Math-Net.Ru

Общероссийский математический портал

Т. И. Смышляева, Критерий ограниченной детерминированности функций, задаваемых автоматами, *Дискрет. матем.*, 2013, том 25, выпуск 2, 121–134

DOI: <https://doi.org/10.4213/dm1240>

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: 3.85.7.115

26 апреля 2023 г., 17:28:05

Критерий ограниченной детерминированности функций, задаваемых автоматами

© 2013 г. Т. И. Смышляева

В работе установлен критерий конечности числа состояний автомата, задающего детерминированную функцию. Критерий сформулирован в терминах формальных степенных рядов.

Работа поддержана Российским фондом фундаментальных исследований (номер проекта 12-01-00680-а).

1. Введение

Целью данной работы является нахождение необходимого и достаточного условия, при котором детерминированная функция является ограниченно-детерминированной, т. е. задаётся автоматом с конечным числом состояний (см. [9]). Функции, задаваемые автоматами, или детерминированные функции, являются непрерывными в p -адической метрике (см. [1]).

Свойства детерминированных функций как непрерывных в p -адической метрике преобразований изучались с помощью различных инструментов p -адического анализа, рядов Малера, ван дер Пута (см. [5]), а также формальных степенных рядов (см. [7]).

Одним из первых математический аппарат p -адических чисел к теории автоматов применил А.Е. Лунц в работе [8]. Связь p -адических функций с автоматными, возможность использования p -адических методов для исследования автоматов подробно описана в статье В.С. Анашина [3]. Критерий конечности автоматов в данной метрике был получен В.С. Анашиным, его доказательство представлено в терминах рядов Ван дер Пута в работе [2]. Формулировка критерия конечности автоматов для $p = 2$ в терминах формальных степенных рядов была представлена Вюйеменом в [7], но, к сожалению, работа содержала неточности. В данной статье критерий Вюйемена обобщается на случай любого простого p . Использование этого критерия удобно в случае, когда функция представлена в так называемом «координатном» виде, который определяется далее в работе.

2. Определения и предварительные результаты

Если входной и выходной алфавиты автомата $\mathcal{A}$ имеют мощность p , то входную и выходную последовательности можно рассматривать как бесконечные слова, кото-

рые можно ассоциировать с целыми p -адическими числами, где p — простое число.

Целое p -адическое число a можно представить в каноническом виде:

$$a = \dots a_i a_{i-1} \dots a_1 a_0 = \sum_{i=0}^{\infty} a_i \cdot p^i,$$

где $a_i \in \{0, 1, \dots, p-1\}$, $i = 0, 1, 2, \dots$

Операции сложения и вычитания для p -адических чисел, представленных в каноническом виде, задаются теми же алгоритмами, что и для чисел, представленных в системе счисления с основанием p . Относительно заданных таким образом операций целые p -адические числа образуют кольцо, которое обозначается $\mathbb{Z}_p$. С математическим строгим определением p -адических чисел можно ознакомиться по любой монографии, посвященной p -адическому анализу, см., например, [5].

На кольце целых p -адических чисел можно задать метрику следующим образом: расстояние $d_p(a, b) = |a - b|_p$ между целыми p -адическими числами a и b , представленными в виде бесконечных строк, полагается равным $\frac{1}{p^i}$ тогда и только тогда, когда

$$\begin{aligned} a &= \dots a_{i+1} a_i c_{i-1} \dots c_1 c_0; \\ b &= \dots b_{i+1} b_i c_{i-1} \dots c_1 c_0; \end{aligned}$$

причем если бесконечные строки совпадают, то расстояние $d_p(a, b)$ полагается равным 0.

Функции, заданные и принимающие значения на пространстве целых p -адических чисел и удовлетворяющие условию Липшица с константой 1 относительно введенной метрики, называются *совместимыми*, см., например, [1].

Теперь напомним определение автомата Мили:

по определению автоматом называется кортеж $\mathfrak{A} = \langle J, S, O, S, O, s_0 \rangle$, где J — входной алфавит; O — выходной алфавит, S — множество состояний; $O : J \times S \rightarrow O$ — функция выхода; $S : J \times S \rightarrow O$ — функция перехода; $s_0 \in S$ — начальное состояние. Автомат преобразует (бесконечное) входное слово $\dots, w_2, w_1, w_0$ в (бесконечное) выходное слово $\dots, z_2, z_1, z_0$, при этом он переходит из состояния $s_i \in S$ в состояние $s_{i+1} \in S$. В начальный момент времени автомат $\mathfrak{A}$ находится в состоянии s_0 .

