Волинський О. Систематизація характеристик теоретико-числових базисів та їх застосування для побудови високопродуктивних спецпроцесорів / Волинський О., Пуюл В. // Вісник ТНТУ. — 2011. — Том 16. — № 3. — С.183-189. — (приладобудування та іформаційно-вимірювальні технології).

УДК 681.325

О. Волинський; В. Пуюл

Тернопільський національний економічний університет

СИСТЕМАТИЗАЦІЯ ХАРАКТЕРИСТИК ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСІВ ТА ЇХ ЗАСТОСУВАННЯ ДЛЯ ПОБУДОВИ ВИСОКОПРОДУКТИВНИХ СПЕЦПРОЦЕСОРІВ

Резюме. *Представлено класифікацію найбільш широко використовуваних теоретико-числових базисів, зокрема, проаналізовано взаємозв'язки між базисом Уолша, в середовищі якого базис Радемахера, а також окремі ортогональні функції, які з особливими рекурентними властивостями утворюють базис Галуа. Систематизовано характеристики ортогональних функцій та кодових матриць у різних теоретико-числових базисах. Проведено дослідження та оцінювання функціональних можливостей реалізації арифметики та базових функцій над числами в базисах Радемахера, Крестенсона та Галуа.*

Ключові слова: *теоретико-числовий базис, базисна функція, кодова матриця, алгоритмічна складність.*

O. Volynskyy, V. Puyul

SYSTEMATIZATION CHARACTERISTICS THEORETICAL AND DIGITAL BASIS AND THEIR APPLICATION FOR PROJECTION A HIGH PURPOSEPROCESSORS

The summary. *In this paper presents the classification of the most widely used theoretical-digital basis, analyzed the relationship between the Walsh basis in an environment whose Rademacher's basis, as well as separate orthogonal functions with special properties generate recurrent Galois's basis. The systematization of the functions and characteristics of orthogonal code matrices in various theoretical-digital basis. It was the research and evaluation of functionality and basic arithmetic functions over numbers in Rademacher's, Krestenson's and Galois's bases.*

Key words: *theoretical- digital basis, basis functions, code matrix, algorithmic complexity.*

Постановка проблеми. Теоретико-числові базиси (ТЧБ) породжуються системами ортогональних функцій на деякому інтервалі зміни аргументу [1,2]. Найширше вживаним у системах формування, передавання та цифрового опрацювання сигналів є відомий ТЧБ Фур'є, в основу якого поставлені гармонічні функції. Названий базис традиційно широко використовується для побудови процесорів кореляційного та спектрального аналізів, цифрових фільтрів, перетворення та опрацювання інформації в комплексній області. Основним функціональним обмеженням ТЧБ Фур'є, який призводив до низької швидкодії процесорів, зумовлений необхідністю високоточного генерування гармонічних функцій на основі рядів Маклорена й Тейлора. Інше функціональне обмеження базису Фур'є полягає в тому, що для обчислення спектрів з високою точністю необхідно реалізувати великий об'єм обчислювальних операцій.

Аналіз останніх досліджень і публікацій. Розроблення ТЧБ на основі систем кусково-постійних ортогональних функцій, до яких належать базиси: унітарний, Хаара, Крейга, Радемахера, Крестенсона, Уолша та Галуа, дозволило суттєво спростити обчислювальні процеси генерації та арифметико-логічного опрацювання базисних функцій на основі їх представлення у вигляді логічних кодових матриць. Тобто кожна базисна функція, яка представлена в нормованому діапазоні ±1 шляхом зміщення в позитивний квадрант декартової системи координат на +1 та нормування в діапазоні 0 –

1, подається у вигляді кодової матриці об'ємом $V = N \cdot n$, де N – число ортогональних функцій, n – інтервал зміни аргументу.

