УДК: 621.391

РЕАЛІЗАЦІЯ ДИСКРЕТНИХ ТЕОРЕТИКО-ЧИСЛОВИХ ПЕРЕТВОРЕНЬ НАД ПОЛЯМИ ГАЛУА

Превисокова Н.В., асистент кафедри інформатики Прикарпатського національного університету імені Василя Стефаника, м. Івано-Франківськ, natvolo@rambler.ru

Для виконання основних завдань цифрового оброблення інформації (ЦОІ) розробляються методи дискретних теоретико-числових перетворень. Зростання обсягів інфопотоків зумовлює необхідність збільшення ефективності використання обчислювальних потужностей засобів ЦОІ, яка залежить від методу формування, перетворення, оброблення, схемотехнічної реалізації, форми подання інформації та, зокрема, від швидкості виконання арифметичних операцій при реалізації перетворень.

Для подання чисел в цифрових системах найчастіше використовується двійкова система числення. Проте, час виконання арифметичних операцій в двійковій системі залежить від розрядності пристрою внаслідок формування та поширення міжрозрядних переносів. Аналіз результатів розробки сучасних методів ефективних обчислень вказав на існування альтернативних методів кодування, зокрема, розроблений метод виконання арифметичних операцій додавання-віднімання та перемноження, що ґрунтується на паралельній обробці операндів із використанням рекурсивного упорядкування кодування Галуа.

З метою встановлення ефективності застосування методу кодування Галуа проаналізовано особливості виконання арифметичних модульних операцій, тобто

операцій додавання та множення за модулем $2^n - 1$ над розширеними полями Галуа GF(p^n), де p – просте, n – натуральне, у двійковій системі та операцій із використанням кодування Галуа і визначено час їх виконання.

Тривалість виконання операції додавання із поданням інформації у двійковій системі залежить від типу двійкового суматора. Проаналізовано час виконання додавання двійковими суматорами для паралельних операндів з паралельними переносами, які забезпечують досягнення максимальної швидкодії.

Порівняно із звичайним перемножувачем двійкових чисел, модульний перемножувач містить матрицю із n суматорів. Час виконання перемноження визначається сумою часу виконання операції перемноження двох чисел без приведення результату за модулем та часу зведення добутку за модулем $2^n - 1$.

Специфіка рекурсивного упорядкування методу кодування Галуа передбачає реалізацію арифметичних операцій додавання та перемноження на основі матриці програмованих логічних елементів, час доступу до яких не перевищує часу виконання відповідних операцій в двійковій системі числення.

Проаналізовано швидкодію пристроїв виконання арифметичних операцій двійковій системі числення та при Галуа-кодуванні. Встановлено, що час виконання арифметичних операцій в кодових системах Галуа менший, ніж при використанні двійкової системи числення. Проведені дослідження доводять ефективність за показником часу застосування Галуа-кодування для виконання арифметичних операцій над полями Галуа.