ДО ОЦІНКИ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ТЕОРЕТИКО-ЧИСЛОВИХ ПЕРЕТВОРЕНЬ

Івашко А.В., Лунін Д.О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

У завданнях цифрової обробки сигналів, наприклад в спектральному і кореляційному аналізі, часто виникає необхідність в точному обчисленні перетворень, інваріантних до циклічного зсуву, наприклад так званих теоретико-числових перетворень (ТЧП). Використання таких перетворень дозволяє швидко розраховувати кореляцію і згортання на основі обчислювальної схеми, розглянутої в [1].

ТЧП послідовності x_i, $i = 0 \ldots N-1$ визначається як

$$X_k = \sum_{i=0}^{N-1} x_i \cdot g^{ik} \pmod{p}, \qquad (1)$$

де p – просте, g- первісний корінь числа p.

При розрахунку ТЧП важливим є вибір модуля p, що визначає обсяг обчислень. В якості модуля найчастіше використовують числа Ферма $2^{2^m}+1$ і Мерсена $2^q - 1$ (де q - просте). Операція складання по модулю числа Мерсена виконується досить просто, з використанням q-розрядного суматора з циклічним перенесенням [1].

Відома, однак, невелика кількість чисел Ферма і Мерсена, що дозволяють обчислювати ТЧП необхідної розмірності, тому можуть бути використані також модулі виду $p=p_1 \cdot p_2+1=(2^a-1)\cdot 2^b+1$, що допускають просту апаратну і програмну реалізацію ТЧП розмірності 2^n.

Оскільки операція множення по модулю виконується за допомогою операцій додавання і зсуву, то трудомісткість розрахунку ТЧП в значній мірі залежить від кількості одиниць в двійковому представлення ступенів первісного кореня g. Для часто використовуваної в обробці сигналів розмірності 1024 був проведений порівняльний аналіз можливих простих модулів, результати якого зведені в табл. 1.

Таблиця 1

Модуль p	12289	15361	61441	64513	114689
Число складань A	29785	28968	32555	33067	33799

Аналіз таблиці показує, що мінімальний обсяг обчислень при розрахунку швидкого ТЧП забезпечують значення модуля p = 15361 і первісного кореня g = 84.

Література:

1. Івашко А.В. Оцінювання автокореляційних функцій з використанням теоретико-числових перетворень / Івашко А.В., Лунін Д.О. // Вісник НТУ «ХПІ». – 2005.– № 38 – С. 50-54.