СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

1. $\mathbb{Z}$ – кольцо целых рациональных чисел
2. $\mathbb{Z}_+$ – множество натуральных чисел $\mathbb{N}$
3. $N_0 = \{0, 1, \dots\}$
4. $\mathbb{P}$ – множество простых чисел
5. Сепарабельное пространство – топологическое пространство, в котором можно выделить счётное всюду плотное подмножество
6. Плотное множество – подмножество пространства, точками которого можно сколь угодно хорошо приблизить любую точку объемлющего пространства.
7. Счётное множество – бесконечное множество, элементы которого возможно пронумеровать натуральными числами.
8. Хаусдорфово пространство — топологическое пространство, удовлетворяющее сильной аксиоме отделимости T_2.
9. Множество из $\mathbb{R}^n$ называется компактом, если из любой последовательности его точек можно выделить сходящуюся подпоследовательность, предел которой принадлежит этому множеству.
10. Локально компактное пространство — топологическое пространство, у каждой точки которого существует открытая окрестность, замыкание которой компактно.
11. Размерностью полного метрического пространства X называется наименьшее целое число n такое, что для любого покрытия пространства X существуют вписанное в него подпокрытие кратности $n + 1$.
12. Конечный автомат — абстрактный автомат, число возможных внутренних состояний которого конечно.
13. Абстрактный автомат с выделенным начальным состоянием называется инициальным автоматом. [1]
14. Автомат Мили конечный автомат, выходная последовательность которого зависит от состояния автомата и входных сигналов. Это означает, что в графе состояний каждому ребру соответствует некоторое значение (выходной символ). В вершины графа автомата записываются выходящие сигналы, а дугам графа приписывают условие перехода из одного состояния в другое, а также входящие сигналы. [1]

15. Автомат Мура (абстрактный автомат второго рода) - конечный автомат, выходное значение сигнала в котором зависит лишь от текущего состояния данного автомата, и не зависит напрямую, в отличие от автомата Мили, от входных значений. [1]

ВВЕДЕНИЕ

Со времен Ньютона и Лейбница вещественные числа применялись как основной математический объект, который казалось бы отлично подходил для описания окружающего мира. В большинстве практических задач обычно составлялись уравнения и в последствии искалось числовое решение над полем действительных чисел $\mathbb{R}$. Обоснования почему в качестве описательного элемента выбрали именно поле $\mathbb{R}$ даже не стоял. В качестве пространства стандартом де-факто долгое время являлось пространство $\mathbb{R}^3$, а уже после открытий Римана и Эйнштейна $\mathbb{R}^4$.

С течением времени и наращиванием математического аппарата представление о том, что пространство $\mathbb{R}^3$ является наиболее подходящим для описания реального мира все усиливалось, но надо понимать, что евклидово пространство $\mathbb{R}^3$ не более чем удачно выбранная модель описания реального физического пространства.

Так как реальный мир построен на евклидовой геометрии, то получается, что и она очень хорошо описывается вещественными числами, но в случае если бы мы могли отказаться от использования данной геометрии для изучения реального мира мы бы могли отказаться и от вещественной числовой системы. Но какую выбрать систему в данном случае? На этот ответ лучше всего отвечает теория p-адического исчисления, которая является с математической точки зрения более подходящей для описания тех объектов, с которыми приходиться работать в задачах физики, биологии и криптографии.[2]

Целью данной курсовой работы является построение p-адического автомата для функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$ вида $f(x) = cx$, где $c = \frac{n}{m}, n, m \in \mathbb{Z}$. В первых двух разделах будет приведен обзор на инструменты p-адического анализа, а в третьем разделе будет описана основная теорема[3] для детерминированных функций и непосредственно пошаговое построение автомата для функции $f(x) = cx$.

1 p-Адические числа

1.1 p-Адическая норма

Определение 1. Пусть M - некоторое непустое множество, и пусть $d : M \times M \to \mathbb{R}_{\geq 0}$ – функция двух переменных, определенная на этом множестве и принимающая значения во множестве действительных неотрицательных чисел. Функция d называется метрикой (а множество M – метрическим пространством), если d удоволетворяет трем условиям:

1. Для каждой пары $a, b \in M$ справедливо: $d(a, b) = 0$ тогда и только тогда, когда $a = b$.
2. Для каждой пары $a, b \in M$ справедливо равенство $d(a, b) = d(b, a)$.
3. Для каждой тройки $a, b, c \in M$ справедливо неравенство $d(a, b) \leq d(a, c) + d(c, b)$.

Пример 1. Множество $\mathbb{R}$ всех действительных чисел есть метрическое пространство с метрикой $d(a, b) = |a - b|$, где $|.|$ есть абсолютная величина.

Определение 2. Функция $\|.\|$, определенная на произвольном коммутативном кольце R и принимающая значения в $\mathbb{R}_{\geq 0}$ называется нормой (также, абсолютной величиной), если она удовлетворяет следующим условиям:

1. Для любого $a \in R$ справедливо, что $\|a\| = 0$ тогда и только тогда, когда $a = 0$.
2. Для каждой пары $a, b \in R$ справедливо равенство $\|a \cdot b\| = \|a\| \cdot \|b\|$.
3. Для каждой пары $a, b \in R$ справедливо неравенство треугольника: $\|a + b\| \leq \|a\| + \|b\|$

Из определения следует, что если положить $d(a, b) = \|a - b\|$, то фактически будет задана метрика d на кольце R. Данная метрика называется метрикой, индуцированной нормой $\|.\|$.

