

Проблема полноты в классе линейных p -адических автоматов

М. Э. Калашников*

В работе исследована проблема K -полноты в классе линейных p -адических автоматов для нечётного простого числа p . Получены критерии полноты для однородных и неоднородных линейных p -адических функций. Полученные результаты обобщают известные свойства линейных 2-адических автоматов на случай произвольного нечётного простого основания. Кроме того, построена континуальная строго возрастающая цепочка K -замкнутых классов I_α , $\alpha \in (0, 1]$.

Ключевые слова: конечный автомат, p -адическое число, линейный p -адический автомат, операции композиции, обратная связь, проблема полноты, замкнутый класс.

Введение

В настоящее время активно изучаются свойства класса конечных автоматов и его многочисленных подклассов. В частности, в работах [2–4] рассматривается задача K -полноты для линейных автоматов над конечными полями.

Важным подклассом множества конечных автоматов является класс p -адических автоматов, систематическое изучение которого началось с работы [5]. Для исследования таких автоматов используется аппарат p -адических чисел.

В работе [1] была решена проблема K -полноты для класса линейных 2-адических автоматов: описаны все предполные классы и доказана алгоритмическая разрешимость проверки полноты конечных систем.

В настоящей работе полученные результаты обобщаются на случай линейных p -адических автоматов для произвольного нечётного простого числа p .

* *Калашников Максим Эдуардович* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: maxkalash98@gmail.com.

Kalashnikov Maksim Eduardovich — Postgraduate student, Chair of Mathematical Theory of Intelligent Systems, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

1. Начальные установки

В работе изучается класс L_p линейных p -адических автоматов, вычисляющих линейные функции на кольце целых p -адических чисел $\mathbb{Z}_p$ с коэффициентами из подкольца

$$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}.$$

Здесь и далее p обозначает произвольное нечётное простое число. Множество $E_p = \{0, 1, \dots, p-1\}$ представляет собой используемый алфавит.

Определение 1. Конечный инициальный автомат с входным алфавитом E_p^n и выходным алфавитом E_p называется линейным p -адическим автоматом, если для определяемого им отображения $f(x_1, \dots, x_n)$ существуют числа $r_0, r_1, \dots, r_n \in \mathbb{Z}_{(p)}$ такие, что для любых $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_p$

$$f(\alpha_1, \dots, \alpha_n) = \sum_{i=1}^n r_i \alpha_i + r_0.$$

В этом случае будем говорить, что функция f имеет разложение

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0. \quad (1)$$

Всюду в работе будут использоваться следующие обозначения и соглашения. Запись Gb_x обозначает операцию применения обратной связи к переменной x .

Пусть A — числовое множество и $k \in \mathbb{Q}$. Положим

$$kA = \{ka \mid a \in A\}, \quad k + A = \{k + a \mid a \in A\}.$$

Если $k \neq 0$, то также положим

$$\frac{A}{k} = \left\{ \frac{a}{k} \mid a \in A \right\}.$$

Для простого числа q определим q -адическую оценку

$$v_q: \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}.$$

Если $r \neq 0$, то единственным образом

$$r = q^k \frac{u}{v}, \quad k \in \mathbb{Z}, \quad u, v \in \mathbb{Z}, \quad v > 0, \quad (u, v) = 1, \quad q \nmid uv.$$

Положим $v_q(r) = k$. Кроме того, $v_q(0) = +\infty$.

Для $r \in \mathbb{Z}_{(p)}$ через $\bar{r}$ будем обозначать его остаток от деления на p . Другими словами, $r \in \bar{r} + p\mathbb{Z}_{(p)}$, $\bar{r} \in E_p$.

Переменная x_i называется непосредственной, если для соответствующего коэффициента $v_p(r_i) = 0$. Операция обратной связи применима к переменной тогда и только тогда, когда соответствующая переменная не является непосредственной. Через L_p^0 будем обозначать подмножество L_p , состоящее из однородных функций (свободный член в разложении (1) равен нулю).

Для функции

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0$$

положим

$$U(f) = \{r_i \mid 1 \leq i \leq n\},$$

причем, при использовании представителей из $U(f)$ договоримся брать дроби в несократимом виде. Переменная x_i называется существенной, если $r_i \neq 0$.

Для $M \subseteq L_p$ через $K(M)$ обозначим замыкание M относительно отождествления и переименования переменных, подстановки и обратной связи. Множество M называется K -замкнутым, если $K(M) = M$, и K -полным в L_p , если $K(M) = L_p$.

2. Некоторые свойства L_p

Начнём с леммы, описывающей действие операций композиции на линейные p -адические функции. Аналогичное утверждение для 2-адического случая доказано в работе [1].

