Math-Net.Ru

Общероссийский математический портал

Р. В. Богонатов, Представления над кольцом Галуа линейной рекуррентной последовательности максимального периода над полем Галуа, *Дискрет. матем.*, 2007, том 19, выпуск 1, 141–157

DOI: <https://doi.org/10.4213/dm15>

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: 3.89.185.249

26 апреля 2023 г., 09:44:04

Представления над кольцом Галуа линейной рекуррентной последовательности максимального периода над полем Галуа

© 2007 г. Р. В. Богонатов

Исследуются представления над кольцом Галуа линейной рекуррентной последовательности максимального периода над полем Галуа. Описываются характеристические и минимальные многочлены этих представлений.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ 2358.2003.9.

1. Введение

Пусть R — коммутативное кольцо с единицей и $\sigma: \Omega \rightarrow R$ — произвольное отображение. Последовательностью u над множеством Ω будем называть отображение $u: \mathbf{N}_0 \rightarrow \Omega$ и ее i -й член обозначим через $u(i)$, $i \in \mathbf{N}_0$. Последовательность $v = \sigma(u)$ над R , определяемую условием $v(i) = \sigma(u(i))$, $i \in \mathbf{N}_0$, назовем представлением последовательности u над кольцом R или R -представлением u .

Если u — периодическая последовательность с длиной подхода λ и периодом T , то $\sigma(u)$ — линейная рекуррентная последовательность (ЛРП) над R , имеющая характеристический многочлен $x^{T+\lambda} - x^\lambda$. Однако она может иметь и характеристические многочлены значительно меньших степеней.

В статье [2] были найдены минимальный многочлен и характеристические многочлены представления $\sigma(u)$ над кольцом вычетов $R = \mathbf{Z}_{p^n}$ ЛРП u максимального периода над полем $P = GF(p)$. В качестве открытой задачи оставалось исследование произвольного представления $\sigma: GF(p^n) \rightarrow \mathbf{Z}_{p^n}$. В данной работе эта задача решена.

Для ее решения рассматривается более общая ситуация. Пусть u — ЛРП максимального периода над полем $GF(p^r)$. В работе исследуются ее представления $\sigma(u)$ над кольцом Галуа $GR(p^{rn}, p^n)$: дается описание всех характеристических и минимальных многочленов ЛРП $\sigma(u)$.

Работа обобщает результаты работы [2]. Мы используем сходные методы исследования с учетом того, что нами рассматривается более общая ситуация.

2. Предварительные сведения

Кольцом Галуа называется конечное коммутативное кольцо R с единицей, в котором множество всех делителей нуля имеет вид pR для некоторого простого числа p .

Характеристика кольца Галуа равна p^n для подходящего $n \in \mathbb{N}$, при этом число элементов в R равно p^{rn} для некоторого $r \in \mathbb{N}$. Кольцо Галуа определяется однозначно с точностью до изоморфизма своей характеристикой и числом элементов. Это делает корректным обозначение $GR(p^{rn}, p^n)$ для кольца Галуа из p^{rn} элементов, имеющего характеристику p^n . В частности, $\mathbb{Z}_{p^n} = GR(p^n, p^n)$, $GF(p^r) = GR(p^r, p)$.

Будем обозначать через $\bar{a}$ образ элемента $a \in R$ при действии естественного эпиморфизма кольца R в его поле вычетов $\bar{R} = R/pR = GF(p^r)$. Эпиморфизм $R \rightarrow \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \rightarrow \bar{R}[x]$. Образ многочлена $F(x) \in R[x]$ при этом эпиморфизме будем обозначать $\bar{F}(x)$. Унитарный многочлен $F(x) \in R[x]$ назовем многочленом Галуа, если $\bar{F}(x)$ — неприводимый многочлен над полем $\bar{R}$.

Пусть $F(x)$ — многочлен Галуа степени M над кольцом Галуа $R = GR(p^{rn}, p^n)$. Тогда кольцо $S = R[x]/F(x)$ есть кольцо Галуа $S = GR(p^{rM}, p^n)$. Можно считать, что R — подкольцо в S ; тогда S называется расширением Галуа степени M кольца R . В кольце S всякий многочлен Галуа $H(x)$ степени M над R имеет в точности M корней, попарно несравнимых по модулю идеала pS , и раскладывается над S на линейные множители. Если $\theta \in S$ — корень $H(x)$, то кольцо S порождается элементом θ над кольцом R : $S = R[\theta]$.

Для колец Галуа справедливо следующее утверждение.

Лемма Гензеля. Пусть $F(x)$, $G_0(x)$, $H_0(x)$ — унитарные многочлены над кольцом Галуа R такие, что

$$\bar{F}(x) = \bar{G}_0(x)\bar{H}_0(x)$$

и наибольший общий делитель

$$(\bar{G}_0(x), \bar{H}_0(x)) = \bar{e}.$$

Тогда существуют единственные унитарные многочлены $G(x)$, $H(x) \in R[x]$, для которых

$$F(x) = G(x)H(x), \quad \bar{G}(x) = \bar{G}_0(x), \quad \bar{H}(x) = \bar{H}_0(x).$$

Доказательства всех перечисленных свойств колец Галуа приведены в [4, 6].

3. Формулировка основного результата

Пусть p — простое число, $P = GF(p^r)$ — поле с единицей e_P , $f(x) \in P[x]$ — многочлен максимального периода степени $M \geq 1$, $u \in L_P(f) \setminus 0$ — линейная рекуррентная последовательность над полем P максимального периода $T = p^{rM} - 1$ (см. [1, 3]). Пусть $n \geq 2$ и $R = GR(p^{rn}, p^n)$ — кольцо Галуа. Всюду далее $q = p^r$, $\sigma: P \rightarrow R$ — произвольное отображение, $\sigma(u)$ — R -представление ЛРП u , $\bar{R}$ — поле вычетов кольца R .

Нашей целью является исследование последовательности $\sigma(u)$ как ЛРП над кольцом R .

Обозначим через $\bar{f}(x)$ образ многочлена $f(x) \in P[x]$ при действии естественного изоморфизма $P[x] \rightarrow \bar{R}[x]$. Очевидно, что $\bar{f}(x)$ является многочленом максимального

периода над полем $\bar{R}$ степени M , а значит, $\bar{f}(x) \mid x^T - \bar{e}$. По лемме Гензеля существует единственный унитарный многочлен $f_*(x) \in R[x]$ (см. [5]) такой, что $f_*(x) \mid x^T - e$ и $\bar{f}_*(x) = \bar{f}(x)$. Пусть $S = GR(p^{Mrn}, p^n)$ — расширение Галуа степени M кольца Галуа R , содержащее корень θ многочлена $f_*(x)$.

