МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Автоматы Мура и функции класса Lip-1 в полях p-адических чисел

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направление 02.03.01 — Математика и компьютерные науки

механико-математического факультета

Шикина Никиты Сергеевича

Научный руководитель
зав. каф., к.ф.-м.н., доцент. ________________ А.М. Водолазов

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент ________________ А.М. Водолазов

Саратов 2022 г.

Введение. P-адический анализ - довольно молодое ответвление современной науки. Введенные в конце 19 века немецким ученым Куртом Гензелем р-адические числа составляют неотъемлемую часть теории чисел, алгебраической геометрии и других разделов современной математики. И действительные, и p-адические числа получаются из рациональных при помощи процедуры под названием пополнение (которая может быть применена к любому метрическому пространству), если использовать различные расстояния на множестве рациональных чисел: обычное евклидово расстояние для действительных чисел и новое p-адическое для p-адических, для произвольного простого числа p. Тот факт, что p-адическое расстояние удовлетворяет «сильному неравенству треугольника», является причиной многих удивительных свойств

p-адических чисел, а также приводит к интересным отличиям от классического вещественного анализа, подобно тому как отрицание пятого постулата Евклида о параллельных прямых приводит к неевклидовой геометрии. Неархимедова геометрия и p-адический анализ применяются в физике для описания геометрии на малых растояниях и в рамках традиционной теоритической физики для описания сложных систем, например, фракталов.

Основное содержание работы. Для определения поля p-адических чисел понадобятся понятия нормы, архимедовых и неархимедовых метрических пространств, последовательности Коши, пополнения поля и некоторые другие, поэтому ниже будут определения данных понятий и некоторые их свойства.

Определение 1. Пусть X — непустое множество. Функция d, определенная на множестве всех упорядоченных пар (x, y) элементов X и принимающая неотрицательные вещественные значения $d(x, y)$, называется *расстоянием* или *метрикой* в X, если она обладает следующими свойствами:

(1) $d(x, y) = 0$ тогда и только тогда, когда $x = y$;

(2) $d(x, y) = d(y, x)$;

(3) $d(x, y) \leqslant d(x, z) + d(z, y)$ для всех $z \in X$.

Множество X вместе заданной в нем метрикой называется *метрическим пространством.* Одно и то же множество X может допускать много различных структур метрического пространства (X, d).

Определение 3. Пусть $p \in 2, 3, 5, 7, 11, 13, ...$ - некоторое простое число. Для произвольного ненулевого целого числа a положим $ord_p a$ равным кратности вхождения p в разложение a на простые сомножители, т.е. наибольшему целому неотрицательному числу m, для которого $a = b(mod\ p^m)$. Тогда для произвольного рационального числа $x = a/b$ данная величина будет равна $ord_p x = ord_p a - ord_p b$.
Определение 4. Отображение

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p x}}, \text{если } x \neq 0; \\ 0, \text{если } x = 0. \end{cases} \tag{1}$$

является *нормой* на поле $\mathbb{Q}$.
Определение 5. Последовательность x_n точек метрического пространства называется *последовательностью Коши*, если для любого $\varepsilon > 0$ существует такое натуральное число N, что если $n, m > N$, то $d(x_n, x_m) < \varepsilon$.

Если любая последовательность Коши из M имеет предел в M, то называется *полным метрическим пространством.*
Определение 6. Если пространство M не полное, то существует такое метрическое пространство , что

(1) $\overline{M}$ полное;
(2) $\overline{M}$ содержит подмножество $\overline{M}_0$, изометрическое пространству M;
(3) $\overline{M}_0$ всюду плотно в $\overline{M}$ (т.е. каждая точка из $\overline{M}$ явлется предельной точкой множества $\overline{M}_0$[1].

Определение 7. Норма называется *неархимедовой*, если всегда выполнено неравенство $\|x + y\| \leqslant max(\|x\|, \|y\|)$. Соответственно метрика называется неархимедовой, если $d(x, y) \leqslant max(d(x, z), d(x, y))$.

