УДК 681.32

В.М. Кузик[1], С.В. Івасьєв[2], Н.З. Кульчинська[1], Л.І. Маланчук[1]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

СПОСОБИ КОДУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ НА ОСНОВІ ТЕОРЕТИКО - ЧИСЛОВИХ БАЗИСІВ РАДЕМАХЕРА ТА КРЕСТЕНСОНА

Вступ. Способи кодування інформаційних потоків визначаються теоретико числовими базисами (ТЧБ), які застосовуються для їх представлення [1]. Найбільш поширеними ТЧБ в сучасних КС є наступні: унітарний, Хаара, Грея, Радемахера, Крестенсона та Галуа.

Світовий досвід створення процесорів для КС, поряд з застосуванням ТЧБ Радемахера, що призводить до породження двійкової системи числення, за останні роки демонструє тенденцію застосування інших ТЧБ. Реалізація спеціалізованих, кореляційних, спектральних, ентропійних, спецпроцесорів на базі Галуа та проблемно-орієнтованих процесорів цифрової обробки даних часто виконується на базі сумісного використання комбінацій названих ТЧБ, наприклад Радемахера - Крестенсона, Радемахера - Хаара, Крестонсона - Галуа та ін [2].

У зв'язку з цим існує проблема глибокого дослідження характеристик різних ТЧБ та граничних можливостей їх застосування для реалізації компонентів як спеціалізованих, так і універсальних процесорів. При цьому перспективним, крім розповсюдженого одновимірного (векторного) представлення чисел та виконання арифметико-логічних операцій у базисі Радемахера, є застосування змішаного базису Радемахера- Крестенсона [3,4].

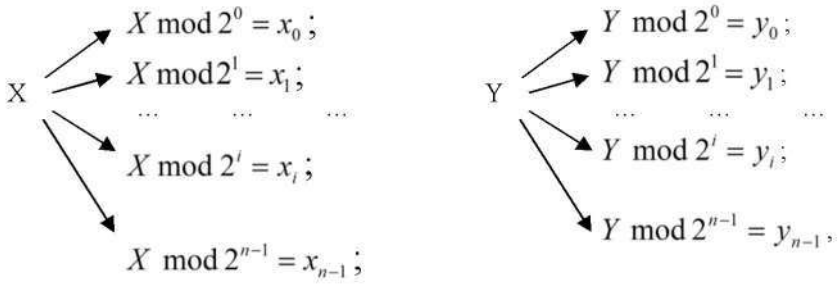
Метою роботи є дослідження способів кодування інформаційних потоків в комп'ютерних системах на основі теоретико - числових базисів радемахера та крестенсона

1. Дослідження базису Радемахера

Арифметичні операції над двома числами у двійковій системі числення базису Радемахера описуються наступними виразами:

$$X = \sum_{i=0}^{n-1} x_i 2^i \ , \ x_i \in \overline{0,1}; \ Y = \sum_{i=0}^{n-1} y_i 2^i \ , \ y_i \in \overline{0,1}.$$

Тобто двійкові коди чисел X і У: $X=(x_{n-1},x_{n-2},\ldots,x_i,\ldots,x_0)$; $Y=(y_{n-1},y_{n-2},\ldots,y_i,\ldots,y_0)$ визначаються на основі модульних операцій згідно аналітичних виразів:



Приведені характеристики кодових матриць ТЧБ Радемахера, Крестенсона, які найширше використовуються для кодування та цифрової обробки даних в інформаційних системах, мають властивості мінімальної надлишковості по відношенню до наступних базисів: унітарного, Хаара, Крейга, Уолша та Грея [2].

У таблиці 1.2 N – діапазон представлення чисел, p_1, p_2, … , p_i, … , p_m – набір взаємо простих модулів СЗК базису Крестенсона, $a_i=p_i-1$.

Система числення залишкових класів базису Крестенсона, детально описана Акушським І.Я. та Юдіцьким Д.І. [3].