Таким образом, выходной символ z_i может зависеть только от входных символов $w_0, w_1, \dots, w_i$: $z_i = \psi_i(w_0, \dots, w_i) \in O$.

Далее будем считать, что $J = O = \{0, 1, \dots, p-1\}$, где p — простое число. Каждый автомат $\mathfrak{A}$, преобразуя целое p -адическое число, соответствующее входной последовательности $\omega_0, \omega_1, \dots$, в целое p -адическое число, соответствующее выходной последовательности $z_0 = \psi_0(\omega_0), z_1 = \psi_1(\omega_0, \omega_1), \dots, z_i = \psi_i(\omega_0, \omega_1, \dots, \omega_i), \dots$, задает тем

самым функцию на кольце целых p -адических чисел, значениями которой также являются целые p -адические числа. Эта функция называется детерминированной функцией, соответствующей автомату $\mathfrak{A}$, или автоматной функцией:

$$f_{\mathfrak{A}} : \omega_0 + \omega_1 \cdot p + \omega_2 \cdot p^2 + \dots \mapsto z_0 + z_1 \cdot p + z_2 \cdot p^2 + \dots$$

Поскольку $z_i = \psi_i(\omega_0, \omega_1, \dots, \omega_i)$, $i = 0, 1, 2, \dots$, постольку преобразование $f_{\mathfrak{A}}$ удовлетворяет p -адическому условию Липшица с константой 1. Обратно, каждое такое преобразование f пространства бесконечных слов может быть задано с помощью некоторого автомата $\mathfrak{A} : f = f_{\mathfrak{A}}$ (см. [3]). Таким образом, класс всех детерминированных функций (при фиксированном p) совпадает с классом всех функций, удовлетворяющих p -адическому условию Липшица с константой 1.

В дальнейшем мы будем использовать тот факт, что p -адическая функция, удовлетворяющая условию Липшица с константой 1 (совместимая), представима в виде суммы

$$f(x) = \sum_{i=0}^{\infty} f_i(x_i, x_{i-1}, \dots, x_0) p^i,$$

где $f_i(x_i, x_{i-1}, \dots, x_0) \in \{0, 1, \dots, p-1\}$, $i = 0, 1, 2, \dots$, — функции, называемые *координатными*.

Кроме представления бесконечных последовательностей в виде целых p -адических чисел, эти последовательности можно представлять также в виде формальных степенных рядов. Именно, последовательности $a = \dots a_i a_{i-1} \dots a_1 a_0$, $a_i \in \{0, 1, \dots, p-1\}$, $i \geq 0$, можно сопоставить формальный степенной ряд $\sum_{i=0}^{\infty} a_i \cdot X^i$, являющийся элементом кольца $\mathbb{F}_p[[X]]$:

$$\mathbb{F}_p[[X]] = \left\{ \sum_{0 \leq i < \infty} \alpha_n X^n, \alpha_n \in \mathbb{F}_p \right\},$$

на котором операции сложения и умножения определяются как для степенных рядов.

Таким образом, между p -адическими числами и формальными степенными рядами есть взаимно однозначное соответствие, а на входное слово автомата $\mathfrak{A}$ можно смотреть как на p -адическое число, так и как на формальный степенной ряд.

3. Основные результаты

Детерминированная функция $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ полностью определяется своими значениями на конечных входных словах. Упорядочив эти слова лексикографически и выписав соответствующую последовательность значений функции, мы получим последовательность, которую будем обозначать $\text{truth}(f)$. Более формально эта последовательность определяется следующим образом.

Определение 1. Последовательность $\{z_n\}$ для совместимой функции $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ называется *последовательностью значений* $\text{truth}(f)$ если $z_n = f_i(x_i, x_{i-1}, \dots, x_0)$, где $i = \lfloor \log_p((p-1)n + p) \rfloor - 1$, $\sum_{k=0}^i x_k p^k = n - \sum_{k=1}^i p^k$.

Для дальнейшего изложения нам потребуется понятие p -автоматной последовательности, см., например, [4]. Последовательность $\{z_i\}$ над $\{0, 1, \dots, p-1\}$ называется p -автоматной, если существует такой конечный автомат с входным и выходным алфавитами $\{0, 1, \dots, p-1\}$, что, получая на вход слово, соответствующее представлению числа n в системе с основанием p , на выход он выдает слово, последняя буква которого есть n -й элемент последовательности $\{z_n\}$.

Определение 2. Для совместимой функции $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ определим последовательность $\{a_n\} = \text{auto}(f)$ следующим образом: $a_n = f_j(x_j, x_{j-1}, \dots, x_0)$, где $j = \lfloor \log_p n \rfloor$, $\sum_{k=0}^j x_k p^k = n$.