Нормой $\|c\|$ элемента $c \in S$ называется величина

$$\|c\| = \max\{r \in \{0, 1, \dots, n\} : c \in p^r S\}.$$

Будем говорить, что элементы $a, b \in S$ сравнимы по модулю p^r , $r \geq 0$, если $a - b \in p^r S$. Норму представления σ и многочлена $H(x) \in S[x]$ определим следующим образом:

$$\begin{aligned} \|\sigma\| &= \max\{r \in \{0, 1, \dots, n\} : \sigma(a) \in p^r R \text{ для всех } a \in P\}, \\ \|H\| &= \max\{r \in \{0, 1, \dots, n\} : H(x) \in p^r S[x]\}. \end{aligned}$$

Обозначим через $\Gamma(R)$ множество всех корней в R многочлена $x^{p^r} - x$:

$$\Gamma(R) = \{\beta \in R : \beta^q = \beta\}.$$

Выполняются следующие свойства (см. с. 128 в [4]).

Свойство 1. $\Gamma(R)$ замкнуто относительно операции умножения и состоит ровно из q попарно не сравнимых по модулю pR элементов.

Свойство 2. Для любого элемента $a \in R$ существует единственный элемент $\gamma(a) \in \Gamma(R)$ такой, что $\bar{a} = \overline{\gamma(a)}$. При этом функцию γ можно представить полиномом:

$$\gamma(a) = a^{q^{n-1}}, \quad a \in R. \quad (1)$$

Зададим на $\Gamma(R)$ операцию сложения $\oplus$, полагая

$$a \oplus b = \gamma(a + b), \quad a, b \in \Gamma(R).$$

Свойство 3. $(\Gamma(R), \oplus, \cdot)$ есть поле из q элементов.

Рассмотрим элементы $P = \{a_0, \dots, a_{q-1}\}$ и $\Gamma(R) = \{\beta_0, \dots, \beta_{q-1}\}$ полей P и $\Gamma(R)$ соответственно. Пронумеруем элементы полей P и $\Gamma(R)$ так, чтобы отображение $a_t \rightarrow \beta_t$, $t = 0, 1, \dots, q-1$, являлось изоморфизмом.

Предложение 1. Существует единственный многочлен

$$\Psi_\sigma(x) = \psi_{q-1}x^{q-1} + \psi_{q-2}x^{q-2} + \dots + \psi_1x + \psi_0 \in R[x]$$

такой, что

$$\Psi_\sigma(\beta_t) = \sigma(a_t), \quad t = 0, 1, \dots, q-1.$$

При этом

$$\|\Psi_\sigma(x)\| = \|\sigma\|.$$

Доказательство данного утверждения с незначительными изменениями повторяет доказательство, приведенное в [2].

Для целого числа $k \geq 0$ обозначим m -й разряд p -ичного разложения k через $v_m(k)$, а через $w(k)$ — сумму (в кольце целых чисел) разрядов p -ичного разложения k :

$$k = \sum_{m \geq 0} p^m v_m(k), \quad w(k) = \sum_{m \geq 0} v_m(k), \quad v_m(k) \in \{0, 1, \dots, p-1\}.$$

Для целых чисел $k \geq 0, q \geq 1$ обозначим через $k \bmod q$ наименьший неотрицательный вычет числа k по модулю q .

Для формулировки основного результата потребуются также следующие обозначения. Пусть

$$L = \|q^{M-1} \sum_{a \in P} \sigma(a) - \sigma(0)\|.$$

Для $k = 1, \dots, T-1$ введем обозначения

$$l = k \bmod (q-1), \quad t = \frac{1}{p-1}(w(k) - w(l)).$$

Для $s = 0, 1, \dots, n-1$ положим

$$\Delta_s(x) = \begin{cases} e, & 0 \leq s < L, \\ x - e, & L \leq s \leq n-1, \end{cases}$$

$$H_s(x) = \Delta_s(x) \prod_{1 \leq k \leq T-1, t + \|\psi_t\| \leq s} (x - \theta^k).$$

Произведение, состоящее из пустого множества сомножителей, будем полагать равным единице. Отметим, что так как

$$\|\Psi_\sigma(x)\| = \|\sigma\|, \quad L \geq \|\sigma\|,$$

то

$$H_s(x) = e, \quad 0 \leq s < \|\sigma\|.$$

Идеал в $R[x]$, порожденный множеством $K \subset R[x]$, обозначим через (K) . Теперь основной результат можно сформулировать следующим образом.

Теорема 1. Пусть

$$\|\sigma\| = 0.$$

Тогда при введенных выше условиях

$$\text{Ann}(\sigma(u)) = (H_{n-1}(x), pH_{n-2}(x), \dots, p^{n-1}H_0(x)).$$

В частности, $H_{n-1}(x)$ является минимальным многочленом ЛРП $\sigma(u)$.

Следствие 1. Если

$$\|\sigma\| = t > 0,$$

то

$$\text{Ann}(\sigma(u)) = (H_{n-1}(x), pH_{n-2}(x), \dots, p^{n-t-1}H_t(x), p^{n-t}).$$

4. Вспомогательные утверждения

Пусть $H(x) \in R[x]$ — унитарный сепарабельный (это означает, что $\bar{H}(x) \in \bar{R}[x]$ — сепарабелен, то есть не имеет кратных корней в поле разложения) многочлен степени N , S — расширение Галуа кольца Галуа R , содержащее все корни $\theta_1, \dots, \theta_N$ многочлена $H(x)$ и порожаемое ими: $S = R[\theta_1, \dots, \theta_N]$. Тогда справедливо следующее утверждение.

Предложение 2. Любая последовательность $v \in L_R(H)$ однозначно представляется в виде

$$v(i) = c_1 \theta_1^i + \dots + c_N \theta_N^i, \quad i \in \mathbb{N}_0, \quad (2)$$

для некоторых фиксированных $c_1, \dots, c_N \in S$. Положим

$$H_s(x) = \prod_{1 \leq k \leq N, \|c_k\| \leq s} (x - \theta_k), \quad s = 0, 1, \dots, n-1.$$

Тогда $H_s(x) \in R[x]$ и

$$\text{Ann}(v) = (H_{n-1}(x), pH_{n-2}(x), \dots, p^{n-1}H_0(x)).$$

Доказательство этого утверждения приведено на с. 101–102 в [2].

Применим предложение 2 к ЛРП $\sigma(u)$. Так как

$$T(\sigma(u)) = T = q^M - 1,$$

справедливо включение $\sigma(u) \in L_R(x^T - e)$. Поскольку $f_*(x) \mid x^T - e$, корнем многочлена $x^T - e$ является корень θ многочлена $f_*(x)$, а значит, и его степени $\theta^2, \dots, \theta^{T-1}, \theta^T = e$. Так как $\bar{f}_*(x)$ — многочлен максимального периода степени M , элементы $\bar{\theta}, \bar{\theta}^2, \dots, \bar{\theta}^T$ попарно различны. Следовательно, многочлен $x^T - e$ сепарабелен, и согласно предложению 2 ЛРП $\sigma(u)$ однозначно представляется в виде

$$\sigma(u)(i) = \sum_{k=1}^T c_k \theta^{ik}, \quad i \in \mathbb{N}_0, \quad (3)$$

для некоторых фиксированных $c_1, \dots, c_T \in S$, где

$$S = R[\theta, \theta^2, \dots, \theta^T] = R[\theta]$$

— расширение Галуа степени M кольца R .