Таблиця 1 – Характеристики кодових матриць ТЧБ

	Радемахера	Крестенсона
Кодові матриці	$M_{Rad}=\begin{vmatrix}000\ldots00\\000\ldots01\\000\ldots10\\000\ldots11\\\ldots\ldots\ldots\\111\ldots11\end{vmatrix}$	$M_{Cres}=\begin{vmatrix}P_1 & P_2 & \ldots & P_m\\0 & 0 & \ldots & 0\\1 & 1 & \ldots & 1\\2 & 2 & \ldots & 2\\0 & 3 & \ldots & 3\\\ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots\\2 & 4 & \ldots & 6\end{vmatrix}$
n - число активних кодових елементів	$n=\frac{\mathrm{N}\cdot\log_2 N}{2}$	$n=\prod_{i=1}^{m}P_i$
V – об'єм кодової матриці	$\mathrm{V}=\mathrm{N}\cdot\log_2\mathrm{N}$	$V=\sum_{i=1}^{m}\log_2(P_i-1)$

Результати досліджень часової складності реалізації операції множення над числами в базисах Радемахера (O1(n)) та Радемахера - Крестенсона (O2(n)) приведені на рисунку 1 [3].

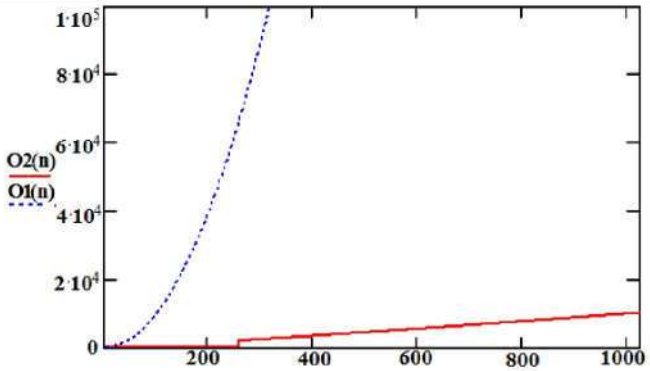


Рисунок 1 – Часова складність реалізації операції множення в базисах Радемахера (O1(n)) та Радемахера - Крестенсона (O2(n))в залежності від розмірності

Нормалізована форма СЗК, запропонована науковою школою проф. Николайчука Я.М., найбільш поширена в телекомунікаційних процесорах інформаційних систем нафтогазової промисловості [3].

З рисунка 1 видно, що методи множення у базисі Радемахера - Крестенсона характеризується суттєвим збільшенням швидкодії, що є важливою перевагою його застосування шляхом використання спеціалізованих процесорів та контролерів.

В роботі [4] проведено дослідження та розробка операції експоненціювання (рисунок 2). В результаті у роботі [3] розроблено метод модулярного експоненціювання, який з допомогою використання особливостей базису Радемахера – Крестенсона (O4(n)) призводить до кардинального зменшення обчислювальної складності порівняно з базисом Радемахера (O3(n)), що ілюструє рисунок 2.

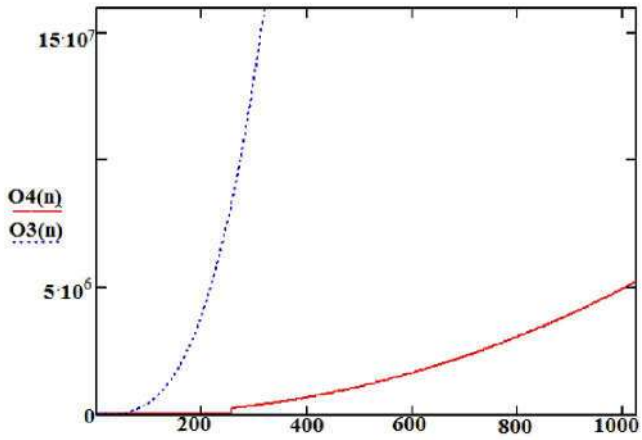


Рисунок 2 – Порівняння характеристики виконання модулярного експоненціювання БРЧ в базисах Радемахера (O3(n)) та Радемахера – Крестенсона (O4(n))

Проведені дослідження показують перспективність використання мультибазисних методів опрацювання багаторозрядних інформаційних потоків в прикладних задачах теорії чисел.