В частности, метрика, индуцированная неархимедовой нормой, неархимедова, так как в этом случае $d(x, y) = \|x - y\| = \|(x - z) + (z - y)\| \leqslant max(\|x - z\|, \|z - y\|) = max(d(x, z), d(z, y))$. Таким образом, $| \ |_p$ является неархимедовой нормой на поле $\mathbb{Q}$.

[1]Яковлев, Г.Н. ЭФункциональные пространства / Г.Н. Яковлев М.: Московский физико-технический институт (государственный университет), 2000. - 128 с.

Норму (или метрику), не являющуюся неархимедовой, называют *архимедовой*. Обычная абсолютная величина на поле $\mathbb{Q}$ дает пример архимедовой нормы.

Для каждого метрического пространства X определено понятие *последовательности Коши*. Последовательность $a_1, a_2, a_3, \ldots$ элементов X называется последовательностью Коши, если для всякого положительного числа ε найдется такой номер N, что $d(a_m, a_n) < \varepsilon$ при любых $m, n > N$.

По определению, две метрики d_1 и d_2 на множестве X эквивалентны, если отвечающие им классы последовательностей Коши совпадают. Соответственно две нормы эквивалентны, если они индуцируют эквивалентные метрики.

Например, если зафиксировать вещественное число $\rho \in (0, 1)$, а затем в определении $|\ |_p$ подставить $\rho^{ord_p x}$ вместо $\frac{1}{p^{ord_p x}}$, то получится неархимедова норма, эквивалентная $|\ |_p$.

Обычной абсолютной величине $|\ |$ также соответствует семейство эквивалентных ей архимедовых норм, а именно $|\ |^{\alpha}$, где $0 < \alpha \leqslant 1$.

Тривиальной называется такая норма $\|\ \|$, что $\|0\| = 0$ и $\|x\| = 1, \forall x \neq 0$.

Свойство (3): $d(x, y) \leqslant d(x, z) + d(z, y)$ из определения () известно как «неравенство треугольника». В случае поля комплексных чисел $\mathbb{C}$ (с метрикой $d(a + bi, c + di) = \sqrt{(a - c)^2 + (b - d)^2}$) оно означает, что сумма длин двух сторон треугольника на комплексной плоскости больше длины третьей стороны.

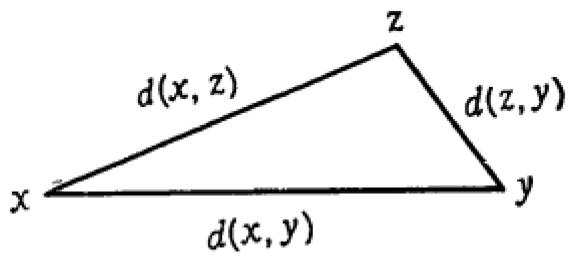

Рисунок 1 — Неравенство треугольника

Что происходит в случае поля F с неархимедовой нормой? Для простоты пусть $z = 0$ в соответствии с рисунком 1. Тогда неархимедово неравенство треугольника утверждает, что «стороны» x и y умеют разную «длину», например, $\|x\| < \|y\|$. Третья сторона имеет длину $\|x-y\| \leqslant \|y\|$. Но

$$\|y\| = \|x-(x-y)\| \leqslant max(\|x\|, \|x-y\|),$$

и, значит, $\|y\| \leqslant \|x-y\|$, так как неравенство $\|y\| \leqslant \|x\|$ не выполнено. Поэтому $\|y\| = \|x-y\|$. Итак, если две «стороны» x и y не равны, то наибольшая из них должна совпадать по длине с третьей стороной. Получается, что все «треугольники» равнобедренные. Для поля $\mathbb{Q}$ с нормой $|\ |_p$ это свойство утверждает, что кратность вхождения p в разность двух рациональных чисел с неодинаковыми кратностями вхождения p совпадает с наименьшей из этих кратностей. Таким образом для неархимедова поля: $\|x \pm y\| \leqslant max(\|x\|, \|y\|)$ и при $\|x\| \neq \|y\|$ достигается равенство. Это свойство называется *принципом равнобедренного треугольника.*

Определение 10. Множество M' элементов метрического пространства M называется *плотным* в M, если его замыкание совпадает с M.