Чтобы описать $\text{Ann}(\sigma(u))$, достаточно, ввиду предложения 2, найти нормы коэффициентов $c_1, \dots, c_T$.

На с. 103–104 в [2] приведены две следующие леммы комбинаторного характера, которыми мы будем пользоваться.

Лемма 1. Пусть $\alpha \geq 1$, $k_1, \dots, k_\alpha \in \mathbb{N}_0$, $k = k_1 + \dots + k_\alpha$, E — максимальная степень простого числа p , делящая полиномиальный коэффициент $k!/(k_1!k_2!\dots k_\alpha!)$. Тогда

$$(a) \quad E = \frac{w(k_1) + \dots + w(k_\alpha) - w(k)}{p-1},$$

$$(б) \quad \frac{k!}{k_1!k_2!\dots k_\alpha!} \equiv (-p)^E \prod_{m \geq 0} \frac{v_m(k)!}{v_m(k_1)! \dots v_m(k_\alpha)!} \pmod{p^{E+1}}.$$

Лемма 2. Пусть

$$M \geq 1, \quad T = p^M - 1, \quad \alpha \geq 1, \quad k_1, \dots, k_\alpha \in \{1, \dots, T\},$$

$$k = (k_1 + \dots + k_\alpha) \bmod T.$$

Тогда

- (a) $w(pk \bmod T) = w(k)$;
- (б) $w(k) \equiv k \pmod{p-1}$;
- (в) $w(k) \equiv w(k_1 + \dots + k_\alpha) \equiv w(k_1) + \dots + w(k_\alpha) \pmod{p-1}$;
- (г) $w(k) \leq w(k_1 + \dots + k_\alpha) \leq w(k_1) + \dots + w(k_\alpha)$;
- (д) соотношение

$$w(k) = w(k_1) + \dots + w(k_\alpha)$$

эквивалентно равенствам

$$v_m(k) = v_m(k_1) + \dots + v_m(k_\alpha), \quad m = 0, 1, \dots, M-1,$$

и в частности, влечет равенство

$$k = k_1 + \dots + k_\alpha.$$

Пусть p — простое число, $q = p^r$, $M \in \mathbb{N}$, $k \in \mathbb{N}$,

$$l = k \bmod (q-1), \quad t = (w(k) - w(l))/(p-1).$$

Легко видеть, что для $k \in \{1, \dots, p^{rM} - 1\}$ верно неравенство $t \leq rM$, но нам потребуется чуть более точная оценка.

Лемма 3. При введенных выше условиях для всех $k \in \{1, \dots, p^{rM} - 1\}$ выполняется неравенство $t \leq r(M-1)$.

Доказательство. Нужно доказать, что

$$w(k) - w(l) \leq r(M-1)(p-1) = rM(p-1) - r(p-1).$$

Докажем это индукцией по $w(k)$, от $w(k) = rM(p-1)$ до $w(k) = 1$.

1. Пусть $w(k) = rM(p-1)$, тогда

$$k = (p-1) + (p-1)p + \dots + (p-1)p^{rM-1} = p^{rM} - 1.$$

Так как $q - 1$ делит $p^{rM} - 1$, справедливы равенства $l = q - 1$, $w(l) = r(p - 1)$. Значит,

$$w(k) - w(l) = r(M - 1)(p - 1).$$

2. Пусть утверждение верно для любого k такого, что $w(k) = t$, где $t \geq 2$. Докажем, что оно верно для любого k' такого, что $w(k') = t - 1$.

Пусть $k' \in \{1, \dots, p^{rM} - 2\}$ и $w(k') = t - 1$. Тогда существует $d \in \{0, 1, \dots, rM - 1\}$ и существует k такое, что $w(k) = t$ и $k' = k - p^d$. Пусть $l = l_0 + l_1 p + \dots + l_{r-1} p^{r-1}$. Тогда

$$l' = (l - p^d) \bmod (q - 1) = (l - p^{d_1}) \bmod (q - 1),$$

где $d_1 = d \pmod{r}$. Представим l' в виде

$$l' = l_0 + l_1 p + \dots + (l_{d_1} - 1)p^{d_1} + \dots + l_{r-1} p^{r-1} \bmod (q - 1).$$

Рассмотрим три случая.

(а) Если $l_{d_1} \geq 1$, то $w(l') = w(l) - 1$ и

$$w(k_1) - w(l_1) = (w(k) - 1) - (w(l) - 1) \leq r(M - 1)(p - 1).$$

Последнее неравенство верно по предположению индукции.

(б) Если $l_{d_1} = 0$ и существует d_2 — минимальное число с таким свойством, что $d_2 > d_1$ и $l_{d_2} \neq 0$, то

$$\begin{aligned} l' = l_0 + l_1 p + \dots + (l_{d_1-1})p^{d_1-1} + (p - 1)p^{d_1} + \dots + (p - 1)p^{d_2-1} \\ + (l_{d_2} - 1)p^{d_2} + l_{d_2+1}p^{d_2+1} + \dots + l_{r-1}p^{r-1}. \end{aligned}$$

Следовательно,

$$w(l') = w(l) - 1 + (p - 1)(d_2 - d_1),$$

и утверждение верно.

(в) В противном случае существует $d_3 < d_1$ такое, что $l_{d_3} \neq 0$ (так как $l > 0$). Выберем наименьшее d_3 с таким свойством. Тогда

$$\begin{aligned} l' = (p - 1) + (p - 1)p + \dots + (p - 1)p^{d_3-1} + (l_{d_3} - 1)p^{d_3} \\ + l_{d_3+1}p^{d_3+1} + \dots + l_{d_1-1}p^{d_1-1} + (p - 1)p^{d_1} + \dots + (p - 1)p^{r-1}. \end{aligned}$$

Отсюда

$$w(l') = w(l) - 1 + (p - 1)(d_3 + r - d_1),$$

и утверждение верно.

Лемма 4. Пусть $a \in S$, $j \in \mathbb{N}$. Тогда

$$a^{q^{n-1}} \equiv a^{q^{j-1}} \pmod{p^{r(j-1)+1}}.$$

Доказательство. Из свойства 2 параграфа 2 следует, что $\gamma(a) \equiv a \pmod{p}$. Ввиду (1) достаточно показать, что $\gamma(a) \equiv a^{q^{j-1}} \pmod{p^{r(j-1)+1}}$. Докажем это индукцией по j . Для $j = 1$ утверждение верно. Пусть оно верно для некоторого $j \in \mathbb{N}$. Тогда существует $z \in \mathbb{Z}$ такое, что $\gamma(a) = a^{q^{j-1}} + zp^{r(j-1)+1}$. Возведя равенство в степень q , получим, что

$$\gamma(a)^q = a^{q^j} + qp^{r(j-1)+1}za^{q^{j-1}(q-1)} + \sum_{i=2}^q \binom{q}{i} p^{(r(j-1)+1)i} z^i a^{q^{j-1}(q-i)}.$$

Так как $j \geq 2$, то $rj + 1 \leq (r(j-1) + 1)i$ для любого $i \in \{2, \dots, q\}$. Значит, число p^{rj+1} делит каждое слагаемое в сумме $\sum_{i=2}^q \binom{q}{i} p^{(r(j-1)+1)i} z^i a^{q^{j-1}(q-i)}$. Следовательно, $\gamma(a)^q \equiv a^{q^j} \pmod{p^{rj+1}}$. Для завершения доказательства леммы осталось напомнить, что $\gamma(a)^q = \gamma(a)$.

