МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра компьютерной алгебры и теории чисел

Кластеризация в полях p-адических чисел

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Кононыхина Даниила Владимировича

Научный руководитель

зав. каф., к. ф.-м. н., доцент _____ А.М.Водолазов

подпись, дата

Зав. кафедрой

зав. каф., к. ф.-м. н., доцент _____ А.М.Водолазов

подпись, дата

Саратов 2019

Введение. К настоящему времени приложения математики были, в первую очередь, основаны на вещественном анализе, линейной алгебре над полем вещественных чисел, евклидовой и аналитической геометрии в вещественных линейных пространствах. Применение этих областей математики привело к впечатляющим достижениям в физике, химии, механике, и связанных с ними областях техники

Причем зачастую прогресс в физике был связан с развитием математики. В течение тысячелетий в физике использовалась евклидова геометрия. В каком-то смысле физическое пространство отождествлялось с этой геометрией. Например, так считал Кант. В 19 веке русский математик из Казани Николай Лобачевский показал, что существуют и другие геометрические модели — неевклидовы. Сейчас различные неевклидовы модели играют огромную роль в физике, особенно в теории относительности. Работы Лоренца, Минковского, Пуанкаре, Эйнштейна перевернули традиционные представления о геометрии физического пространства. Это была революция в физике. Заметим, математическая революция.

В математике известно семейство геометрических моделей с необычными свойствами, применение которых в естественных науках было весьма ограниченным. Наиболее ярким примером является теория неархимедовых числовых полей, основным примером которых являются поля p-адических чисел. Такие поля являются важнейшим инструментом в теории чисел и алгебраической геометрии. В 80-х годах в Математическом институте имени Стеклова группой И.Воловича было предложено использование p-адических чисел в физике. Совместно с академиком Владимировым в отделе математической физики был разработан соответствующий математический аппарат, приспособленный для приложений.

Первоначальной мотивировкой была следующая идея: наблюдаемы только целые и рациональные числа. Вещественное число, т.е. бесконечная десятичная дробь — это идеализация, которая в реальных прикладных задачах не встречается. Какова структура пространства на очень малых расстояниях? На Планковских масштабах происходят большие флуктуации метрики и топологии. Это приводит к тому, что аксиома измеримости Архимеда становится неприменимой, и И.Волович предложил использовать неархимедову

геометрию и p-адические числа. Сейчас достаточно сказать, что все обычные целые и рациональные числа являются также и p-адическими. Здесь p — простое число, $p-2,3,5,7,....$ Неархимедова геометрия имеет замечательные свойства. P-Адический шар состоит из конечного числа шаров меньшего радиуса, при этом нет пустот между меньшими шарами. В отличие от шаров в обычном эвклидовом пространстве, когда нельзя составить шар из конечного числа шаров меньшего радиуса так, чтобы не было пустот. Это свойство неархимедовой геометрии очень важно, т.к. оно означает, что здесь имеется естественная иерархическая структура. Имеется в виду, что меньшие шары строго подчинены большему шару.

В последние несколько десятилетий, начиная с 80-х годов XX века, мы были свидетелями первых применений p-адического анализа и ультраметрики в различных областях физики.

В частности, В.С.Владимиров и И.В.Волович разработали p-адические модели квантовой механики и теории струн, описывающие изменение геометрии пространства на планковских масштабах. Дж.Паризи предложил использовать ультраметрику в моделях спиновых стекол — примере сложной неупорядоченной системы. А.Ю.Хренников применял p-адический анализ к описанию моделей мышления. С.В.Козырев показал эквивалентность подхода Паризи в теории спиновых стекол и анализа p-адических псевдодифференциальных операторов, что дает надежду построения последовательного математического подхода в теории сложных систем. Также С.В.Козырев показал, что теория всплесков (вейвлетов), имеющая многочисленные прикладные применения, в частности, к сжатию и анализу изображений, нейросетям, анализу экспериментальных данных, связана с анализом p-адических псевдодифференциальных операторов. В.А.Аветисовым, С.В.Козыревым, и А.Х.Бикуловым разрабатывались подходы к описанию динамики биополимеров и макромолекул, основанные на ультраметрическом анализе.

Целью бакалаврской работы является определение полей p-адических чисел, рассмотрение кластеризации, а так же определение и основные свойства ультраметрических пространств.