Определение 11. Полное метрическое пространство M^* называется *пополнением* метрического пространства M, если M содержится в M^* и плотно в нём.

Важной для построения поля p- адических чисел является следующая теорема:

Теорема 1. Любое метрическое пространство имеет пополнение.

Обладая вышенаписанными знаниями, можно приступить к определению поля $\mathbb{Q}_p$ и p-адических чисел.

Пусть $\mathbb{Q}_p$ - пополнение множества $\mathbb{Q}$ с помощью нормы $|\ |_p$, S - множество последовательностей Коши в $\mathbb{Q}$, $\{x\} \in \mathbb{Q}$ - постоянная последовательность Коши, все члены которой равны $x \in \mathbb{Q}$. Очевидно, $\{x\} \sim \{x'\}$ тогда и только тогда, когда $x = x'$. Класс $\{0\}$ будет обозначаться через 0.

Норма $|\ |_p$ класса эквивалентности a будет обозначаться как предел $\lim_{i\to\infty} |a_i|_p$, где $\{a_i\}$ - некоторый представитель класса a. Этот предел существует, так как:

1) если $a = 0$, то $lim_{i\to\infty}|a_i|_p = 0$ по определению;
2) если $a \neq 0$, то для некоторого $\varepsilon > 0$ и любого N существует $i_N > N$ и $|a_{i_N}|_p > \varepsilon$.

Если N выбрано настолько большим, что $|a_i - a_{i'}|_p < \varepsilon$, при $i, i' > N$, то

$$|a_i - a_{i_N}|_p < \varepsilon \text{ для всех } i > N.$$

Так как $|a_{i_N}|_p > \varepsilon$, то $|a_i|_p = |a_{i_N}|_p$ по принципу равнобедренного треугольника. Поэтому $|a_i|_p$ имеет постоянное значение $|a_{i_N}|_p$ при всех $i > N$. А тогда предел $\lim_{i\to\infty} |a_i|_p$ равен этому постоянному значению.

Множество $\mathbb{Q}_p$ клаасов эквивалентности Коши вместе с введенными на нем операциями сложения, умножения и нахождения обратных элементов является полем[2].

Лемма 1. Пусть $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$. Тогда для любого натурального i существует целое $\alpha \in \mathbb{Z}$, для которого $|\alpha - x|_p \leqslant p^{-i}$. Более того, α можно выбрать из множества $\{0, 1, 2, 3, ..., p^i - 1\}$.

Теорема 2. Каждый класс эквивалентности a из $\mathbb{Q}_p$ с $|a|_p \leqslant 1$ содержит ровно одну последовательность Коши целых чисел $\{a_i\}$, для которой:

(1) $0 \leqslant a_i < p^i$ при $i = 1,\ 2,\ 3,\ \ldots$;

(2) $a_i \equiv a_{i+1} (mod\ p_i)$ при $i = 1,\ 2,\ 3,\ \ldots$.

В случае, когда $|a|_p \leqslant 1$ необходимо умножить a на подходящую степень p^m числа p, например, на степень числа p равную $|a|_p$, чтобы новое число $a' = ap^m$ удовлетворяло неравенству $|a'|_p \leqslant 1$. Затем нужно выбрать в соответствии с теоремой () последовательность $\{a'_i\}$, представляющую a'. Тогда число $a = a'p^{-m}$ представляется последовательностью $\{a_i\}$ с $a_i = a'_i p^{-m}$.