Лемма 1. Пусть для функций f и f' выполнено:

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0,$$

$$f'(x_{n+1}, \dots, x_{n+n'}) = \sum_{i=n+1}^{n+n'} r_i x_i + r'_0.$$

Через f_1, f_2, f_3 обозначим функции, получаемые, соответственно, отождествлением переменных x_{n-1} и x_n функции f (при $n \geq 2$), переименованием переменных функции f с $x_1, \dots, x_n$ на $x'_1, \dots, x'_n$, подстановкой функции f вместо переменной $x_{n+n'}$ функции f' . Если к переменной x_n

функции f применима обратная связь, то через f_4 обозначим результат применения обратной связи к этой переменной. Тогда выполнены следующие равенства:

$$\begin{aligned} f_1(x_1, \dots, x_{n-1}) &= \sum_{i=1}^{n-2} r_i x_i + (r_{n-1} + r_n) x_{n-1} + r_0, \\ f_2(x'_1, \dots, x'_n) &= \sum_{i=1}^n r_i x'_i + r_0, \\ f_3(x_1, \dots, x_{n+n'-1}) &= \sum_{i=n+1}^{n+n'-1} r_i x_i + \sum_{i=1}^n r_i r_{n+n'} x_i + r'_0 + r_{n+n'} r_0, \\ f_4(x_1, \dots, x_{n-1}) &= \sum_{i=1}^{n-1} \frac{r_i}{1 - r_n} x_i + \frac{r_0}{1 - r_n}. \end{aligned}$$

Далее покажем, что класс линейных p -адических функций порождается простым сумматором и константой.

Определение 2. Автомат, реализующий p -адический сумматор $x_1 + x_2$, задаётся следующей системой канонических уравнений:

$$\begin{aligned} q(0) &= 0, \\ q(t+1) &= \left\lfloor \frac{a(t) + b(t) + q(t)}{p} \right\rfloor, \\ y(t) &= a(t) + b(t) + q(t) - p q(t+1). \end{aligned}$$

Лемма 2.

$$K(\{x_1 + x_2, 1\}) = L_p.$$

Доказательство. Положим $M = \{x_1 + x_2, 1\}$. Будем последовательно получать всё более сложные функции из $K(M)$.

Последовательно применяя к сумматору $x_1 + x_2$ операции подстановки и переименования переменных, получаем

$$x_1 + \dots + x_n \in K(M),$$

а значит, отождествляя переменные, имеем

$$\forall n \in \mathbb{N}: \quad nx \in K(M).$$

В частности, получаем $py \in K(M)$ и $(p-1)x \in K(M)$, следовательно,

$$(p-1)x + py \in K(M).$$

Применим обратную связь по переменной y :

$$\text{Fb}_y((p-1)x + py) = \frac{p-1}{1-p}x = -x \in K(M).$$

Подставляя функцию nx в функцию $-x$, для каждого $n \in \mathbb{N}$ получаем функцию $-nx$. Следовательно,

$$\forall k \in \mathbb{Z} : \quad kx \in K(M).$$

Пусть $r \in \mathbb{Z}_{(p)}$. Тогда $r = \frac{a}{b}$, где $a \in \mathbb{Z}$, $b \in \mathbb{N}$ и $p \nmid b$. Так как $(p, b) = 1$, по алгоритму Евклида существуют $k, \ell \in \mathbb{Z}$ такие, что

$$kp + \ell b = 1, \quad \text{то есть} \quad b = \frac{1 - kp}{\ell}.$$

Рассмотрим функцию

$$g(x, y) = a\ell x + kp y \in K(M).$$

Применяя обратную связь к переменной y , получаем

$$\text{Fb}_y(g) = \frac{a\ell}{1 - kp}x = \frac{a}{(1 - kp)/\ell}x = \frac{a}{b}x = rx.$$

Значит,

$$\forall r \in \mathbb{Z}_{(p)} : \quad rx \in K(M).$$

Пусть $f \in L_p$, то есть

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0, \quad r_i, r_0 \in \mathbb{Z}_{(p)}.$$

По доказанному выше для каждого i имеем $r_i x_i \in K(M)$, а также $r_0 x_0 \in K(M)$. Тогда

$$\sum_{i=1}^n r_i x_i + r_0 x_0 \in K(M),$$

и, подставив 1 вместо x_0 , получаем $f \in K(M)$. Значит, $L_p \subseteq K(M)$.