Определение 3. Пусть $p \in \mathbb{P}$ – некоторое простое число. В поле $\mathbb{Q}$ введем другую норму $\|.\|_p$ по правилу:

1. $\|0\|_p = 0$,
2. $\|n\|_p = p^{-ord_p n}$,

где $n > 0$ некоторое натуральное число, а $ord_p n$ показатель степени, в которой число p входит в это произведение. В этом случае норма $\|.\|_p$ называется p-адической нормой.

Норма $\|.\|_p$ удовлетворяет всеми характерными свойствами нормы даже в более сильной форме, а именно:

1. $\|x\|_p \geq 0$, причем $\|x\|_p = 0$ если $x = 0$.
2. $\|xy\|_p = \|x\|_p \cdot \|y\|_p$.
3. $\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p)$ [4]

Заметим, что норма $\|x\|_p$ может принимать лишь счетное число значений $p^{-ord_p n}$.

Также, норма $\|x\|_p$ определяет ультраметрику на $\mathbb{Q}$. Данная норма неархимедова, так как $\|nx\|_p \leq \|x\|_p \, \forall n \in \mathbb{Q}_+$.

Теорема 1. *Нормы* $\|.\|$ *и* $\|.\|_p \; \forall p = 2, 3, \ldots$ *исчерпывают все нетривиальные неэквивалентные нормы поля рациональных чисел* $\mathbb{Q}$.

1.2 p-Адические числа

Определение 4. Пополнение поля $\mathbb{Q}$ по p-адической норме образует поле $\mathbb{Q}_p$ p-адических чисел. Поле $\mathbb{Q}_p$ аналогично полю $\mathbb{R} = \mathbb{Q}_\infty$ вещественных чисел, получаемых пополнение поля $\mathbb{Q}$ по норме $\|x\| = \|x\|_\infty$.

Определение 5. Любое p-адическое число $x \neq 0$ однозначно представляется в каноническом виде

$$x = p^\gamma \cdot (x_0 + x_1 \cdot p + x_2 \cdot p^2 + \ldots \tag{1}$$

где $\gamma = \gamma(x) \in \mathbb{Z}$ и x_j – целые числа такие, что $0 \leq x_j \leq p - 1$, $x_0 > 0$, $(j = 0, 1, \ldots)$.

Представление (1) аналогично разложению любого вещественного числа x в бесконечную десятичную дробь:

$$x = \pm 10^\gamma \cdot (x_0 + x_1 \cdot 10^{-1} + x_2 \cdot 10^{-2} + \ldots),$$
$$\gamma \in \mathbb{Z}, x_j = 0, 1, \ldots, 9, x_0 > 0,$$

и доказывается аналогично.

Помимо разложения, представление (1) дает рациональные числа тогда и только тогда, когда, начиная с некоторого номера числа $x_j, j = 0, 1, \ldots$ образуют периодическую последовательность.

Определение 6. Поле $\mathbb{Q}_p$ является коммутативно-ассоциативной группой по сложению;

Определение 7. Поле $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$ является коммутативно-ассоциативной группой по умножению;

Определение 8. Поле $\mathbb{Q}_p^*$ называется мультипликативной группой поля $\mathbb{Q}_p$[5];

Определение 9. p-адические числа x, для которых $\|x\|_p \leq 1$ (т.е. $\gamma(x) \geq 0$ или $\{x\}_p = 0$), называются целыми p-адическими числами, и их множество обозначается $\mathbb{Z}_p$. Множество $\mathbb{Z}_p$ является подкольцом кольца $\mathbb{Q}_p$; $\mathbb{Z}_+$ плотно в $\mathbb{Z}_p$. Целые числа $x \in \mathbb{Z}_p$, для которых $\|x\|_p = 1$, называютсяются единицами в $\mathbb{Z}_p$. [6]

Совокупность элементов x из $\mathbb{Z}_p$, для которых $\|x\|_p < 1$ (т.е. $\gamma(x) \geq 0$ или $\|x\|_p \leq \frac{1}{p}$) образуют главный идеал кольца $\mathbb{Z}_p$; Данный идеал имеет вид $p\mathbb{Z}_p$. Поле вычетов $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ состоит из p элементов. В мультипликативной группе поля $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ существует единица $\eta \neq 1$ порядка $p-1$ такая, что элементы $0, \eta, \eta^2, \ldots, \eta^{p-1} = 1$ образуют полный набор представителей классов вычетов поля $\mathbb{Z}_p \setminus p\mathbb{Z}_p$.

1.3 Пространство p-адических чисел $\mathbb{Q}_p$

В силу свойств p-адической нормы норма в поле $\mathbb{Q}_p$ удовлетворяет неравенству треугольника:

$$\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p) \leq \|x\|_p + \|y\|_p, x, y \in \mathbb{Q}_p.$$

Следовательно в $\mathbb{Q}_p$ можно ввести метрику:

$$\rho(x,y) = \|x-y\|_p. \tag{2}$$

При этом $\mathbb{Q}_p$ становится полным метрическим пространством. Из представления (1) следует сепарабельность $\mathbb{Q}_p$.