5. Доказательство теоремы

Как отмечено выше, необходимо найти нормы коэффициентов $c_1, \dots, c_T$ в разложении (3). Это сделано в следующих двух утверждениях.

Предложение 3. *Справедливы равенства*

$$c_T = (Te)^{-1} \left(q^{M-1} \sum_{a \in P} \sigma(a) - \sigma(0) \right), \quad \|c_T\| = L.$$

Доказательство. Посчитаем сумму элементов на периоде последовательности $\sigma(u)$, то есть на отрезке $(\sigma(u(0)), \sigma(u(1)), \dots, \sigma(u(T-1)))$. С одной стороны, ввиду (3), она равна

$$\sum_{i=0}^{T-1} \sigma(u)(i) = \sum_{i=0}^{T-1} \sum_{k=1}^T c_k \theta^{ik} = \sum_{k=1}^T c_k \sum_{i=0}^{T-1} \theta^{ik}.$$

Для каждого $k \in \{1, \dots, T-1\}$

$$\sum_{i=0}^{T-1} \theta^{ik} = \sum_{i=0}^{T-1} (\theta^k)^i = \frac{(\theta^k)^T - e}{\theta^k - e} = 0.$$

Поэтому

$$\sum_{i=0}^{T-1} \sigma(u)(i) = c_T \sum_{i=0}^{T-1} \theta^{iT} = Tc_T.$$

С другой стороны, поскольку $T = T(u)$ и у ЛРП максимального периода u на периоде все ненулевые элементы поля встречаются q^{M-1} раз, а ноль — $(q^{M-1} - 1)$ раз (см. теорему 16 на с. 400 в [1]), получим, что

$$\sum_{i=0}^{T-1} \sigma(u)(i) = (q^{M-1} - 1)\sigma(0) + q^{M-1}(\sigma(a_1) + \dots + \sigma(a_{q-1})).$$

Таким образом, получено равенство

$$Tc_T = q^{M-1} \sum_{a \in P} \sigma(a) - \sigma(0).$$

Обозначим через $\bar{u}$ последовательность над полем $\bar{R}$, знаки которой $\bar{u}(i)$ являются образами элементов $u(i) \in P$ при изоморфизме $P \rightarrow \bar{R}$. Тогда $\bar{u}$ — ЛРП ранга M максимального периода $T(u) = T$, минимальный многочлен которой выше был обозначен $\bar{f}(x)$.

Пусть

$$\text{tr}(x) = x + x^q + \dots + x^{q^{M-1}}$$

— функция след из поля $\bar{S}$ в поле $\bar{R}$. Согласно [1] существует единственный элемент $\bar{c} \in \bar{S} \setminus \bar{0}$ такой, что $\bar{u}(i) = \text{tr}(\bar{c} \bar{\theta}^i)$, $i \in \mathbb{N}_0$. Зафиксируем в кольце S элемент c , определенный однозначно по модулю p этим соотношением.

Предложение 4. Для $k = 1, \dots, T-1$ коэффициенты c_k из разложения (3) удовлетворяют соотношениям

$$\|c_k\| = \min\{t + \|\psi_l\|, n\}, \quad (4)$$

$$c_k \equiv (-p)^t \psi_l \frac{c^k v_0(l)! \dots v_{r-1}(l)!}{v_0(k)! \dots v_{rM-1}(k)!} \pmod{p^{t+\|\psi_l\|+1}}, \quad (5)$$

где

$$l = k \bmod (q-1), \quad t = (w(k) - w(l))/(p-1).$$

Доказательство. Равенство (4) следует из (5), поскольку $\bar{c} \neq \bar{0}$. Докажем (5).

1. Для произвольного $i \geq 0$ обозначим s число из множества $\{0, 1, \dots, q-1\}$, для которого $u(i) = a_s \in P$. Тогда согласно предложению 1 $\sigma(u)(i) = \Psi_\sigma(\beta_s)$. Поскольку $\bar{\beta}_s = \bar{a}_s$ (так введена нумерация), то $\bar{\beta}_s = \bar{u}(i) = \text{tr}(\bar{c} \bar{\theta}^i)$. Тогда в силу (1)

$$\beta_s = \text{tr}(c\theta^i)^{q^{n-1}} = (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{n-1}}.$$

Отсюда

$$\begin{aligned} \sigma(u)(i) &= \Psi_\sigma(\beta_s) = \psi_0 + \sum_{\lambda=1}^{q-1} \psi_\lambda (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{n-1}\lambda} \\ &= \psi_0 \theta^{Ti} + \sum_{\lambda=1}^{q-1} \psi_\lambda \sum_{k_0+\dots+k_{M-1}=q^{n-1}\lambda} \frac{(q^{n-1}\lambda)!}{k_0! \dots k_{M-1}!} (c\theta^i)^{k_0+qk_1+\dots+q^{M-1}k_{M-1}}. \end{aligned}$$

С другой стороны, согласно (3)

$$\sigma(u)(i) = \sum_{k=1}^T c_k \theta^{ik}, \quad i \in \mathbb{N}_0.$$

В силу двух последних равенств и в силу предложения 2 (однозначность представления последовательности в виде (2)) для любого $l = 1, \dots, q-1$

$$\sum_{k=1, k \equiv l \bmod (q-1)}^T c_k \theta^{ik} = \psi_0 \varepsilon + \sum_{\lambda=1}^{q-1} \psi_\lambda \sum_{k_0, \dots, k_{M-1}} \frac{(q^{n-1}\lambda)!}{k_0! \dots k_{M-1}!} (c\theta^i)^{k_0+qk_1+\dots+q^{M-1}k_{M-1}}, \quad (6)$$

где $\varepsilon = 1$ при $l = q - 1$ и 0 при $l < q - 1$ и суммирование во внутренней сумме проводится по всевозможным наборам целых неотрицательных чисел $k_0, \dots, k_{M-1}$, удовлетворяющим условиям

$$k_0 + \dots + k_{M-1} = q^{n-1}\lambda, \quad k_0 + qk_1 + \dots + q^{M-1}k_{M-1} \equiv l \pmod{q-1}. \quad (7)$$