Обратное включение также выполняется, поскольку $M \subseteq L_p$ и класс L_p замкнут относительно операций композиции, то есть $K(M) \subseteq L_p$. Следовательно, $K(M) = L_p$. $\square$

Теперь определим некоторые важные классы функций в L_p :

Определение 3.

$$T_a = \{f \in L_p \mid f(\alpha_1, \dots, \alpha_n) \in a + p\mathbb{Z}_p \text{ для всех } \alpha_1, \dots, \alpha_n \in a + p\mathbb{Z}_p\}.$$

$$V_1 = \{f \in L_p \mid f \text{ имеет не более одной непосредственной переменной}\}.$$

$$V_o = \left\{ f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0 \mid \sum_{i=1}^n r_i \equiv 1 \pmod{p} \right\}.$$

$$I = \left\{ f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0 \mid \sum_{i=1}^n |r_i| \leq 1 \right\}.$$

$$R_c(q) = \{f \in L_p \mid f \text{ имеет не одну существенную переменную, и}$$

$$\forall \frac{u}{v} \in U(f), (u, v) = 1 : (u, q) = q, (q, v) = 1\} \cup$$

$$\cup \{f \in L_p \mid f \text{ имеет одну существенную переменную, и}$$

$$\forall \frac{u}{v} \in U(f) \setminus \{0\}, (u, v) = 1 : (v, q) = 1\}, \quad q - \text{простое, не равное } p.$$

$$R_d(q) = \{f \in L_p \mid f \text{ имеет не одну непосред. переменную, и}$$

$$\forall \frac{u}{v} \in U(f), (u, v) = 1 : (u, q) = q, (q, v) = 1\} \cup$$

$$\cup \{f \in L_p \mid f \text{ имеет одну непосред. переменную, и } \forall \frac{u}{v} \in U(f) \cap p\mathbb{Z}_{(p)}, (u, v) = 1 :$$

$$(u, q) = q, \forall \frac{u}{v} \in U(f), \frac{u}{v} \notin p\mathbb{Z}_{(p)}, (u, v) = 1 : (v, q) = 1\}, \quad q - \text{простое, } q \neq p.$$

Лемма 3. *Классы T_a ($a \in E_p$), V_1 , V_o , I , а также $R_c(q)$ и $R_d(q)$ для всех простых $q \neq p$ являются попарно различными замкнутыми классами в L_p .*

Доказательство. Доказательство замкнутости может быть проведено аналогично 2-адическому случаю [1]. Доказательство попарной взаимной неэквивалентности также аналогично 2-адическому случаю. $\square$

3. Теорема о полноте для линейных p -адических автоматов

3.1. Случай однородных функций

Положим

$$J_p^0 = \{V_o \cap L_p^0, V_1 \cap L_p^0, I \cap L_p^0\} \cup \{R_c(\pi) \cap L_p^0, R_d(\pi) \cap L_p^0 \mid \pi \neq p - \text{простое}\}.$$

Далее нам понадобится теорема Коши-Дэвенпорта:

Теорема 1 (Дэвенпорт, [6]). Пусть p — простое число, а A, B — непустые подмножества поля $\mathbb{F}_p$. Тогда

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Лемма 4. Пусть

$$M \subseteq L_p^0, \quad M \not\subseteq V_1, \quad M \not\subseteq V_0.$$

Тогда

$$0 \in K(M).$$

Доказательство. Так как $M \not\subseteq V_0$, по определению, найдётся функция

$$g(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i \in M$$

такая, что

$$\sum_{i=1}^n \bar{r}_i \neq 1.$$

Отождествим все переменные функции g и получим одноместную однородную функцию $g_1(x) = qx$.

Если $\bar{q} = 0$, то $q \in p\mathbb{Z}_{(p)}$. Следовательно, к переменной x функции qx применима обратная связь. Так как свободный член функции qx равен нулю, получаем

$$\text{Fb}_x(qx) = \frac{0}{1 - q} = 0 \implies 0 \in K(M).$$

Остаётся рассмотреть случай $\bar{q} \neq 0$, $\bar{q} \neq 1$.

Так как $M \not\subseteq V_1$, существует функция

$$h(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i \in M$$

имеющая не менее двух непосредственных переменных. Перенумеруем переменные функции h так, чтобы $x_1, \dots, x_m$ были непосредственными, где $m \geq 2$. Тогда

$$h(x_1, \dots, x_n) = \sum_{i=1}^m a_i x_i + p \sum_{i=m+1}^n b_i x_i, \quad \bar{a}_i \neq 0.$$

Положим

$$S = \sum_{i=1}^m \overline{a_i}.$$

Если $S = 0$, положим

$$\alpha = a_1, \quad \beta = \sum_{i=2}^m a_i + p \sum_{i=m+1}^n b_i.$$

Тогда

$$\overline{\alpha} = \overline{a_1} \neq 0, \quad \overline{\beta} = S - \overline{a_1} = -\overline{a_1} \neq 0.$$

