Аналіз ефективності ортогональних базисів Ґалуа у задачах зменшення надлишковості

Превисокова Н.В.

Доц. кафедри інформатики, Прикарпатський національний університет імені Василя Стефаника
вул. Шевченка 57, м. Івано-Франківськ, Україна, natvolo@rambler.ru

***Анотація* — Побудовано ортогональні системи функцій із рекурсивних функцій Ґалуа, які породжуються різними векторами над полями GF(2). Досліджено ефективність застосування дискретного ортогонального перетворення в базисах функцій Ґалуа в задачах зменшення надлишковості одновимірних інформаційних потоків. Здійснено порівняльний аналіз з відомими перетвореннями Уолша та Хаара. Визначено породжуючі вектори і відповідні базиси перетворення, застосування яких забезпечує максимальний ступінь зменшення надлишковості.**

Ключові слова: системи функцій Ґалуа, дискретне ортогональне перетворення, поле Ґалуа, породжуючий поліном .

Analysis of efficiency the orthogonal Galois basis in data compression

Prevysokova N.V.

Doc., Department of Computer Science, Vasyl Stefanyk Precarpathian National University
Shevchenko str., 57, Ivano-Frankivsk, Ukraine, natvolo@rambler.ru

***Abstract* — It is constructed orthogonal functions system from the recursive Galois functions, which are generated by different vectors above prime Galois field GF(2). The using efficiency of the discrete orthogonal transform in Galois functions bases is researched in the problems of compression one-dimensional signals. The comparative analysis of known Walsh and Haar transforms is made. In every Galois field of the fixed order n it is find generating vector and proper transform base, application of which provides the maximum data compression.**

Keywords: Galois functions system, discrete orthogonal transform, Galois field, generating polinomial, data compression.

Вступ

Методи аналізу, фільтрації, кодування та зменшення надлишковості інформаційних потоків на основі дискретних ортогональних перетворень широко застосовуються у галузі цифрової обробки інформації. Обробка результатів дискретних перетворень дозволяє ефективно розв'язувати задачі зменшення надлишковості при зберіганні та передаванні даних [1 – 3].

У задачах зменшення надлишковості інформації використовуються дискретні ортогональні перетворення Фур'є, Уолша, Хаара [1, 2], Ґалуа [3]. Характерною особливістю базисів Ґалуа є властивість рекурсивного формування [3] значень базисних функцій, що дозволяє спростити обчислення шляхом використання циркулянтних перетворень.

Перша функція базису Ґалуа формується за правилом, що визначається породжуючим поліномом [3]. Кожна наступна функція базису утворюється із попередньої.

Відомо, що вибір породжуючого поле Ґалуа полінома не істотний, оскільки всі скінченні поля одного і того ж порядку ізоморфні. Водночас, при розв'язуванні задач зменшення надлишковості інформації з використанням ортогонального перетворення в системах фунцій Ґалуа [4] не розв'язаною залишається проблема вибору породжуючого полінома для забезпечення найефективнішого розв'язування задачі. Це зумовило необхідність побудови ортогональних базисів перетворень Ґалуа, породжених різними векторами і дослідження ефективності їх застосування в задачах зменшення надлишковості інформації.

Основна частина

Базисом дискретного перетворення в системах функцій Ґалуа є повна ортогональна система $\{G(n,\theta,i)\}$ [4], одержана із рекурсивної системи функцій Ґалуа.

Рекурсивні системи функцій Ґалуа $\{Gal(n,\theta,i)\}$ [3], утворюються відповідно до породжуючого вектора поля Ґалуа $GF(2^n)$. Наприклад, у полі $GF(2^3)$ із початкових векторів $(g_0,g_1,g_2)=(1,1,1)$ і $(g_0,g_1,g_2)=(0,0,0)$ формуються рекурсивні послідовності $g_0,g_1,g_2,\ldots g_{2^n-1}$ за правилами, які відповідають наступним породжуючим векторам: $(1,0,1,1)\rightarrow g_{j+3}=g_j\oplus g_{j+2}$; $(1,1,0,1)\rightarrow g_{j+3}=g_j\oplus g_{j+1}$

, $(1,0,1,\bar{1}) \to g_{j+3} = \overline{g_j \oplus g_{j+2}}$; $(1,1,0,\bar{1}) \to g_{j+3} = \overline{g_j \oplus g_{j+1}}$, $j = 0,1,\ldots 2^n - 2$.