Ясно, что

$$k_0 + qk_1 + \dots + q^{M-1}k_{M-1} \equiv k_0 + k_1 + \dots + k_{M-1} \pmod{q-1},$$

а также

$$k_0 + k_1 + \dots + k_{M-1} = q^{n-1}\lambda \equiv \lambda \pmod{q-1}.$$

Тогда второе условие в (7) равносильно условию $\lambda \equiv l \pmod{q-1}$, то есть $\lambda = l$ (так как $\lambda, l \in \{0, 1, \dots, q-1\}$). Следовательно, условия (7) равносильны условию $k_0 + \dots + k_{M-1} = q^{n-1}l$, и соотношение (6) можно записать следующим образом:

$$\begin{aligned} \sum_{\substack{k=1 \\ k \equiv l \pmod{q-1}}}^T c_k \theta^{ik} &= \psi_0 \varepsilon + \psi_l \sum_{k_0 + \dots + k_{M-1} = q^{n-1}l} \frac{(q^{n-1}l)!}{k_0! \dots k_{M-1}!} (c\theta^i)^{k_0 + qk_1 + \dots + q^{M-1}k_{M-1}} \\ &= \psi_0 \varepsilon + \psi_l (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{n-1}l}. \end{aligned}$$

Полагая в условии леммы 4 $a = c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}}$ и $j = M$, получим, что

$$\begin{aligned} (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{n-1}} \\ \equiv (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{M-1}} \pmod{p^{r(M-1)+1}}. \end{aligned}$$

Это сравнение тем более выполнено по модулю p^{t+1} для любого $t = 0, 1, \dots, r(M-1)$. Следовательно,

$$\sum_{\substack{k=1 \\ k \equiv l \pmod{q-1}}}^T c_k \theta^{ik} \equiv \psi_0 \varepsilon + \psi_l (c\theta^i + (c\theta^i)^q + \dots + (c\theta^i)^{q^{M-1}})^{q^{M-1}l} \pmod{p^{t+\|\psi_l\|+1}}$$

или

$$\begin{aligned} \sum_{\substack{k=1 \\ k \equiv l \pmod{q-1}}}^T c_k \theta^{ik} &\equiv \psi_0 \varepsilon \theta^{Ti} \\ &+ \psi_l \sum_{k_0 + \dots + k_{M-1} = q^{M-1}l} \frac{(q^{M-1}l)!}{k_0! \dots k_{M-1}!} (c\theta^i)^{k_0 + qk_1 + \dots + q^{M-1}k_{M-1}} \pmod{p^{t+\|\psi_l\|+1}} \end{aligned}$$

для всех $l = 1, \dots, q-1, t = 0, 1, \dots, r(M-1), i \in \mathbb{N}$. Пусть теперь k, l, t — числа, определенные в условии предложения 4. Тогда в силу леммы 3 и предложения 2 (однозначность) получаем, что

$$c_k \equiv \psi_l \sum_{k_0, \dots, k_{M-1}} \frac{(q^{M-1}l)!}{k_0! \dots k_{M-1}!} c^{k_0 + \dots + q^{M-1}k_{M-1}} \pmod{p^{t+\|\psi_l\|+1}}, \quad (8)$$

где суммирование производится по всевозможным наборам целых неотрицательных чисел $k_0, \dots, k_{M-1}$ таким, что

$$k_0 + \dots + k_{M-1} = q^{M-1}l, \quad (9)$$

$$(k_0 + qk_1 + \dots + q^{M-1}k_{M-1}) \bmod T = k. \quad (10)$$

Теперь наша цель — посчитать сумму (8).

2. Рассмотрим произвольное слагаемое суммы (8). Согласно п. (а) леммы 1 и п. (а), (г) леммы 2 максимальная степень E числа p , на которую делится полиномиальный коэффициент в (8), удовлетворяет соотношениям

$$\begin{aligned} E &= \frac{1}{p-1} \left(\sum_{j=0}^{M-1} w(k_j) - w(q^{M-1}l) \right) \\ &= \frac{1}{p-1} \left(\sum_{j=0}^{M-1} w(q^j k_j \bmod T) - w(l) \right) \geq \frac{w(k) - w(l)}{p-1} = t, \end{aligned}$$

причем равенство $E = t$ выполняется тогда и только тогда, когда

$$w(k) = \sum_{j=0}^{M-1} w(q^j k_j \bmod T). \quad (11)$$

Согласно п. (б) леммы 1 при условии (11) справедливо сравнение

$$\frac{(q^{M-1}l)!}{k_0! \dots k_{M-1}!} \equiv (-p)^t \frac{v_0(l)! \dots v_{r-1}(l)!}{v_0(k_0)! v_1(k_0)! \dots v_{rM-1}(k_{M-1})!} \pmod{p^{t+1}}.$$

Следовательно, опуская в сумме (8) нулевые по модулю $p^{t+\|\psi_l\|+1}$ слагаемые, получим сумму слагаемых, индексы которых $k_0, \dots, k_{M-1}$ удовлетворяют условиям (9), (10), (11):

$$c_k \equiv \psi_l \sum_{k_0, \dots, k_{M-1}} (-p)^t \frac{v_0(l)! \dots v_{r-1}(l)!}{v_0(k_0)! v_1(k_0)! \dots v_{rM-1}(k_{M-1})!} c^{k_0 + \dots + q^{M-1}k_{M-1}}$$

по модулю $p^{t+\|\psi_l\|+1}$. Так как ввиду (10) $\bar{c}^{k_0 + \dots + q^{M-1}k_{M-1}} = \bar{c}^k$, получим, что

$$c_k \equiv (-p)^t \psi_l c^k v_0(l)! \dots v_{r-1}(l) \sum_{k_0, \dots, k_{M-1}} \prod_{s=0}^{rM-1} \prod_{j=0}^{M-1} \frac{1}{v_s(k_j)!} \pmod{p^{t+\|\psi_l\|+1}}. \quad (12)$$

Перепишем условия (9), (10), (11) в другом виде, так чтобы новые условия связывали не числа k_j , а разряды их p -ичного разложения $v_s(k_j)$. Согласно п. (д) леммы 2 соотношения (10), (11) эквивалентны равенствам

$$v_s(k) = \sum_{j=0}^{M-1} v_s(q^j k_j \bmod T) = \sum_{j=0}^{M-1} v_{s \ominus rj}(k_j), \quad s = 0, 1, \dots, rM-1, \quad (13)$$

где $\ominus$ — вычитание по модулю rM . Равенство (9) может быть записано следующим образом:

$$q^{M-1}l = \sum_{j=0}^{M-1} k_j = \sum_{j=0}^{M-1} \sum_{s=0}^{rM-1} p^s v_s(k_j). \quad (14)$$

Таким образом, соотношения (9), (10), (11) равносильны условиям (13), (14). Следовательно, заменяя в сумме (12) индексы суммирования и полагая $v_{s,j} = v_s(k_j)$, получим, что

$$c_k \equiv (-p)^t \psi_l c^k v_0(l)! \dots v_{r-1}(l)! \sum_{v_{s,j}}^{rM-1} \prod_{s=0}^{M-1} \prod_{j=0}^{M-1} \frac{1}{v_{s,j}!} \pmod{p^{t+\|\psi_l\|+1}},$$

