International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Design Polynomial Matrix Multiplication by Using Circular Convolution Theorem

N. Swathi Lakshmi & Dr. K Amit Bindaj

[1]p.G Scholar, Dept. Of Vlsi Design, Sai Tirumala Nvr Engineering College, Jonnalagadda, Guntur

[2]professor & H.O.D, Dept. Of Vlsi Design, Sai Tirumala Nvr Engineering College, Guntur

ABSTRACT:

The main aim of this project is design polynomial matrix multiplication by using circular convolution theorem. This work exhibits a scientific system for the advancement of productive calculations for cyclic convolution calculations. The system depends on the Chinese Reminder Theorem (CRT).In especially, this work concentrates on the number-crunching multifaceted nature of a grid vector item when this item speaks to a CC computational operation or it speaks to a polynomial duplication modulo the polynomial z N-1, where N speaks to the most extreme length of every polynomial factor what's more, it is set to be an energy of 2. The proposed calculations are looked at against existing calculations created making utilization of the CRT and it is demonstrated that these proposed calculations display favorable position in computational effectiveness. They are additionally thought about against different calculations that influence utilization of the Fast Fourier to change (FFT) to perform circuitous CC operations, accordingly, showing a portion of the benefits of the proposed advancement structure.

I.INTRODUCTION

Coordinate calculation of a network vector item takes 2 N complex duplications; in any case, by misusing the uncommon structure of a circular framework, the computational exertion could be considerably diminished for substantial grids. One approach is to utilize the quick Fourier change (FFT), which makes conceivable to process a network vector item in (N)log (N) 2 complex increases for a framework of request N . In this work calculations are created by methods for pulverization in time approach, and the utilization of the underlying foundations of the solidarity (considering the polynomial z N - 1 in the intricate field). They require just N duplications, with a few favorable circumstances over FFT, for example, memory utilize and tending to strategies.

Vector multiplications:

In mathematics, Vector multiplication refers to one of several techniques for the multiplication of two (or more) vectors with themselves. It may concern any of the following articles: Dot product — also known as the "scalar product", an operation that takes two vectors and returns a scalar quantity.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

II.CHARACTERISTIC POLYNOMIALS

So far our discussion has dealt only theoretically with the existence of Eigen values of an operator T ∈ L(V). From a practical standpoint, it is much more convenient to deal with the matrix representation of an operator. Recall that the definition of an Eigen value $\lambda \in F$ and Eigen vector $v = \Sigma v_i e_i$ of a matrix $A = (a_{ij}) \in M_n(\mathcal{F})$ is given in terms of components by $\Sigma_j a_{ij} v_j = \lambda v_i$ for each i = 1, . . . , n. This may be written in the form

$$\sum_{j=1}^{n} a_{ij} v_j = \lambda \sum_{j=1}^{n} \delta_{ij} v_j$$

Alternatively it can be written as

$$\sum_{j=1}^{n} (\lambda \delta_{ij} - a_{ij}) v_j = 0$$

In matrix notation, this is

$$(\lambda I - A)v = 0$$

Multiplication

Multiplication of two polynomials is the convolution of the two coefficient sequences. Given the polynomials the product is written as

$$c(z) = a(z)b(z) = \left(\sum_{v=-V_1}^{V_2} C_{a,v} z^{-v} \right) \left(\sum_{u=-U_1}^{U_2} C_{b,u} z^{-u} \right)$$
$$= \sum_{v=-V_1}^{V_2} \sum_{u=-U_1}^{U_2} C_{a,v} C_{b,u} z^{-(v+u)}.$$

In particular, the coefficient associated with Z^r in the product will be given by

$$C_{c,r} = \sum_{\substack{u,v \\ u+v=r}} C_{a,v} C_{b,u} = \sum_{v=-V_1}^{V_2} C_{a,v} C_{b,r-v}.$$

Defining

$$C_{a,v} = 0 \, \forall v \notin [-V_1, V_2], \quad C_{b,r-v} = 0 \, \forall (r-v) \notin [-U_1, U_2]$$

the sum can be written as an infinite sum

$$C_{c,r} = \sum_{v=-\infty}^{\infty} C_{a,v} C_{b,r-v}$$

which can be identified as the convolution sum. Let d1; d2 be the maximum degrees of the polynomials a(z); b(z). Then by zero-padding the two coefficient vectors to length d1 + d2 ▪ 1, the convolution can efficiently be evaluated using the convolution theorem That is,

$$c(z) = \mathcal{F}_d^{-1} \left(\mathcal{F}_d(a(z)) \mathcal{F}_d(b(z)) \right)$$

Where the transforms are understood to be working on the coefficient vectors of the polynomials.

