}$, $\forall r \in \mathbb{N}$, $\forall a \in E(G)$ выполнено $A^{(r)}\gamma = A^r\gamma$ и $A(a + \gamma) = Aa + A\gamma$.

Будем последовательно умножать слева начальный вектор на сопровождающую матрицу: $x_1 = Ax_0, \quad x_2 = A^2x_0 + \gamma_1, \quad \ldots$

Таким же образом будем приводить все возникающие слагаемые к произведению с участием степени матрицы A, обозначая при этом "ошибку неассоциативности" для каждого $A \cdot A^r x_0$ через γ_r. Тогда с учётом сказанного выше получим формулу

$$x_i = A^i x_0 + \sum_{k=1}^{i-1} A^{i-k-1}\gamma_k. \tag{8}$$

Поскольку умножение на матрицу из $\mathfrak{J}$ даёт в результате всегда матрицу из $\mathfrak{J}$, то сумма в формуле (8) есть элемент из $\mathfrak{J}$. Поэтому для порядка q матрицы A и некоторого $\eta \in \mathfrak{J}$ можно записать

$$x_q = A^q x_0 + \eta,$$

откуда следует

$$x_q = x_0 + \eta. \tag{9}$$

Продолжим процесс и получим

$$x_{2q} = A^{(q)}(x_0 + \eta) = A^{(q)}x_0 + A^q\eta = x_q + \eta,$$

что с учётом (9) приводит к

$$x_{2q} = x_0.$$

Итак, мы пришли к соотношению

$$2q = kp, \quad k \in \mathbb{Z}.$$

А это означает, что доказана

Теорема 1. *Если период последовательности вида* (3) *больше мультипликативного порядка соответствующей сопровождающей матрицы, то он вдвое больше мультипликативного порядка этой матрицы.*

3. Результаты экспериментов

Целью экспериментов было определение периодов и линейной сложности последовательностей небольшой глубины. Было выбрано небольшое почтикольцо — $E(D_8)$. D_8 — группа диедра порядка 8. По теореме 1 из [3] известно, что $|E(D_8)| = 256$.

Описанные ниже алгоритмы реализованы на языке программирования C++ в интегрированной среде разработки Microsoft® Visual Studio® 2008. Исходный код доступен в Интернете по адресу https://near-ring.googlecode.com/svn/tags/near-ring-1.1

3.1 Моделирование вычислений в почтикольце

В качестве модели любой структуры, представляющей собой замкнутое относительно определённых операций множество из n элементов, рассматривается очевидное машинное представление — таблицы операций. Это означает, что каждому элементу поставлен в соответствие порядковый номер, а каждой операции — таблица $n \times n$ следующего содержания. Каждой строке таблицы, равно как и каждому столбцу, соответствует элемент множества. В ячейке таблицы на пересечении i-й строки и j-го столбца хранится номер результата операции с i-м элементом множества в качестве левого операнда и с j-м элементом множества в качестве правого операнда. Номера элементов для кодирования выбираются от 0 до $n - 1$.

Таким образом, алгебраическая структура задаётся таблицами, по одной для каждой операции, при этом каждый элемент представляется номером строки или столбца этих таблиц.

Например, в таблице 1 описано умножение в группе $G = D_8$.

Почтикольцо $E(G)$ задаётся двумя таблицами 256×256, содержащими 8-битные числа. Таблица группы G используется для вычисления таблиц почтикольца. Для этого сначала строится явная модель. Любой элемент $M(G)$ представляется как вектор $f = (f_i)_8$ из 8 элементов, где $f_i \in G$. Каждый такой вектор задаёт отображение из G в G, при этом для любого $x \in G$ по определению $f(x) = f_x$. Соответствие таких векторов отображениям $M(G)$ взаимно однозначно.

Сложение и умножение отображений реализуются в соответствии с определением почтикольца $M(G)$ и с помощью таблицы операций группы G следующим образом: если $h = f + g$, то $h_i = f_i + g_i$; если $h = fg$, то $h_i = f_{g_i}$.

Таблица 1. Сложение в группе G

	0	a	z	$-a$	b	$a+b$	$z+b$	$-a+b$
0	0	a	z	$-a$	b	$a+b$	$z+b$	$-a+b$
a	a	z	$-a$	0	$a+b$	$z+b$	$-a+b$	b
z	z	$-a$	0	a	$z+b$	$-a+b$	b	$a+b$
$-a$	$-a$	0	a	z	$-a+b$	b	$a+b$	$z+b$
b	b	$-a+b$	$z+b$	$a+b$	0	$-a$	z	a
$a+b$	$a+b$	b	$-a+b$	$z+b$	a	0	$-a$	z
$z+b$	$z+b$	$a+b$	b	$-a+b$	z	a	0	$-a$
$-a+b$	$-a+b$	$z+b$	$a+b$	b	$-a$	z	a	0

Процесс построения таблиц основан на следующих действиях.