или

$$c_k \equiv (-p)^t \psi_l c^k \frac{v_0(l)! \dots v_{r-1}(l)!}{v_0(k)! \dots v_{rM-1}(k)!} \sum_{v_{s,j}}^{rM-1} \prod_{s=0}^{M-1} \frac{v_s(k)!}{\prod_{j=0}^{M-1} v_{s,j}!} \pmod{p^{t+\|\psi_l\|+1}}, \quad (15)$$

где суммирование проводится по всевозможным наборам целых неотрицательных чисел $v_{s,j}$, $s = 0, 1, \dots, rM-1$, $j = 0, 1, \dots, M-1$, удовлетворяющих условиям

$$\sum_{j=0}^{M-1} v_{s \ominus rj, j} = v_s(k), \quad s = 0, 1, \dots, rM-1, \quad (16)$$

$$\sum_{j=0}^{M-1} \sum_{s=0}^{rM-1} p^s v_{s,j} = q^{M-1}l. \quad (17)$$

Обозначим через Σ_v сумму в соотношении (15). Остается показать, что $\Sigma_v \equiv 1 \pmod{p}$.

3. Заметим, что

$$\prod_{s=0}^{rM-1} \prod_{j=0}^{M-1} v_{s,j}! = \prod_{s=0}^{rM-1} \prod_{j=0}^{M-1} v_{s \ominus rj, j}!, \quad \sum_{j=0}^{M-1} \sum_{s=0}^{rM-1} p^s v_{s,j} = \sum_{j=0}^{M-1} \sum_{s=0}^{rM-1} p^{s \ominus rj} v_{s \ominus rj, j},$$

где первое равенство получено заменой порядка множителей, а второе заменой порядка слагаемых. Поэтому сумма Σ_v примет вид

$$\Sigma_v = \sum_{v_{s,j}} \prod_{s=0}^{rM-1} v_s(k)! / \prod_{j=0}^{M-1} v_{s \ominus rj, j}!,$$

а условия (16), (17) заменяются на эквивалентные:

$$\sum_{j=0}^{M-1} v_{s \ominus rj, j} = v_s(k), \quad s = 0, 1, \dots, rM-1, \quad \sum_{j=0}^{M-1} \sum_{s=0}^{rM-1} p^{s \ominus rj} v_{s \ominus rj, j} = q^{M-1}l.$$

Теперь видно, что сумма Σ_v равна коэффициенту при $y^{q^{M-1}l}$ в следующем произведении rM многочленов над кольцом целых чисел:

$$\begin{aligned} f_0(y) &= \prod_{s=0}^{rM-1} (y^{p^s} + y^{p^{s \ominus r}} + y^{p^{s \ominus 2r}} + \dots + y^{p^{s \ominus r(M-1)}})_{v_s(k)} \\ &= \prod_{s=0}^{r-1} (y^{p^s} + y^{p^{s+r}} + y^{p^{s+2r}} + \dots + y^{p^{s+r(M-1)}})_{v_s(k)+v_{s+r}(k)+\dots+v_{s+r(M-1)}(k)}. \end{aligned}$$

Рассмотрим q -ичное разложение натуральных чисел. Пусть $t \in \mathbb{N}$ и

$$t = t_0 + qt_1 + \dots + q^d t_d + \dots, \quad t_i \in \{0, 1, \dots, q-1\}, \quad i \in \mathbb{N}_0.$$

Определим q -ичный вес числа t как $w_q(t) = t_0 + t_1 + \dots + t_d + \dots$. Напомним, что $l = k \bmod (q-1)$. Нетрудно показать, что $l = w_q(k) \bmod (q-1)$. Ясно, что

$$w_q(k) = \sum_{s=0}^{r-1} p^s (v_s(k) + v_{s+r}(k) + \dots + v_{s+r(M-1)}(k)).$$

Введем обозначения

$$\lambda_0^{(s)} = \lambda_0^{(s)}(k) = v_s(k) + v_{s+r}(k) + \dots + v_{s+r(M-1)}(k), \quad s = 0, 1, \dots, r-1.$$

Тогда

$$f_0(y) = \prod_{s=0}^{r-1} (y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})_{\lambda_0^{(s)}}, \quad w_q(k) = \sum_{s=0}^{r-1} p^s \lambda_0^{(s)}.$$

Напомним, что нам нужно показать, что сумма Σ_v , равная коэффициенту при $y^{q^{M-1}l}$, $l = w_q(k) \bmod (q-1)$, многочлена $f_0(y)$, сравнима с единицей по модулю p .

Если $M = 1$, то

$$f_0(y) = \prod_{s=0}^{r-1} (y^{p^s})_{\lambda_0^{(s)}} = y^{\sum_{s=0}^{r-1} p^s \lambda_0^{(s)}} = y^{w_q(k)}.$$

Заметим, что $\lambda_0^{(s)} \leq M(p-1) = p-1$, и значит, $w_q(k) \leq q-1$. Учитывая, что $l = w_q(k) \bmod (q-1)$, получаем равенство $l = w_q(k)$. Следовательно, $f_0(y) = y^l$ и $\Sigma_v = 1$.

Пусть $M \geq 2$. Далее мы будем переходить от многочлена $f_0(y)$ к более простым многочленам, у которых коэффициенты при $y^{q^{M-1}l}$ сравнимы по модулю p .

Шаг 1. Число $\lambda_0^{(s)}$, $s \in \{0, 1, \dots, r-1\}$, представим в виде

$$\lambda_0^{(s)} = a_0^{(s)} + pb_0^{(s)}, \quad 0 \leq a_0^{(s)} < p, \quad b_0^{(s)} \geq 0.$$

Тогда справедливо сравнение по модулю p

$$\begin{aligned} f_0(y) &\equiv_p \prod_{s=0}^{r-1} ((y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})_{a_0^{(s)}} (y^{p^{s+1}} + y^{p^{r+s+1}} + \dots + y^{p^{r(M-1)+s+1}})_{b_0^{(s)}}) \\ &= \prod_{s=1}^{r-1} (y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})_{a_0^{(s)} + b_0^{(s-1)}} (y + y^{p^r} + \dots + y^{p^{r(M-1)}})_{a_0^{(0)}} \\ &\quad \times (y^{p^r} + y^{p^{2r}} + \dots + y^{p^{rM}})_{b_0^{(r-1)}}. \end{aligned}$$

Так как $0 \leq a_0^{(0)} < p$, $M > 1$ и $p^{rM} > q^M l$, коэффициент при $y^{q^{M-1}l}$ в последнем многочлене равен коэффициенту при $y^{q^{M-1}l}$ в многочлене

$$f_1(y) = \prod_{s=1}^{r-1} (y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_1^{(s)}} (y^{p^r} + y^{p^{2r}} + \dots + y^{p^{r(M-1)}})^{\lambda_1^{(0)}},$$