Пример:

Для $p = 3$ эти последовательности выглядят следующим образом:

z_n	$\text{truth}(f)$	a_n	$\text{auto}(f)$
z_0	$f_0(0)$	a_0	$f_0(0)$
z_1	$f_0(1)$	a_1	$f_0(1)$
z_2	$f_0(2)$	a_2	$f_0(2)$
z_3	$f_1(00)$	a_3	$f_1(10)$
z_4	$f_1(01)$	a_4	$f_1(11)$
z_5	$f_1(02)$	a_5	$f_1(12)$
$\dots$	$\dots$	$\dots$	$\dots$

Следующее определение p -автоматной последовательности, приведенное в работе [4], эквивалентно определению, данному нами выше.

Определение 3. Последовательность $\{a_n\}$ называется p -автоматной, если существует такая функция $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, реализуемая конечным автоматом, что $\{a_n\} = \text{auto}(f)$.

Напомним определение p -алгебраичной последовательности, приведенное в работе [2].

Определение 4. Назовем последовательность $\{b_n\}$, где $b_n \in \mathbb{F}_p$, p -алгебраичной, если ряд $b(X) = \sum_{n=0}^{\infty} b_n X^n$ алгебраичен над $\mathbb{F}_p[X]$, т.е. существуют такие $l \in \mathbb{N}$ и ненулевые полиномы $u_0(X), \dots, u_l(X) \in \mathbb{F}_p[X]$, что выполняется равенство

$$u_0(X) + u_1(X)b(X) + \dots + u_l(X)(b(X))^l = 0.$$

Понятия p -автоматности и p -алгебраичности являются эквивалентными, что отражает теорема Кристола.

Теорема 1 ([4]). Пусть существует непустое конечное множество $\Delta = \{0, 1, \dots, p-1\}$, p — простое число. Последовательность $\{a_i\}$, $a_i \in \Delta$, $i \geq 0$, является p -автоматной тогда и только тогда, когда существуют такие $n > 0$ и инъективное отображение $\beta: \Delta \rightarrow \mathbb{F}_{p^n}$, что формальный степенной ряд $\sum_{i \geq 0} \beta(a_i) X^i$ алгебраичен над $\mathbb{F}_{p^n}[X]$.

Очевидно, что по последовательности $\text{truth}(f)$ можно однозначно восстановить совместимую функцию f . В терминах этих последовательностей мы можем сформулировать критерий ограниченной детерминированности функций — основную теорему данной статьи.

Теорема 2. Пусть функция $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ удовлетворяет условию Липшица с константой 1. Таблица значений $\text{truth}(f)$ p -алгебраична тогда и только тогда, когда функция f может быть задана конечным автоматом.

Для доказательства этого критерия сначала мы сформулируем и докажем утверждения, в которых определяются функции, связывающие последовательности truth и auto . Затем мы докажем вспомогательные леммы, определяющие достаточные условия конечности автоматов, задающих эти функции.

Пусть функция $f(x) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ удовлетворяет условию Липшица с константой 1.

Для $f(x)$ введем совместимую функцию $g^f(x) = \sum_{i=0}^{\infty} g_i^f(x_i, x_{i-1}, \dots, x_0)p^i$, где координатные функции g_i^f определены следующим образом:

$$g_i^f(x_i, \dots, x_0) = \begin{cases} f_i(y_i, \dots, y_0), & \text{где } \sum_{k=0}^i y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k, \\ & \text{если } \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k < p^{i+1}; \\ f_{i+1}(y_{i+1}, y_i, \dots, y_0), & \text{где } \sum_{k=0}^{i+1} y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k, \\ & \text{в противном случае.} \end{cases} \quad (1)$$

Утверждение 1. Пусть $f(x) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ — функция, удовлетворяющая p -адическому условию Липшица с константой 1. Тогда для совместимой функции $g^f(x) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, определяемой в соответствии с системой (1), верно

$$\text{auto}(f) = \text{truth}(g).$$

Доказательство. Пусть $\{z_n\} = \text{truth}(g)$, а $\{a_n\} = \text{auto}(f)$. Покажем, что при любом целом $n \geq 0$ верно $a_n = z_n$.