Функції рекурсивної системи $\{Gal(n,\theta,i)\}$ в точках $\theta = j/N$ інтервалу $\theta \in [0;1)$ визначаються із послідовності $\{g_j\}$ та доозначаються до неперервних на інтервалах $\theta \in [\frac{j}{N}; \frac{j+1}{N})$

$$Gal(n,\theta,0) = Gal(n,\, j/N\,,0) = 1 - 2g_j,$$
$$Gal(n,\theta,i+1) = Gal(n,\theta+1/N,i).$$

де $n = 1,2,\ldots$ – порядок функції, $N = 2^n$.

Із рекурсивної системи $\{Gal(n,\theta,i)\}$ будується модифікована система $Gal_m(n,\theta,i)$

$$Gal_m(n,\theta,0) = 1,$$
$$Gal_m(n,\theta,i) = Gal(n,\theta,i-1), \quad (1)$$

$i = 1,\ldots 2^n - 1$.

Ортогональні функції $\{G(n,\theta,i)\}$ [4] одержують застосуванням процедури ортогоналізації Грама - Шмідта [2] до функцій модифікованої системи

$$G(n,\theta,0) = 1,$$
$$G(n,\theta,k+1) = Gal_m(n,\theta,k+1) - \sum_{i=0}^{k} \frac{\langle Gal_m(n,\theta,k+1), G(n,\theta,i)\rangle}{\|G(n,\theta,i)\|_{L_2}^2} G(n,\theta,i), \quad (2)$$

де $k = 0,1,\ldots,N-1$, $\|G(n,\theta,i)\|_{L_2}^2$ – норма в просторі інтегровних з квадратом функцій $L_2[0,1)$, $\langle Gal_m(n,\theta,k+1), G(n,\theta,i)\rangle$ – скалярний добуток.

Дискретне матричне ортогональне перетворення Ґалуа [4] одновимірного інформаційного потоку $\{X(0), X(1),\ldots,X(N-1)\}$ визначається як добуток

$$Y = GX, \quad (3)$$

де $Y = [Y(0), Y(1),\ldots,Y(N-1)]^T$ – вектор спектральних коефіцієнтів перетворення Ґалуа вектора $X = [X(0), X(1),\ldots,X(N-1)]^T$, G – матриця розміру $N \times N$ значень ортогональних функцій Ґалуа в точках $\theta = j/N$.

У пропонованій роботі за формулами (1), (2) побудовано ортогональні системи функцій Ґалуа, на основі різних породжуючих векторів полів $GF(2^n)$. У табл. 1 наведено основні використані для побудови рекурсивних систем функцій Ґалуа поліноми характеристики 2 з коефіцієнтами із простого поля $GF(2)$ та відповідні їм породжуючі вектори, елементами яких є коефіцієнти полінома.

У побудованих ортогональних базисах виконано перетворення (3), досліджено ефективність та здійснено порівняльний аналіз з перетвореннями Уолша-Адамара і Хаара у задачах зменшення надлишковості інформаційних потоків.

Таблиця 1 – Поліноми $p(x)$ характеристики 2 з коефіцієнтами із поля $GF(2)$ та відповідні їм породжуючі вектори