2 Аналіз існуючих бібліотек для роботи з багаторозрядними числами, постановка задачі дослідження

Серед сучасних програмних засобів опрацювання БРЧ виділяються ряд бібліотек для реалізації відповідних алгоритмів [3], а саме: бібліотека для роботи з БРЧ Ленстра, Arageli, NTL, GMP, Crypto++ та інші. Наведемо особливості організації деяких з них.

В роботі [2] наведений порівняльний аналіз швидкодії реалізації алгоритмів опрацювання БРЧ з використанням різних бібліотек (таблиця 2).

В результаті дослідження отримані відповідні значення RANK[4] та наведені в таблиці 2. Для кожного алгоритму було виконано 100 тестів та встановлено відносні показники продуктивності.

Таблиця 2 - Характеристики швидкодії алгоритмів з використанням різних бібліотек опрацювання БРЧ

Бібліотека	*RANK(ALG$_i$)*				AES-192	TDES	RSA (2048)		ECDSA (F2m=283)		HMAC SHA-1	SHA-1 (/&=256)	RANK
	MUL	POWMOD	xGCD	ECMUL			*sign*	*verf*	*sign*	*Verf*			
NTL	1,01	1,18	1,0	-	-	-	-	-	-	-	-	-	1,06
MIRACLE	3,58	2,62	3,15	1	1,00	-	2,29	1,72	2,02	2,76	-	1,12	1,40
Botan	3,41	5,21	1,09	1,42	2,16	1,98	1,00	1,00	1,60	1,95	1,15	1,13	1,67
Crypto++	4,49	5,04	16,82	4,35	2,68	1,90	1,12	1,15	1,00	1,00	1,05	1,07	2,19
OpenSSL	2,80	2,43	12,49	1,15	4,49	3,39	1,68	1,51	1,85	2,53	1,00	1,00	2,26
OpenPGP	2,87	2,31	3,11	1,41	1,12	1,37	2,35	1,73	1,54	2,00	-	1,06	1,79
GNU Crypto	1,0	1,0	1,01	1,24	1,38	1,00	2,71	1,80	1,75	2,13	1,06	1,08	1,35
CryptLib	5,25	4,17	8,59	1,7	1,03	1,47	1,09	1,08	1,07	2,05	1,02	1,06	1,82
LenstraLib	1,02	1,15	1,03	1,3	-	-	-	-	-	-	-	-	1,12

Для роботи з БРЧ бібліотека Lenstra є досить гнучким інструментом, що забезпечує найбільш ефективне використання обчислювальних ресурсів, а також реалізацію основних арифметичних та криптографічних алгоритмів, тому для реалізації розроблених методів обрана саме вона.

Факторизацію доцільно застосовувати для підбору модулів у СЗК [2], яка на даний час є однією з альтернатив двійковій системі числення, що дозволяє застосовувати нові підходи до організації обчислювальних систем при виконанні елементарних математичних операцій [3]. Хоча СЗК не позбавлена недоліків, до яких відносяться, зокрема, відсутність ділення та порівняння чисел, необхідність визначення умов переповнення розрядної сітки, однак її успішно можна застосовувати для додавання, віднімання та множення цілих багаторозрядних чисел. Безсумнівною перевагою СЗК є можливість виконання операцій над числами, які менші за вибрані модулі, розпаралелення процесу обчислень та відсутність міжрозрядних переносів.

СЗК – це непозиційна система числення, десяткові числа в якій представляються невід'ємними залишками від ділення на кожен з системи взаємно простих модулів p_i. Додавання, віднімання і множення в СЗК відбуваються незалежно по кожному модулю без переносів між розрядами. Зворотне перетворення з СЗК у десяткову систему числення ґрунтується на використанні китайської теореми про залишки і є досить громіздким процесом, що є ще одним недоліком СЗК, який стримував її розвиток і поширення:

$$N = \left(\sum_{i=1}^{n} b_i B_i \right) \bmod P, \qquad (1)$$

де $B_i = M_i m_i$, $M_i = \dfrac{P}{p_i}$, базисні числа m_i шукаються з виразу $(M_i m_i) \bmod p_i = 1$.

