

АППАРАТНАЯ РЕАЛИЗАЦИЯ ТЕОРЕТИКО-ЧИСЛОВОГО ПРЕОБРАЗОВАНИЯ ФЕРМА НА БАЗЕ FPGA

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белый В.Л.

Качинский М.В. – к.т.н., доцент

Аннотация – Во многих задачах цифровой обработки сигналов приходится сталкиваться со сверткой, поэтому особый интерес представляют различные преобразования обладающие свойством свертки, а также преобразования, имеющие быстрый алгоритм, аналогичный быстрому преобразованию Фурье. Одним из таких преобразований является преобразование, которое определено в кольце целых чисел с операциями сравнения по модулю некоторого числа Ферма.

Теоретико-числовые преобразования привлекательны с точки зрения реализации свертки, т.к. могут выполняться без умножений. Реализовывалось 32-точечное преобразование со следующими параметрами: $F_t = 2^{16}$, $\alpha = 2$, длина кодового слова – 16 бит. Теоретико-числовое преобразование Ферма последовательности $x(k)$ определяется следующим образом:

$$X(n) = \sum_{k=0}^{N-1} x(k) \alpha^{-nk \bmod N} \bmod F_t$$

где F_t – число Ферма, α – корень N -й степени из единицы, N – степень 2.

На рисунке 1 приведена структурная схема, реализующая быстрый алгоритм преобразования Ферма:

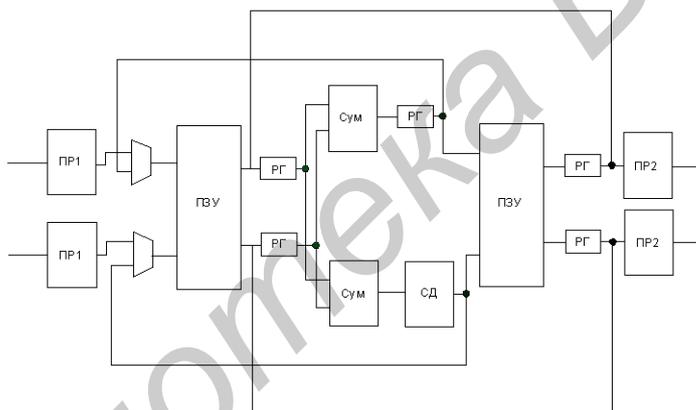


Рисунок 1 – Структурная схема быстрого алгоритма преобразования Ферма

Реализация ТЧФФ осуществляется в специальной кодировке, отличной от обычного двоичного представления чисел. В связи с этим на входах и выходах системы находятся преобразователи из двоичной системы в систему по модулю F_t , и наоборот.

Решение задачи сводилось к циклическому выполнению алгоритма “бабочка”, аналогичного БПФ. Устройство было разбито на две параллельные ветви, выполняющие операции и формирующие промежуточные и конечные отсчеты.

Система была описана на языке описания аппаратуры VHDL, синтезирована в среде Xilinx ISE и промоделирована в ModelSim.

Таким образом, были разработаны преобразователь двоичного кода в код по модулю числа Ферма, обратный ему преобразователь, реализовано 32-точечное преобразование Ферма на базе FPGA.

Список использованных источников:

1. J.M. Pollard, "The fast Fourier transform in a finite field", Math. Comp., vol. 25, pp. 365-374, Apr. 1971.
2. R.C. Agarwal, C.S. Burrus, "Fast convolution by using Fermat number transforms with applications to digital filtering", IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-22, pp. 1-10, Feb 1974.
3. L.R. Rabiner, B. Gold, "Theory and Application of Digital Signal Processing", Englewood Cliffs, NJ: Prentice-Hall, 1974.
4. Библио П.Н., "Основы языка VHDL", Изд. 3-е доп., - М.: Издательство ЛКИ, 2007.