Определение 10. $B_\gamma(a)$ – круг радиуса p^{γ^p} с центром в точке $a \in \mathbb{Q}_p$:

$$B_\gamma(a) = \left\{ x : \|x-a\|_p \leq p^\gamma \right\}, \gamma \in \mathbb{Z} \tag{3}$$

Определение 11. $S_\gamma(a)$ – граница радиуса p^{γ_p}.

$$S_\gamma(a) = \left\{ x : \|x - a\|_p = p^\gamma \right\}, \gamma \in \mathbb{Z} \tag{4}$$

Лемма 1. *Если $b \in B_\gamma(a)$, то $B_\gamma(b) = B_\gamma(a)$.*

Замечание 1. *Круг $B_\gamma(a)$ и окружность $S_\gamma(a)$ – открыто-замкнутые множества в $\mathbb{Q}_p$.*

Замечание 2. *Всякая точка круга $B_\gamma(a)$ является его центром.*

Замечание 3. *Любые два круга в $\mathbb{Q}_p$ либо не имеют общих точек, либо один содержится в другом.*

Замечание 4. *Всякое открытое множество в $\mathbb{Q}_p$ есть объединение не более чем счетного числа кругов без общих точек.*

Лемма 2. *Если множество $M \subset \mathbb{Q}_p$ содержит две различные точки a и b, $a \neq b$, то его можно представить в виде объединения непересекающихся открыто-замкнутых (в M) множеств M_1, M_2 таких, что $a \in M_1, b \in M_2$.*

Лемма (2) утверждает, что всякое множество пространства $\mathbb{Q}_p$, состоящее из более чем одной точки, несвязно. Другими словами, связная компонента любой точки совпадает с самой точкой. Из этого следует, что $\mathbb{Q}_p$ является вполне несвязным пространством.

Если рассматривать лемму для случая, когда множество M состоит только из двух точек a и b, убеждаемся, что существует непересекающиеся окрестности этих точек. Из этого можно сделать вывод, что пространство $\mathbb{Q}_p$ хаусдорфово.

Лемма 3. *Для того чтобы множество $K \subset \mathbb{Q}_p$ было компактом, необходимо и достаточно, чтобы оно было замкнутым и ограниченным в $\mathbb{Q}_p$*

Замечание 5. *Всякий круг $B_\gamma(a)$ является и окружность $S_\gamma(a)$ компакты.*

Замечание 6. *Пространство $\mathbb{Q}_p$ локально компактное.*

Замечание 7. *Всякий компакт можно покрыть конечным числом кругов фиксированного радиуса без общих точек.*

Замечание 8. *В пространстве $\mathbb{Q}_p$ справедлива лемма Гейне-Бореля: из каждого бесконечного покрытия компакта K можно выбрать конечное покрытие K.*

Теорема 2. *Размерность пространства $\mathbb{Q}_p$ равна* 0.

2 p-Адический анализ в $\mathbb{Z}_p$

Так как компакт $\mathbb{Z}_p$ есть пополнение множества $\mathbb{N}_0$ по метрике $d_p(x,y) = \|x-y\|_p$, то любое число из $\mathbb{Z}_p$ есть предел последовательности чисел из $\mathbb{N}_0$.

Определение 12. p-адическое целое z является пределом последовательности $\{z_i\}_{i=0}^{\infty}$, если если для любого $\epsilon > 0$ найдется N такое, что $\|z_i - z\|_p < \epsilon$ как только $i > N$. [7]

Определение 13. p-адическое целое z есть предел последовательности $\{z_i\}_{i=0}^{\infty}$, если для любого (достаточно большого) положительного рационального целого K найдется N такое, что $z_i \equiv z \pmod{p}^K$ при всех $i > N$. [7]

Замечание 9. *По определению p-адической метрики* $\|z_i - z\|_p \leq p^{-K}$ *тогда и только тогда, когда* $z_i \equiv z \pmod{p}^K$. *[7]*

Определение 14. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется непрерывной в точке $z \in \mathbb{Z}_p$, если для любого (достаточно большого) положительного рационального целого M найдется положительное рациональное целое L такое, что $f(x) \equiv f(z) \pmod{p}^M$ как только $x \equiv z \pmod{p^L}$. [7]

Определение 15. Функция f называется равномерно непрерывной на $\mathbb{Z}_p$, если f непрерывна в каждой точке $z \in \mathbb{Z}_p$, и L зависит только от M и не зависит от z.[8]

2.1 p-адическая дифференцируемость

Определение 16. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется дифференцируемой в точке $z \in \mathbb{Z}_p$, если существует p-адическое число $f'(x) \in \mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$ справедливо

$$\left\| \frac{f(x+h) - f(x)}{h} - f'(x) \right\|_p \leq \frac{1}{p^M}, \tag{5}$$

если h достаточно мало, т.е. когда $\|h\|_p \leq p^{-K}$, где $K = K(M)$ достаточно велико.

Определение 17. Функция f называется равномерно дифференцируемой (на $\mathbb{Z}_p$), если неравенство (5) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало. [9]

Лемма 4. *Если совместимая функция* $f : \mathbb{Z}_p \to \mathbb{Z}_p$ *дифференцируема в точке* $x \in \mathbb{Z}_p$, *то* $f'(x) \in \mathbb{Z}_p$.

Определение 18. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется дифференцируемой в точке $x \in \mathbb{Z}_p$, если существует p-адическое число $f'(x) \in \mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$ справедливо

$$f(x+h) \equiv f(x) + h \cdot f'(x) \pmod{p}^{M+ord_p h} \tag{6}$$

Определение 19. Функция f называется равномерно дифференцируемой (на $\mathbb{Z}_p$), если неравенство (6) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало, т.е. когда $ord_p h \geq K = K(M)$ для достаточно большого $K \in \mathbb{N}$.

Замечание 10. *Правила дифференцирования не зависят от метрики: для вычисления производных суммы, частного и сложной функции в p-адическом анализе используются те же формулы, что и в действительном.*

Замечание 11. *Между действительным и p-адическим анализом существует резкое различие например в том, что в и в том, и в в другом случае производная константы равна* 0, *однако в p-адическом анализе в отличии от действительного равенство нулю производной некоторой функции не означает, что эта функция константа.*

3 p-Адические автоматы

В данном разделе мы будем заниматься построением автомата для функции вида $f(x) = cx$, где $c = \frac{n}{m}, n, m \in \mathbb{Z}$. Перед тем как рассматривать построение автомата, рассмотрим основные определения [10] и основную теорему, которая говорит о том, что для каждой совместимой функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$ можно построить соответствующий ей автомат.