Polynomial matrices:

The terms matrix and polynomial matrix will be used interchangeably, with the understanding that an ordinary matrix is just a polynomial matrix of maximum degree 0 with a single coefficient matrix.

A polynomial matrix A(z) is a matrix whose elements are polynomials, or equivalently, a polynomial whose coefficients are matrix-valued. An arbitrary polynomial matrix

$$\mathbf{A}(z) = \sum_{v=-V_1}^{V_2} \mathbf{A}_v z^{-v}$$

belongs to thec^{p*q} if $A_v \in C^{p*q}$For the given V1; V2, we can also write

$\{A_v\} \in \mathbb{C}^{p\times q\times(V_1+V_2+1)}$

The transpose AT (z), conjugate $A^T(z)$ and Hermitian conjugate $A^H(z)$=$A^T(z)$ of a polynomial matrix are obtained by applying the respective operation on each of the coefficient matrices. In addition, $\mathbf{A}^H(z^{-*})$ will be termed the Para - Hermitian conjugate of A(z). A polynomial matrix which satisfies $\mathbf{A}^H(z^{-*})\mathbf{A}(z) = \mathbf{I}$is called a Para unitary matrix [4]. This type of matrices will play an important part in the algorithms to be developed in Chapter 4,

as their columns are mutually orthogonal over all frequencies. Due to this orthogonality, the

multiplication of an arbitrary matrix with a par unitary matrix preserves the Frobenius norm

of the original matrix.

Polynomial matrix multiplication:

Suppose we are given two polynomials:

p(x) = a0 + a1x + · · · + an−1xn−1,

q(x) = b0 + b1x + · · · + bn−1xn−1.

Their product is defined by

$$p(x)\cdot q(x) = c_0 + c_1x + \cdots c_{2n-2}x^{2n-2}$$

$$c_i = \sum_{\max\{0,i-(n-1)\}\le k\le \min\{i,n-1\}} a_k b_{i-k}.$$

In computing the product polynomial, every a_i is multiplied with every b_j , for 0 ≤ i, j ≤ n −1. So

there are at most n^2 multiplications, given that some of the coefficients may be zero. Obtaining

every c_i involves one fewer additions than multiplications. So there are at most n^2−2n+1 addition is involved. In short, the number of arithmetic operations is O(n^2).

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

This is hardly efficient. But can we obtain the product more efficiently, by the use of a well-known method called fast Fourier transform, or simply, FFT.

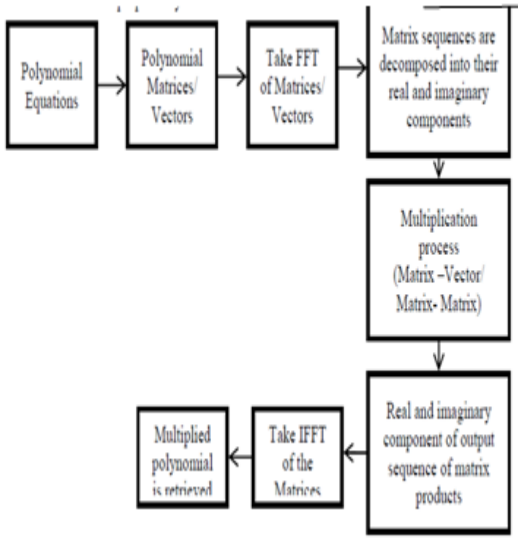
Use FFT to compute the convolution of two vectors

a = $(a_0, \ldots, a_{n-1})$ and b = $(b_0, \ldots, b_{n-1})$, Which is defined as a vector c = $(c_0, \ldots, c_{n-1})$

Where

$$c_j = \sum_{k=0}^{j} a_k b_{j-k}, \qquad j = 0, \ldots, n-1$$

.



The Multiplication of Polynomials

Let $\alpha(z) = \alpha 0+\alpha 1z+\alpha 2z2+ \cdot \cdot \cdot \alpha pzp$ and $y(z) = y0+y1z+y2z2+ \cdot \cdot \cdot ynzn$ be two polynomials of degrees p and n respectively.

Then, their product $\gamma(z) = \alpha(z)y(z)$ is a polynomial of degree $p + n$ of which the coefficients comprise combinations of the coefficient of $\alpha(z)$ and $y(z)$.

