УДК 004

ИССЛЕДОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ АППРОКСИМАЦИИ ФУНКЦИЙ С ПОМОЩЬЮ ОРТОГОНАЛЬНЫХ БАЗИСОВ И ИХ ИСПОЛЬЗОВАНИЕ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

© 2024 Ю. А. Андрусенко[1], О. А. Евстафиади[2], Н. С Бойков[3], А. М. Афанасьев[3]

[1] старший преподаватель
e-mail: iuandrusenko@ncfu.ru
Северо-Кавказский федеральный университет, Ставрополь
[2] учитель математики
e-mail: ksyev1977@gmail.com
Гимназия 24, Ставрополь
[3]студент,
e-mail: nikitaboickov4@gmail.com
Северо-Кавказский федеральный университет, Ставрополь

В статье рассматриваются методы аппроксимации функций с помощью ортогональных базисов и их применение в системах защиты информации. Основное внимание уделяется теоретическим аспектам аппроксимации, включая понятие ортогонального базиса и методы аппроксимации, такие как полиномиальная аппроксимация и интерполяция. Описаны различные подходы, включая интерполяцию Лагранжа, интерполяцию Ньютона и метод наименьших квадратов. Рассматриватся также аппроксимация тригонометрическими функциями, такими как ряды Фурье, и использование специальных функций, включая многочлены Чебышева, Лежандра и Эрмита. Приводятся примеры программной реализации этих методов на языке C++ с использованием специализированных библиотек для повышения эффективности вычислений. Особое внимание уделено применению методов аппроксимации в криптографии и стеганографии для обеспечения безопасности данных. Описаны преимущества использования аппроксимационных методов для создания стойких к атакам криптографических ключей и скрытия информации.

Ключевые слова: аппроксимация функций, ортогональный базис, интерполяция Лагранжа, интерполяция Ньютона, метод наименьших квадратов, ряды Фурье, многочлены Чебышева, многочлены Лежандра, криптография, стеганография.

RESEARCH AND SOFTWARE IMPLEMENTATION METHODS APPROXIMATION FUNCTIONS USING ORTHOGONAL BASES AND THEIR USE IN THE FIELD OF INFORMATION SECURITY

© 2024 Yu.A. Andrusenko[1], O. A. Evstafiadi [2], N.S. Boykov[3], A.M. Afanasiev[3]

[1]Senior Lecturer, North Caucasus Federal University, Stavropol
e-mail: iuandrusenko@ncfu.ru
[2] mathematics teacher, Gymnasium 24, Stavropol
e-mail: ksyev1977@gmail.com
[3] student, North Caucasus Federal University
e-mail: nikitaboickov4@gmail.com

The article examines methods of function approximation using orthogonal bases and their application in information security systems. The focus is on the theoretical aspects of approximation, including the concept of an orthogonal basis and approximation methods such as polynomial approximation and interpolation. Various approaches are described, including Lagrange interpolation, Newton interpolation, and the least squares method. The article also discusses approximation with trigonometric functions, such as Fourier series, and the use of special functions, including Chebyshev polynomials, Legendre polynomials, and Hermite polynomials. Examples of software implementation of these methods in C++ are provided, utilizing specialized libraries to enhance computational efficiency. Particular attention is given to the application of approximation methods in cryptography and steganography to ensure data security. The advantages of using approximation methods for creating attack-resistant cryptographic keys and hiding information are described.

Keywords: Function approximation, orthogonal basis, Lagrange interpolation, Newton interpolation, least squares method, Fourier series, Chebyshev polynomials, Legendre polynomials, cryptography, steganography.

Аппроксимация функций позволяет решать широкий спектр задач, включая моделирование сложных систем, обработку сигналов и численный анализ. В данной работе рассматриваются теоретические аспекты, связанные с аппроксимацией функции, понятие ортогонального базиса, а также методы аппроксимации, основанные на использовании ортогональных базисов. Обсуждаются приложения этих методов в системах защиты информации, таких как криптография и стеганография. Криптографические алгоритмы, использующие аппроксимационные методы, обеспечивают высокую стойкость к атакам, а стеганографические методы позволяют передать информацию, скрывая сам факт передачи. Исследуется программная реализация этих методов на языке C++, в том числе с использованием специализированных библиотек для повышения эффективности вычислений.

