УДК 502.2:519.8

С.А. Велянський

ВИКОРИСТАННЯ ОРТОГОНАЛЬНИХ ФІНІТНИХ ФУНКЦІЙ У КОДУВАННІ

Вінницький національний технічний університет

Анотація

Аналізується використання ортогональних фінітних функцій та симетричного алгоритму шифрування, заснованого на їх використанні.

Ключові слова: ортогональні фінітні функції, чисельне моделювання, шифрування.

Abstract

The use of orthogonal finite functions and a symmetric encryption algorithm based on their use are analyzed.

Keywords: orthogonal finite functions, numerical modeling, encryption.

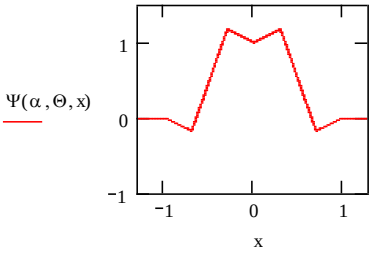
Вступ

Використання ортогональних фінітних функцій дозволяє знизити розмірність системи сіткових рівнянь за рахунок виключення вузлових значень частини невідомих функцій в аналітичній формі до розв’язання системи на комп’ютерах. При цьому зберігаються всі переваги алгоритмів чисельних методів, пов'язаних з використанням базисних функцій, що мають компактні носії. Крім того, застосування ортогональних фінітних функцій дає можливість дослідження збіжності змішаних чисельних методів із застосуванням класичної методики доказу збіжності різницевих схем і методики доказу збіжності методу Ритца. У лінійній або геометрично нелінійній теорії пружності варіаційний принцип не має переваг перед іншими методами. Принцип стаціонарності функціонала не вимагає виконання цієї операції й тому відіграє більш значну роль у фізично нелінійній теорії пружності. В існуючих комплексах програм, призначених для моделювання конструкцій і для дослідження їх напружено-деформованого стану, використовується в якості основного варіаційний принцип Лагранжа. Він не дозволяє одержувати розв’язок для переміщень, деформацій і напруг одного рівня якості. Застосування в цих комплексах програм змішаних варіаційних принципів, що дають високоякісні наближені розв’язки як для переміщень, так і для деформацій і напружень, є не правилом, а виключенням - для окремих типів завдань. Ці застосування визнають перспективність цього напрямку як основного з універсальних відповідних чисельних методів дослідження математичних моделей. Комплекси програм, що використовують змішані варіаційні принципи в якості основних, практично відсутні. Причина полягає в наступному. Ортогональні вейвлети з компактними носіями й ортогональні фінітні функції, що роблять такі комплекси програм конкурентоспроможними, створено порівняно недавно, тому їхнє використання тільки починається.

$$f_i(x) = \begin{cases} 2\alpha(x_{i-1} - x)/h, & x \in [x_{i-1}, x_{i-1} + h/2], \\ 2(\alpha + 1)(x - x_i)/h + 1, & x \in [x_{i-1} + h/2, x_i], \\ 2(\beta - 1)(x - x_i)/h + 1, & x \in [x_i, x_i + h/2], \\ 2\beta(x_{i+1} - x)/h, & x \in [x_i + h/2, x_{i+1}], \\ 0, \ x \notin [x_{i-1}, x_{i+1}]. \end{cases}$$

У статті пропонується симетричний алгоритм шифрування, заснований на використанні ортогональних фінітних функцій (ОФФ). Теорія ОФФ та її застосування в числових алгоритмах викладена в алгоритмах [1, 2, 3]. Основна ідея запропонованого алгоритму полягає в апроксимації полінома з використанням функцій ОФФ-базиса. Після подачі інформаційного блоку у вигляді полінома, він апроксимується за допомогою ОФФ-базиса у вибраних вузлах сітки, потім обчислити значення ОФФ-апроксимації з урахуванням довільно заданого значення ключа, а потім результат шифрування буде подано у вигляді блоку ОФФ-апроксимації.

$$\Phi(\alpha,\Theta,x) := \begin{cases} 0 \text{ if } x > 1 \\ \left[\frac{(x-1)\cdot\alpha}{\Theta}\right] \text{ if } 1-\Theta \le x \le 1 \\ \frac{-(1+2\cdot\alpha)\cdot(x-0.5)}{1-2\cdot\Theta} + 0.5 \text{ if } \Theta \le x \le 1-\Theta \\ \left(\frac{\alpha\cdot x}{\Theta}+1\right) \text{ if } 0 \le x \le \Theta \end{cases}$$



Оскільки координати точок, у яких здійснено апроксимацію, відомі, то можна відновити початковий вигляд полінома. Використання алгоритму шифрування на основі ортогональних фінітних функцій значно підвищує стійкість шифрування.

Висновки

Побудовано системи ортогональних функцій, адаптованих до широкого класу задач Побудований метод суттєво відрізняється від методів, що ґрунтуються на інших системах ОФФ. Головна відмінність полягає в тому, що розглянуті функції задовольняють не одній умові ортогональності $\langle f(x), f(x-1)\rangle = 0$, а декільком умовам ортогональності за рахунок чого може бути використана для побудови математичних моделей об'єктів, у яких окремому елементу відповідає одна сіткова ОФФ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Леонтьев В.Л. Ортогональные финитные функции и численные методы —Ульяновск: УлГУ, 2003. — 178 с.

2. *Леонтьев В.Л., Лукашанец Н.Ч.* Сеточные базисы ортогональных финитных функций // Журнал вычислительной математики и математической физики. — 1999. —т.39, №7. — с. 1158

3. *Леонтьев В.Л.* Об ортогональных финитных функциях и о численных методах, связанных с их применением // Обозрение прикладной и промышленной математики. — 2002. — т.9, №3. — с. 497

4. Клочко В.І. Вища математика. Диференціальні рівняння (з комп'ютерною підтримкою). Навч. посібник / В.І. Клочко, З.В. Бондаренко. – Вінниця: ПП «ТД «Едельвейсі К», 2013. – 252 с.

5. Михалевич В.М. Maple. Комп'ютерна підтримка курсу вищої математики в технічному вузі. Частина 1. Лінійна й векторна алгебра. Аналітична геометрія. Навч. посібник / В.М. Михалевич. – Вінниця: ВНТУ, 2004. – 111 с.

Науковий керівник Віталій Іванович Клочко – доктор педагогічних наук, професор кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: klochko@vntu.edu.ua;

Сергій Андрійович Велянський – студент групи СП-19б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця;

Klochko Vitaliy I. – Dr. Sc. (Eng), Professor of mathematics, Vinnytsia National Technical University, Vinnytsia;

Velianskiy Sergiy A. – D Vinnytsia National Technical University, Vinnytsia.