2. Николайчук Л. М. Дослідження впливу відео-, аудіо-, алфавітно-цифрової та іншої інформації на суспільно-комунікаційну поведінку суб'єктів права. *Оптико-електронні інформаційно-енергетичні технології.* 2015. № 1 (29). С. 51–55.
3. Пітух І. Р., Возна Н. Я., Процюк Г. Я., Николайчук Я. М. Спосіб контролю параметрів технологічного процесу. Патент України на корисну модель № 107039. Бюл. № 10. 2016.

Outlined methodological and system characteristics of processes modeling and building information models of subject of law. Investigated attributes of existing models from the standpoint of subjective analysis and functions of a computerized system operator, which carries out functions subject of law. The proposed a structure of neuro-model of subject of law that implements the presence of Markov processes to availability of memory and thresholds functions of values of individual data flows.

Key words: *computerized system neuro-models, subject of law.*

Одержано 16.02.2017

УДК 681.32

Я. М. Николайчук, д-р. техн. наук, професор,
О. І. Волинський, канд. техн. наук,
П. В. Гуменний, канд. техн. наук,
Т. І. Пастух, аспірант

Тернопільський національний економічний університет, м. Тернопіль

МЕТОДИ МІЖБАЗИСНИХ ПЕРЕТВОРЕНЬ БАГАТОРОЗРЯДНИХ КОДІВ ТЕОРЕТИКО-ЧИСЛОВИХ БАЗИСІВ РАДЕМАХЕРА – КРЕСТЕНСОНА

Наведено методи міжбазисних перетворень багаторозрядних кодів.

Ключові слова: *теоретико-числовий базис (ТЧБ), система залишкових класів (СЗК), міжбазисне перетворення.*

Вступ. Теоретико-чиловий базис Крестенсона, що породжує непозиційну систему числення залишкових класів (СЗК) характеризується суттєвими перевагами по відношенню до базису Радемахера [1]. Існує три типи основних перетворень СЗК: цілочисельне $N_k = res\sum_{i=1}^{k} b_i \cdot B_i (\text{mod } P)$; нормалізоване $[N_k]_0 = res\sum_{i=1}^{k} [b_i]_0 \cdot m_i (\text{mod} 1)$; досконале $[N_k]_0 = res\sum_{i=1}^{k} [b_i]_0 (\text{mod} 1)$, які дозволяють реалізувати спец-

процесори базису Крестенсона з різними характеристиками апаратної та часової складності.

Представлення чисел в розмежованій СЗК. Існує ще одна форма СЗК — розмежована СЗК (РСЗК). Теоретичною основою РСЗК є цілочисельна форма СЗК, рівняння якої представлено у вигляді суми: $N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk}$, де N_{ik} — m-розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення, числового базису Радемахера. Наприклад, 64-х розрядний процесор СЗК може бути розмежований на 4-ри фрагменти по 16 біт (рис. 1).

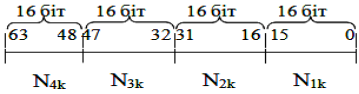

Рис. 1. *Процес розмежування 32-х розрядного процесора*

При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще більш глибокий рівень розпаралелювання опрацювання інформації, а відповідно підвищення швидкодії процесора СЗК [2].

Зі структури розмежованого процесора зрозуміло, що вона потребує обчислення залишків для кожного компонента згідно виразу $b_{ij} = resN_{ij} (\mathrm{mod}\, p_i)$. При цьому, процедура обчислення загального залишку виконується згідно виразу

$$b_i = res(b_{i1} + b_{i2} + ... + b_{in}) \bmod p_i .$$

Модифікований метод отримання залишу з двійкового числа. Для реалізації міжбазисного перетворення Радемахер – Крестенсона розглянемо модифікований метод отримання залишу з двійкового числа (рис. 1) [3]. Залишок b_i отримується з двійкового числа представленого, починаючи з старшого розряду $X_{(2)} = (a_0, a_1, ...a_i ... a_{n-1})$, де $a_i \in \overline{0,1}$ за заданим модулем P_j, що описується рекурентною формулою: $b_i = (a_i + 2 \cdot b_{i-1}) \bmod P_j$, де a_i — значення i-го біта двійкового числа; b_{i-1} — значення залишку $i-1$-го біта двійкового числа (рис. 2). Початкова умова рекурентної формули отримання залишку задається наступними даними: $i = n-1$, $b_{i-1} = 0$. Отримане b_0 — шуканий залишок згідно виразу: $b_0 = resX (\mathrm{mod}\, P_j)$, де res — символ операції отримання залишку.