Аналіз літературних джерел щодо застосування різних ТЧБ для перетворення, передавання та опрацювання інформаційних потоків у сучасних комп'ютерних системах показує, що:

1) унітарний базис найширше застосовується в інформаційно-вимірювальних системах при реалізації багатоканальних АЦП розгортуючого типу, в спецпроцесорах цифрової томографії та оптоелектронних процесорах розпізнавання зображення;
2) базис Хаара широко використовується для реалізації процесорів швидких Вейвлет-перетворень, а також організації доступу інформації в базах даних на основі інформаційних вікон;
3) базис Крейга широко використовується в інформаційно-вимірювальних системах та око-процесорах;
4) в базисі Радемахера [3] реалізована виключна більшість універсальних процесорів комп'ютерної та комунікаційної техніки, а також сигнальних процесорів різних застосувань [4];
5) найпоширеніше застосування базису Уолша для цифрового опрацювання та стиснення зображень;
6) базис Крестенсона, який породжує систему числення залишкових класів, успішно застосовується для побудови спецпроцесорів стиснення інформації [2] та реалізації високопродуктивних процесорів опрацювання інформаційних потоків [5], в системах протиповітряної оборони та опрацювання великорозрядних чисел у системах криптозахисту інформації;
7) базис Галуа серед відомих базисів набув особливо широкого застосування для побудови спецпроцесорів та в розв'язанні прикладних задач у галузях:
   а) аналого-цифрового перетворення та кодування інформації;
   б) передавання інформації на основі кодів Баркера та М-послідовностей;
   в) стиснення інформації [6].

Значних успіхів досягненно при побудові спецпроцесорів на основі комбінованого використання різних ТЧБ. Наприклад, Хаара-Крестенсона, Крестенсона-Галуа [7], а також для реалізації високопродуктивних мультибазисних RCG-процесорів на основі базисів Радемахера, Крестенсона та Галуа [5]. Оскільки найбільш взаємопов'язаними між собою є названі процесори, тобто обчислювальні операції арифметики, які виконуються за один такт, найбільш швидкодійні у базисі Крестенсона, представляються залишками базису Галуа в кодах базису Крестенсона. Тому поглиблення теоретичних засад арифметики базису Крестенсона є найважливішим фактором удосконалення та покращення системних характеристик широкого спектра спецпроцесорів опрацювання великорозрядних чисел, що визначає високий рівень актуальності дослідження в цьому напрямку.

Метою роботи є систематизація характеристик класифікованих ТЧБ та їх кодових матриць, а також оцінювання особливостей арифметики систем числення, які вони породжують, та їх використання для створення високопродуктивних спецпроцесорів для великорозрядних чисел.

Постановка завдання. Провести аналіз та класифікацію теоретико-числових базисів, а також дослідити та здійснити оцінювання функціональних можливостей реалізації арифметики та базових функцій над числами в досліджуваних теоретико-числових базисах.

Класифікація та аналіз взаємозв'язків, широко використовуваних ТЧБ (рис. 1), де показано взаємозв'язки між базисом Уолша, в середовищі якого як частковий випадок існує базис Радемахера, а окремі ортогональні функції з особливими

рекурентними властивостями породжують базис Галуа. Вейвлет-перетворення формується на основі особливих сімейств функцій різних ТЧБ.