Пусть теперь $S \neq 0$. Если существует $j \in \{1, \dots, m\}$ такой, что

$$\overline{a_j} \neq S,$$

то положим

$$\alpha = a_j, \quad \beta = \sum_{\substack{i=1 \\ i \neq j}}^m a_i + p \sum_{i=m+1}^n b_i.$$

В этом случае

$$\overline{\alpha} = \overline{a_j} \neq 0, \quad \overline{\beta} = S - \overline{a_j} \neq 0.$$

Остаётся случай, когда

$$\overline{a_j} = S \quad \text{для всех } j \in \{1, \dots, m\}.$$

Тогда

$$S = \sum_{i=1}^m \overline{a_i} = mS.$$

Поскольку $S \neq 0$, имеем

$$m \equiv 1 \pmod{p}.$$

Следовательно, $m \geq p + 1$. Положим

$$\alpha = a_1 + a_2, \quad \beta = \sum_{i=3}^m a_i + p \sum_{i=m+1}^n b_i.$$

Так как в рассматриваемом случае $p > 2$, получаем

$$\overline{\alpha} = 2S \neq 0, \quad \overline{\beta} = (m - 2)S = -S \neq 0.$$

Таким образом, соответствующим отождествлением переменных функции h получаем

$$B(x, y) = \alpha x + \beta y \in K(M), \quad \bar{\alpha} \neq 0, \quad \bar{\beta} \neq 0.$$

Теперь рассмотрим множество

$$C = \{\bar{c} \in \mathbb{F}_p \mid c \in \mathbb{Z}_{(p)}, \quad cx \in K(M)\}.$$

Иными словами, C состоит из остатков коэффициентов при x у одноместных однородных функций, выражимых из M .

Так как $g_1(x) = qx \in K(M)$, имеем $\bar{q} \in C$. Кроме того, подставляя функцию qx в саму себя, получаем $q^2x \in K(M)$, поэтому $\bar{q}^2 \in C$.

Поскольку $\bar{q} \neq 0$ и $\bar{q} \neq 1$, имеем $\bar{q}^2 \neq \bar{q}$. Следовательно, $|C| \geq 2$.

Предположим, что $|C| < p$. Поскольку $B(x, y) \in K(M)$, множество C удовлетворяет включению

$$\bar{\alpha}C + \bar{\beta}C \subseteq C.$$

Так как $\bar{\alpha} \neq 0$, $\bar{\beta} \neq 0$, умножение на $\bar{\alpha}$ и $\bar{\beta}$ является биекцией поля $\mathbb{F}_p$. Поэтому

$$|\bar{\alpha}C| = |C|, \quad |\bar{\beta}C| = |C|.$$

По теореме Коши–Дэвенпорта имеем

$$|\bar{\alpha}C + \bar{\beta}C| \geq \min\{p, 2|C| - 1\}.$$

Если $2|C| - 1 \leq p$, то $|\bar{\alpha}C + \bar{\beta}C| \geq 2|C| - 1 > |C|$ (так как $|C| > 1$).

Если $2|C| - 1 \geq p$, то $|\bar{\alpha}C + \bar{\beta}C| \geq p > |C|$ (по предположению).

Таким образом, имеем $|\bar{\alpha}C + \bar{\beta}C| > |C|$. С другой стороны, из включения $\bar{\alpha}C + \bar{\beta}C \subseteq C$ следует $|\bar{\alpha}C + \bar{\beta}C| \leq |C|$. Пришли к противоречию. Следовательно, $|C| = p$ и, в частности, $0 \in C$.

Значит, существует функция $sx \in K(M)$ такая, что $\bar{c} = 0$, то есть $c \in p\mathbb{Z}_{(p)}$. К переменной x функции sx применима обратная связь, и, поскольку функция однородна, получаем $\text{Fb}_x(cx) = 0$. Следовательно,

$$0 \in K(M).$$

Лемма доказана. □

Следующие четыре леммы описывают основные этапы доказательства теоремы о полноте. Их доказательство полностью аналогично 2-адическому случаю [1].

Лемма 5 (Получение масштабированного сумматора). Пусть

$$M \subseteq L_p^0, \quad 0 \in K(M), \quad M \not\subseteq V_1.$$

Тогда существует число

$$s \in \mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}, \quad s > 0,$$

такое, что

$$sx_1 + sx_2 \in K(M).$$

Лемма 6 (Получение множителя, большего единицы). Пусть

$$M \subseteq L_p^0, \quad 0 \in K(M), \quad M \not\subseteq I.$$

Тогда существует число $r \in \mathbb{Z}_{(p)}$, $r > 1$, такое, что

$$rx \in K(M).$$

Лемма 7 (Получение дробного множителя с простым q в знаменателе).