1. Пусть имеется некоторое количество известных элементов $E(G)$ (то есть известны несколько векторов, соответствующих элементам $E(G)$). Добавить эти векторы в список найденных векторов класса $E(G)$ (что означает присвоить каждому вектору уникальный номер).

2. Вычислить некоторые суммы и произведения элементов из списка. Найти в списке номера векторов, идентичных результатам выполненных операций (а отсутствующие в этом списке векторы добавить в список). После выполнения этого шага для всех выполненных сложений и умножений имеются номера операндов и результатов. Этими данными заполняются таблицы операций.

Для начала построения таблиц нужен начальный набор элементов $E(G)$. Доказательство предложения 1 из [3] проливает свет на структуру $E(G)$. Известна система из 4 линейно независимых элементов из $J \subset E(G)$. Векторное представление этих элементов выглядит так:

$$(0, z, z, 0, 0, z, z, 0),$$
$$(0, z, 0, z, z, 0, z, 0),$$
$$(0, 0, 0, 0, z, z, z, z),$$
$$(0, z, 0, z, 0, 0, 0, 0).$$

Для построения всего множества необходимо задать 4 линейно независимых отображения из $E(G)$, индуцирующих систему из 4 линейно независимых отображений из $E(G)/J$, а затем вычислить все линейные комбинации этих 8 элементов.

Искомые четыре отображения являются линейными преобразованиями пространства $G/Z(G)$ над полем $GF(2)$. Система (a, b) берётся в качестве базиса пространства $G/Z(G)$. Все линейные преобразования задаются матрицами размерности 2×2 над полем $GF(2)$. Искомую систему представляют матрицы

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

которые соответствуют следующим векторам из класса элементов $E(G)$:

$$(0, a, 0, a, 0, a, 0, a),$$
$$(0, 0, 0, 0, a, a, a, a),$$
$$(0, b, 0, b, 0, b, 0, b),$$
$$(0, 0, 0, 0, b, b, b, b).$$

3.2 Исследование периодов последовательностей

Любая рекуррентная последовательность определяется своими коэффициентами и начальным вектором. Требуется выбрать некоторые значения коэффициентов и элементов начальной последовательности и явно вычислить получающиеся периоды.

Для определения периода последовательности был использован следующий алгоритм.

Алгоритм вычисления периода рекуррентной последовательности

В работе алгоритма используется динамическая структура данных map. Это список пар "ключ-значение", упорядоченный по ключу. Такая структура позволяет быстро находить значение по данному ключу или определять, что данного ключа в списке нет. Поиск записи по ключу, так же как и вставка новой записи, производится в такой структуре за время $O(\log N)$, где N — текущее количество записей.

Алгоритм последовательно вызывает генератор для получения очередного элемента последовательности и заканчивает своё выполнение, когда будет обнаружен период. Это случится, когда состояние генератора повторится, так как состояние генератора – содержимое регистра – полностью определяет его следующее состояние и следующий элемент последовательности. Получается, что в процессе работы алгоритма не производится лишних вызовов генератора.

Требуется, генерируя последовательность, распознать повторение состояния генератора. Для этого каждое очередное его состояние сохраняется в map. Состояние служит ключом, а информационным полем является номер такта, результатом которого стал переход генератора в данное состояние.

Перед тем, как сохранить новое состояние генератора, алгоритм запускает поиск в map. Если такое же состояние уже содержится в map, то алгоритм завершает свою работу, возвращая в качестве результата разность между текущим тактом и тактом, хранящимся в map по данному повторившемуся состоянию. В противном случае это состояние помещается вместе с номером текущего такта в map, и процесс продолжается дальше.

Результаты

Сначала был рассмотрен случай глубины рекурсии 2. Всего различных последовательностей глубины 2 существует 2^{32} — именно столько комбинаций образуют два коэффициента и два элемента начальной последовательности (напомним, что каждый элемент почтикольца кодируется 8 битами). Так что перебор всех возможных вариантов с вычислением периода для каждого из них — трудоёмкая задача.

Вместо полного перебора всех последовательностей был осуществлён перебор всех наборов коэффициентов и для каждого набора были случайным образом выбраны несколько вариантов начальных векторов. Максимальный из найденных в результате данного эксперимента период для правого умножения — 84, а для левого — 30.

Следующий эксперимент заключался в поиске максимального мультипликативного порядка сопровождающей матрицы (2) также перебором всех коэффициентов. Результат эксперимента численно совпал с предыдущим. Порядок матриц относительно правого умножения — 84, а порядок матриц относительно левого умножения — 30. Значит, согласно теореме 1 период последовательности глубины 2 для левого умножения не превышает $2 \cdot 30 = 60$.

Таким образом, было получено уточнение теоретически установленной Л. С. Казариным и В. М. Сидельниковым верхней границы для периода — 225.

Для глубины рекурсии более 2 становится проблематичным даже перебор коэффициентов рекуррентной формулы. Поэтому были рассмотрены лишь определённые классы последовательностей:

$$x_i = ax_{i-2} + bx_{i-3},$$
$$x_i = ax_{i-3} + bx_{i-4},$$
$$x_i = ax_{i-3} + bx_{i-5}.$$

Выбор данных классов основан на простой интуиции. Если представить, что эти формулы действуют над полем GF(2), то при $a = b = 1$ они будут соответствовать последовательностям максимального периода.

