A Novel Derivation of the Agarwal-Cooley Fast Cyclic Convolution Algorithm Based on the Good-Thomas Prime Factor Algorithm

Marvi Teixeira
Polytechnic University of Puerto Rico
Electrical Engineering Department
377 Ponce de Leon, San Juan, P.R. 00918

Domingo Rodriguez
University of Puerto Rico
Electrical Engineering Department
Mayagüez, P. R. 00681-5000, U.S.A.

***Abstract*—The Agarwal-Cooley fast cyclic convolution algorithm and the Good-Thomas Prime Factor algorithm have been traditionally independently derived. In this work we show how the Prime Factor Algorithm triggers the Agarwal-Cooley decomposition in the discrete time domain. A new polynomial expression based on the tensor product formulation of the Prime Factor Algorithm is used in conjunction with the cyclic convolution theorem, to obtain a novel and insightful derivation of the Agarwal-Cooley fast cyclic convolution algorithm.**

I. Introduction

Traditionally, the Prime Factor FFT Algorithm and the Agarwal-Cooley fast cyclic convolution algorithm, have been, each, independently derived in the discrete frequency domain and in the discrete time domain respectively [1]. In this work we show how the Agarwal-Cooley fast cyclic convolution algorithm can be directly derived from the Prime Factor algorithm. We first establish a new polynomial expression based on the tensor product formulation of the Prime Factor algorithm. This decomposition, following a methodology used in [2], [3], is then inserted into the expression of the cyclic convolution theorem. Comparing both sides, using the indeterminate coefficients method, and noting that the polynomial multiplication is modular, we obtain the Agarwal-Cooley fast cyclic convolution algorithm. This approach not only gives a novel derivation for the algorithm, but also a better understanding of the underlying relations between both decompositions.

II. Algorithm Formulation

Given a discrete Fourier transform of size N, with $N = R.S$ and $(R,S) = 1$ (relatively primes), one form of the Good-Thomas PFA is given by [1]

$$F_N = Q_1(F_R \otimes F_S)Q_2 \tag{1}$$

where Q_1 and Q_2 are permutation matrices and F_N, F_R and F_S are Fourier matrices of size N by N, R by R and S by S respectively.

0-7803-2972-4/96$5.00©1996 IEEE

Let $x[n]$, $h[n]$ and $y[n]$ be sequences of length N, where $y[n]$ is the cyclic convolution of $x[n]$ and $h[n]$

$$y[n] = \sum_{k=0}^{N-1} x[k]h[n-k] \tag{2}$$

which can also be written in matrix form as follows

$$y = Hx$$

where H is the circulant matrix formed with the vector h.

The cyclic convolution theorem gives

$$Y[k] = H[k].X[k]$$

or in matrix form

$$F_N y = F_N h.F_N x \tag{3}$$

Substituting (1) into (3) we obtain the following:

$$[Q_1(F_R \otimes F_S)Q_2]y = ([Q_1(F_R \otimes F_S)Q_2]h).([Q_1(F_R \otimes F_S)Q_2]x) \tag{4}$$

Since Q_1 is a permutation matrix and the multiplication is point wise Q_1 cancels

$$(F_R \otimes F_S)Q_2 y = ((F_R \otimes F_S)Q_2 h).((F_R \otimes F_S)Q_2 x) \tag{5}$$

The remaining tensor product expressions can be formulated in a polynomial form as follows

$$\sum_{i=0}^{R-1}[W_R^{ki} \otimes F_S]y_{qi} = (\sum_{i=0}^{R-1}[W_R^{ki} \otimes F_S]h_{qi}).(\sum_{i=0}^{R-1}[W_R^{ki} \otimes F_S]x_{qi}) \tag{6}$$

where

$$y_{qi} = Q_2 y, \quad h_{qi} = Q_2 h, \quad x_{qi} = Q_2 x$$

are the permuted vectors y, h and x, partitioned in R sections ($i = 0,\ldots,R-1$) of length S. The W_R^{ki}, in turn, are the columns of the size R by R, Fourier matrix, F_R.