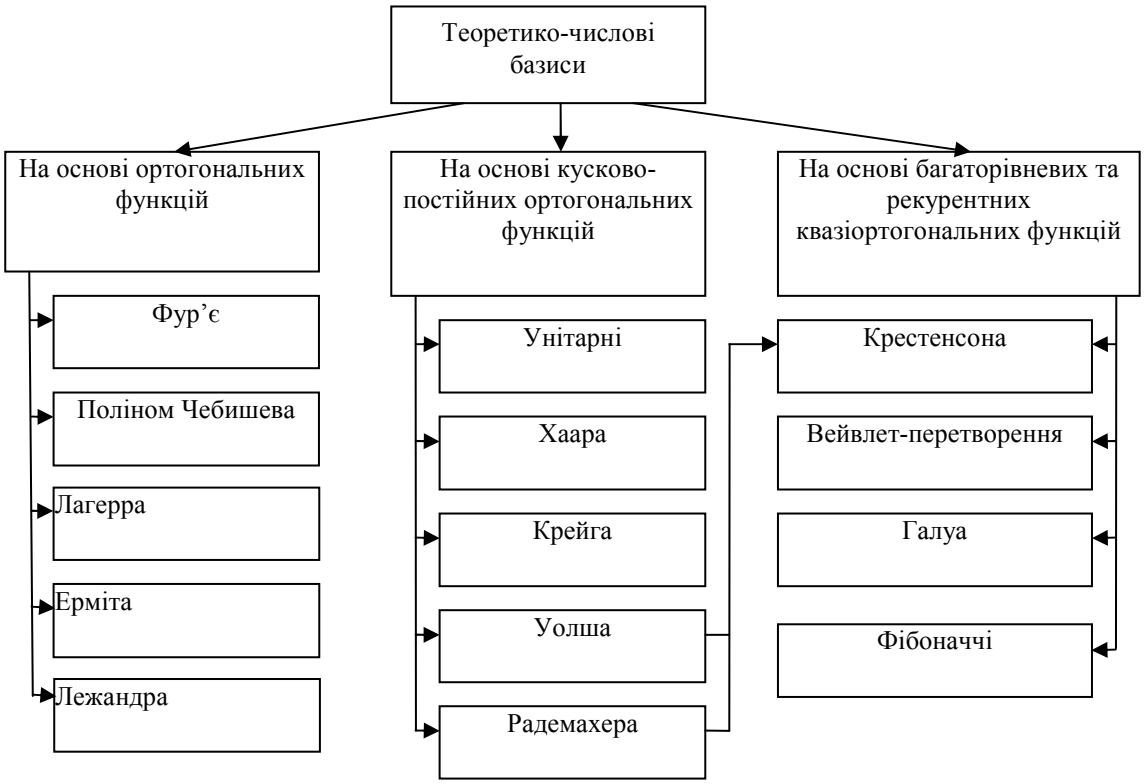
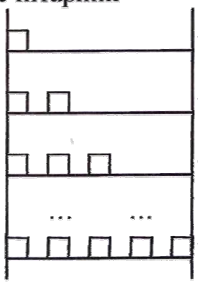
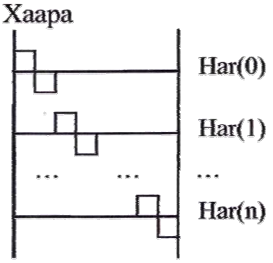
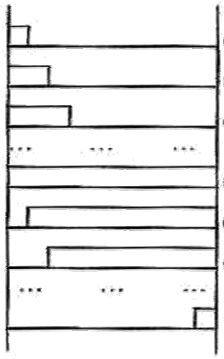
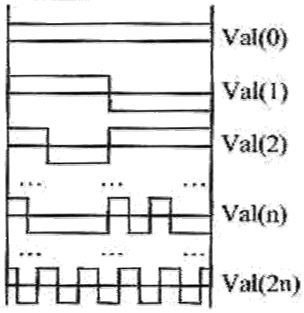
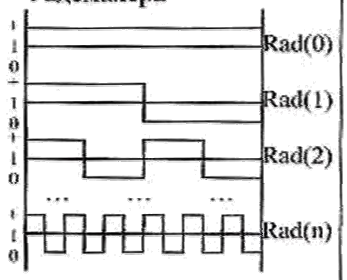
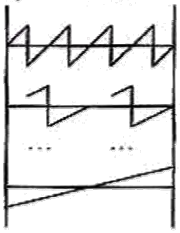
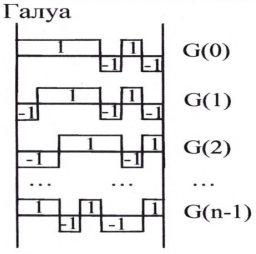


Рисунок 1. Класифікація та функціональні зв'язки різних ТЧБ

Систематизація характеристик та кодових матриць ТЧБ. Систематизація характеристик ортогональних функцій та кодових матриць у ТЧБ, які породжують системи числення, наведена в табл. 1.

Таблиця 1. Систематизація характеристик і кодових матриць ТЧБ

Базис та його ортогональні функції	Базисна функція	Кодова матриця та її об'єм
Унітарний 	$Uni(n,\theta,i)=sign[\sin(2^n\pi(\theta+i\cdot 2^{-n}))]$	$M_{Uni}=\begin{vmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 & 0 & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 & 1 \end{vmatrix}$ $V=N^2$
Хаара 	$Har(n,\theta,i)=sign[\sin(i2^n\pi,\theta]$	$M_{Har}=\begin{vmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{vmatrix}$ $V=N^2$