Пусть $q \neq p$ — простое число. Пусть

$$M \subseteq L_p^0, \quad 0 \in K(M),$$

и пусть для некоторого $s \in \mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}$ выполнено

$$sx_1 + sx_2 \in K(M).$$

Если $M \not\subseteq R_c(q)$ и $M \not\subseteq R_d(q)$, то существует число $\rho_q \in \mathbb{Z}_{(p)}$ такое, что

$$v_q(\rho_q) < 0 \quad \text{и} \quad \rho_q x \in K(M).$$

Лемма 8 (Переход от масштабированного сумматора к точному сумматору). Пусть

$$M \subseteq L_p^0, \quad 0 \in K(M).$$

Предположим, что в $K(M)$ содержатся функции

$$sx_1 + sx_2, \quad rx,$$

где

$$s, r \in \mathbb{Z}_{(p)}, \quad s \notin p\mathbb{Z}_{(p)}, \quad s > 0, \quad r > 1.$$

Пусть для каждого простого $q \neq p$, делящего числитель числа s в несократимой записи, в $K(M)$ содержится функция $\rho_q x$ со свойством $v_q(\rho_q) < 0$. Тогда

$$x_1 + x_2 \in K(M).$$

Теорема 2 (Теорема полноты для однородных линейных p -адических автоматов). Пусть

$$M \subseteq L_p^0.$$

Если для каждого класса $\Theta \in J_p^0$ выполняется $M \not\subseteq \Theta$, тогда

$$K(M) = L_p^0.$$

Доказательство. По условию $M \not\subseteq V_1, M \not\subseteq V_0$. По лемме о получении нуля имеем $0 \in K(M)$.

Так как $M \not\subseteq V_1$, по лемме о масштабированном сумматоре существует $s \notin p\mathbb{Z}_{(p)}, s > 0$, такое, что $sx_1 + sx_2 \in K(M)$.

Так как $M \not\subseteq I$, по лемме о функции вне I существует $r \in \mathbb{Z}_{(p)}, r > 1$, такое, что $rx \in K(M)$.

Запишем

$$s = \frac{u}{v}, \quad (u, v) = 1, \quad u > 0, \quad v > 0.$$

Пусть $q_1, \dots, q_m$ — все простые делители числителя u . Так как $s \notin p\mathbb{Z}_{(p)}$, ни один из этих простых не равен p . Для каждого q_j из условия теоремы имеем

$$M \not\subseteq R_c(q_j), \quad M \not\subseteq R_d(q_j).$$

По лемме о дробном множителе получаем

$$\rho_{q_j}x \in K(M), \quad v_{q_j}(\rho_{q_j}) < 0.$$

Теперь применяем лемму о переходе от масштабированного сумматора к точному. Получаем $x_1 + x_2 \in K(M)$. Следовательно, вспоминая доказательство, что $K(\{x_1 + x_2, 1\}) = L_p$:

$$L_p^0 \subseteq K(M).$$

Обратное включение очевидно, поскольку класс L_p^0 замкнут относительно операций композиции.

Следовательно,

$$K(M) = L_p^0.$$

□

Так как все классы из J_p^0 являются собственными несовпадающими замкнутыми подклассами (лемма 3), обратное условие также верно: из полноты некоторой системы M следует ее невключение во все классы из J_p^0 . Следовательно, J_p^0 является критериальной системой предполных классов.

3.2. Неоднородный вариант

Положим

$$J_p = \{T_a \mid a \in E_p\} \cup \{V_o, V_1, I\} \cup \{R_c(\pi), R_d(\pi) \mid \pi \neq p - \text{простое}\}.$$

Теорема 3 (Теорема полноты для линейных p -адических автоматов). Пусть $M \subseteq L_p$. Если для каждого класса $\Theta \in J_p$ выполнено $M \not\subseteq \Theta$, то

$$K(M) = L_p.$$

Доказательство. Для функции

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0$$

обозначим через f^0 её однородную часть. Положим

$$M^0 = \{f^0 \mid f \in M\} \subseteq L_p^0.$$

Из условия $M \not\subseteq \theta$ для каждого $\theta \in J_p$ следует, что $M^0 \not\subseteq \theta_0$ для каждого $\theta_0 \in J_p^0$. Следовательно, выполнены условия теоремы о полноте в однородном случае и

$$K(M^0) = L_p^0.$$

Для любой однородной функции $h \in L_p^0$ существует функция $\tilde{h} \in K(M)$ такая, что $\tilde{h}^0 = h$. Иначе говоря, $\tilde{h}$ имеет вид $\tilde{h} = h + c_h$ с некоторым $c_h \in \mathbb{Z}_{(p)}$.

В частности, множество констант, выражимых из M , непусто. Обозначим его через

$$C = \{c \in \mathbb{Z}_{(p)} \mid c \text{ как константная функция принадлежит } K(M)\}.$$

Непустота C следует из только что доказанного утверждения при $h = 0$.