Бакалаврская работа состоит из следующих пяти разделов:

1) P-адические числа.

2) Архимедовы и неархимедовы нормированные поля.

3) Кластеризация в полях.

4) Переход к p-адическим числам.

5) P-адические числа и кластеризация.

Основное содержание работы. Рассмотрим некоторые понятия. В первом разделе вводятся поля p–адических чисел и обсуждаются свойства ультраметрических пространств. Напомним, что кольцом R называется множество, на котором определены операции сложения и умножения, причём выполнены следующие свойства:

1) Сложение определяет на R структуру коммутативной группы;

2) Умножение ассоциативно

$$a(bc) = (ab)c, \forall a, b, c \in R$$

и согласовано со сложением по закону дистрибутивности

$$a(b + c) = ab + ac; (a + b)c = ac + bc, \forall a, b, c \in R,$$

в частности, $a0 = 0a = 0, \forall a \in R$.

Если умножение коммутативно (то есть $ab = ba, \forall a, b \in R$), то кольцо называется коммутативным. Если существует такой элемент $1 \in R$, что $1a = a1 = a, \forall a \in R$, то такой элемент называется единицей, а кольцо называется кольцом с единицей.

Коммутативное кольцо с единицей, на котором определена операция взятия обратного элемента, причём

$$aa^{-1} = a^{-1}a = 1, \forall a \in R$$

называется полем.

Поле имеет характеристику p, если p есть наименьшее такое натуральное число, что выполнено

$$pa = 0, \forall a \in R.$$

Если такого натурального p не существует, то поле будет иметь характеристику нуль.

Примеры полей:

1) Поле рациональных чисел Q;

2) Поле вещественных чисел R;

3) Поле комплексных чисел C;

4) Поле вычетов F_p по простому модулю p. В качестве элементов такого поля можно рассматривать числа $0, 1, ..., p-1$ со сложением и умножением по модулю p;

5) Поле $K(x)$ рациональных функций над числовым полем K (например, $K = Q, R, C$). Элементами такого поля являются рациональные функции над полем K, то есть дроби вида $\frac{P[x]}{Q[x]}$, PQ суть многочлены над полем K и Q не равен нулю. Поле вычетов имеет характеристику p, остальные перечисленные выше поля имеют характеристику нуль.

Любое рациональное число x можно единственным образом представить в виде несократимой дроби

$$x = p^y \frac{m}{n}$$

где p есть простое число, y есть целое число, m целое, n натуральное, p, m, n взаимно просты.

Определение 1.2. Полем F называют коммутативное кольцо с единицей, в котором каждый ненулевой элемент имеет мультипликативный обратный элемент (т.е. обратный по умножению).Другими словами, полем называют множество, которое является аддитивной абелевой группой; ненулевые же элементы этого множества образуют мультипликативную абелевую группу, и выполняется закон дистрибутивности.

По аналогии с группами число элементов поля называется порядком поля. Поля, порядки которых конечны, называются конечными полями. Конечные поля имеют наибольшее значение в теории кодирования.

Отметим некоторые свойства полей, вытекающие из их определения.

1. Для любого элемента поля $a * 0 = 0 * a = 0$.

2. Для ненулевых элементов a и b поля $a * b \neq 0$.

3. Для любых элементов a и b поля $a = b \neq 0$.

4. Если $a * b = a * c$ и $a \neq 0$, то $b = c$.

Определение 1.3. Целым p-адическим числом для произвольного простого p называется бесконечная последовательность $x = \{x_1, x_2, \ldots\}$ вычетов x_n по модулю p^n, удовлетворяющих условию $x_n \equiv x_{n+1} \bmod p^n$. Сложение и умножение целых p-адических чисел определяется как почленное сложение и умножение таких последовательностей. Для них непосредственно проверяются все аксиомы кольца.

Определение 1.4. P–адической нормой вышеприведенного рационального числа x называется число

$$|x|_p = p^{-y}$$

Таким образом, p–адическая норма измеряет, на какую степень p делится рациональное число, и норма тем меньше, чем больше эта степень, то есть последовательность $\{p^y\}, y \to +\infty$, будет стремиться к нулю в p–адической норме.

Определение 2.1. Пусть X – непустое множество. Расстояние, или метрика, на X – это отображение $d : X \times X \to R_+$, такое что для всех $x, y, z \in X$:

$(1) d(x, y) = 0 \Leftrightarrow x = y$;

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

$(3) d(x, y) \leq (x, z) + d(z, y)$ (неравенство треугольника).