A simple way of performing the multiplication is via a table of which the margins contain the elements of the two polynomials and in which the cells contain their products. An example of such a table is given below:

	α_0	$\alpha_1 z$	α_2
y_0	$\alpha_0 y_0$	$\alpha_1 y_0 z$	$\alpha_2 y_0 z^2$
$y_1 z$	$\alpha_0 y_1 z$	$\alpha_1 y_1 z^2$	$\alpha_2 y_0 z^3$
$y_2 z^2$	$\alpha_0 y_1 z^2$	$\alpha_1 y_2 z^3$	$\alpha_2 y_2 z^4$

The product is formed by adding all of the elements of the cells. However, if the elements on the SW–NE diagonal are gathered together, then a power of the argument z can be factored from their sum and then the associated coefficient is a coefficient of the product polynomial.

$$\begin{array}{lcl} \gamma_0 & & \alpha_0 y_0 \\ +\gamma_1 z & & +(\alpha_0 y_1 + \alpha_1 y_0) z \\ +\gamma_2 z^2 & = & +(\alpha_0 y_2 + \alpha_1 y_1 + \alpha_2 y_0 +) z^2 \\ +\gamma_3 z^3 & & +(\alpha_1 y_2 + \alpha_2 y_1) z^3 \\ +\gamma_4 z^4 & & +\alpha_2 y_4 z^4. \end{array}$$

The coefficients of the product polynomial can also be seen as the products of the convolutions of the sequences *{α0, α1, α2 . . . αp}* and *{y0, y1, y2 . . . yn}*.

The coefficients of the product polynomials can also be generated by a simple multiplication of a matrix by a vector. Thus, from the example, we should have

$$\begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_2 \\ \gamma_v \end{bmatrix} = \begin{bmatrix} y_0 & 0 & 0 \\ y_1 & y_0 & 0 \\ y_2 & y_1 & y_0 \\ 0 & y_2 & y_1 \\ 0 & 0 & y_2 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} \alpha_0 & 0 & 0 \\ \alpha_1 & \alpha_0 & 0 \\ \alpha_2 & \alpha_1 & \alpha_0 \\ 0 & \alpha_2 & \alpha_1 \\ 0 & 0 & \alpha_2 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix}$$

To form the elements of the product polynomial $\gamma(z)$, powers of z may be associated with elements of the matrices and the vectors of values indicated by the subscripts. The argument z is usually described as an algebraic indeterminate. Its place can be taken by any of a wide variety of operators. Examples are provided by the difference operator and the lag operator that are defined in respect of doubly-infinite sequences. It is also possible to replace z by matrices. However, the fundamental theorem of algebra indicates that all polynomial equations must have solutions that lie in the complex plane. Therefore, it is customary, albeit unnecessary, to regard z as a complex number.

Polynomial decomposition:

This chapter will investigate a couple of polynomial decomposition algorithms which are based on the idea of iterative nulling of single coefficients. Polynomial Givens Rotations (PGRs)are employed for the coefficient nulling, Through the application of consecutive PGRs on a matrix, decompositions such as PQRD and PSVD can be found. The remaining two are slightly modified versions of the original algorithms. The decompositions generated by the algorithms will be approximations, because as shown by an exact FIR decomposition of a FIR matrix is impossible to achieve. In this thesis, approximate polynomial decomposition algorithms will be used for the channel diagonalization problem of spatial multiplexing in wireless communications.

There, a sequential best rotation algorithm is introduced using generalized Kogbetliantz transformations. The algorithm, which is not

studied in this thesis, is shown to perform better than previous sequential best rotation procedures. The _rst section of this chapter will describe the performance measures employed in the study of the algorithms. As these are defined, the following sections will investigate one algorithm at a time, with respect to function, convergence and complex it.

The PSVD of a matrix has an interesting application in spatial multiplexing for wideband wireless channels. By pre coding and receive filtering by the obtained Para unitary matrices, a channel matrix can be diagonalized over all frequencies, so that signaling can be performed

over a set of frequency-selective spatial modes.