Понятие и основные методы аппроксимации функции. Аппроксимация функции – это процесс приближения одной функции к другой, более простой. Эта функция позволяет легче анализировать или вычислять исходную. Разнообразие методов аппроксимации функции объясняется рядом факторов. К ним отнесем природу задачи, точность аппроксимации и вычислительные ресурсы. Рассмотрим основные методы аппроксимации функции. Полиномиальная аппроксимация подразумевает использование многочленов (полиномов) для приближения функции. К полиномиальной аппроксимации отнесем интерполяцию Лагранжа, интерполяцию Ньютона, метод наименьших квадратов. Интерполяция – это метод математического анализа, который используется для построения новой функции, проходящей через заданные точки данных [1]. При интерполяции Лагранжа строится многочлен, известный также как интерполяционный многочлен Лагранжа, который проходит через определенные заданные точки. Аппроксимация функции ищется в виде:

$$g(x; a_1, \dots, a_n) = \sum_{i=1}^{n} a_i \varphi_i(x), \#(1)$$

Значения коэффициентов a_i определяются из условия совпадения с аппроксимируемой функцией в узлах интерполяции. Интерполирование Лагранжа представляет собой случай интерполирования многочленами, не прибегая к непосредственному решению системы.

$$g_n(x) \equiv L_n(x) = \sum_{i=1}^{n} f(x_i) \prod_{j \neq 1} \frac{x - x_j}{x_i - x_j}, \#(2)$$

(2) носит название «интерполяционный многочлен Лагранжа».

При интерполяции Ньютона используется метод разделенных разностей для построения интерполяционного многочлена в форме Ньютона. При помощи данного метода и ряда математических преобразований приходим к следующей записи интерполяционного многочлена (2):

$$L_n(x) = f(x_1) + f(x_1; x_2)(x - x_1) + \cdots + f(x_1; \ldots; x_n)(x - x_1) \ldots (x - x_{n-1}), \#(4),$$

который и носит название интерполяционного многочлена Ньютона. Метод наименьших квадратов – один из методов регрессивного анализа для оценки неизвестных величин по результатам измерений, содержащих случайные ошибки. Аппроксимация тригонометрическими функциями включает ряды Фурье и дискретное преобразование Фурье. Ряд Фурье функции $f(x)$ на интервале [-L, L] представляют в следующем виде [4]:

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n cos\left(\frac{n\pi x}{L}\right) + b_n sin\left(\frac{n\pi x}{L}\right)\right), \#(5).$$

Дискретное преобразование Фурье может применяться при решении большого количества прикладных задач [5]. Данный способ аппроксимации имеет следующий вид:

$$f(x) \approx \sum_{-\frac{N}{2}<q<\frac{N}{2}} A_q \; exp \; exp\,\{2\pi i q x\} \; \#(6)$$

и носит название тригонометрической интерполяции, а представленное соотношение называют конечным или дискретным рядом Фурье. Аппроксимация с использованием специальных функций включает в себя функции Чебышева, функции Лежандра, Эрмита. Многочлены Чебышева используются для минимизации максимальной ошибки аппроксимации. Многочлены Чебышева $T_n(x)$, где $n \geq 0$, определяются соотношениями:

$$T_0(x) = 1, \qquad T_1(x) = x \; T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \; \#(7).$$

Решение задач математической физики нередко исследуют при помощи поиска их разложения по ортогональным функциям, в частности по ортогональным многочленам. Многочлены Лежандра являются ортогональными многочленами, используемыми для аппроксимации функций на интервале [-1, 1]. Они обладают свойством ортогональности относительно скалярного произведения [3]:

$$\int_{-1}^{1} L_m(x)L_n(x)dx = 0, \;\; \text{для } m \neq n \#(8),$$

где $L_n(x)$ – многочлен Лежандра степени n. Многочлен Лежандра имеет вид:

$$L_n(x) = \frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2 - 1)^n \#(9).$$

Многочлены Эрмита являются ортогональными многочленами, применяемыми для аппроксимации функций, особенно в задачах, связанных со статистикой. Они ортогональны относительно весовой функции e^{-x^2}

$$\int_{-\infty}^{\infty} H(x)H_n(x)e^{-x^2}dx = 0, \;\; \text{для } m \neq n \#(10),$$

где $H_n(x)$ – многочлен Эрмита степени n. Многочлен Эрмита имеет вид:

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n}(e^{-x^2}) \#(11).$$

Аппроксимация с использованием полиномов Лежандра и Эрмита предоставляет мощные инструменты для приближения сложных функций. Методы аппроксимации являются фундаментальными инструментами в математике и прикладных науках. Они позволяют заменить сложные функции их более простыми аналогами, что значительно облегчает их анализ и использование в вычислительных задачах, в чем позволяют убедиться рассмотренные методы [6].