Множество, снабженное метрикой, называется метрическим пространством. Метрика d называется неархимедовой (или ультраметрикой), если она удовлетворяет дополнительному условию

$(3') d(x, y) \leq max(d(x, z) + d(z, y))$ (сильное неравенство треугольника).

Соответствующее метрическое пространство называется ультраметрическим пространством.

Поскольку $max(d(x, z), d(z, y))$ не превосходит суммы $d(x, z) + d(z, y)$, из сильного неравенства треугольника $(3')$, вытекает неравенство треугольника (3).

Одно и то же множество X может образовывать много разных метрических пространств (X, d).

Определение 2.2. (i) Пусть X – метрическое пространство относительно метрики d. Последовательность $\{x_n : x_n \in X\}$ называется последова-

тельностью Коши если для любого $\varepsilon > 0$ существует число $N(\varepsilon)$, такое что $d(x_m, x_n) < \varepsilon$ для всех $m, n > N(\varepsilon)$, т.е.

$$\lim_{m,n\to\infty} d(x_m, x_n) = 0.$$

(ii) Если всякая последовательность Коши $\{x_n\}$ в метрическом пространстве X имеет предел в X, то X называется полным метрическим пространством.

(iii) Подмножество $M \subset X$ называется плотным в X, если каждый открытый шар $U_r^-(a) = \{x \in X : d(x, a) < r\}$ с центром в $a \in X$ содержит элемент из M, т.е. для каждого $a \in X$ и каждого $r > 0$ имеем $U_r^-(a) \cap M \neq \emptyset$.

Если X не является полным метрическим пространством, то его можно пополнить, непосредственным построением. Доказательство этой важной теоремы можно найти в многих учебниках функционального анализа. Доказательство заключается в явном построении пополнения $\hat{X}$ и метрики $\hat{d}$ на нем.

Определение 2.4. Пусть F – поле. Норма на F определяется как отображение $||\cdot|| : F \to R_+$, такое что для всех $x, y \in F$:

(1) $||x|| = 0 \Leftrightarrow x = 0$;

(2) $||xy|| = ||x||||y||$;

(3) $||x + y|| \leq ||x|| + ||y||$ (неравенство треугольника).

В общем случае, вместо аксиомы (2) используется следующая:

(2') $||xy|| \leq ||x||||y||$.

В этом случае функция $||\cdot||$ называется псевдонормой.

Норма называется неархимедовой, если она удовлетворяет дополнительному условию:

(3') $||x + y|| \leq max(||x||, ||y||)$ (сильное неравенство треугольника).

Определение 2.5. Две нормы $||x_1||$ и $||x_2||$ на нормированном поле F будем называть эквивалентными ($||x||_1 \sim ||x||_2$), если они индуцируют эквивалентные метрики.

Теорема 2.1. [1] Пусть $||x||_1 \sim ||x||_2$.

(i) Если норма $||x||_1$ тривиальна,то $||x||_2$ также тривиальна.

(ii) $||x||_1 < 1$ тогда и только тогда, когда $||x||_2 < 1; ||x||_1 > 1$ тогда и только тогда, когда $||x||_2 > 1; ||x||_1 = 1$ тогда и только тогда, когда $||x||_2 = 1$.

Теорема 2.2. [1] Пусть $||x||_1$ и $||x||_2$ – две нормы на поле F. $||x||_1 \sim ||x||_2$ тогда и только тогда, когда существует положительное вещественное число α, такое что

$$||x||_2 = ||x||_1^{\alpha}, \forall x \in F. \tag{1}$$

Теорема 2.3. [3] Для того, чтобы норма $||\cdot||$ была неархимедовой необходимо и достаточно, чтобы $||n|| \leq 1$ для любого $n \in Z$.

Следствие 2.1. Норма $||\cdot||$ будет неархимедовой в том и только в том случае, если $\sup\{||n|| : n \in Z\} = 1$.

Теорема [3] показывает различие между архимедовой и неархимедовой нормами. Согласно этой теореме, норма является архимедовой тогда и только тогда, если она удовлетворяет свойству (аксиоме) архимедовости: для любого $x, y \in F, x \neq 0$, существует такое $n \in N$, что $||nx|| \geq ||y||$.