Реалізація міжбазисного перетворювача на основі пристрою визначення залишку двійкового числа з використанням ПЗП має структуру, показану на рис. 3.

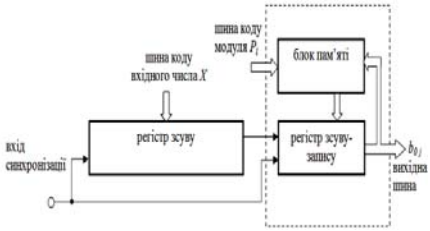

Рис. 2. *Структура пристрою визначення залишку двійкового числа з використанням ПЗП*

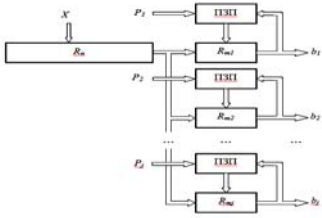

Рис. 3. *Структура міжбазисного перетворювача з використанням ПЗП*

В даному пристрої відсутня операція додавання для визначення проміжного залишку по модулю рі, що притаманна аналогічним перетворювачам, яка зменшує швидкодію, для її заміни використано регістр зсуву та ПЗП, в якому зберігаються обчислювані залишки по модулю.

Пристрій перетворення чисел з позиційної системи в систему залишкових класів. Для реалізації швидкого міжбазисного перетворення Радемахера – Крестенсона доцільно застосовувати пристрій для перетворення чисел з позиційної системи в систему залишкових класів на основі рандомізаторів [4]. Структурна схема такого міжбазисного перетворювача зображена на рис. 4, що складається: 1 — вхідні шини *K*-розрядного позиційного числа, 2 — комутаційні мультиплексори, 3 — виходи коду b_i системи залишкових класів.

На рис. 5 показана структурна схема компонента міжбазисного перетворювача Радемахера – Крестенсона на основі комутаційного мультиплексора 2, до складу якого входять: рандомізатор по модулю P_j(Rand) інкрементний пристрій по модулю P_j (Incr); *P*-канальний двохвходовий мультиплексор (MX).

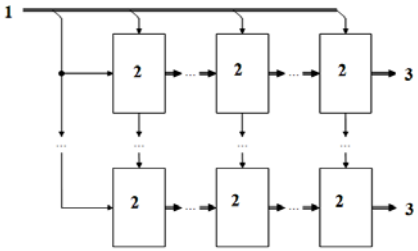

Рис. 4. *Структурна схема міжбазисного перетворювача Радемахера – Крестенсона*

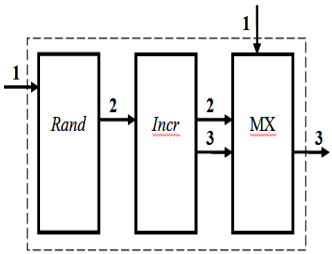

Рис. 5. *Модуль рандомізації та обчислення проміжного значення залишку*

Рис. 6, показаний у вигляді графа, наглядно демонструє роботу супершвидкодіючого міжбазисного перетворення Радемахера – Крес-

тенсона (час перетворення 4 мікротакти незалежно від розрядності двійкового числа).

Зворотнє перетворення СЗК. На рис. 7 показаний приклад визначення $[N_k]_0$ для двох чисел $N_{k1} = 5,\ N_{k2} = 7$. Операція міжбазисного перетворення реалізується у вигляді графа задаємо сумування нормалізованих значень залишків в заданій системі модулів [5]. Наприклад: для двох чисел отримаємо їх коди у нормалізованій СЗК $N_{k1} = (0{,}5;\ 0{,}66;\ 0)$, $N_{k2} = (0{,}5;\ 0{,}33;\ 0{,}4)$ і, згідно графу рис. 7, отримуємо їх нормалізовані значення у системі модулів (2, 3, 5) $[N_{k1}]_0 = 0{,}16$ і $[N_{k2}]_0 = 0{,}23$.

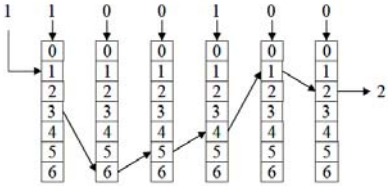

Рис. 6. *Граф міжбазисного переретворення Радемахера-Крестенсона по mod7*

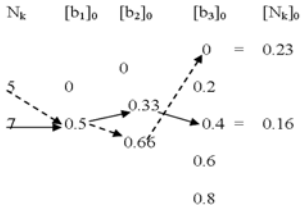

Рис. 7. *Граф визначення* $[N_k]_0$

Дані операції виконуються за табличним методом. Це дає перевагу перед виконанням тих самих операцій в інших базисах, що дозволяє суттєво спростити спецпроцесор на основі заданого базису.