Теперь можно записать все числа a'_i последовательности, соответствующей a', в p-ичной системе счисления, т.е.

$$a'_i = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1},$$

где коэффициенты b_j обозначают «p-ичные знаки», т.е. целые числа из множества $\{0, 1, ..., p-1\}$. Сравнение $a'_i \equiv a'_{i+1} (mod\ p_i)$ из теоремы () эквивалентно тому, что все знаки числа

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1} + b_i p^i,$$

[2]Коблиц, Н. p-адические числа, p-адический анализ и дзета-функции / Н. Коблиц, В.В. Шокурова, Ю.И. Манина М.: Мир, 1982. - 90 с.

от b_0 до b_{i-1} включительно, совпадают с соответствующими знаками числа a'_i. Поэтому a' можно предствалять как число, имеющее бесконечную вправо p-ичную запись: всяких раз, при переходе от a'_i к a'_{i+1} в этой записи будет добавляться новый знак.

Таким образом и исходное число a можно предствлять как p-ичное число с конечным числом знаков справа от запятой (т.е. знаков соответствующих отрицательным степеням p), но с бесконечным числом знаков при положительных степенях p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + ...$$

Правая часть этой записи - сокращенная запись последовательности $\{a_i\}$, где $a_i = b_0p^{-m} + ... + b_{i-1}p^{i-1-m}$, т.е. удобный способ изображения всей последовательности $\{a_i\}$. Это равенство называется «p-адическим разложением» числа a. Пусть $\mathbb{Z}_p = \{a \in \mathbb{Q}_p| \ |a|_p \leqslant 1\}$. Это множество всех чисел из $\mathbb{Q}_p$, p-адическое разложение которых не имеет отрицательных степеней p. Элементы $\mathbb{Z}_p$ называются *целыми p-адическими числами.* Сумма, разность и произведение двух элементов из $\mathbb{Z}_p$ снова принадлежит $\mathbb{Z}_p$, поэтому $\mathbb{Z}_p$ - подкольцо поля $\mathbb{Q}_p$.

Пусть $a, b \in \mathbb{Q}_p$. Тогда обозначается $a \equiv b(mod\ p^n)$, если $|a-b|_p \leqslant p^{-n}$, или, эквивалентно, $(a-b)/p^n \in \mathbb{Z}_p$, т.е. если первый отличный от нуля знак в p-адическом разложении числа $a-b$ встречается не ранее, чем на p^n-м месте.

Теперь можно основные определения теории автоматов.

Теория автоматов как научная дисциплина возникла в пределах теории управляющих систем (теоретической кибернетики) в середине XX века, в период начавшегося бурного развития средств электронной вычислительной техники и соответствующих областей математического знания. Потребовалась разработка теоретической базы для решения проблем, возникавших при проектировании реальных цифровых ЭВМ, а также в процессе построения и исследования гипотетических систем, таких как нейронные сети. В качестве моделей последних рассматривались конечные автоматы.

Определение 12. Абстрактным автоматом называют модель, описываемую пятиместным кортежем:

$$A = (X, Y, S, f_y, f_s),$$

где первые три компонента – непустые множества:

X – множество входных сигналов АА;

Y – множество выходных сигналов АА;

S – множество состояний АА.

Два последних компонента кортежа – характеристические функции:

f_y – функция выходов;

f_s – функция переходов АА из одного состояния в другое.

Если множества X, Y, S – конечные, то такой АА называют *конечным автоматом* (КА). Если хотя бы одно из перечисленных множеств не является конечным, то такой АА называют *бесконечным.*

Предметом теории автоматов является изучение математических моделей преобразователей дискретной информации. В данной теории решаются следующие основные задачи: анализ и синтез автоматов, определение полноты, минимизация и эквивалентные преобразования автоматов.

С целью классификации автоматов рассматривают ряд признаков, таких как определенность функции переходов и функции выходов, однозначность заданных функций, устойчивость состояний. Можно перечислить виды абстрактных автоматов, распределив их по трем классификационным признакам.