Крейга  	$Crg(n,\theta) = sign[\sin((2^n - 1)\cdot\pi\cdot\theta)]$	$M_{Crej} = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{vmatrix}$ $V = \frac{N^2}{2}$
Уолша  	$Had(h,x) = \prod_{i=1}^{K} [ri(x)]hi$	$M_{Uolh} = \begin{vmatrix} 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \dots & 0 & 1 & 1 & 1 & 1 \\ 1 & \dots & 0 & 0 & 0 & 1 & 1 \\ 1 & \dots & 0 & 1 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & 0 & 0 & 1 & 0 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \dots & 0 & 1 & 0 & 1 & 0 \end{vmatrix}$ $V = N \cdot \log_2 N$
Радемахера  	$Rad(n,\theta) = sign[2^n \pi\cdot\theta]$	$M_{Rad} = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 & 1 & \\ 1 & 1 & 1 & \dots & 1 & 1 & 1 \end{vmatrix}$ $V = N \cdot \log_2 N$
Крестенсона  	$N_i = res\sum_{i=1}^{n}(B_i \cdot b_i) \bmod P$	$M_{Cres} = \begin{vmatrix} P_1 & P_2 & \dots & P_n \\ 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \\ 2 & 2 & \dots & 2 \\ 0 & 3 & \dots & 3 \\ \dots & \dots & \dots & \dots \\ b_1 & b_2 & \dots & b_n \end{vmatrix}$ $V = \sum_{i=1}^{m} \log_2(P_i)$
Галуа  	$N_j = f(C_{j-n-1},\dots C_{j-1}, C_j),$ $C_j = res\sum_{j=0}^{n=1} C_{j-1}\cdot A(\bmod 2)$	$M_G = \begin{vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \\ \dots \\ 1 \\ 1 \end{vmatrix}$ $V = N$

З таблиці 1 бачимо, що найбільш компактні кодові матриці формують системи ортогональних функцій базисів Радемахера, Крестенсона та Галуа. Причому кожен з названих базисів породжує окрему систему числення, які використовуються для реалізації арифметики відповідних універсальних та спеціальних процесорів. Висока популярність та широке застосування базису Радемахера ґрунтується на достатньо простій реалізації арифметики позиційної двійкової системи числення, яка включає шість базових операцій [3]:

1) додавання «+»;
2) зсув «→ ←»;
3) множення «×»;
4) рівності «=»;
5) знакова (старшинства) «< >»;
6) віднімання «-»;
7) ділення «/»;
8) модульна «mod».

З метою підвищення ефективності міжбазисних перетворень запропонована бінарно-розмежована система числення залишкових класів (БРСЗК) [8].

Важливе значення також має програмно-апаратна, структурна та алгоритмічна складність міжбазисних перетворень у середовищі досліджуваних ТЧБ.

Дослідження та оцінювання функціональних можливостей реалізації арифметики та базових функцій над числами в базисах Радемахера, Крестенсона та Галуа. Порівняльна оцінка функціональних можливостей досліджуваних ТЧБ наведено в табл. 2.

Таблиця 2. Функціональні можливості досліджуваних ТЧБ

№	Базові операції	Радемахер	Крестенсон	Галуа	БРСЗК
1	Додавання	$2nv$	v	$3v$	v
2	Зсув	v	-	$2v$	v
3	Множення	$2v(2n+1)$	v	?	?
4	Рівності	v	v	v	v
5	Знакова (старшинстта)	nv	?	?	nv
6	Віднімання	$(3n+5)v$	?	?	2nv
7	Ділення	n^2v	?	-	?
8	Модульна	n^2v	$2nv$	?	$2nv$

У таблиці 2 n – розрядність представлення чисел, а v – тривалість спрацювання мікроелектронного обладнання.

Оцінка існування та складності алгоритмів міжбазисних перетворень досліджуваних ТЧБ наведена в табл.3.