n	**Породжуючий поліном** $p(x)$	**Породжуючі вектори**
3	$x^3 + x + 1$	$(1,0,1,1)$, $(1,0,1,\bar{1})$
3	$x^3 + x^2 + 1$	$(1,1,0,1)$, $(1,1,0,\bar{1})$
4	$x^4 + x + 1$	$(1,0,0,1,1)$, $(1,0,0,1,\bar{1})$
4	$x^4 + x^3 + 1$	$(1,1,0,0,1)$, $(1,1,0,0,\bar{1})$
4	$x^4 + x^2 + 1$	$(1,0,1,0,1)$, $(1,0,1,0,\bar{1})$
5	$x^5 + x^2 + 1$	$(1,0,0,1,0,1)$, $(1,0,0,1,0,\bar{1})$
5	$x^5 + x^3 + 1$	$(1,0,1,0,0,1)$, $(1,0,1,0,0,\bar{1})$
6	$x^6 + x + 1$	$(1,0,0,0,0,1,1)$, $(1,0,0,0,0,1,\bar{1})$
6	$x^6 + x^5 + 1$	$(1,1,0,0,0,0,1)$, $(1,1,0,0,0,0,\bar{1})$
7	$x^7 + x + 1$	$(1,0,0,0,0,0,1,1)$, $(1,0,0,0,0,0,1,\bar{1})$
7	$x^7 + x^6 + 1$	$(1,1,0,0,0,0,0,1)$, $(1,1,0,0,0,0,0,\bar{1})$

Досліджено ефективність ортогональних перетворень у системах функцій Ґалуа, породжених різними векторами в полях $GF(2^n)$, основна частина яких наведена у табл. 1.

Оцінювання ефективності перетворень здійснено на статистичній моделі вхідного одновимірного інфопотоку, яка застосовується для дослідження та визначення ефективності ортогональних перетворень [2, 5]. У даній моделі X – вектор довжини N, елементи якого є реалізацією одновимірного марківського процесу першого порядку з нульовим математичним сподіванням та одиничною дисперсією, з коефіцієнтом кореляції ρ між сусідніми елементами вибірки та коваріаційною матрицею C_X, кожний (i, j)-й елемент якої дорівнює $\rho^{|i-j|}$.

Для ортогонального перетворення коваріаційна матриця C_Y вектора коефіцієнтів перетворення Y визначається за формулою [5]:

$$C_Y = E[YY^T] = MC_X M^T = B = \{b(i,j)\}.$$

Здійснено дослідження теоретичної границі зменшення затрат на один коефіцієнт перетворення, що вимірюється в бітах на один елемент – “maximum reducible bits” (MRB) [5] при використанні перетворень Уолша-Адамара, Хаара та Ґалуа в базисах з різними породжуючими векторами:

$$MRB = -\frac{1}{2N} \sum_{i=1}^{N} \log_2 b(i,i),$$

де $\sigma^2(i) = b(i,i)$, Ω – множина, яка містить K коефіцієнтів перетворення, що відповідають найбільшим значенням дисперсій $\sigma^2(i)$.

Показник *MRB* визначає міру надлишковості, зменшеної в результаті перетворення.

Досліджено значення параметру *MRB* при використанні перетворень Уолша-Адамара (MRB_{had}), Хаара (MRB_{har}) та Ґалуа (MRB_{gal}) від коефіцієнта кореляції ρ між сусідніми елементами вибірки для розмірностей матриць перетворень від $N = 8$ до $N = 128$.

Залежності параметру *MRB* при використанні ортогональних перетворень довжини $N = 8$ у системах функцій Уолша-Адамара, Хаара і Ґалуа, породжених векторами $(1,0,1,1)$, $(1,1,0,1)$, $(1,0,1,\bar{1})$, $(1,1,0,\bar{1})$ в полі $GF(2^3)$ від коефіцієнта кореляції ρ між сусідніми елементами вибірки наведено на рис. 1.

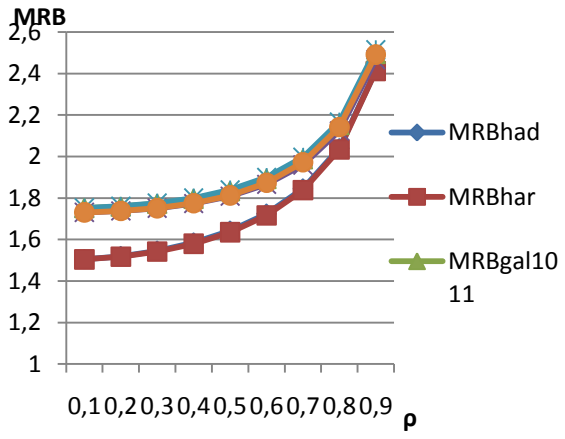

Рисунок 1 – Залежності теоретичної границі зменшення затрат від кореляції ρ для перетворень розмірності *N=8*.