Из приведенных уравнений видно, что аргументами характеристических функций являются текущее значение входного сигнала и текущее состояние. Конечный автомат, заданный парой уравнений (2), называется *автоматом I рода* или, по имени автора модели, *автоматом Мили.*

На практике часто встречаются автоматы, выходные сигналы которых в момент времени t однозначно определяются текущим состоянием автомата и не зависят от компонентов вектора входных сигналов:

$$\begin{aligned} s'(t+1) &= f'_s(x(t), s'(t)) \\ y(t) &= f'_y(x(t), s'(t)) \end{aligned} \tag{2}$$

Автомат, заданный парой уравнений (2), называют *автоматом II рода* или *автоматом Мура*. Штрих введен в обозначения для отличия записи функций и состояний автомата Мура от автомата Мили. Можно заметить, что автомат Мили по отношению к автомату Мура «запаздывает» на один дискретный момент времени по входному сигналу.

Автоматы I и II рода являются двумя базовыми моделями, изучаемыми теорией автоматов.

Если для выходного сигнала некоторого КА имеет место уравнение:

$$y(t) = f_y(x(t)),$$

то такой автомат называется *тривиальным*. Строго говоря, это уже не автомат, а комбинационная схема (КС), которая реализует совокупность булевых функций $f_y^1, ..., f_y^q$ для компонентов вектора выходных сигналов Y[3].

На практике КА представляет собой совокупность двух устройств – операционного и управляющего автоматов. Операционный автомат выполняет ряд действий над входными данными и выдает результат, а управляющий автомат задает последовательность этих действий, то есть алгоритм функционирования операционного автомата. Например, в случае кодового замка операционным автоматом является электромагнит, управляющий засовом, а управляющим автоматом – электронная схема, обеспечивающая считывание и анализ сигналов от клавиш, проверку кода, выдачу сигнала операционному автомату на открытие замка, сброс в начальное состояние.

Определение Отношение эквивалентности θ называется *конгруэнцией* относительно операции $\top$, если для любых элементов $a, b, c, d \in A$ из $a\theta c$ и $b\theta d$ следует $(a\top b)\theta(c\top d)$.

Определение Функция $f(x)$ удовлетворяет на отрезке $[a, b]$ условию Липшица, если существует такое число $L > 0$ (константа Липшица), что

$$|f(x_1) - f(x_2)| \leqslant L|x_1 - x_2| \tag{3}$$

для всех x_1 и x_2, принадлежащих $[a, b]$.

[3]Гуренко, В.В. Введение в теорию автоматов / В.В. Гуренко М.: МГТУ имени Н.Э. Баумана, 2013. – 63 с.

Если неравенство (3) выполняется с константой L, то оно справедливо и для всех $L' > L$. Поэтому для функции, удовлетворяющей условию Липшица, существует бесконечное множество констант L из (3). Также, из условия (3) следует непрерывность $f(x)$ на отрезке $[a, b]$.

Если функция $f(x)$ имеет на отрезке $[a, b]$ непрерывную производную, то она удовлетворяет на этом отрезке условию Липшица с константой

$$L = max_{[a,b]}|f'(x)|.$$

Если

$$z = z_0 + z_1 p + z_2 p^2 + \dots,$$

где, $z_j \in \{0, 1, \dots, p-1\}, j = 0, 1, 2, \dots,$ - каноническая запись целого p-адического числа $x \neq 0$, то

$$\operatorname{ord}_p z = \min\{j : z_j \neq 0\}$$

- показатель масимальной степени p, делящей z. По определению $\|z\|_p = p^{-ord_p z}$ есть p-адическая норма z, $\|0\|_p = 0$. Эта норма распространяется на все поле p-адических чисел $\mathbb{Q}_p$, которое есть поле частных кольца всех целых p-адических чисел $\mathbb{Z}_p$ и задает на Q_p метрику

$$d_p(u, v) = \|u - v\|_p,$$

относительно которой $\mathbb{Q}_p$ является пополнением пространства рациональных чисел $\mathbb{Q}$. Кольцо

$$\mathbb{Z}_p = \{u \in Q_p : \|u\|_p \leqslant 1\}$$

есть компакт в пространстве $\mathbb{Q}_p$, являющийся замыканием множества $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. Таким образом, $\mathbb{Z}_p$ есть сепарабельное компактное метрическое пространство. Множество всех различных смежных классов $a + p^k\mathbb{Z}_p$ по всем идеалам кольца $\mathbb{Z}_p$ образует базу соответствующего топологического пространства. Каждое множество $a + p^k\mathbb{Z}_p, a \in \mathbb{Z}_p$, $k = 0, 1, 2, \dots$, есть открытый (и одновременно замкнутый) шар радиуса p^{-k}.