Покажем, что

$$C = \mathbb{Z}_{(p)}.$$

По доказанному утверждению, применённому к однородной функции $h(x_1, x_2) = x_1 - x_2$, найдётся функция

$$D(x_1, x_2) = x_1 - x_2 + d \in K(M)$$

с некоторым $d \in \mathbb{Z}_{(p)}$. Выберем любую константу $c \in C$. Тогда $D(c, c) = d$, откуда $d \in C$.

Рассмотрим множество

$$G = C - d = \{c - d \mid c \in C\}.$$

Докажем, что G является идеалом кольца $\mathbb{Z}_{(p)}$.

Так как $d \in C$, то $0 = d - d \in G$. Пусть

$$u = c_1 - d, \quad v = c_2 - d,$$

где $c_1, c_2 \in C$. Тогда

$$D(c_1, c_2) = c_1 - c_2 + d \in C.$$

Следовательно,

$$u - v = c_1 - c_2 = (c_1 - c_2 + d) - d \in G.$$

Значит, G является аддитивной подгруппой кольца $\mathbb{Z}_{(p)}$.

Теперь пусть $r \in \mathbb{Z}_{(p)}$. По доказанному выше утверждению, примененному к однородной функции rx , найдется функция

$$A_r(x) = rx + a_r \in K(M)$$

с некоторым $a_r \in \mathbb{Z}_{(p)}$. Если $c \in C$, то

$$A_r(c) \in C, \quad A_r(d) \in C.$$

Поскольку разность любых двух элементов из C принадлежит G , имеем

$$A_r(c) - A_r(d) = r(c - d) \in G.$$

Следовательно,

$$rG \subseteq G \quad \text{для всех } r \in \mathbb{Z}_{(p)}.$$

Итак, G является идеалом кольца $\mathbb{Z}_{(p)}$.

Предположим, что $G \subseteq p\mathbb{Z}_{(p)}$. Тогда все элементы множества $C = d + G$ имеют один и тот же остаток по модулю p . Обозначим этот остаток через $a \in \mathbb{F}_p$. Тогда $C \subseteq a + p\mathbb{Z}_{(p)}$.

Возьмем произвольную функцию $f \in M$ и произвольную константу $c \in C$. Так как $f \in M \subseteq K(M)$ и $c \in C$, то после подстановки c во все переменные получаем константу $f(c, \dots, c) \in C$. Следовательно, $c \equiv a \pmod{p}$ и $f(c, \dots, c) \equiv a \pmod{p}$. Но $f(c, \dots, c) = r_0 + c \sum_{i=1}^n r_i$. Поэтому $r_0 + a \sum_{i=1}^n r_i \equiv a \pmod{p}$, то есть $r_0 + a (\sum_{i=1}^n r_i - 1) \equiv 0 \pmod{p}$. Это в точности означает, что $f \in T_a$. Так как $f \in M$ было выбрано произвольно, получаем $M \subseteq T_a$, что противоречит условию теоремы.

Следовательно,

$$G \not\subseteq p\mathbb{Z}_{(p)}.$$

Значит, G содержит элемент $g \notin p\mathbb{Z}_{(p)}$. Такой элемент обратим в кольце $\mathbb{Z}_{(p)}$. Поскольку G является идеалом, содержащим обратимый элемент, получаем

$$G = \mathbb{Z}_{(p)}.$$

Отсюда

$$C = d + G = \mathbb{Z}_{(p)}.$$

Таким образом, все константы из $\mathbb{Z}_{(p)}$ принадлежат $K(M)$. В частности,

$$1 \in K(M).$$

Осталось получить сумматор $x_1 + x_2$. По доказанному выше утверждению, примененному к однородной функции

$$x_1 + x_2 + x_3,$$

существует функция

$$S(x_1, x_2, x_3) = x_1 + x_2 + x_3 + s \in K(M)$$

с некоторым $s \in \mathbb{Z}_{(p)}$. Так как уже доказано, что все константы принадлежат $K(M)$, имеем

$$-s \in K(M).$$

Подставляя константу $-s$ вместо переменной x_3 , получаем

$$S(x_1, x_2, -s) = x_1 + x_2.$$

Следовательно,

$$x_1 + x_2 \in K(M).$$

Итак,

$$x_1 + x_2 \in K(M), \quad 1 \in K(M).$$

По лемме о порождении класса L_p сумматором и константой 1 имеем окончательно

$$K(M) = L_p.$$

□

Так как все классы из J_p являются собственными несовпадающими замкнутыми подклассами (лемма 3), обратное условие также верно: из полноты некоторой системы M следует ее невключение во все классы из J_p . Следовательно, J_p является критериальной системой предполных классов.