Понятие ортогонального базиса. Базис – это набор векторов, с помощью которых можно представить любой вектор в данном пространстве. Ортогональный базис векторного пространства V – это базис, состоящий из ортогональных векторов. Два вектора называются ортогональными, если они перпендикулярны друг другу. Если каждый вектор базиса имеет единичную длину, то такой базис называется ортонормированным. Для построения ортогонального базиса из произвольного набора векторов используют процесс ортогонализации Грама-Шмидта. Этот процесс берет исходный набор векторов и шаг за шагом преобразует его в набор ортогональных векторов. Процесс ортогонализации заключается в вычитании проекции на каждый из предыдущих векторов. Операции над векторами и матрицами в ортогональном базисе часто более устойчивы численно, что уменьшает ошибки округления и повышает точность вычислений [2].

Методы аппроксимации функции с помощью ортогонального базиса. Аппроксимация функций с помощью ортогональных базисов включает различные методы, которые используют ортогональные функции для представления сложных функций в удобной форме. Ряды Фурье представляют функцию в виде суммы синусоидальных функций, которые являются ортогональными на заданном интервале:

$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n cos\left(\frac{n\pi x}{L}\right) + b_n sin\left(\frac{n\pi x}{L}\right)) \#(12).$$

Многочлены Чебышева минимизируют максимальную ошибку аппроксимации и используются в задачах приближения на отрезке $[-1,1]$. Ряд Чебышева:

$$f(x) \approx a_0 + \sum_{n=0}^{N} (\mathrm{c}_n T_n(x)), \#(13),$$

где $T_n(x) = cos\,(narccos(x))$ – многочлен Чебышева, а коэффициенты c_n определяются:

$$c_n = \frac{2}{\pi}\int_{-1}^{1} \frac{f(x)T_n(x)}{\sqrt{1-x^2}} dx \#(14).$$

Многочлены Лежандра используются для аппроксимации функций на интервале $[-1,1]$ и также являются ортогональными. Ряд Лежандра:

$$f(x) \approx a_0 + \sum_{n=0}^{N} (\mathrm{c}_n L_n(x)), \#(15),$$

где $L_n(x)$ – многочлен Лежандра степени n, а коэффициенты a_n определяются:

$$a_n = \frac{2n+1}{2}\int_{-1}^{1} f(x)L_n(x)dx \#(16).$$

Многочлены Эрмита применяются для задач аппроксимации функций с весовой функцией. Ряд Эрмита имеет следующий вид:

$$f(x) \approx \sum_{n=0}^{N} (b_n H_n(x) e^{-\frac{x^2}{2}}), \#(17),$$

где $H_n(x)$ – многочлен Эрмита степени n, а коэффициенты b_n определяются:

$$\mathrm{b_n} = \int_{-\infty}^{\infty} \mathrm{f(x) H_n(x) e^{-\frac{x^2}{2}} dx} \#(18).$$

Дискретное преобразование Фурье используется для аппроксимации дискретных функций и сигналов, представляя их как сумму синусоидальных функций:

$$\mathrm{X_k} \approx \sum_{\mathrm{n=0}}^{\mathrm{N-1}} (\mathrm{x_n e^{-\frac{i2\pi kn}{N}}}), \mathrm{k} = 0, 1, \dots, \mathrm{N} - 1, \#(19),$$

где $\mathrm{x_n}$ – исходные данные, а $\mathrm{X_k}$ – коэффициент преобразования.

Программная реализация методов аппроксимации функции с помощью ортогонального базиса. В современных системах защиты информации методы аппроксимации функций с помощью ортогональных базисов находят широкое применение. Эти методы обеспечивают высокую степень конфиденциальности, целостности и подлинности данных. Реализация рядов Фурье в C++ требует вычисления интегралов для нахождения коэффициентов an и bn. Эти вычисления можно выполнять с использованием численных методов интегрирования, таких как метод трапеций или метод Симпсона. Важно учитывать периодичность функции и дискретизацию интервала для точных вычислений. Не стоит забывать про поддержание точности и стабильности внедренной информации, особенно при изменении данных. Для реализации аппроксимации многочленами Чебышева необходимо вычислить сами многочлены и соответствующие интегралы для нахождения коэффициентов. Это можно сделать с помощью рекурсивных отношений для полиномов и численных методов интегрирования для вычисления коэффициентов. Реализация вычисления полиномов и их обратного преобразования может быть сложной задачей. Аппроксимация с использованием полиномов Лежандра также требует вычисления ортогональных многочленов и интегралов. В C++ это можно реализовать, используя рекурсивные формулы для полиномов Лежандра и численные методы для интеграции. Важно правильно обозначить интервал. Реализация рядов Эрмита требует вычисления полиномов Эрмита и интегралов с весовой функцией. Это сложнее, так как интегралы берутся по всему интервалу (–∞, ∞). В C++ для вычисления таких интегралов могут использоваться методы Гаусс-Эрмитова квадратурного интегрирования. Реализация дискретное преобразование Фурье в C++ проста благодаря существованию библиотек, FFTW, которые эффективно реализуют как дискретное преобразование Фурье в C++, так и его быстрый вариант. Эти библиотеки хорошо оптимизированы и позволяют быстро производить преобразования. Важно оптимизировать вычисления для эффективной работы с большим объемом данных.

