УДК 681.32

ДОСЛІДЖЕННЯ СТРУКТУР КОМПОНЕНТІВ СПЕЦПРОЦЕСОРІВ МІЖБАЗИСНИХ ПЕРЕТВОРЕНЬ РАДЕМАХЕРА-КРЕСТЕНСОНА

Волинський О.І.[1)], Давлетова А.Я.[2)]
Тернопільський національний економічний університет
[1)] к.т.н. [2)] інженер

I. Постановка проблеми

В наш час все більшого поширення набувають непозиційні системи числення, зокрема система залишкових класів. Основною перевагою її в порівнянні з позиційними системами є відсутність міжрозрядних переносів в операціях додавання та множення. Другою, не менш важливою перевагою є те, що помилка в одному з модулів не впливає на розрахунки в інших модулях. Цей факт дозволяє проектувати пристрої з підвищеною стійкістю до відмов і корекцією помилок [1]. При розробці компонентів процесорів обчислювальної техніки критерієм оптимальності вважаються мінімальна апаратні та часові затрати [2]. Підвищення швидкодії особливо важливе при зростанні розрядності процесорів в діапазоні 64, 128, 256, …, 1024 біт.

II. Мета роботи

Метою роботи є дослідження та вибір оптимальних характеристик спецпроцесорів міжбазисного перетворення Радемахера-Крестенсона, які забезпечують досягнення максимальної швидкодії з урахуванням апаратних затрат при заданій розрядності процесорів.

III. Спецпроцесор 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. Структурна схема такого міжбазисного перетворювача зображена на рисунку 1, що складається: 1 – вхідні шини K –розрядного позиційного числа, 2 – комутаційні мультиплексори, 3 – виходи коду b_i системи залишкових класів. На рисунку 2 зображена структурна схема компонента міжбазисного перетворювача Радемахера-Крестенсона 2 – комутаційного мультиплексора до складу якого входять: 2.1 – рандомізатор по модулю P_j, 2.2 – інкрементний пристрій по модулю P_j, 2.3 – P-канальний двохвходовий мультиплексор.

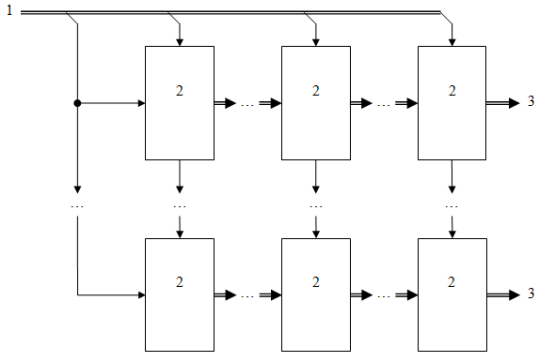

Рисунок 1 - Структурна схема міжбазисного перетворювача Радемахера-Крестенсона

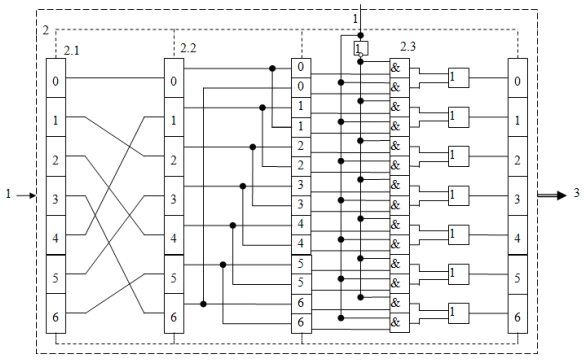

Рисунок 2 - Структурна схема комутаційного мультиплексора міжбазисного перетворювача Радемахера-Крестенсона

На рисунку 3 представлений граф супершвидкодіючого міжбазисного перетворення Радемахера-Крестенсона (час перетворення 4 мікротакти незалежно від розрядності двійкового числа), компонентом якого є модуль рандомізації.

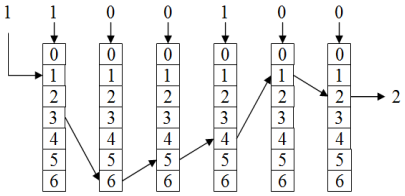

Рисунок 3 - Граф міжбазисного перетворення Радемахера-Крестенсона по mod7

IV. Аналіз системних характеристик компонентів процесорів міжбазисних перетворень

Для реалізації міжбазисного перетворювача використовуються відповідні набори модулів представлені в таблиці 1, що дозволяє продемонструвати переваги вибору модулів при різній розрядності спецпроцесора.