Пусть в соответствии с определением 1 (определение функции truth)

$$i = \lfloor \log_p((p-1)n + p) \rfloor - 1, \quad (2)$$

наборы $(x_i, \dots, x_1, x_0)$ таковы, что

$$\sum_{k=0}^i x_k p^k = n - \sum_{k=1}^i p^k. \quad (3)$$

Пусть в соответствии с определением 2 (определение функции auto)

$$j = \lfloor \log_p n \rfloor, \quad (4)$$

наборы $(y_j, \dots, y_1, y_0)$ таковы, что

$$\sum_{k=0}^j y_k p^k = n. \quad (5)$$

Покажем, что $g_i^f(x_i, \dots, x_1, x_0) = f_j(y_j, \dots, y_1, y_0)$.

Действительно, если $n = \sum_{k=0}^j y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k < p^{i+1}$, то из равенств (4) и (3) следует, что

$$j = \lfloor \log_p n \rfloor = \lfloor \log_p \left(\sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k \right) \rfloor < \lfloor \log_p (p^{i+1}) \rfloor = i + 1,$$

из равенств (2) и (5) следует, что

$$\begin{aligned} i &= \lfloor \log_p ((p-1)n + p) \rfloor - 1 = \lfloor \log_p ((p-1) \sum_{k=0}^j y_k p^k + p) \rfloor - 1 \leq \\ &\leq \lfloor \log_p ((p-1)(p^{j+1} - 1) + p) \rfloor - 1 = \\ &= \lfloor \log_p (p^{j+2} - p - p^{j+1} + 1 + p) \rfloor - 1 = j + 1 - 1 = j. \end{aligned}$$

Следовательно, $i \leq j < i + 1$, т. е. $j = i$. Это значит, что при $i = j$, таких наборах $x_i, \dots, x_1, x_0, y_j, \dots, y_1, y_0$, что $\sum_{k=0}^j y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k < p^{i+1}$, имеет место равенство

$$g_i^f(x_i, \dots, x_1, x_0) = f_j(y_j, \dots, y_1, y_0).$$

Аналогично рассмотрим случай, когда $n = \sum_{k=0}^j y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k \geq p^{i+1}$.

Так как $j = \lfloor \log_p n \rfloor$, то $j \geq \lfloor \log_p (p^{i+1}) \rfloor = i + 1$. Следовательно, $j \geq i + 1$.

Предположим, что $y_j = 0$, тогда $n = \sum_{k=0}^j y_k p^k < p^j$.

В соответствии с равенством (4) $j = \lfloor \log_p n \rfloor < \lfloor \log_p (p^j) \rfloor < j$.

Следовательно, $y_j \neq 0$ и $n = \sum_{k=0}^j y_k p^k \geq p^j$.

Из равенств (2) и (5) следует, что

$$\begin{aligned} i &= \lfloor \log_p ((p-1)n + p) \rfloor - 1 = \lfloor \log_p ((p-1) \sum_{k=0}^j y_k p^k + p) \rfloor - 1 \geq \lfloor \log_p ((p-1)p^j + p) \rfloor - 1 = \\ &= \lfloor \log_p (p-1)p^{j-1} \rfloor = \lfloor \log_p (p-1) \rfloor + j - 1 = j - 1. \end{aligned}$$

Следовательно, $i + 1 \leq j \leq i + 1$, т. е. $j = i + 1$.

Это значит, что при $j = i + 1$ для таких наборов $x_i, \dots, x_1, x_0, y_j, \dots, y_1, y_0$, что

$$\sum_{k=0}^j y_k p^k = \sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k \geq p^{i+1}, \text{ имеем}$$

$$g_i^f(x_i, \dots, x_1, x_0) = f_j(y_j, \dots, y_1, y_0).$$

Следовательно, для заданной функции $g^f(x)$ выполняется равенство

$$\text{truth}(g^f) = \text{auto}(f).$$

Пример: при $p = 3$ имеем:

n	$\text{auto}(f)$	$\text{truth}(g)$
0	$f_0(0)$	$g_0(0)$
1	$f_0(1)$	$g_0(1)$
2	$f_0(2)$	$g_0(2)$
3	$f_1(10)$	$g_1(00)$
4	$f_1(11)$	$g_1(01)$
5	$f_1(12)$	$g_1(02)$
...	...	...