Методы защиты информации на основе понятий об аппроксимации функции с помощью ортогонального базиса. В современных системах защиты информации методы аппроксимации функций с помощью ортогональных базисов находят широкое применение в криптографии и стеганографии. Криптография является важной областью защиты информации, направленной на обеспечение

конфиденциальности, целостности и подлинности данных. Генерация ключей основана на использовании ортогональных функций для создания случайных и непредсказуемых последовательностей. Гомоморфная система шифрования представляет собой четыре вероятностных полиномиальных алгоритма: генерация ключа, шифрование, расшифровка, гомоморфное вычисление. В данном случае представление функции является важным вопросом. Полностью гомоморфное шифрование используется не только в многочисленных сценариях, где выгодно хранить все данные в зашифрованном виде и выполнять вычисления над зашифрованными данными, но и для решения ряда других задач в криптографии. Один из современных подходов заключается в определении полиномов как последовательностей, состоящих из конечного числа ненулевых элементов. Полиномы могут быть сложены и умножены, причем эти операции естественным образом определены, если их коэффициенты образуют алгебраическую структуру, такую как кольцо. Ортогональные преобразования, такие как дискретное преобразование Фурье, могут применяться для преобразования данных перед шифрованием, добавляя дополнительный уровень сложности для потенциального злоумышленника. Использование ортогональных преобразований делает криптографические алгоритмы более стойкими к различным атакам, включая линейный криптоанализ и дифференциальный криптоанализ. Стеганография – это метод скрытия информации внутри других данных, таких как изображения, аудиофайлы или текстовые документы, так чтобы скрытая информация оставалась незаметной для посторонних. Ряды Фурье могут использоваться для разложения аудиосигнала на частотные компоненты. Скрытая информация внедряется в амплитуды или фазы определенных частотных диапазонов. Методы аппроксимации могут быть использованы для создания стеганографических алгоритмов, скрывающих информацию в текстах путем изменения характеристик символов или слов.

Таким образом, методы аппроксимации функций с помощью ортогональных базисов играют ключевую роль в современных системах анализа данных и защиты информации. Они позволяют эффективно и точно моделировать сложные функции, анализировать данные и скрывать информацию, обеспечивая высокую степень безопасности и надежности. Аппроксимация функций с использованием многочленов, рядов Фурье и других методов позволяет решать широкий круг задач в математике и прикладных науках. Полиномиальная аппроксимация, интерполяция и тригонометрические ряды являются основными подходами, которые используются для представления сложных функций в удобной и вычислительно эффективной форме. Ортогональные базисы обеспечивают математическую основу для многих методов аппроксимации. Ортогональные векторы в базисе упрощают вычисления и повышают численную устойчивость алгоритмов. Криптография и стеганография с использованием методов аппроксимации и ортогональных базисов предоставляют мощные средства для обеспечения безопасности данных. Эти методы позволяют создавать сложные и устойчивые к атакам криптографические ключи, скрывать информацию в мультимедийных данных.

Библиографический список

1. *Бахвалов, Н. С., Жидков, Н. П., Кобельков, Г. М.* Численные методы. – Москва: БИНОМ, 2015. – 639 с.

2. *Езерский, В. В.* Методы аппроксимации функций. Москва – Омск: СибГУФК, 2011. – 52 с.

3. *Житников, В. П., Шерыхалина, Н. М., Камалова, Э. И.* Аппроксимация с помощью ортогональных функций // Информационные технологии интеллектуальной поддержки принятия решений. – Уфа, 2018.

4. *Мудров, А. Е.* Численные методы для ПЭВМ. – Томск: РАСКО, 2005. – 272 с.

5. *Прохоров, С. А., Газетова, Я. В.* Аппроксимативный корреляционно-спектральный анализ в спектральном базисе Бесселя // Проблемы автоматизации и управления в технических системах: материалы международной научно-технической конференции / ИИЦ ПГУ. – Пенза, 2009. – С. 383–387.

6. *Ростовцев А., Богданов А., Михайлов М.* Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец // Проблемы информационной безопасности. Компьютерные системы. – 2011. – №. 2. – С. 76–85.