Зафиксируем простое число p. Если рассматривать стандартный алгоритм сложения столбиком двух многоразрядных чисел в p-адической системе счисления, то видно, что эта операция может быть реализована с помощью конечного автомата Мили Σ_p, называемого последовательным сумматором, у которого два p-ичных входа и один p-ичный выход.

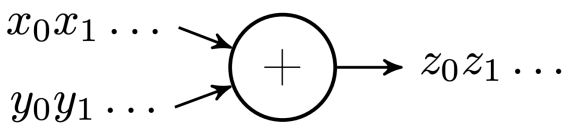

Рисунок 1 – Автомат Σ_p

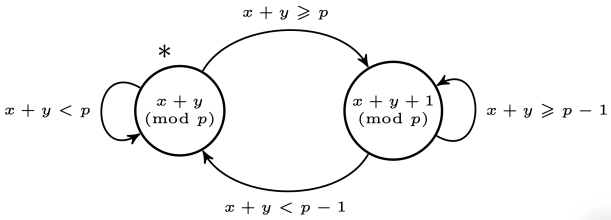

Рисунок 2 – Диаграмма переходов автомата Σ_p

Как видно из диаграммы переходов автомата Σ_p на рис. 2, у автомата два состояния, соответствующие наличию и отсутствию переноса на данный момент вычисления, а его состоянием является состояние с отсутствием переноса. Внутри каждого состояния указана соответствующая функция выхода, а на стрелках - условия при которых происходит данный переход.

Автомат Σ_p реализует ограниченно-детерминированную функцию $\Sigma_p(x, y)$, которую можно отождествить со сложением $x + y$ в кольце $\mathbb{Z}_p$, если рассмат-

ривать сверхслова $x_0x_1\cdots$ над алфавитом $E_p = \{0, 1, \cdots, p-1\}$ как элементы $\sum_{i\geq 0} x_i p^i$ кольца $\mathbb{Z}_p$. Такое отождествление позволяет рассматривать любую детерминированную функцию $f(x_1, \cdots, x_n)$, определенную и принимающую свои значения на множестве сверхслов над алфавитом E_p, как функцию $f : \mathbb{Z}_p^n \to \mathbb{Z}_p$.

Такая интерпретация детерминированных функций рассматривалась Лунцем в его работе [11], где такие функции назывались p-адическими автоматами. При этом выделяется класс p-адических автоматов, являющихся линейными однородными функциями вида:

$$f(x_1, \cdots, x_n) = c_1x_1 + c_2x_2 + \cdots + c_nx_n,$$

где $c_1, \cdots, c_n \in Q \cap \mathbb{Z}_p$, и показано, что это в точности все линейные однородные функции, реализуемые конечными автоматами. Отметим также, что p-адическая интерпретация детерминированных функций позволяет изучать их свойства, привлекая аппарат теории динамических систем [12] и p-адического анализа [13].

Рассмотрим автоматы реализующие функцию вида $f(x) = cx$, где $c \in Q \cap \mathbb{Z}_p$. Множество таких автоматов образует кольцо $Z_{(p)}$ относительно операции сложения, определенной с помощью автомата Σ_p (рис. 3), и операции умножения, определенной как суперпозиция двух автоматов (рис.4).

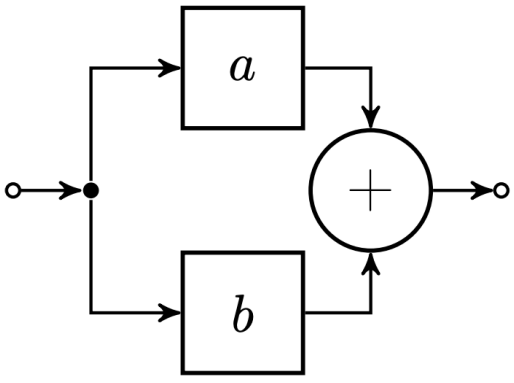

Рисунок 3 – Сложение автоматов ax и bx

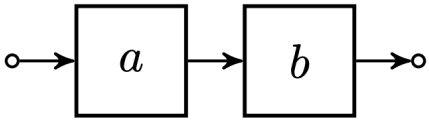

Рисунок 4 – Умножение автоматов ax и bx

Данное кольцо, изоморфно кольцу $Q \cap \mathbb{Z}_p$, состоящему из рациональных чисел, знаменатели которых не делятся на p. В этом примере как элементы, так и операция сложения реализуется с помощью конечных автоматов, которые могут быть получены из единственного автомата Σ_p при помощи операций суперпозиции и обратной связи. Для того чтобы в этом убедиться, достаточно показать, что любой автомат, реализующий функцию $f(x) = \frac{n}{m}x$, где $m, n \in \mathbb{Z}$ и p не является делителем m, можно получить из Σ_p. Действительно, функция $f(x) = nx$, где $n \in \mathbb{N}$, реализуется при помощи суперпозиции из $n-1$ экземплярова автомата Σ_p, поскольку $nx = \underbrace{x + \cdots + x}_{n}$. Заметим, что автомат соответствующий функции px, является единичной задержкой, поскольку

$$p(x_0 + x_1 p + \cdots) = x_0 p + x_1 + p^2 + \cdots,$$

и сверхслово $x_0 x_1 \cdots$ переходит под его действием в сверхслово $0 x_0 x_1 \cdots$. Из работы [11] вытекает то, что мы уже умеем строить автоматы реализующие функции ax и bx. Тогда, используя суперпозицию, построим функцию двух переменных $g(x, y) = ax + pby$ и, применив к ней операцию обратной связи по переменной y (рис. 5), получим функцию $h(x) = \frac{a}{1-pb}x$. Корректность построенной функции вытекает из уравнения $ax + pby = y$ и того факта, что $g(x, y)$ зависит от переменной y с задержкой. Если взять $a = p - 1$ и $b = 1$, то $h(x) = -x$.