Для совместимой функции $f(x) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ введем совместимую функцию $h(x) = \sum_{i=0}^{\infty} h_i(x_i, x_{i-1}, \dots, x_0) p^i$, где координатные функции h_i определены следующим образом:

$$h_i(x_i, \dots, x_0) = \begin{cases} f_0(x_0), & \text{если } i = 0, \\ f_0(0), & \text{если } \sum_{k=0}^i x_k p^k < p^i, \\ f_{i-1}(y_{i-1}, \dots, y_0), & \text{где } \sum_{k=0}^{i-1} y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^{i-1} p^k, \\ & \text{если } p^i \leq \sum_{k=0}^i x_k p^k < \sum_{k=1}^i p^k, \\ f_i(y_i, y_{i-1}, \dots, y_0), & \text{где } \sum_{k=0}^i y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^i p^k, \\ & \text{если } \sum_{k=0}^i x_k p^k \geq \sum_{k=1}^i p^k. \end{cases} \quad (6)$$

Утверждение 2. Пусть $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ — функция, удовлетворяющая условию Липшица с константой 1. Тогда для совместимой функции $h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, задаваемой в соответствии с системой (6), верно

$$\text{truth}(f) = \text{auto}(h).$$

Доказательство. Пусть $\{z_n\} = \text{truth}(f)$, $\{a_n\} = \text{auto}(h)$. Покажем, что при любом целом $n \geq 0$ верно $z_n = a_n$.

Пусть в соответствии с определением 1 (определение функции truth),

$$j = \lfloor \log_p((p-1)n + p) \rfloor - 1, \quad (7)$$

наборы $(y_j, \dots, y_1, y_0)$ таковы, что

$$\sum_{k=0}^j y_k p^k = n - \sum_{k=1}^j p^k. \quad (8)$$

Пусть в соответствии с определением 2 (определение функции auto),

$$i = \lfloor \log_p n \rfloor, \quad (9)$$

наборы $(x_i, \dots, x_i, x_0)$ таковы, что

$$\sum_{k=0}^i x_k p^k = n. \quad (10)$$

Покажем, что $h_i(x_i, \dots, x_1, x_0) = f_j(y_j, \dots, y_1, y_0)$

В соответствии с определением функции h рассмотрим три случая.

1. Если $\sum_{k=0}^i x_k p^k < p^i$, то $\lfloor \log_p n \rfloor < \log_p p^i = i$, так как $n = \sum_{k=0}^i x_k p^k$, следовательно, все значения $h_i(x_i, \dots, x_1, x_0)$, кроме $h_0(x_0)$, не удовлетворяют равенству (9) и определению 2 последовательности *auto*, а значит, не входят в нее. Пусть поэтому каждому значению $h_i(x_i, \dots, x_1, x_0)$ соответствует $f_0(0)$. Тогда для всех таких наборов $j = 0$, $y_0 = 0$, следовательно, $h_i(x_i, \dots, x_1, x_0) = f_j(y_j, \dots, y_1, y_0)$.

2. Пусть $p^i \leq \sum_{k=0}^i x_k p^k < \sum_{k=1}^i p^k$.

Из равенств (9) и (8) следует, что

$$\begin{aligned} i = \lfloor \log_p n \rfloor &= \lfloor \log_p \sum_{k=0}^j y_k p^k + \sum_{k=1}^j p^k \rfloor \leq \lfloor \log_p (p^{j+1} + \sum_{k=1}^j p^k) \rfloor = \\ &= \lfloor \log_p \sum_{k=1}^{j+1} p^k \rfloor = j + 1, \\ i &< j + 1. \end{aligned} \quad (11)$$

Из равенств (7) и (10) следует, что

$$j = \lfloor \log_p ((p-1)n + p) \rfloor - 1 = \lfloor \log_p ((p-1) \sum_{k=0}^i x_k p^k + p) \rfloor - 1,$$

$$j + 1 = \lfloor \log_p ((p-1) \sum_{k=0}^i x_k p^k + p) \rfloor = \log_p ((p-1) \sum_{k=0}^i x_k p^k + p) - \alpha,$$

где $\alpha = \log_p ((p-1) \sum_{k=0}^i x_k p^k + p) - \lfloor \log_p ((p-1) \sum_{k=0}^i x_k p^k + p) \rfloor$, $0 \leq \alpha < 1$,

$$p^{j+1} = p^{\log_p ((p-1) \sum_{k=0}^i x_k p^k + p) - \alpha} = p^{-\alpha} ((p-1) \sum_{k=0}^i x_k p^k + p).$$

Так как здесь мы рассматриваем случай, когда $\sum_{k=0}^i x_k p^k < \sum_{k=1}^i p^k$, то

$$\begin{aligned} p^{j+1+\alpha} &= (p-1) \sum_{k=0}^i x_k p^k + p < (p-1) \sum_{k=1}^i p^k + p = p^{i+1}, \\ p &> 1, j + \alpha < i. \end{aligned} \quad (12)$$

Из неравенств (11) и (12) мы получаем, что $i-1 \leq j < i$, следовательно, $j = i-1$.