Expanding each factor in (6) gives

$$[W_R^{k0} \otimes F_S]y_{q0} + [W_R^{k1} \otimes F_S]y_{q1} + \ldots + [W_R^{k(R-1)} \otimes F_S]y_{q(R-1)}$$
$$= ([W_R^{k0} \otimes F_S]h_{q0} + [W_R^{k1} \otimes F_S]h_{q1} + \ldots + [W_R^{k(R-1)} \otimes F_S]h_{q(R-1)})$$
$$.([W_R^{k0} \otimes F_S]x_{q0} + [W_R^{k1} \otimes F_S]x_{q1} + \ldots + [W_R^{k(R-1)} \otimes F_S]x_{q(R-1)}) \tag{7}$$

and since

$$W_R^{ki} = W_R^{k(R+i)} \tag{8}$$

the indicated polynomial multiplication is modulo x^R-1.

After performing the multiplication and collecting similar terms we obtain

$$W_R^{k0} \otimes F_S y_{q0} + W_R^{k1} \otimes F_S y_{q1} + \ldots + W_R^{k(R-1)} \otimes F_S y_{q(R-1)}$$
$$= W_R^{k0} \otimes (F_S h_{q0} . F_S x_{q0} + F_S h_{q(R-1)} . F_S x_{q1} + \ldots$$
$$+ F_S h_{q1} . F_S x_{q(R-1)}) + W_R^{k1} \otimes (F_S h_{q1} . F_S x_{q0} + F_S h_{q0} . F_S x_{q1} + \ldots$$
$$+ F_S h_{q2} . F_S x_{q(R-1)}) + \ldots + W_R^{k(R-1)} \otimes (F_S h_{q(R-1)} . F_S x_{q0}$$
$$+ F_S h_{q(R-2)} . F_S x_{q1} + \ldots + F_S h_{q0} . F_S x_{q(R-1)}) \tag{9}$$

Note that the following tensor product properties were used:

$$(A \otimes B)(D) = A \otimes BD \tag{10}$$

$$(A \otimes B)(C \otimes D) = AC \otimes BD \tag{11}$$

Comparing both sides in (9) using the indeterminate coefficients method yields

$$F_S y_{q0} = F_S h_{q0} . F_S x_{q0} + F_S h_{q(R-1)} . F_S x_{q1} + \ldots + F_S h_{q1} . F_S x_{q(R-1)}$$
$$F_S y_{q1} = F_S h_{q1} . F_S x_{q0} + F_S h_{q0} . F_S x_{q1} + \ldots + F_S h_{q2} . F_S x_{q(R-1)}$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$F_S y_{q(R-1)} = F_S h_{q(R-1)} . F_S x_{q0} + F_S h_{q(R-2)} . F_S x_{q1} + \ldots$$
$$+ F_S h_{q0} . F_S x_{q(R-1)} \tag{12}$$

and after multiplying by F_S^{-1} at both sides, we obtain:

$$y_{q0} = F_S^{-1}(F_S h_{q0} . F_S x_{q0}) + F_S^{-1}(F_S h_{q(R-1)} . F_S x_{q1}) + \ldots$$
$$+ F_S^{-1}(F_S h_{q1} . F_S x_{q(R-1)})$$
$$y_{q1} = F_S^{-1}(F_S h_{q1} . F_S x_{q0}) + F_S^{-1}(F_S h_{q0} . F_S x_{q1}) + \ldots$$
$$+ F_S^{-1}(F_S h_{q2} . F_S x_{q(R-1)})$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$y_{q(R-1)} = F_S^{-1}(F_S h_{q(R-1)} . F_S x_{q0}) + \ldots$$
$$+ F_S^{-1}(F_S h_{q0} . F_S x_{q(R-1)}) \tag{13}$$