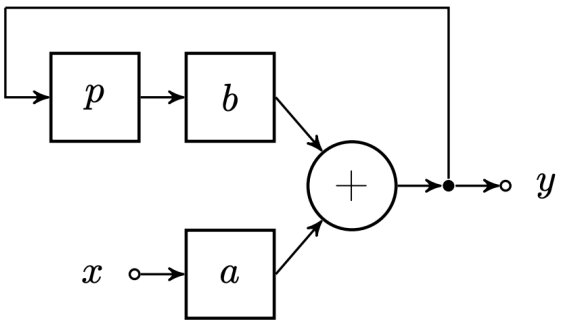

Рисунок 5 – Автомат, реализующий функцию $h(x) = \frac{a}{1-pb}x$

Тогда, используя суперпозицию, сможем выразить функцию $-nx = (-nx)$, где $n \in \mathbb{N}$, а так же константную функцию $0 = x + (-x)$. Таким образом, мы можем реализовать любую функцию ax, где $a \in \mathbb{Z}$. Покажем, реализацию функции $\frac{1}{n}x$, где $n \in \mathbb{N}$ и p не является делителем n. Поскольку числа n и p взаимно простые, всегда найдутся такие целые числа a и b, что $na + pb = 1$. Тогда, используя эти a и b в конструкции (рис. 5, получим $h(x) = \frac{a}{1-pb}x = \frac{a}{na} = \frac{1}{n}x$. Заметим, что мы можем реализовать функцию $\frac{n}{m}x = n(\frac{1}{m}x)$ как суперпозицию функций. Таким образом, все функции вида $f(x) = cx$, где $c \in Q \cap \mathbb{Z}_p$, могут быть построены из Σ_p.

3.1 Основные определения и обозначения

Зафиксируем простое число p. Сопоставим каждому слову $\alpha = a(1) \cdots a(l)$ в алфавите $E_p = \{0, 1, \cdots, p-1\}$ целое неотрицательное число $[\alpha] = a(1) + a(2)p + \cdots + a(l)p^{l-1}$. Договоримся, что пустому слову Λ будет соответствовать число 0. Таким образом, слово $\alpha = a(1)a(2) \cdots a(l)$ является обращением записи $(a(1)a(2) \cdots a(l))_p$ числа $[\alpha]$ в p-ичной системе счисления [14, 15].

Определение 20. [16] Сверхсловом в алфавите A называется проивзольная бесконечная последовательность $\alpha = a(1)a(2) \cdots$ элементов алфавита A. Сверхслова $\alpha = a(1)a(2) \cdots$ над алфавитом E_p можно отождествлять с элементами $a(1) + a(2)p + \cdots$ множества $\mathbb{Z}_p$ целых p-адических чисел.

Определение 21. [16] Будем обозначать через $A|_l$ префикс $a(1)a(2) \ldots a(l)$ длины l, а через $a \downarrow_l$ соотвествующий бесконечных суффикс $a(l+1)a(l+2) \ldots a(l)$ сверхслова α.

Определение 22. A^ω - множество всех сверхслов над алфавитом A.

Определение 23. Функция $f : A^\omega \to B^\omega$ является детерминированной если для любых двух сверхслов $\alpha_1, \alpha_2 \in A^\omega$ и натурального l из $\alpha_1|_l = \alpha_2|_l$ следует $f(\alpha_1)|_l = f(\alpha_2)|_l$.

Определение 24. Для каждой детерминированной функции $f : A^\omega \to B^\omega$ и слова $\alpha \in A^*$ введем функцию $f_\alpha(x) := f(\alpha x) \downarrow_{|\alpha|}$, которую будем называть остаточной функцией для f, соответствующую слову α.

Определение 25. Детерминированную функцию $f : A^\omega \to B^\omega$, имеющую конечное число различных остаточных функций, назовем ограниченно-детерминированной функцией.

Известно[17], что класс всех ограниченно-детерминированных функций совпадает с классом всех конечно-автоматных функций, реализуемых конечными инициальными детерминированными автоматами Мили.

Определение 26. Детерминированную функцию $f : A^\omega \to B^\omega$ назовем обратимой, если она биективна, и, тем самым, для нее существует обратное отображение $f^{-1} : B^\omega \to A^\omega$, такое, что $f \circ f^{-1} = id_{A^\omega}$, $f \circ f^{-1} = id_{B^\omega}$.

