СТРУКТУРА СУМАТОРА ДЛЯ ТЕОРЕТИКО-ЧИСЛОВИХ ПЕРЕТВОРЕНЬ ЗА МОДУЛЕМ $7 \cdot 2^N + 1$

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

У завданнях дискретного спектрального і кореляційного аналізу широке застосування знайшли теоретико-числові перетворення (ТЧП), які дозволяють швидко розраховувати кореляцію і згортку на основі обчислювальної схеми, розглянутої в [1].

Зазвичай визначення ТЧП починається з вибору модуля p, а потім досліджуються можливі значення N. В якості модуля вибираються прості числа, що дозволяє провадити як пряме, так і зворотне ТЧП

Серед простих модулів найчастіше використовують числа Ферма $2^{2^m}+1$ та Мерсена $2^q - 1$ [2]. (де q - просте) [2]. Також існує ряд модулів виду $p=p_1 \cdot p_2+1=(2^a-1)\cdot 2^b+1$. Ці модулі забезпечують обчислення ТЧП розмірності 2n, що дозволяє застосовувати ефективні алгоритми швидких перетворень.

У роботі розглядається структура суматора за модулем $p= 7\cdot 2^n+1$. Для цього виду модуля було знайдено просте число $p= 7\cdot 2^n+1= 114\ 689$, для якого $n = 14$, довжина послідовності $N = 16384$ і первісний коріння g = 15.

Результати арифметичних дій за модулем $7\cdot 2^n+1$можуть бути легко приведені до залишків, якщо врахувати, що $8\cdot 2^n$ порівняно з (2^n-1) за модулем $7\cdot 2^n+1$. Тому при додаванні, розряд перенесення з вагою $8\cdot 2^n$ формує значення, що складається з n одиничних біт. Далі це сформоване значення необхідно скласти з n - молодшими розрядами вийшла суми. В результаті формується сума за модулем $p=7\cdot 2^n+1$.

Структура суматора була промоделювати і протестована в середовищі Active-HDL ver.9.1, що довело її працездатність і можливість побудови процесорів ТЧП на основі ПЛІС або спеціалізованих БІС.

Література:

1. Ивашко А.В. Оценивание автокорреляционных функций с использованием теоретико-числовых преобразований / Ивашко А.В., Лунин Д.А. – Вестник НТУ «ХПИ». – 2005.- № 38 – стр. 50-54.

2. Andrey Ivashko, Igor Liberg, Denis Lunin Synthesis of fast-operating devices for digital signal processing based on the number-theoretic transforms. Eastern-European Journal of Enterprise Technologies. 2020. № 1/4 (103). P. 6–10.