Пространство $\mathbb{Z}_p$ наделяется мерой μ : положив $\mu\left(a+p^k\mathbb{Z}_p\right)=p^{-k}$, продолжим эту меру на все σ-кольцо множеств, порожденное компактами из $\mathbb{Z}_p$ (последние являются в точности всеми замкнутыми множествами в $\mathbb{Z}_p$). Это продолжение единственно, является мерой Хаара на $\mathbb{Z}_p$ и представляет собой неотрицательную σ-аддитивную регулярную нормированную борелевскую меру. Таким образом, μ - естественная вероятностная мера на пространстве $\mathbb{Z}_p$. Аналогично задается вероятностная мера на n-мерном пространстве $\mathbb{Z}_p^{(n)}$ как соответствующая нормированная мера Хаара.

Понятия целозначности и совместимости естественным образом переносятся и на функции нескольких переменных, норма (и, следовательно, метрика) пространства $\mathbb{Z}_p$ естественным образом индуцирует норму (и, следовательно, метрику) n-мерного пространства $\mathbb{Z}_p^{(n)}$: для $u=(u_1,\ldots,u_n)\in\mathbb{Z}_p^{(n)}$ полагаем

$$\|u\|_p=\max\left\{\|u_i\|_p\,,\quad i=1,2,\ldots,n\right\}.$$

Таким образом, функция

$$F=(f_1,\ldots,f_m):\mathbb{Z}_p^{(n)}\to\mathbb{Z}_p^{(m)}$$

совместима тогда и только тогда, когда она удовлетворяет условию Липшица с коэффиэнтом 1. В частности, все совместимые функции на $\mathbb{Z}_P$ непрерывны как p-адические функции.

Этот вывод является весьма важным для приложений. Именно, каждое машинное слово из теории автоматов, то есть слово некоторой конечной длины в алфавите $\{0,1\}$, можно интерпретировать как неотрицательное рациональное целое число, записанное в двоичной системе счисления. Тогда все вышеупомянутые поразрядные логические и машинные операции естественным образом продолжаются на все множество Z_2 целых 2 -адических чисел, представленных в канонической форме. Кроме того, на Z_2 продолжаются и вышеупомянутые арифметические операции. Все эти операции (то есть их продолжения на Z_2), а значит, и все их композиции, являются совместимыми функциями. Следовательно, все эти операции являются непрерывными на Z_2 функциями в 2 -адической метрике. Отметим, что сдвиг на m шагов двоичной записи числа в сторону младших разрядов, то есть операция $\lfloor\cdot 2^m\rfloor$

деления на 2^m с последующим отбрасыванием дробной части, тоже является непрерывной на Z_2, хотя и не совместимой функцией.

Заключение. В данной работе были собраны и изложены основные понятия, связанные с p-адическим анализом и его актуальность в современном мире. Были рассмотрены базовые понятия архимедовых и неархимедовых норм, метрических пространств, расширений полей и их свойств. Эти понятия необходимы для построения поля p-адических чисел и его сравнения с другими полями.

Также были рассмотрены основы теории автоматов, функции Липшица и их связь между собой. Функции, известные в теории автоматов как детерминированные, являются в точности теми функциями, которые удовлетворяют условию Липшица с коэффициентом 1. Данное свойство демонстрирует неархимедову сущность компьютерных операций.

В практической части задания был реализован детерминированный конечный автомат, для наглядной демонстрации его работы. Код реализации данной задачи на языке программирования Python приведен в приложении.