Поскольку все остаточные функции f_α у обратимой функции f так же обратимы, то у инициального автомата, реализующего f, в каждом состоянии q функция выхода $\psi_q(x) = \psi(q, x)$ является биекций. В тоже время несложно показать, что любой обратимый автомат с таким свойством реализует обратимую ограниченно-детерминированную функцию. Для обратимой ограниченно-детерминированной функции f функция f^{-1} тоже является ограниченно-детерминированной функцией, причем с тем же весом, что и у f. Для того, чтобы в этом убедиться, достаточно рассмотреть диаграмму Мура автомата $\mathfrak{A}$ с начальным состоянием q_0, реализующего f и каждую стрелку $q \xrightarrow{a/b} q'$ в ней заменить на $q \xrightarrow{b/a} q'$. Видно, что в результате получилась диаграмма некоторого нового автомата $\mathfrak{A}^{-1}$, и если в нем в качестве начального состояния выбрать опять q_0, то соответствующая ему ограниченно-детерминированная функция будет равна f^{-1}. В качестве примера можно посмотреть на рисунок 6, где изображен обратимый автомат. Обратный к нему автомат показан на рисунке 7. Он получается путем изменения a/b на b/a на всех его переходах.

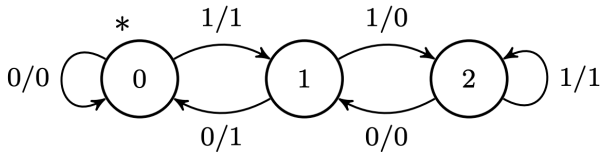

Рисунок 6 – Диаграмма автомата $\mathfrak{A}_3$

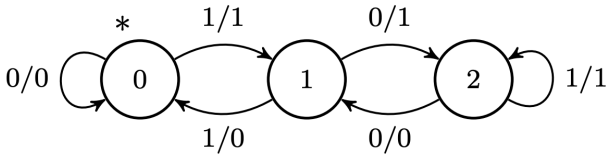

Рисунок 7 – Диаграмма автомата $\mathfrak{A}_{\frac{1}{3}}$

3.2 Основная теорема о детерминированных функциях

Теорема 3. *[3] Детерминированная функция $f_{\mathfrak{A}}(s_0) : \mathbb{Z}_p \to \mathbb{Z}_p$ соответствующая автомату $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$, совместима, т.е. удовлетворяет p-адическому условию Липшица с константой* 1. *Обратно, для каждой совместимой функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$ существует автомат $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$ такой, что $f = f_{\mathfrak{A}(s_0)}$.*

Доказательство. Действительно, поскольку каждый i-й выходной символ $\psi_i = O(s_i, \chi_i)$ автомата зависит только от i-го состояния s_i и от i-го входного символа χ_i, и поскольку состояние $s_i = S(s_{i-1}, \chi_{i-1})$ зависит только от s_{i-1} и от χ_{i-1}, и т.д. Таким образом, каждый выходной символ $\psi_i = \psi_i(\chi_0, \ldots, \chi_i) \in \mathbb{F}_p, i = 0, 1, 2, \ldots$, зависит только от входных символов $\chi_0, \ldots, \chi_i \in \mathbb{F}_p$ и не зависит от символов $\chi_{i+1}, \chi_{i+2}, \ldots$. Следовательно, детерминированная функция $f = f_{\mathfrak{A}} : \mathbb{Z}_p \to \mathbb{Z}_p$ имеет вид:

$$f : x = \sum_{i=0}^{\infty} \chi_i p^i \mapsto f(x) = \sum_{i=0}^{\infty} \psi_i(\chi_0, \ldots, \chi_i) p^i \tag{7}$$

Другими словами, каждой детерминированной функции f соответствует единственная последовательность отображений $\psi_i : \mathbb{F}_p^n \to \mathbb{F}_p$. Однако каждая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$, имеющая вид (7), очевидно совместима, т.е. удовлетворяет p-адическому условию Липшица с константой 1.

Обратно, пусть дана совместимая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$; тогда ее можно представить в виде (7). Построим автомат $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathcal{S}, \mathbb{F}_p, S, O, s_0 \rangle$ такой

что $f_{\mathfrak{A}}(s_0) = f$. Возьмем множество $\mathbb{F}_p^*$ всех непустых конечных слов над алфавитом $\mathbb{F}_p$, рассмотрим эти слова как представления натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$ в системе счисления с основанием p и перенумеруем слова в лексикографическом порядке в соответствии с естественным порядком на $\mathbb{N}$. Таким образом мы установим взаимнооднозначное соответствие между всеми непустыми словами w над алфавитом $\mathbb{F}_p$ и числами $i = 1, 2, 3, \ldots : w \leftrightarrow \nu(w), i \leftrightarrow \omega(i)(\nu(w) \in \mathbb{N}, \omega(i) \in \mathbb{F}_p^*)$. Заметим, что $\nu(\omega(i)) = i, \omega(\nu(w)) = w$ для всех $i \in \mathbb{N}$ и всех непустых слов $w \in \mathbb{F}_p^*$. Будем считать, что $\omega(0)$ есть пустое слово.

В качестве множества $\mathcal{S}$ всех состояний автомата $\mathfrak{A}$ возьмем множество $N_0 = \{0, 1, 2, 3, \ldots\}$, и возьмем $s_0 = 0$ в качестве начального состояния. Зададим функцию перехода S следующим образом: $S(i, r) = \nu(r\omega(i))$, где $i = 0, 1, 2, \ldots r \in \mathbb{F}_p$; т.е. $S(i, r)$ равна номеру слова $r\omega(i)$, которое есть результат конкатенации слова $\omega(i)$ (с номером i) в качестве префикса (начала) с однобуквенным словом r в качестве суффикса (окончания). Зададим функцию выхода следующим образом: $O(i, r) = \psi_{|\omega(i)|}(r\omega(i))$, где символом $|w|$ обозначается длина слова w (длина пустого слова равна 0). Отображение $\psi_i : F_p^{i+1} \to \mathbb{F}_p$ может рассматриваться как отображение множества всех слов длины $i + 1$ над алфавитом $\mathbb{F}_p$ во множество всех однобуквенных слов $\mathbb{F}_p, i = 0, 1, 2, \ldots$. Отметим, что при необходимости здесь и далее мы будем использовать без дополнительных оговорок естественное соответствие между словами длины n и элементами кольца вычетов m $\mathbb{Z}/p^n\mathbb{Z}$, также как и соответствие между множеством всех бесконечных слов $\mathbb{F}_p^\infty$ и кольцом $\mathbb{Z}_p$.