Таблиця 3. Міжбазисні перетворення досліджуваних ТЧБ

Теоретико-числові базиси	***Алгоритм міжбазисних перетворень***
Радемахера-Крестенсона	$N_k = (a_{n-1},...,a_i,..,a_0); a_i \in \overline{0,1}; N_k = \sum_{i=0}^{n-1} a_i \cdot 2^i;$ $N_k = \begin{matrix} \nearrow b_1 \\ \cdots \\ \rightarrow b_i \\ \cdots \\ \searrow b_k \end{matrix}$ $b_i = res N_k (mod p_i); N_k = a_i p_i + b_i, P = \prod_{i=1}^{k} p_i;$ $0 \le N_k \le P, \ p_i \not\equiv p_j.$
Радемахера-Галуа	$N_k \to \sum_{i=0}^{n-1} i \to G_0 G_1 ... G_{i-1}; G_0 = (11...1); G_{i+1} = G_i \oplus G_{i-n}; i \in \overline{0, n-1}.$
Крестенсона-Радемахера	$N_k = res \sum_{i=1}^{k} b_i \cdot B_i (\text{mod } P), B_i = \frac{P}{p_i} \cdot m_i \equiv 1 (\text{mod } P_i).$
Крестенсона-Галуа	$N_k = (b_1,..,b_i,..,b_k) \to \sum_{i=0}^{n-1} i \to G_i ... G_{i-n}; G_0 = (11...1); G_{i+1} = G_i \oplus G_{i-n}; i \in \overline{0,n-1}.$
Галуа-Радемахера	$G_i G_{i-1} ... G_{i-n} \to \sum_{i=0}^{n-1} i \to N(a_{n-1},...,a_i,..,a_0) \to N_k; a_i \in \overline{0,1}.$
Галуа-Крестенсона	$G_i G_{i-1} ... G_{i-n} \to \sum_{i=0}^{n-1} i \to N_k = (b_1, b_2, ..., b_i, ..., b_k).$

Міжбазисне перетворення Радемахера-Галуа та Крестенсона-Галуа виконується на основі проміжного перетворення в унітарний базис.

Аналіз сучасного стану реалізації базисних функцій досліджуваних ТЧБ, орієнтованих на створення високопродуктивних спецпроцесорів, опрацювання великорозрядних чисел дозволяє зробити висновок, що успішний розвиток теорії ТЧБ Крестенсона, з метою реалізації всіх базових функцій арифметики процесорів, є перспективною та актуальною науково-технічною задачею.

Висновки. Проведено аналіз сучасних характеристик відомих ТЧБ, які широко використовуються для реалізації програмно-апаратних процесорних компонентів комп'ютерних систем. Систематизовано аналітику, кодові матриці та функціональні можливості арифметики різних ТЧБ. Обґрунтовано перспективу поглиблення теорії базису Крестенсона з метою ефективної реалізації всіх базових функцій арифметики та міжбазисних перетворень, які забезпечать умови побудови та реалізації високопродуктивних спецпроцесорів опрацювання великорозрядних чисел.

Література

1. Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 460 с.
2. Николайчук, Я.М. Теорія джерел інформації [Текст] / Видання друге, виправлене / Я.М. Николайчук. – Тернопіль: ТзОВ "Терно-граф", 2010. – 536 с.
3. Мельник, А.О. Архітектура комп'ютера [Текст] / А.О. Мельник // Наукове видання. – Луцьк: Волинська обласна друкарня, 2008. – 470с.
4. Advanced Micro Devices, AMD – Processor Homepage [Електронний ресурс]. – Режим доступу: http://amd.com.
5. Круцкевич, Н.Д. Принципи побудови RCG процесора [Текст] / Н.Д. Круцкевич, Я.М. Николайчук // Тези міжнар. науково-технічної конф. "Контроль і управління в складних системах" (КУСС-2003). – Вінниця: «УНІВЕРСУМ – Вінниця», 2003. – С. 73.
6. Теорія та принципи побудови спецпропесора на основі базисів Радемахера, Крестенсона, Галуа [Текст] / О.М. Заставний, Я.М. Николайчук, Н.Д. Круцкевич, Р.І. Король // Тези доповідей сьомої міжнародної науково - технічної конференції. – Вінниця: «УНШЕРСУМ – Вінниця», 2003. – 114с.
7. Спецпроцесори обробки даних на основі перетворення Крестенсона – Галуа [Текст] / Н.Г. Яцків, Р.І. Король, В.В. Яцків, Т.Г. Федчишин // Вісник Технологічного університету Поділля. – 2003. – ТІ, №3. – С. 105–108.

8. Волинський, О.І. Розмежована система числення залишкових класів та спецпроцеси на її основі [Текст] / О.І. Волинський, І.З. Якименко // Поступ в науку. Збірник праць Бучацького інституту менеджменту і аудиту – Бучач, 2010. – №6, Т1. – С. 80–83.

Отримано 16.05.2011