Where each term is a cyclic convolution and thus can be written in terms of appropriate circulant matrices such

$$H_{qi} x_q = F_S^{-1}(F_S h_{qi} . F_S x_q) \tag{14}$$

using (14) to rewrite (13) gives

$$y_{q0} = H_{q0} x_{q0} + H_{q(R-1)} x_{q1} + \ldots + H_{q1} x_{q(R-1)}$$
$$y_{q1} = H_{q1} x_{q0} + H_{q0} x_{q1} + \ldots + H_{q2} x_{q(R-1)}$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$y_{q(R-1)} = H_{q(R-1)} x_{q0} + H_{q(R-2)} x_{q1} + \ldots + H_{q0} x_{q(R-1)} \tag{15}$$

which writing in matrix form yields:

$$\begin{bmatrix} Y_{q0} \\ Y_{q1} \\ . \\ . \\ Y_{q(R-2)} \\ Y_{q(R-1)} \end{bmatrix} = \begin{bmatrix} H_{q0} & H_{q(R-1)} & . & . & H_{q2} & H_{q1} \\ H_{q1} & H_{q0} & . & . & H_{q3} & H_{q2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ H_{q(R-2)} & H_{q(R-3)} & . & . & H_{q0} & H_{q(R-1)} \\ H_{q(R-1)} & H_{q(R-2)} & . & . & H_{q1} & H_{q0} \end{bmatrix} \begin{bmatrix} X_{q0} \\ X_{q1} \\ . \\ . \\ X_{q(R-2)} \\ X_{q(R-1)} \end{bmatrix} \tag{16}$$

Where $Y_{q0}, \ldots, Y_{q(R-1)}$, are the R sections of length S in the permuted version of y, $y_{qi} = Q_2 y$, and $H_{q0}, \ldots, H_{q(R-1)}$, are circulant matrices of size S by S which are the entries of the block circulant matrix, H_q, of size R by R. Thus, (16) can now be written as

$$Q_2 y = H_q Q_2 x \tag{17}$$

or

$$y = Q_2^{-1} H_q Q_2 x \tag{18}$$

which is the well known Agarwal-Cooley fast cyclic convolution algorithm [1], where H_q is a block circulant matrix such that,

$$H_q = Q_2 H Q_2^{-1} \tag{19}$$

This methodology automatically accounts for the fact, that the same permutation Q_2, is used in both, the PFA and the Agarwal-Cooley fast cyclic convolution algorithm.

III. Previous Work

When the permutations involved are stride permutations, such in the case of the radix r decimation in time decomposition, we obtain through a similar procedure [2], [3], a fast cyclic convolution algorithm based on block pseudocirculant matrices. Additional details on the traditional derivation of the PFA and the Argawal Cooley fast cyclic convolution algorithm, including their tensor product formulations, can be found in [1].

IV. Conclusions

Using a novel methodology the Agarwal-Cooley fast cyclic convolution algorithm has been directly derived from the Prime Factor factorization in the discrete frequency domain. Since the traditional methodology derives both algorithms independently and within respective domains, the present approach gives a better understanding of the underlying relations between both decompositions. A useful polynomial expression for certain tensor product formulations involving the Fourier matrix, has also been proposed and illustrated.

References

[1] R. Tolimieri and C. Lu, *Algorithms for Discrete Fourier Transform and Convolution,* Springer-Verlag, New York, N.Y. 1989.

[2] M. Teixeira and D. Rodriguez, "A class of fast cyclic convolution algorithms based on block pseudocirculants," IEEE Signal Processing Letters, pp 92-94, Vol 2. No.5, May 1995.

[3] M. Teixeira and D. Rodriguez, "A new method mathematically links fast Fourier transform algorithms with fast cyclic convolution algorithms," Proc. 37th Midwest Symposium on Circuit and Systems, Lafayette, Lousiana, August 1994.