Спецпроцесор РСЗК в системах базису Радемахера. Отримані результати дозволяють створити процесор СЗК, що може бути інтегрований в будь-яку систему для проведення обчислень з високою швидкодією над багаторозрядними числами, згідно структури показаної на рис. 8.

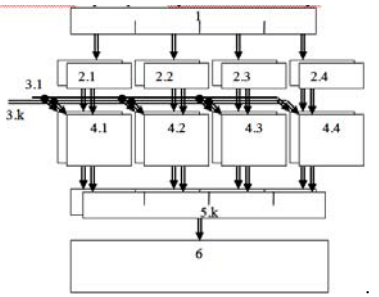

Рис. 8. *Адаптований спецпроцесор РСЗК до кодових систем базису Радемахера*

Спецпроцесор РСЗК складається з регістра зберігання двійкового N-розрядного числа X – 1, яке розмежовується на n-розрядні блоки та

подається на 2 — пристрій для міжбазисного перетворення на основі рандомізаторів (рис. 4) з розрядністю n, що дозволяє отримати залишки числа *X* у РСЗК; отримані залишки поступають на арифметичний блок — 4, який виконує потрібні операції над залишками числа X та Y, що подається на цей блок через шину 3.*k* (*k* — кількість шин, що відповідає числу модулів *p*), результат обчислень подається на пристрій для міжбазисного перетворення на основі рандомізаторів — 5 (див. рис. 4) з розрядністю *N*, який дозволяє перейти з РСЗК у цілочисельну СЗК. Отримані залишки подаються на міжбазисний перетворювач Крестенсона – Радемахера — 6.

Одним із перспективних способів реалізації пристрою зворотного перетворення Крестенсона – Радемахера є використання асоціативної пам'ять з паралельним доступом.

Асоціативна пам'ять колективного користування з паралельним доступом на основі вертикально-інформаційної технології. Паралельний доступ до пам'яті колективного користування виконується шляхом кодування ідентифікаційної, службової та адресної інформації користувачів кодами поля Галуа [6], що дозволяє здійснити паралельний запис даних в абонентські поштові скриньки багатопортової пам'яті, а також здійснити одночасне паралельне зчитування з будь-якого адресованого масиву сторінки даних багатопортової пам'яті колективного користування (рис. 9).

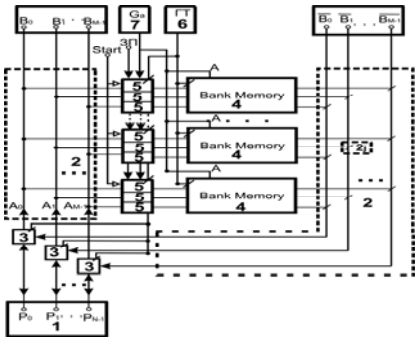

Рис. 9. *Структура ПКК на основі ВІТ: 1 — порти вводу/виводу ПКК; 2 — комутаційна мережа; 3 — контролери комутаційної мережі; 4 — банки пам'яті; 5 — ідентифікаційно адресні модулі абонентів; 6 — генератор імпульсів синхронізації; 7 — Галуа кодонний адресний генератор банків пам'яті*

Суть розробленого пристрою пояснюється тим, що на початку циклу доступу до ПКК, багатопортовий адресний дешифратор Галуа паралельно генерує всі еталонні ідентифікаційні коди, попередньо внесені через адміністративну шину в адреси абонентських скриньок

вводу даних у кільцеві регістри, які порівнюються шляхом логічної операції "XOR" з кодами запитів обслуговування всіх абонентів. При цьому абонентам надається дозвіл запису даних у власну абонентську скриньку та дозвіл зчитування з будь-якого замовленого адресного простору пам'яті колективного користування при співпаданні адресів замовлених сторінок з кодами сторінкового генератора Галуа.