Із аналізу результатів обчислень показника *MRB* та рис. 1 можна підсумувати, що ортогональне перетворення Ґалуа розмірності $N = 8$ для усіх досліджених значень кореляції ρ та розмірностей від $N = 16$ до $N = 128$ для низькокорельованих та середньокорельованих вхідних інфопотоків з коефіцієнтом $0{,}1 \le \rho \le 0{,}6$ мають вищий показник *MRB*. Обчислені відношення теоретичних границь зменшення затрат біт на один елемент перетворення дозволяють зробити висновок, що використання ортогонального перетворення Ґалуа забезпечує підвищення граничного значення зменшення затрат на 16% порівняно із перетвореннями Уолша-Адамара та Хаара.

На основі проведених досліджень встановлено, що у загальному випадку більший ступінь зменшення надлишковості інформації при фіксованій похибці відновлення інформаційного потоку забезпечується при використанні базисів перетворень Ґалуа, породжених поліномами з мінімальним числом ненульових коефіцієнтів і відповідно векторами з мінімальним числом ненульових елементів.

На основі аналізу результатів обчислень *MRB* у полях $GF(2^n)$ порядку $n \le 8$ визначено наступні породжуючі вектори базисів перетворень, які забезпечують найменшу похибку відновлення у задачах зменшення надлишковості інформаційних потоків порівняно з іншими для даного поля: $(1,1,0,1)$ у полі $GF(2^3)$, $(1,0,0,1,\bar{1})$ у полі $GF(2^4)$, $(1,0,0,1,0,\bar{1})$ у полі $GF(2^5)$, $(1,0,0,0,0,1,1)$ у полі $GF(2^6)$ та ін.

Таким чином, за допомогою перетворення Ґалуа у порівнянні із перетвореннями Уолша-Адамара та Хаара здійснюється кодування з мінімальною кількістю біт на один коефіцієнт перетворення чим забезпечується зменшення надлишковості.

ВИСНОВКИ

Таким чином, побудовано базиси дискретних ортогональних перетворень в системах функцій Ґалуа, породжених різними векторами полів $GF(2^n)$, досліджено ефективність застосування даних перетворень та здійснено порівняльний аналіз з перетвореннями Уолша і Хаара у задачах зменшення надлишковості інформаційних потоків.

У кожному полі Ґалуа фіксованого порядку n визначено породжуючий вектор і відповідний базис перетворення, застосування якого забезпечує максимальне зменшення надлишковості інформаційних потоків і тим самим дозволяє підвищити ефективність обробки інформації.

Результати проведених досліджень дають можливість зробити висновок, що метод обробки інформації на основі ортогонального перетворення Ґалуа дозволяє зменшити затрати на подання одного елемента перетворення і може використовуватись для кодування інформації на основі ортогонального перетворення та зменшення надлишковості інформаційних потоків.

REFERENCES

[1] Залманзон Л. А. Преобразования Фурье, Уолша, Хаара и их применение в управлении связи и других областях / Л. А. Залманзон – М.: Наука. Гл. ред. физ.-мат. лит., 1989. – 496 с.

[2] Прэтт У. Цифровая обработка изображений: в 2-х кн. / Прэтт У.: Пер. с англ. – М.: Мир, 1980.

[3] Петришин Л. Б. Теоретичні основи перетворення форми та цифрової обробки інформації в базисі Галуа: [навчальний посібник] / Л. Б. Петришин. – К.: ІзіМН МОУ, 1997. – 237 с.

[4] Превисокова Н. В. Метод обробки інформації на основі дискретного ортогонального перетворення Ґалуа / Н. В. Превисокова // Вісник Хмельницького нац. ун-ту. Технічні науки. – 2010. – № 2 (146). – С.149 –156.

[5] Гнатив Л. А. Методы синтеза эффективных ортогональных преобразований высокой и низкой корреляции и их быстрых алгоритмов для кодирования и сжатия цифровых изображений / Л. А. Гнатив, Е. С. Шевчук // Кибернетика и системный анализ. – 2002. – № 6. – С. 104–117.