В таблице 2 собраны результаты поиска периодов.

Таблица 2. Максимальные из найденных периоды

Глубина рекурсии	Левое умножение	Правое умножение	Теоретическая верхняя граница $(2^{2n}-1)^2$
2	30	84	225
3	217	2 604	3 969
4	3 255	15 240	65 025
5	27 559	316 820	1 046 529

3.3 Профиль линейной сложности

Линейная сложность показывает, насколько последовательность “непредсказуема”, и потому является важным критерием при выборе генератора для построения криптосистем. Напомним определение этой характеристики.

Определение 4. *Линейная сложность $\Lambda(s^l)$ последовательности $s^l = (s_0, s_1, \ldots, s_{l-1})$ — это наименьшее неотрицательное целое L такое, что существует линейная*

рекуррента с фиксированными константами $c_0, c_1, \ldots, c_L$, *удовлетворяющая равенству*

$$s_j + c_1 s_{j-1} + \ldots + c_L s_{j-L} = 0, \quad L \leqslant j \leqslant l.$$

Определение 5. *Пусть* L_i — *линейная сложность подпоследовательности* $s^i = (s_0, s_1, \ldots, s_{i-1})$. *Тогда последовательность* $L_1, L_2, \ldots, L_l$ *называется профилем линейной сложности последовательности* s^l.

В ходе эксперимента рассматривались некоторые последовательности глубины рекурсии 2 с наибольшими из найденных периодами. Для анализа линейной сложности последовательность элементов почтикольца, кодируемых байтами, была представлена как последовательность бит, то есть элементов $GF(2)$. К таким последовательностям применялся алгоритм Берлекэмпа–Мэсси [1] и определялись их линейная сложность и профиль линейной сложности.

В результате выяснилось, что значения линейной сложности L рассмотренных последовательностей попадают в промежуток от 62 до 152, профили линейной сложности для первых битов последовательностей близки к линейной функции $L_i \approx i/2$. Линейная сложность становится постоянной в точке приблизительно равной $2L$, что в случае правого умножения может составлять более трети периода, а в случае левого умножения – до одного периода и более.

4. Заключение

Основным результатом данной работы является полученное уточнение верхней границы для периода рекуррентных последовательностей глубины 2 над почтикольцом группы диедра порядка 8. Уточнение верно для случая, когда генерация последовательности выполняется с левым умножением. Однако эксперимент показывает, что для правого умножения обнаруживается аналогичная закономерность соотношения периода последовательности и порядка сопровождающей матрицы. Так, последовательностям с правым умножением глубины 2, имеющим максимальный из найденных до сих пор периодов, соответствуют сопровождающие матрицы, порядки которых либо 42, либо 84. То есть как будто выполняется теорема 1 и для правого умножения.

Состояние рекурренты при умножении матрицы справа изменяется похожим на случай левого умножения образом, но постоянно добавляется дополнительное слагаемое из $\mathfrak{J}$ – искажение неассоциативности — и неизвестно, сокращается ли оно всегда при достижении двойного порядка матрицы:

$$x_q = x_0 + \mu, \quad x_{2q} = x_0 + \theta,$$

где $\mu,\ \theta \in \mathfrak{J}$.

Правда, μ есть искажение неассоциативности для x_0, а θ — уже только для элемента из $\mathfrak{J}$. К тому же μ, θ — векторы, у которых все компоненты, кроме последнего, равны 0 (для краткости не будем приводить вывод этого факта). Всё это наводит на мысль, что дополнительные слагаемые, вообще говоря, должны быстро сокращаться.

Список литературы

1. Massey J.L. Shift-register synthesis and BCH decoding // IEEE Trans. Inform. Theory. Jan. 1969. Vol. IT-15. P. 122–127.

2. Reeds J.A., Sloane N.J.A. Shift register synthesis (modulo m) // SIAM Journal on Computing. 1985. 14(3). P. 505–513.

3. Гарипова Е.С. , Казарин Л.С. О конечных почтикольцах, порождённых эндоморфизмами экстраспециальной 2-группы // Дискретная математика. 2010. 22, №1. С. 104-114

4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2001. 480 с.

5. Кнут Д. Искусство программирования: в 3 т. Т. 2. Получисленные алгоритмы. М.: Мир, 1976.

6. Shneier B. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C. John Wiley & Sons, Inc., 1996.

Recurrence sequences over near-rings

Sboev A.V.

Keywords: recurrence sequences, near-rings, extra-special p-groups, endomorphisms of groups

Periods and statistics of linear recurrence sequences over near-rings generated by endomorphisms of finite non-abelian extra-special 2-groups are investigated.

Сведения об авторе:
Сбоев Андрей Валерьевич,
Ярославский государственный университет им. П. Г. Демидова, аспирант