При використані ПКК з постійним зростанням кількості вхідних задач чи кількості вхідних процесорних елементів, що спілкуються з ПКК, час відповіді процесора не змінюється і завжди залишається постійним. Таким чином, як показав аналіз, продуктивність і час відповіді системи, в першу чергу, залежать від структури і технічних характеристик загальносистемних ресурсів. Проте, на значення продуктивності і часу відповіді процесора не другорядним чином впливають засоби, що забезпечують доступ процесора до загальних ресурсів. Звідси пам'ять колективного користування забезпечує реалізацію багатопортового доступу із захистом даних від несанкціонованого доступу та подальші перспективи реалізації такої пам'яті засобами ПЛІС.

Міжбазисний перетворювач Крестенсона – Рademахера на основі асоціативної пам'яті з паралельним доступом. Такий перетворювач містить наступні компоненти (рис. 10): 1 — вхідна шина; 2 — пам'ять кодів залишків СЗК; 3 — ПКД (асоціативна пам'ять з паралельним доступом); 4 — регістрова пам'ять зкоректованих базисних чисел; 5 — суматори унітарних кодів 2^i розрядні; 6 — двійковий суматор з прискореним переносом; 7 — двійковий суматор з швидким прискореним переносом; 8 — блок синхронізації; 9 — вихідна шина.

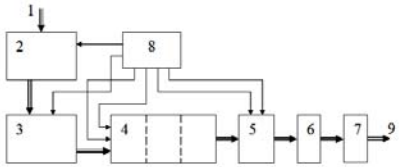

Рис. 10. *Міжбазисний перетворювач Крестенсона – Рademахера*

Особливості такої структури між базисного перетворювача Крестенсона – *Рademахера є застосування швидкодіючої ПКД з паралельним формуванням зкоректованих згідно M_i базисних чисел швидкого додавання унітарних кодів у їх кожному розряді та застосування паралельного модульного суматора з прискореним переносом. Оцінка швидкодії такого перетворювача при розрядності вхідного коду 1024 біт та застосування 107 взаємнопростих модулів з розрядністю 10 біт не перевищує 128 мікротактів, це визначає значну перспективу застосування такого між базисного перетворювача Крестенсона – Рademахера при проектуванні багаторозрядних процесорів шифрування даних.

Висновки. Представлені методи міжбазисних перетворень багаторозрядних чисел з теоретико-числового базису Радемахера в базис Крестенсона, а також запропоновані структури пристроїв, які їх реалізують, що забезпечують велику швидкодію міжбазисного перетворення. Дані пристрої дають доступ до використання швидкодіючих арифметичних операцій в РСЗК та СЗК в результаті чого отриманий результат за допомогою запропонованого пристрою зворотнього перетворення повернути у звичну систему числення для сучасної обчислювальної техніки. Тобто, розроблений спецпроцесор, який дозволяє інтегрувати високошвидкісні арифметичні пристрої базису Крестенсона в базис Радемахера.

Список використаних джерел:

1. Николайчук Я. М. Коди поля Галуа : теорія і застосування: монографія. Тернопіль: ТзОВ «Терно-граф», 2012. 576 с.
2. Волинський О. І. Methods of interbase transformations are on the basis of the delimited scale of notation of remaining classes. *Advanced Computer Systems and Networks: Design and Application*. 2009. № 4. Т 1. С. 314–317.
3. Волинський О. І. Вибір оптимальних наборів модулів для реалізації міжбазисного перетворювача Радемахера-Крестенсона. Праці міжнародної наукової конференції *«Питання оптимізації обчислень (ПОО-XL)»*, присвяченої 90-річчю від дня народження академіка В. М. Глушкова. Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013р. С. 60–61.
4. Krulikovskyi B., Volynskyy O., Davletova A., Kimak V. Theoretical Foundations Synthesis of Components and Accelerators for Haars, Rademachers and Krestensons Basis Multi-digit processors. Матеріали XIII-th Міжнародної науково-технічної конференції *Досвід розробки та застосування прилado-технологічних САПР в мікроелектроніці CADSM*. Видавництво Львівської політехніки. 2015. С.129–133.
5. Zadiraka Valeriy, Nykolaichuk Yaroslav. Computer technologies in information security. Petro Humenniy and others: Monograph. Ternopil: Kart-blansh, 2015. 387 p.
6. Гуменний П. В. Теоретичні засади організації асоціативної пам'яті колективного користування на основі вертикально-інформаційної технології. *Вісник Хмельницького національного університету.* Хмельницький, 2015. № 4(227). С. 153–159.

The method of the between-bases transformations for codes with many bits.

Key words: *theoretical-numerical basis (TNB), residual number system (RNS), between-bases transformations.*

Одержано 16.02.2017