где

$$\lambda_1^{(s)} = a_0^{(s)} + b_0^{(s \ominus 1)}, \quad s = 0, 1, \dots, r-1,$$

а $\ominus$ — вычитание по модулю r . При этом

$$\begin{aligned} w_q(k) &= \sum_{s=0}^{r-1} p^s \lambda_0^{(s)} = \sum_{s=0}^{r-1} p^s (a_0^{(s)} + p b_0^{(s)}) \\ &= \sum_{s=1}^{r-1} p^s (a_0^{(s)} + b_0^{(s-1)}) + a_0^{(0)} + b_0^{(r-1)} p^r \equiv \sum_{s=1}^{r-1} p^s \lambda_1^{(s)} + \lambda_1^{(0)} = \sum_{s=0}^{r-1} p^s \lambda_1^{(s)}. \end{aligned}$$

Шаг 2. Представим $\lambda_1^{(s)}$, $s \in \{0, 1, \dots, r-1\}$, в виде

$$\lambda_1^{(s)} = a_1^{(s)} + p b_1^{(s)}, \quad 0 \leq a_1^{(s)} < p, \quad b_1^{(s)} \geq 0.$$

Тогда

$$\begin{aligned} f_1(y) &\equiv_p \prod_{s=1}^{r-1} ((y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})^{a_1^{(s)}} (y^{p^{s+1}} + y^{p^{r+s+1}} + \dots + y^{p^{r(M-1)+s+1}})^{b_1^{(s)}}) \\ &\quad \times (y^{p^r} + y^{p^{2r}} + \dots + y^{p^{r(M-1)}})^{a_1^{(0)}} (y^{p^{r+1}} + y^{p^{2r+1}} + \dots + y^{p^{r(M-1)+1}})^{b_1^{(0)}} \\ &= \prod_{s=2}^{r-1} (y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})^{a_1^{(s)} + b_1^{(s-1)}} \\ &\quad \times (y^{p^p} + y^{p^{r+1}} + \dots + y^{p^{r(M-1)+1}})^{a_1^{(1)}} (y^{p^r} + y^{p^{2r}} + \dots + y^{p^{rM}})^{b_1^{(r-1)}} \\ &\quad \times (y^{p^r} + y^{p^2} + \dots + y^{p^{r(M-1)}})^{a_1^{(0)}} (y^{p^{r+1}} + y^{p^{2r+1}} + \dots + y^{p^{r(M-1)+1}})^{b_1^{(0)}}. \end{aligned}$$

Так как $0 \leq a_1^{(1)} < p$, $M > 1$ и $p^{rM} > q^M l$, коэффициент при $y^{q^{M-1}l}$ в последнем многочлене равен коэффициенту при $y^{q^{M-1}l}$ в многочлене

$$f_2(y) = \prod_{s=2}^{r-1} (y^{p^s} + y^{p^{r+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_2^{(s)}} \times \prod_{s=0}^1 (y^{p^{r+s}} + y^{p^{2r+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_2^{(s)}},$$

где $\lambda_2^{(s)} = a_1^{(s)} + b_1^{(s \ominus 1)}$, $s = 0, 1, \dots, r-1$. При этом

$$\begin{aligned} w_q(k) &\equiv_{q-1} \sum_{s=0}^{r-1} p^s \lambda_1^{(s)} = \sum_{s=0}^{r-1} p^s (a_1^{(s)} + p b_1^{(s)}) \\ &= \sum_{s=1}^{r-1} p^s (a_1^{(s)} + b_1^{(s-1)}) + a_1^{(0)} + b_1^{(r-1)} p^r \equiv_{q-1} \sum_{s=0}^{r-1} p^s \lambda_2^{(s)}. \end{aligned}$$

Шаг r . Действуя таким образом, на r -м шаге получим многочлен

$$f_r(y) = \prod_{s=0}^{r-1} (y^{p^{r+s}} + y^{p^{2r+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_r^{(s)}},$$

где

$$\lambda_r^{(s)} = a_{r-1}^{(s)} + b_{r-1}^{(s \ominus 1)}, \quad s = 0, 1, \dots, r-1, \quad w_q(k) \equiv \sum_{s=0}^{r-1} p^s \lambda_r^{(s)}.$$

Отметим, что по сравнению с $f_0(y)$ многочлен $f_r(y)$ проще: в каждом сомножителе многочлена $f_r(y)$ на одно слагаемое меньше. Если $M \geq 3$, то в каждом сомножителе многочлена $f_r(y)$ более одного слагаемого, и мы продолжим упрощать многочлен тем же образом, делая шаги $r+1, r+2, \dots$. На произвольном шаге i , $r+1 \leq i \leq r(M-1)$, мы получим многочлен

$$f_i(y) = \prod_{s=i_2}^{r-1} (y^{p^{ri_1+s}} + y^{p^{r(i_1+1)+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_i^{(s)}} \\ \times \prod_{s=0}^{i_2-1} (y^{p^{r(i_1+1)+s}} + y^{p^{r(i_1+2)+s}} + \dots + y^{p^{r(M-1)+s}})^{\lambda_i^{(s)}},$$

где $i = ri_1 + i_2$, $0 \leq i_2 < r$; $\lambda_i^{(s)} = a_{i-1}^{(s)} + b_{i-1}^{(s \ominus 1)}$, $s = 0, \dots, r-1$ (считаем, что $\prod_0^{-1} = 1$). При этом

$$w_q(k) \equiv \sum_{s=0}^{r-1} p^s \lambda_i^{(s)}.$$

На последнем шаге с номером $r(M-1)$ получим, что

$$f_{r(M-1)}(y) = \prod_{s=0}^{r-1} (y^{p^{r(M-1)+s}})^{\lambda_{r(M-1)}^{(s)}} \\ = y^{\sum_{s=0}^{r-1} p^{r(M-1)+s} \lambda_{r(M-1)}^{(s)}} = y^{q^{M-1} \sum_{s=0}^{r-1} p^s \lambda_{r(M-1)}^{(s)}}$$

и

$$w_q(k) \equiv \sum_{s=0}^{r-1} p^s \lambda_{r(M-1)}^{(s)}.$$

Напомним, что $l = w_q(k) \bmod (q-1)$. Далее мы докажем неравенства

$$\lambda_{r(M-1)}^{(s)} \leq p-1, \quad s = 0, 1, \dots, r-1,$$

откуда следует справедливость равенств

$$\sum_{s=0}^{r-1} p^s \lambda_{r(M-1)}^{(s)} = l, \quad f_{r(M-1)}(y) = y^{q^{M-1}l},$$

а значит, $\Sigma_v \equiv_p 1$.