Значит, для всех таких наборов $(x_i, \dots, x_i, x_0), (y_j, \dots, y_1, y_0)$, что

$$p^i \leq \sum_{k=0}^i x_k p^k < \sum_{k=1}^i p^k, \quad \sum_{k=0}^{i-1} y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^{i-1} p^k$$

выполняется равенство

$$h_i(x_i, \dots, x_1, x_0) = f_{i-1}(y_{i-1}, \dots, y_1, y_0).$$

3. Пусть

$$\sum_{k=0}^i x_k p^k \geq \sum_{k=1}^i p^k. \quad (13)$$

Из равенств (9) и (8) следует, что

$$i = \lfloor \log_p n \rfloor = \lfloor \log_p \sum_{k=0}^j y_k p^k + \sum_{k=1}^j p^k \rfloor \geq \lfloor \log_p \sum_{k=1}^j p^k \rfloor \geq \lfloor \log_p p^j \rfloor = j.$$

Из равенств (7) и (10) следует, что

$$\begin{aligned} j = \lfloor \log_p((p-1)n + p) \rfloor - 1 &= \lfloor \log_p((p-1) \sum_{k=0}^i x_k p^k + p) \rfloor - 1 \geq \\ &\geq \lfloor \log_p((p-1) \sum_{k=1}^i p^k + p) \rfloor - 1 = \lfloor \log_p(p^{i+1}) \rfloor - 1 = i. \end{aligned}$$

Следовательно, $j \leq i \leq j$, т.е. $i = j$.

Значит, для всех таких наборов $(x_i, \dots, x_1, x_0), (y_j, \dots, y_1, y_0)$, что

$$\sum_{k=0}^i x_k p^k \geq \sum_{k=1}^i p^k, \quad \sum_{k=0}^i y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^i p^k,$$

выполняется равенство

$$h_i(x_i, \dots, x_1, x_0) = f_i(y_i, \dots, y_1, y_0).$$

Следовательно, для заданной функции $h(x)$ выполняется равенство $\text{truth}(f) = \text{auto}(h)$.

Пример: при $p = 3$

n	$\text{truth}(f)$	$\text{auto}(h)$
0	$f_0(0)$	$h_0(0)$
1	$f_0(1)$	$h_0(1)$
2	$f_0(2)$	$h_0(2)$
3	$f_1(00)$	$h_1(10)$
4	$f_1(01)$	$h_1(11)$
5	$f_1(02)$	$h_1(12)$

Лемма 1. Пусть функция $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ удовлетворяет условию Липшица с константой 1 и задается конечным автоматом. Тогда совместимая функция $g^f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, задаваемая системой (1), также задается конечным автоматом.

Доказательство. Пусть автомат A_f задает функцию f , автомат A_g^f задает функцию g^f , причем A_f имеет конечное число состояний.

Зафиксируем произвольное натуральное i , $i > 1$. Рассмотрим, при каком значении входа автомата A_g^f будет выполняться условие

$$\sum_{k=0}^i x_k p^k + \sum_{k=1}^i p^k \geq p^{i+1}. \quad (14)$$

Выполнение этого условия означает, что при сложении двух целых p -адических чисел, соответствующих бесконечным последовательностям

$$\begin{array}{cccccccc} \dots & 0 & 0 & x_i & x_{i-1} & x_{i-2} & \dots & x_1 & x_0 \\ \dots & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 \end{array}$$

происходит перенос единицы в $(i+1)$ -й разряд. Очевидно, что это возможно в двух случаях:

- (1) $x_i = p-1$,
- (2) $x_i = p-2$ и существует элемент такой входной последовательности x_j , $0 < j < i$, что $x_j = p-1$ и $x_{j+1} = x_{j+2} = \dots = x_i = p-2$.

Обозначим множество состояний автомата A_{g^f} , для которых каждому значению $g_i^f(x_i, \dots, x_0)$ соответствует $f_i(y_i, \dots, y_0)$, через M_1 , а множество состояний, для которых каждому значению $g_i^f(x_i, \dots, x_0)$ соответствует $f_{i+1}(y_{i+1}, y_i, \dots, y_0)$, через M_2 . Из рассмотренного выше следует, что как только автомат A_{g^f} получает на вход значение $p-1$ (кроме первого такта), он переходит в состояние из множества M_2 . До тех пор, пока на вход поступают значения $p-1$ или $p-2$, он остается в состоянии из этого множества. Как только A_{g^f} получает значение меньше $p-2$, автомат переходит в состояние из множества M_1 и остается в этом множестве до тех пор, пока на вход не поступит $p-1$.