Действительно, если $||y|| > ||x||$, то из архимедовости нормы вытекает существование такого $n \in N$, что $||n|| > ||y||/||x|| > 1$, т.е. норма является архимедовой. Обратно, если норма $||\cdot||$ – архимедова, то существует такое $n \in N$, что $||n|| > 1$. Значит, $||n||^k \to \infty$, при $k \to \infty$. Следовательно, для любого $x, y \in F, x \neq 0$, существует такое k, что $||n^k|| > ||y||/||x||$. То есть имеет место свойство архимедовости $||n^k x|| > ||y||$.

Если норма неархимедова, то для любого $n \in Z$ будем иметь $||nx|| \leq ||x||$

Из неархимедовости нормы вытекают некоторые необычные следствия.

Предложение 2.2. Если поле F неархимедово, то для

$$x, y \in F||x|| \neq ||y|| \Rightarrow ||x + y|| = max||x||, ||y||$$

Значит, всякий треугольник в ультраметрическом пространстве является равнобедренным, а длина его основания не превосходит длины боковых сторон.

Определение 2.6.. Пусть p - простое число. Определим p-адический порядок $ordp(x)$ рационального числа $x \in Q$ следующим образом:

(i) если $x \in Z$, то $ord_p(x)$ равен высшей степени p, которая является делителем x;

(ii)если $x = a/b$, где $a, b \in Z$, то $ord_p(x) = ord_p(a) - ord_p(b)$. P-адический

порядок числа $x \in Q$ называется также p-адической аддитивной абсолютной величиной и обозначается $v_p(x)$.

(iii)Положим $ord_p(0) = +\infty$.

Теорема 2.4. (Теорема Островского) Всякая нетривиальная норма $||\cdot||$ на поле Q эквивалентна либо вещественной норме $|\cdot|$, либо одной из p-адических норм $|\cdot|_p$.

Определние 5.1. P-адические числа. Пусть p - это простое число, и K - это область, которая конечно задана на поле Q, состоящих из рациональных p-адических чисел. Называем элементы K простых p-адических чисел. K - это нормированное поле, норма которого $||_K$ выходит за рамки p-адической нормы $||_p$ на Q_p. Пусть $O_K = \{x \in K \mid |x|_K \leq 1\}$ обозначим локальным кольцом целых .

Это максимальный идеал $m_K = \{x \in K \mid |x|_k \leq 1\}$ созданный с помощью стандартизации π. Это имеет свойство $v(\pi) = \frac{1}{e}$, где $e \in N$ это последствия степени K/Q_p. Все элементы $x \in K$ имеют π - адическое распространение

$$x = \sum_{i \geq -m} \alpha_i \pi^i$$

С коэффициентом α_i в некотором множестве $R \subseteq K$ представленном в виде остатка $O_K/m_K \cong F_{p^f}$ в случае q=p, выбор $R + \{0, 1, ..., p-1\}$ вполне часто сделан.

Под X будет всегда подразумеваться конечный набор данных, взятых из K.

Определние 5.2.P-адические кластеры. Диск в некотором конечном множестве $\subseteq K$ это подмножество вида

$$\{x \in X \mid |x - a|_K < \varepsilon\}$$

Для некоторого $a \in X$ и $\varepsilon > 0$. В частности, любое единственное $\{x\} \subseteq X$ это диск в X. Свойство кластера из подмножества с состоящим из p-адических данных $X \subseteq K$ представлено в том, что для любого $a \in C$ и учитывая, что справедливо

$$|x - a|_K < \mu(C) \in x \in C,$$

где

$$\mu(C)max\{|x-y|_K|x,y\in C\}$$

Это диаметр кластера. Как следствие, кластер - это объединение дисков в X. Также назовём диск X вертикальным кластером, потому что дендрограмма для X, это вершина отвечающая за эти кластеры, которые являются (не одноэлементными) дисками.

Заключение. Данная тема является достаточно актуальной, так как с точки зрения приложений, потребность изучения p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические динамические системы дают широкий класс превосходных генераторов псевдослучайных чисел, которые играют столь важную роль в криптографии, а также в других прикладных областях, таких как численный анализ и компьютерное моделирование. В данной работе были рассмотрены p-адические числа, являющимися элементами расширения поля рациональных чисел, а также были рассмотрены и построены их поля. Так же была рассмотрены и изучена кластеризация в полях p-адических чисел.