4. Континуальная цепочка замкнутых классов I_α

В этом разделе будет построена нетривиальная цепочка вложенных замкнутых подклассов L_p , имеющая мощность континуума.

Для удобства введем следующее обозначение: для автомата

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0$$

положим

$$\|f\| = \sum_{i=1}^n |r_i|.$$

Для каждого $\alpha \in (0, 1]$ определим класс

$$I_\alpha = \{f \in L_p \mid \|f\| \leq \alpha\}.$$

Отметим, что свободный член r_0 в определении класса I_α не участвует. Очевидно, что I_1 совпадает с ранее определённым классом I .

Теорема 4. *Для любого $\alpha \in (0, 1]$ класс I_α является K -замкнутым:*

$$K(I_\alpha) = I_\alpha.$$

Доказательство. Достаточно проверить, что класс I_α сохраняется при всех операциях композиции.

Пусть

$$f(x_1, \dots, x_n) = \sum_{i=1}^n r_i x_i + r_0, \quad g(y_1, \dots, y_m) = \sum_{j=1}^m s_j y_j + s_0$$

и $f, g \in I_\alpha$.

Переименование переменных не меняет коэффициенты при переменных, поэтому не меняет величину $\|f\|$.

Рассмотрим отождествление переменных. Если в автомате f отождествляются переменные x_{n-1} и x_n , то новый коэффициент при полученной переменной равен $r_{n-1} + r_n$. Поэтому по неравенству треугольника имеем

$$\sum_{i=1}^{n-2} |r_i| + |r_{n-1} + r_n| \leq \sum_{i=1}^n |r_i| = \|f\| \leq \alpha.$$

Следовательно, результат отождествления снова принадлежит I_α .

Рассмотрим подстановку. Подставим f вместо переменной y_m автомата g . Тогда коэффициенты при переменных автомата f умножаются на

s_m , а остальные коэффициенты автомата g сохраняются. Поэтому для результата h имеем

$$\|h\| = \sum_{j=1}^{m-1} |s_j| + |s_m| \sum_{i=1}^n |r_i| = \|g\| - |s_m| + |s_m| \|f\|.$$

Так как $f \in I_\alpha$ и $\alpha \leq 1$, то

$$\|f\| \leq \alpha \leq 1.$$

Следовательно,

$$\|h\| = \|g\| - |s_m| + |s_m| \|f\| \leq \|g\| \leq \alpha.$$

Значит, результат подстановки также лежит в I_α .

Осталось проверить обратную связь. Пусть обратная связь применяется к переменной x_n автомата f . Результат обратной связи имеет вид

$$f_{\text{fb}}(x_1, \dots, x_{n-1}) = \sum_{i=1}^{n-1} \frac{r_i}{1 - r_n} x_i + \frac{r_0}{1 - r_n}.$$

Положим

$$A = \sum_{i=1}^{n-1} |r_i|, \quad B = |r_n| \quad \implies \quad A + B \leq \alpha \leq 1.$$

Поскольку обратная связь применима к x_n , имеем

$$r_n \in p\mathbb{Z}_{(p)}.$$

Если бы $B = |r_n| = 1$, то рациональное число r_n было бы равно 1 или -1 , что невозможно для элемента $p\mathbb{Z}_{(p)}$. Поэтому $B < 1$, и

$$|1 - r_n| \geq 1 - |r_n| = 1 - B > 0.$$

Поэтому

$$\|f_{\text{fb}}\| = \sum_{i=1}^{n-1} \left| \frac{r_i}{1 - r_n} \right| \leq \frac{A}{1 - B}.$$

Из $A + B \leq \alpha$ получаем $A \leq \alpha - B$. Значит,

$$\|f_{\text{fb}}\| \leq \frac{\alpha - B}{1 - B}.$$

Так как $\alpha \leq 1$, выполнено

$$\frac{\alpha - B}{1 - B} \leq \alpha.$$

Следовательно,

$$\|f_{\text{ГБ}}\| \leq \alpha,$$

что и требовалось.

Итак, класс I_α сохраняется при переименовании переменных, отождествлении переменных, подстановке и обратной связи. Поэтому $K(I_\alpha) \subseteq I_\alpha$. Обратное же включение следует из определения замыкания. Следовательно,

$$K(I_\alpha) = I_\alpha.$$

Теорема доказана. □

Теорема 5. Если $0 < \alpha < \beta \leq 1$, то

$$I_\alpha \subsetneq I_\beta.$$

Доказательство. Нестрогое включение непосредственно следует из определения. Если $f \in I_\alpha$, то $\|f\| \leq \alpha < \beta$, следовательно, $\|f\| \leq \beta$, и потому $f \in I_\beta$. Значит,

$$I_\alpha \subseteq I_\beta.$$

Докажем строгость включения. Выберем натуральное число N , не делящееся на p , настолько большим, что

$$\frac{1}{N} < \beta - \alpha.$$

Тогда для некоторого $m \in \mathbb{Z}$ выполнено

$$\alpha < \frac{m}{N} < \beta.$$

Положим $r = m/N$. Поскольку $p \nmid N$, имеем $r \in \mathbb{Z}_{(p)}$.