Необхідність обчислення базисних чисел $m_i = M_i^{-1} \, mod \, p_i$ істотно збільшує складність переведення чисел з СЗК у десяткову систему. Спрощення цієї задачі відбувається у досконалій формі СЗК (ДФ СЗК), коли модулі p_i підібрані таким чином, що усі m_i=1. У роботах [2] була розвинута теорія ДФ СЗК і запропоновано метод для визначення системи модулів ДФ СЗК. Однак у випадку обмеженої кількості модулів або необхідності використання модулів, які мало відрізняються один від одного, цей метод непридатний. У роботі була запропонована модифікована ДФ СЗК (МДФ СЗК), у якій базисні числа m_i=±1, що також виключає необхідність пошуку оберненого числа.

У [3] показано, що після відповідних математичних перетворень можна отримати умову, яка повинна виконуватися для визначення набору модулів для ДФ та МДФ СЗК:

$$(p_2p_3...p_{n-2}+p_1p_3...p_{n-2}+...+p_1p_2...p_{n-3}-p_1p_2...p_{n-2})+(p_1p_2...p_{n-2})^2=ab. \quad (2)$$

$$(p_2p_3...p_{n-2}+p_1p_3...p_{n-2}+...+p_1p_2...p_{n-3}-p_1p_2...p_{n-2})+(p_1p_2...p_{n-2})^2=\pm ab. \quad (3)$$

Це означає, що ліва частина (1.4), (1.5) повинна бути факторизована, на основі чого визначаються параметри a та b для визначення будь-якої кількості модулів.

Висновок. Отже, вирішення задач теорії чисел дозволить спростити процес перетворення з СЗК у позиційну систему числення, що, в свою чергу, можна ефективно використовувати в ряді прикладних задач обчислювальної техніки.

Перелік джерел.

1. Бекчанова Ш.Б. Принципы построения высокопроизводительных вычислительных структур / Ш.Б. Бекчанова, Х.Н. Зайнидинов // Тезисы докладов НТК «Мафкуравий жараёнлар ва Узбекистонда фанлар ривожининг долзарб муаммолари», Андижон. - 2002. – С. 441.
2. Виноградов И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 176с.
3. Грибанов Ю.И. Автоматические цифровые корреляторы./ Ю.И. Грибанов, Г.П. Веселова, В.Н Андреев. – М.: Энергия, 1971. – 240с.
4. Задірака В.К. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання / В.К. Задірака, О.С. Олексюк. – Київ. –2003. – 264 с.
5. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов.– Казань: Казан. ун. 2011.– 190 с.
6. Івасьєв С.В. Збіжність екстремумів залишкової функції в околі розв'язку задачі факторизації/ С.В.Івасьєв, Я.М. Николайчук, І.З.Якименко, І.Р.Колісник // Вісник Хмельницького національного університету. Технічні науки. – 2015, №4. - С.157-164.
7. Мельник А. О. Програмовані процесори обробки сигналів / А.О.Мельник. – Львів: Вид-тво Національного університету "Львівська політехніка", 2000. –55 с.
8. Николайчук Я.М. Методы цифровой обработки шумоподобных сигналов на основе кодовых систем / Я.М. Николайчук, Б.М. Шевчук – Киев, Сб. тр. ИКАН УССР, 1988.
9. Николайчук Я.М. Проблеми реорганізації структури процесорів у різних теоретико-числових базисах / Я.М. Николайчук // Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM-2014). - Тернопіль,2014.- С.110-114.
10. Палагин А.В. Реконфигурируемые структуры на ПЛИС / А.В. Палагин, В.Н. Опанасенко, В.Г. Сахарин // УсиМ. – 2000. – № 3. – С. 33-43.
11. Палагин А.В. Опыт разработки микропроцессорных распределенных систем реального времени. / А.В. Палагин, Я.Н. Николайчук // – Киев: Знание, – 1988. – 19 с.