Таблиця 1

Набори модулів та їх характеристики для різної розрядності спецпроцесора

	Розрядність спецпроцесора (біт)							
	8	16	32	64	128	256	512	1024
Розрядність модулів min (біт)	3	4	5	6	7	8	9	10
Кількість моділів min	3	5	7	12	20	34	61	107
Розрядність модулів max (біт)	5	6	7	8	9	10	11	12
Кількість моділів max	2	3	5	9	15	27	49	91

Апаратні затрати обчислюються згідно формули $A=n2LE+kLE+A_{ПЗП}$, де n – розрядність процесора, LE – логічний елемент, k- розрядність модуля, $A_{ПЗП}=2pk$ - апаратні затрати ПЗП. Апаратні затрати міжбазисних перетворювачів на основі ПЗП [3] та мультиплексованих рандомізаторів [4] згідно наборів модулів табл.1 наведені на рисунку 4.

З графіка видно, що апаратні затрати міжбазисного перетворювача менші при наборі модулів min в 2 рази ніж при наборі модулів з розрядністю max, тому для реалізації спецпроцесора доцільніше застосовувати набори модулів з меншою розрядністю.

Оцінку часових затрат спецпроцесора міжбазисного перетворення на основі рандомізаторів та мультиплексорів розраховуємо згідно виразів: $\tau = 2LE$, що відповідає тривалості переключення двох послідовно підключених елементів мультиплексора. Оскільки всі мультиплексори переключаються одночасно при подачі на їх входи бітових значень великорозрядного двійкового числа, то швидкодія такого міжбазисного перетворювача не залежить від перетворюваного числа базису Радемахера, на відміну від міжбазисного перетворювача на ПЗП, швидкодія якого залежить від розрядності. Часові затрати розробленого методу обчислення залишку великорозрядних чисел по заданому модулю, згідно рекурентного співвідношення $b_i=(a_i+2b_i-1)mod\ p_i$, обчислюються згідно виразу: O(n)=2n. Результатом чисельного експерименту показано (рис.5), що мультиплексований рандомізатор (O) характеризується, в порівнянні з відомими (O1-O3), меншими часовими затратами на 2-3 порядки.

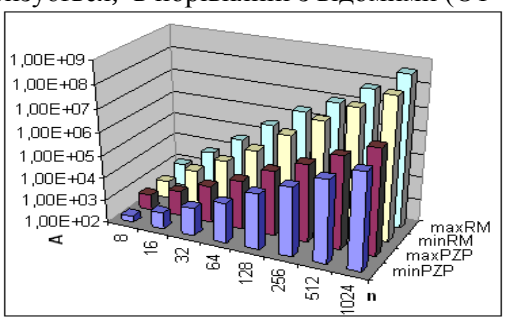

Рисунок 4 - Апаратні затрати міжбазисних перетворювачів

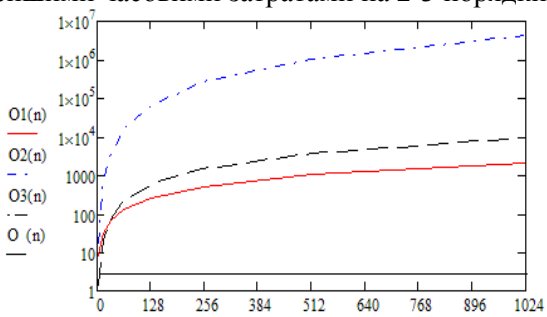

Рисунок 5 - Часові затрати обчислення залишків по модулю

Висновок

У роботі досліджені критерії часової та апаратної складності структур міжбазисних перетворювачів, що можуть бути використані в якості компонентів спецпроцесорів обчислювальних пристроїв, які працюють у двійковій системі числення базису Радемахера та системі числення залишкових класів теоретико-числового базису Крестенсона.

Список використаних джерел

1. B. Krulikovskyi, O. Volynskyy, A. Davletova, V. Kimak Theoretical Foundations Synthesis of Components and Accelerators for Haar's, Rademacher's and Krestenson's Basis Multi-digit Processors / Proceeding of XIII International Conference CADSM, 2015.-Lviv: Lviv Polytechnic Publishing House, 2015.- p. 129-133
2. B.Krulikovskyi, N.Vozna, V.Kimak, A.Davletova The Method to Optimize Structural, Hardware and Time Complexities Characteristics Multi-Bit Adders of Special Processors for Data Encryption / Modern Problem of Radio Engineeriong, Telecommunikations and Computer Science: proceedings of the XIII th International Conference TSET'2016, February 23-26, 2016.- S. 455-459
3. Николайчук Я.М., Волинський О.І. Спосіб визначення залишку двійкового числа / Патент на корисну модель № 74576. МПК G 06 F5/00. Опубл. 12.11.2012. Бюл. № 21
4. Николайчук Я.М., Волинський О.І. Пристрій для перетворення чисел з позиційної системи в систему залишкових класів. / Патент на корисну модель № 76623 МПК G06F5/02 Опублікований 10.01.2013. - Бюл.№1