Рассмотрим функцию

$$f_r(x) = rx.$$

Тогда

$$\|f_r\| = |r| = r,$$

поэтому $f_r \in I_\beta \setminus I_\alpha$. Следовательно,

$$I_\alpha \subsetneq I_\beta.$$

Теорема доказана. □

Следствие 1. Семейство

$$\{I_\alpha \mid \alpha \in (0, 1]\}$$

образует строго возрастающую цепочку K -замкнутых классов:

$$\alpha < \beta \implies I_\alpha \subsetneq I_\beta.$$

В частности, множество попарно различных классов этой цепочки имеет мощность континуума.

Заключение

В работе исследована проблема K -полноты в классе линейных p -адических автоматов для нечётного простого числа p . Получены критерии полноты для однородных и неоднородных линейных p -адических функций. Полученные результаты обобщают известные свойства линейных 2-адических автоматов на случай произвольного нечётного простого основания. Кроме того, построена континуальная строго возрастающая цепочка K -замкнутых классов I_α , $\alpha \in (0, 1]$.

Автор выражает благодарность профессору А. А. Часовских за помощь в постановке задачи и содействие в подготовке статьи.

Список литературы

- [1] А. А. Часовских, “О полноте в классе линейных 2-адических автоматов”, *Интеллектуальные системы. Теория и приложения*, **20**:4 (2016), 209–227.
- [2] А. А. Часовских, “Об алгоритмической разрешимости проблемы полноты для линейных автоматов”, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 1986, № 3, 82–84.
- [3] А. А. Часовских, “Проблема полноты для класса линейно-автоматных функций”, *Дискрет. матем.*, **27**:2 (2015), 134–151. DOI: 10.4213/dm1330; *Discrete Math. Appl.*, **26**:2 (2016), 89–104. DOI: 10.1515/dma-2016-0007.
- [4] А. А. Часовских, “Проблема полноты в классах линейных автоматов”, *Интеллектуальные системы. Теория и приложения*, **22**:2 (2018), 151–153.
- [5] А. Г. Лунц, “Конечные p -адические автоматы”, *Докл. АН СССР*, **150**:4 (1963), 755–758.
- [6] Г. Дэвенпорт, “О сложении классов вычетов”, *УМН*, 1940, № 7, 90–92.

Статья поступила 28 августа 2026 г.

The completeness problem in the class of linear p -adic automata

М. Е. Kalashnikov

The K -completeness problem in the class of linear p -adic automata is studied for an odd prime p . Completeness criteria are obtained for homogeneous and inhomogeneous linear p -adic functions. The results generalize known results for linear 2-adic automata to arbitrary odd prime bases. In addition, a strictly increasing chain of K -closed classes I_α , $\alpha \in (0, 1]$, of continuum cardinality is constructed.

Keywords: finite automaton, p -adic number, linear p -adic automaton, composition operations, feedback, completeness problem, closed class.

References

- [1] A. A. Chasovskikh, “Completeness in the class of linear 2-adic automata”, *Intelligent Systems. Theory and Applications*, **20**:4 (2016), 209–227 (In Russian).
- [2] A. A. Chasovskikh, “On the algorithmic decidability of the completeness problem for linear automata”, *Vestn. Mosk. Univ. Ser. 1. Mat. Mekh.*, 1986, № 3, 82–84 (In Russian).
- [3] A. A. Chasovskikh, “Completeness problem for the class of linear automata functions”, *Diskr. Mat.*, **27**:2 (2015), 134–151. DOI: 10.4213/dm1330; *Discrete Math. Appl.*, **26**:2 (2016), 89–104. DOI: 10.1515/dma-2016-0007 (In Russian).
- [4] A. A. Chasovskikh, “The problem of completeness in the class of linear automata”, *Intelligent Systems. Theory and Applications*, **22**:2 (2018), 151–153 (In Russian).
- [5] A. G. Lunts, “Finite p -adic automata”, *Dokl. Akad. Nauk SSSR*, **150**:4 (1963), 755–758 (In Russian).
- [6] H. Davenport, “On the addition of residue classes”, *Uspekhi Mat. Nauk*, 1940, № 7, 90–92 (In Russian).

Received on August 28, 2026