Поскольку f удовлетворяет p-адическому условию Липшица с константой 1, она непрерывна относительно p-адической метрики, а потому чтобы доказать, что $f = f_{\mathfrak{A}(s_0)}$ достаточно показать, что $f_{\mathfrak{A}(s_0)}(w) \equiv f(w) \pmod{p}^{\lambda(w)}$ для всех непустых слов $\omega \in \mathbb{F}_p^*$: действительно, если это так, то если дано бесконечное слово $w \in \mathbb{F}_p^\infty$, то последовательность $w \pmod{p^n}, n = 1, 2, 3, \ldots$, состоящая из конечных слов, сходится p-адически к w, т.е. $f(w) \pmod{p^n}$ сходится p-адически к $f(w)$ при n стремящимся к бесконечности.

Индукцией по n докажем, что если входное слово w имеет длину $n > 0$, то $f_{\mathfrak{A}(s_0)}(w) \equiv f(w) \pmod{p^n}$. Если $n = 1$, то $w \in \mathbb{F}_p$, и после того, как w подано на вход, автомат $\mathfrak{A}$ перейдет в состояние $S(0, w) = \nu(w)$ и подаст на выход символ $O(0, w) = \psi_0(w) = f(w) \pmod{p}$, см. (7).

Предположим, что утверждение верно для всех $n < k$ и докажем, что оно верно и при $n = k$. Рассмотрим слово w длины n; тогда $w = rv$, где $r \in \mathbb{F}_p, |v| = n-1$ (т.е. w состоит из префикса v и суффикса r). По предположению индукции, после того как слово v будет подано на вход, автомат перейдет в состояние $\nu(v)$ и подаст на выход слово $v' = f(v) \pmod{p^{n-1}}$. Следовательно, после того как на вход будет подан символ r, автомат подаст на выход символ $O(\nu(v), r) = \psi_{|\omega(\nu(v))|}(r\omega(\nu(v))) = \psi_{|v|}(rv)$. Стало быть, если подать на вход слово w, то автомат подаст на выход слово $v'' = (\psi_{|v|}(rv))v'$, которое есть результат конкатенации слова $v' = f(v) \pmod{p^{n-1}}$ в качестве префикса с однобуквенным словом $\psi_{|v|}(rv) \in \mathbb{F}_p$ в качестве суффикса. Однако $v'' = f(w) \pmod{p^n}$. (7). Этим завершается доказательство утверждения и теоремы. □

3.3 Построение автомата для функции вида $f(x) = cx$

Для любого рационального числа $c = \frac{n}{m}$, где $n, m \in \mathbb{Z}$ и где p не является делителем m, существует ограниченно-детерминированная функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ такая, что $f(x) = cx$. Обозначим через $\mathfrak{A}_c$ соотвествующий приведенный конечный автомат. Легко видеть, что для любой детерминированной функции $f : \mathbb{Z}_p \to \mathbb{Z}_p$ и слова $\alpha = a(1)a(2)\dots a(l) \in E_p^l$ для соответствующей остаточной функции $f_\alpha(x)$ выполняется следующее соотношение:

$$f([\alpha] + p^l x) = [\beta] + p^l f_\alpha(x) \tag{8}$$

где $\beta = b(1)b(2)\dots b(l) = f(\alpha) \in E_p^l$:

$$\overbrace{\underbrace{a(1)\dots a(l)}_{\alpha}\underbrace{x(1)x(2)\dots}_{x}}^{[\alpha]+p^l x} \to \boxed{f} \to \overbrace{\underbrace{b(1)\dots b(l)}_{\beta}\underbrace{x(1)x(2)\dots}_{x}}^{[\beta]+p^l f_\alpha(x)} \tag{9}$$

Из соотношения 8 непосредственно следует формула для $f_\alpha(x)$:

$$f_\alpha(x) = \frac{f([\alpha] + p^l x) - [\beta]}{p^l}. \tag{10}$$

Для начала опишем автомат $\mathfrak{A}_n$, где $n \in \mathbb{N}$. Применив формулу 10 к функции $f(x) = nx$, получим:

$$(nx)_\alpha = \frac{n([\alpha] + p^l x) - [\beta]}{p^l} = nx + \frac{n[\alpha] - [\beta]}{p^l}, \tag{11}$$

где $[\beta] = n[\alpha] \pmod{p^l}$ (так как $f(\alpha) = \beta$). Следовательно, $n[\alpha] - [\beta]$ делится на p^l, и мы получаем более короткое представление:

$$(nx)_\alpha = nx + q, \tag{12}$$

где $q = \left[\frac{n[\alpha]}{p^l}\right] \in \{0, \ldots, n-1\}$, так как $n[\alpha] = p^l q + [\beta]$ и $[\alpha], [\beta] \in [0, p^l)$. Покажем, что $\forall q \in \{0, \ldots, n-1\} \quad \exists \alpha : \alpha \in E_p^l$, что $q = \frac{n[\alpha]}{p^l}$.
Действительно, последнее эквивалентно следующему выражению:

$$p^l q \leq n[\alpha] < p^l q + p^l. \tag{13}$$

Возьмем теперь достаточно больше l так, чтобы выполнялось неравенство $p^l > n$, и положим $\alpha \in E_p^l$ равным p-ичной зависи числа $\left[\frac{p^l q}{n}\right]$, т.е. $[\alpha] = \left[\frac{p^l q}{n}\right]$. Тогда:

$$\frac{p^l q}{n} \leq [\alpha] < \frac{p^l q}{n} + 1 \Rightarrow p^l q \leq n[\alpha] < p^l q + n \Rightarrow p^l q \leq n[\alpha] < p^l q + p^l. \tag{14}$$