Из того, что M_1 и M_2 — конечные множества, следует, что A_{g^f} является конечным автоматом.

Лемма 2. Пусть функция $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ удовлетворяет условию Липшица с константой 1 и задается конечным автоматом. Тогда совместимая функция $h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, определённая в (6), также задается конечным автоматом.

Доказательство. Исследуем вначале, как зависят значения функции

$$h(x) = \sum_{i=0}^{\infty} h_i(x_i, x_{i-1}, \dots, x_0) p^i \text{ от входных аргументов } x_i, x_{i-1}, \dots, x_0.$$

Рассмотрим неравенство

$$\sum_{k=0}^i x_k p^k < p^i. \quad (15)$$

Если оно выполняется, то $h_i(x_i, x_{i-1}, \dots, x_0)$ принимает значение $f_0(0)$.

Действительно, неравенство (15) выполняется только при $x_i = 0$: если $x_i \geq 0$, то $\sum_{k=0}^i x_k p^k \geq x_i p^i \geq p^i$.

Рассмотрим теперь неравенство

$$p^i \leq \sum_{k=0}^i x_k p^k < \sum_{k=1}^i p^k. \quad (16)$$

Покажем, что если оба неравенства в (16) выполнены, то $h_i(x_i, x_{i-1}, \dots, x_0)$ принимает значение $f_{i-1}(y_{i-1}, \dots, y_0)$, где y_i определяются из равенства $\sum_{k=0}^{i-1} y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^{i-1} p^k$.

Предположим, что $x_i = 0$. Тогда левое из неравенств (16) принимает вид

$$p^i \leq \sum_{k=0}^{i-1} x_k p^k.$$

Даже если оставшиеся коэффициенты x_k принимают максимально возможные значения, $x_k = (p-1)$, $0 \leq k \leq i-1$, то

$$p^i \leq (p-1) \sum_{k=0}^{i-1} p^k = (p-1) \frac{p^i - 1}{p-1} = p^i - 1.$$

Пришли к противоречию, следовательно, $x_i > 0$.

Предположим, что $x_i > 1$. Для суммы $\sum_{k=0}^i x_k p^k$ в этом предположении возьмем минимально возможные значения всех коэффициентов x_k : пусть $x_i = 2$, а всех остальных коэффициенты равны нулю. Тогда правая часть неравенства (16) примет вид

$$\begin{aligned} 2p^i < \sum_{k=1}^i p^k &\Leftrightarrow p^i < p \frac{p^{i-1} - 1}{p-1} \Leftrightarrow p^i - p^{i-1} < p^{i-1} - 1 \Leftrightarrow \\ &\Leftrightarrow p^{i-1}(p-2) + 1 < 0, \end{aligned}$$

но, с учетом того, что $p \geq 2$, неравенство не является верным.

Следовательно, $x_i = 1$. Тогда из выражения (16) получим:

$$x_{i-1} p^{i-1} + x_{i-2} p^{i-2} + \dots + x_1 p + x_0 < p^{i-1} + p^{i-2} + \dots + p. \quad (17)$$

Если $x_{i-1} = 0$, то (17) выполняется; если $x_{i-1} > 1$, то не выполняется. Проводя аналогичные рассуждения, получаем, что для выполнения неравенства (17) необходимо и достаточно, чтобы существовал такой индекс j , $0 < j < i$, что $x_j = 0$, а $x_{j+1} = x_{j+2} = \dots = x_i = 1$.

Если входные аргументы $x_i, x_{i-1}, \dots, x_0$ не удовлетворяют условию для выполнения неравенств (16), (15), то есть $x_i > 0$, и не существует такого x_j , $0 < j < i$, что $x_j = 0$, а $x_{j+1} = x_{j+2} = \dots = x_i = 1$, то выполняется неравенство

$$\sum_{k=0}^i x_k p^k \geq \sum_{k=1}^i p^k. \quad (18)$$

В таком случае $h_i(x_i, x_{i-1}, \dots, x_0)$ принимает значение $f_i(y_i, y_{i-1}, \dots, y_0)$, где y_i принимают значения из равенства $\sum_{k=0}^i y_k p^k = \sum_{k=0}^i x_k p^k - \sum_{k=1}^i p^k$.

Рассмотрим систему (6). Обозначим автомат, реализующий функцию

$$h(x) = \sum_{i=0}^{\infty} h_i(x_i, x_{i-1}, \dots, x_0) p^i, \text{ через } A_h.$$

С помощью полученных соотношений докажем теперь, что автомат A_h имеет конечное число состояний.