Докажем, что $\lambda_{r(M-1)}^s \leq p-1$, $s = 0, 1, \dots, r-1$. Для этого рассмотрим последовательность векторов

$$\vec{\lambda}_i = (\lambda_i^{(0)}, \lambda_i^{(1)}, \dots, \lambda_i^{(r-1)}), \quad i = 0, 1, \dots, r(M-1),$$

и последовательность чисел

$$\lambda_i = \sum_{s=0}^{r-1} \lambda_i^{(s)}, \quad i = 0, 1, \dots, r(M-1).$$

Лемма 5. Пусть $i \in \{0, 1, \dots, r(M-1)\}$ и $\lambda_i^{(s)} \leq p-1$, $s = 0, 1, \dots, r-1$. Тогда

$$\vec{\lambda}_i = \vec{\lambda}_{i+1} = \dots = \vec{\lambda}_{r(M-1)}.$$

Доказательство. Пусть $\lambda_i^{(s)} \leq p-1$, $s = 0, 1, \dots, r-1$. Тогда $\lambda_i^{(s)} = a_i^{(s)}$ и $b_i^{(s)} = 0$, $s = 0, 1, \dots, r-1$. При этом $\lambda_{i+1}^{(s)} = a_i^{(s)} + b_i^{(s \oplus 1)} = a_i^{(s)} = \lambda_i^{(s)}$. Значит, $\vec{\lambda}_{i+1} = \vec{\lambda}_i$.

Будем говорить, что последовательность $\vec{\lambda}_i$, $i = 0, 1, \dots, r(M-1)$, стабилизировалась на шаге i , если $\lambda_i^{(s)} \leq p-1$ для любого $s = 0, 1, \dots, r-1$.

Далее мы будем пользоваться следующим очевидным фактом. Для любого $c \in \mathbb{N}$ верна импликация

$$\text{если } c = a + pb, \ 0 \leq a < p \text{ и } b \geq 1, \text{ то } a + b \leq c - (p-1). \quad (18)$$

Из определения чисел $\lambda_0^{(s)}$ следует, что $\lambda_0^{(s)} \leq M(p-1)$, $s = 0, 1, \dots, r-1$.

Пусть число элементов $\lambda_0^{(s)}$, $s = 0, 1, \dots, r-1$, таких, что $\lambda_0^{(s)} \geq p$, равно d . Тогда

$$\lambda_0 = \sum_{s=0}^{r-1} \lambda_0^{(s)} \leq dM(p-1) + (r-d)(p-1) = (d(M-1) + r)(p-1).$$

Если $d = 0$, то последовательность векторов $\vec{\lambda}_i$, $i = 0, 1, \dots, r(M-1)$, стабилизировалась.

Пусть $d > 0$. Рассмотрим разность

$$\begin{aligned} \lambda_0 - \lambda_1 &= \sum_{s=0}^{r-1} \lambda_0^{(s)} - \sum_{s=0}^{r-1} \lambda_1^{(s)} = \sum_{s=0}^{r-1} \lambda_0^{(s)} - \sum_{s=0}^{r-1} (a_0^{(s)} + b_0^{(s \oplus 1)}) \\ &= \sum_{s=0}^{r-1} \lambda_0^{(s)} - \sum_{s=0}^{r-1} (a_0^{(s)} + b_0^{(s)}) = \sum_{s=0}^{r-1} (\lambda_0^{(s)} - (a_0^{(s)} + b_0^{(s)})). \end{aligned}$$

В силу (18) $\lambda_0 - \lambda_1 \geq d(p-1)$, то есть $\lambda_1 \leq \lambda_0 - d(p-1)$.

Пусть $i \in \{2, \dots, r(M-1)\}$. Тогда либо последовательность стабилизировалась до шага i , либо существует $j \in \{0, 1, \dots, r-1\}$ такое, что $\lambda_{i-1}^{(j)} = a_{i-1}^{(j)} + pb_{i-1}^{(j)}$, $b_{i-1}^{(j)} \geq 1$. Рассмотрим разность

$$\begin{aligned} \lambda_{i-1} - \lambda_i &= \sum_{s=0}^{r-1} \lambda_{i-1}^{(s)} - \sum_{s=0}^{r-1} \lambda_i^{(s)} \\ &= \sum_{s=0}^{r-1} \lambda_{i-1}^{(s)} - \sum_{s=0}^{r-1} (a_{i-1}^{(s)} + b_{i-1}^{(s \oplus 1)}) = \sum_{s=0}^{r-1} (\lambda_{i-1}^{(s)} - (a_{i-1}^{(s)} + b_{i-1}^{(s)})). \end{aligned}$$

В силу (18) $\lambda_{i-1} - \lambda_i \geq p - 1$, то есть $\lambda_i \leq \lambda_{i-1} - (p - 1)$.

Таким образом, получаем, что либо последовательность стабилизируется до шага $r(M - 1)$, либо

$$\begin{aligned}\lambda_{r(M-1)} &\leq \lambda_0 - d(p - 1) - (r(M - 1) - 1)(p - 1) \\ &\leq (d(M - 1) + r)(p - 1) - (d + r(M - 1) - 1)(p - 1) \\ &= ((d - r)(M - 2) + 1)(p - 1).\end{aligned}$$

Так как $1 \leq d \leq r$ и $M \geq 2$, то $\lambda_{r(M-1)} \leq p - 1$, а значит, и $\lambda_{r(M-1)}^{(s)} \leq p - 1$, $s = 0, 1, \dots, r - 1$, то есть последовательность стабилизировалась на шаге $r(M - 1)$.

Доказательство теоремы 1. Теорема 1 вытекает из предложений 2–4. Действительно, согласно (3)

$$\sigma(u)(i) = \sum_{k=1}^T c_k \theta^{ik}, \quad i \in \mathbb{N}_0, \quad c_1, \dots, c_T \in S.$$

Из предложений 3, 4 и определения многочлена $H_s(x)$ следует, что элемент θ^k , $k = 1, \dots, T$, является корнем $H_s(x)$ тогда и только тогда, когда $\|c_k\| \leq s$. Поэтому в силу предложения 2

$$\text{Ann}(\sigma(u)) = (H_{n-1}(x), pH_{n-2}(x), \dots, p^{n-1}H_0(x)).$$

Автор выражает признательность В. Л. Куракину за постановку задачи и обсуждение результатов статьи.

Список литературы

1. Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, т. 2. Гелиос, Москва, 2003.
2. Куракин В. Л., Представления над кольцом линейной рекуррентной последовательности максимального периода над полем $GF(p)$. *Дискретная математика* (1992) **4**, №4, 96–116.
3. Лидл Р., Нидеррайтер Г., *Конечные поля*, т. 2. Мир, Москва, 1988.
4. Нечаев А. А., Код Кердока в циклической форме. *Дискретная математика* (1989) **1**, №4, 123–139.
5. Нечаев А. А., Цикловые типы линейных подстановок над конечными коммутативными кольцами. *Матем сб.* (1993) **184**, №3, 21–56.
6. McDonald B. R., *Finite rings with identity*. Marcel Dekker, New York, 1974.

Статья поступила 3.02.2005.