Следовательно, слово α удовлетворяет условию (4) и $q = \left[\frac{n[\alpha]}{p^l}\right]$. Таким образом, показано что остаточные функции для $f(x) = nx$ полностью исчерпываются функциями $f^{(q)}(x) = nx + q$, где $q \in \{0, \ldots, n-1\}$. Более того, все эти функции различны, поскольку $f^{(q)}(0) \neq f^{(q')}(0)$ при $q \neq q'$.

Такое наблюдение позволяет выбрать в качестве множества состояний приведенного автомата $\mathfrak{A}_n$, реализующего ограниченно-детерминированная функцию nx, множество $Q = \{0, \ldots, n-1\}$. Опишем функцию переходов и функцию выходов автомата $\mathfrak{A}_n$. Применив формулу 10 к функции $f^{(q)}(x) = nx + q$ и однобуквенному слову $\alpha = a$, получим:

$$(nx + q)_\alpha = \frac{n(px + a) + q - b}{p} = nx + \frac{q + na - b}{p} \tag{15}$$

где $b = na + q \pmod{p}$. Тогда $(nx + q)_\alpha = nx + q'$, где $q' = \frac{q+na-b}{p}$, и в автомате $\mathfrak{A}_n$ переход $q \xrightarrow{a/b} q'$ существует тогда и только тогда, когда выполнено

равенство:

$$q + na = pq^{'} + b \tag{16}$$

Так как $q^{'} \in [0, n)$ и $b \in [0, p)$, то из равенства 16 следует, что

$$q^{'} = p^{-1}(q - a) \pmod{n}, b = n^{-1}(a - q) \pmod{p} \tag{17}$$

где p^{-1} - это обратный элемент для p в кольце целых чисел по модулю n, а n^{-1} - это обратный элемент для элемента n в кольце целых чисел по модулю p. Оба элемента существуют, поскольку n и p - взаимно простые числа.

ЗАКЛЮЧЕНИЕ

В данной курсовой работе был рассмотрен метод построения автомата для функции $f(x) = cx$, где $c = \frac{n}{m}, n, m \in \mathbb{Z}$. В дальнейшей научной работе планируется формализовать метод и расширить его для того, чтобы было возможно в виде автомата представлять любую полиномиальную функцию.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 В.Б., Кудрявцев. Элементы теории автоматов / [Кудрявцев В.Б., Алешин С.В., Подколзин А.С.] : М.: Изд-во МГУ, 1978. 2016 с.

2 Козырев, С. В. Методы и приложения ультраметрического и p-адического анализа: от теории всплесков до биофизики / С. В. Козырев // Совр. пробл. матем. 2008. Т. 12. С. 3–168.

3 Анашин, В.С. Методы неархимедовой алгебраической динамики в криптографии [Электронный ресурс]. URL: https://istina.msu.ru/media/courses/course/f66/226/7102110/SYMB_COMPUT.PDF (дата обращения: 03.04.2019).

4 И.В., Волович. p–Адическая математическая физика: основные конструкции, применения к сложным и наноскопическим системам / [Волович И.В., Козырев С.В.] : Самара, 2009. 30 с.

5 Baker, A. An Introduction to p-adic Numbers and p-adic Analysis / [A. Baker] : University of Glasgow, 2017. 64 p.

6 Владимиров, В.С. p-Адический анализ и математическая физика / [В.С. Владимиров, Волович И.В., Зеленов Е.И.] : М.:Физматлит, 1994. 352 с.

7 Анашин, В.С. Введение в прикладной p-адический анализ .

8 Ciocan, N. P-adic Functions - Part 1 . 2011.

9 Anashin, V. The p-adic ergodic theory and applications / [V. Anashin] : Moscow, 2014. 221 p.

10 Balodis, Kaspars. Unconventional Finite Automata and Algorithms : Ph. D. thesis / Kaspars Balodis ; [University of Latvia] : Riga, 2016.

11 Лунц, А.Г. p-адический аппарат в теории конечных автоматов / А.Г. Лунц // Пробл. кибернетики. 1965. Т. 14. С. 17–30.

12 V., Anashin. Automata finiteness criterion in terms of van der Put series of automata functions / Anashin V. // p-Adic Numbers, Ultrametric Analysis and Applications. 2012. Vol. 4:2. P. 151–160.

13 V., Anashin. Applied Algebraic Dynamics / Anashin V., Khrennikov A. Berlin : W. de Gruyter, 2009. 533 p.

14 Tyapaev, L. B. Automata as p-adic Dynamical Systems [Электронный ресурс]. 2017. arXiv:1709.02644.

15 Tyapaev, L. B. Non-Archimedean dynamics of the complex shift / L. B. Tyapaev // [Компьютерные науки и информационные технологии] : Издательский центр «Наука», 2018. P. 406–412.

16 Klapper, A. Feedback shift registers, 2-adic Span, and combiners with memory / A. Klapper // Journal of Cryptology. 1997. Vol. 10(2). P. 111–147.

17 В.Б., Кудрявцев. Введение в теорию автоматов / [Кудрявцев В.Б., Алешин С.В., Подколзин А.С.] : М.: Наука, 1985. 320 с.