Обозначим множество состояний автомата A_h , для которых каждому значению $h_i(x_i, x_{i-1}, \dots, x_0)$ соответствует $f_0(x_i)$, через N_1 , множество состояний, для которых каждому значению $h_i(x_i, x_{i-1}, \dots, x_0)$ соответствует $f_{i-1}(y_{i-1}, \dots, y_0)$, через N_2 , а множество состояний для которых каждому значению $h_i(x_i, x_{i-1}, \dots, x_0)$ соответствует $f_i(y_i, \dots, y_0)$, через N_3 . Состояние, в которое переходит автомат при получении x_0 , обозначим через N_0 , ему соответствует выход $f_0(x_0)$.

Из начального состояния, получив на вход x_0 , автомат A_h переходит в состояние N_0 . Если следующее полученное значение x_1 равно нулю, то выполняется неравенство $x_0 + x_1 p < p$, и A_h переходит в состояние из множества N_1 . Если $x_1 \geq 0$, то выполняется неравенство $x_0 + x_1 p \geq 0$, и автомат переходит в состояние из множества N_3 .

В каком бы состоянии ни находился автомат, при поступлении на вход $x_i = 0$, $i \neq 0$, A_h будет переходить в состояние из множества N_1 , т.к. всегда будет выполняться неравенство (15).

Если A_h находится в состоянии из N_1 , то при поступлении на вход $x_i = 1$, автомат перейдет в состояние из множества N_2 и будет оставаться там до тех пор, пока на вход поступают единицы, так как будет выполняться неравенство (16).

При любом $i \neq 1$, если на вход поступает $x_i > 1$, то выполняется неравенство (18), и автомат переходит в состояние из N_3 .

Если автомат A_h находится в состоянии из множества N_3 , то, пока на вход поступают положительные x_i , будет выполняться неравенство (18), и автомат будет оставаться в состоянии из N_3 .

Так как множества N_0, N_1, N_2, N_3 конечные, то автомат A_h является конечным.

Теперь мы можем завершить доказательство теоремы 2.

Доказательство. Необходимость. Если последовательность $\text{truth}(f)$ p -алгебраична, то по теореме 1 она является также и p -автоматной последовательностью. Т.е. существует такая функция F , реализуемая конечным автоматом, что $\text{truth}(f) = \text{auto}(F)$. Возьмем функцию g^F , построенную в соответствии с системой (1).

По утверждению 1 выполняется равенство

$$\text{truth}(g^F) = \text{auto}(F).$$

Согласно лемме 1, функция $g^F(x)$ задается конечным автоматом. Получаем цепочку равенств:

$$\text{truth}(f) = \text{auto}(F) = \text{truth}(g^F),$$

следовательно, $f(x) = g^F(x)$, соответственно, функция f , как и g^F , задается конечным автоматом.

Достаточность. Пусть f задается автоматом с конечным числом состояний. Возьмем функцию h , определенную в соответствии с системой (6). Из утверждения 2 следует, что

$$\text{truth}(f) = \text{auto}(h).$$

По лемме 2 функция $h(x)$ задается конечным автоматом, следовательно, $\text{truth}(f)$ — p -автоматная последовательность. Также из теоремы 1 видно, что эта последовательность p -алгебраична.

Список литературы

1. Anashin V., Khrennikov A., *Applied Algebraic Dynamics*. Walter de Gruyter, Berlin - New York, 2009.
2. Anashin V., *Automata finiteness criterion in terms of van der Put series of automata functions*, P-Adic Numbers, Ultrametric Analysis, and Applications, February 2012, Volume 4, Issue 2, pp 151-160.
3. Anashin V., The Non-Archimedean Theory of Discrete Systems. *Mathematics in Computer Science* (December 2012) **6**, №4, 375–393.

4. Allouchie J.-P., Schallit J., *Automatic Sequences*. Cambridge University Press, 2003.
5. Mahler K., *p -adic numbers and their functions*. Cambridge Univ. Press (2nd edition), 1981.
6. Vuillemin J., Digital Algebra and Circuits, Verification: Theory and Practice (2003) 483–493.
7. Vuillemin J., Finite Digital Synchronous Circuits are characterized by 2-Algebraic Truth Tables. *Advances in Computing Science — ASIAN* (2000) **1961**, **2000**, 1-12.
8. Лунц А. Г., p -адический аппарат теории конечных автоматов. *Проблемы кибернетики* (1965) **14**, 17–30.
9. Яблонский С.В., *Введение в дискретную математику*. Наука, 1986.

Статья поступила 18.03.2013.