III.TYPES OF CONVOLUTION

There are two types of convolution. They are

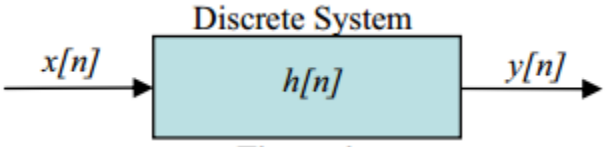
- Linear convolution
- Circular convolution

Discrete Linear Convolution A block diagram representing a basic discrete system is depicted in Figure. A discrete system is defined here as an entity which acts, transforms, or operates on a input signal, termed the input signal in order to produce another signal, termed the output signal. An important class of discrete systems is linear and shift-invariant systems known as discrete filters. A discrete filter is uniquely described by its impulse response signal, denoted by h[n],

n∈ Z, where Z is the set of integers. A discrete filter's impulse response is obtained as a resulting output signal when the input to the filter is a delta function $\delta(n)$, n∈Z , with $\delta[n] = 1$ for n= 0 and $\delta[n] = 0$ n for n $\neq 0$. Consider an arbitrary input signal x[n], to a discrete filter with an associated impulse response signal equal to h[n]. The output signal, say y[n] of the discrete filter is given by the following general expression

$$y[n] = \sum_{m=-\infty}^{m=+\infty} x[m]h[n-m] = \sum_{m=-\infty}^{m=+\infty} h[m]x[n-m], \quad n \in Z$$

This operation is commonly known as the linear convolution sum operation of the input signal x[n], with the impulse response signal h[n] and it is commutative operation.



The set of all discrete complex signals of the type x[n] becomes a linear space denoted by l [Z]. A subspace of this linear space,

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

denoted by 2 l [Z] , is the set of all discrete signals with finite energy. discrete signal, say x[n] , is said to have finite energy if the condition is satisfied.

$$\sum_{n=-\infty}^{n=+\infty} x[n]x^*[n] = \langle x, x \rangle < \infty$$

The symbol "*" in the expression above denotes complex conjugation. The expression x, y is termed an inner product of x and y , with, both, x,y∈ l^2. The norm or length of a finite energy discrete signal 2 x l Z( ) is denoted by

$$\|x\| = \langle x, x \rangle^{\frac{1}{2}}$$

IV.PERIODIC OR CYCLIC CONVOLUTION

Let x,h∈ l^2be two arbitrary sequences, each of length N . The periodic or cyclic convolution modulo N of these two signals is denoted by the expression $x \otimes_N h$ h and it is a new signal, say y , also of length N , defined by the following expression for any N ∈ z_n

$$y[n] = \left(x \otimes_N h\right)[n] = \sum_{m=0}^{N-1} x[m]h[\langle n-m \rangle_N]$$

or

$$y[n] = \left(h \otimes_N x\right)[n] = \sum_{m=0}^{N-1} h[m]x[\langle n-m \rangle_N]$$

The focus of this work is to develop fast and efficient algorithms for the computation of the circular or cyclic convolution operation, reaching the minimal number of multiplications according to the Wino grad's theorem. Normally, two approaches are utilized to compute the cyclic convolution operation, namely, the direct approach and the transform approach. The direct approach evaluates the equation for the cyclic convolution of two N - point signals for each value N ∈ z_n resulting in a system of equations. The transform approach establishes a discrete Fourier transform (DFT) isomorphism between the cyclic convolution operation two signals in the object domain and the point-by-point multiplication operation or Hadamard product of each of the transformed signals.

This section describes a cyclic convolution operator as a linear shift invariant (LSI) operator acting on the finite dimensional linear space l^2 ∈ z_n. In addition, the cyclic convolution operator is also described as a cyclic finite impulse response (FIR) system. Combining these two attributes allows for a deeper study of the properties of the cyclic convolution operator.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

A formal discussion follows, arriving at a matrix representation of a cyclic convolution operation.

V.FPGA FLOW

The basic implementation of design on FPGA has the following steps.

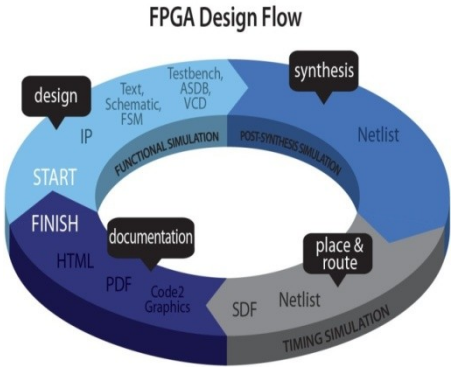


FIG: 1. DESIGN FLOW

- Design Entry
- Logic Optimization
- Technology Mapping
- Placement
- Routing
- Programming Unit
- Configured FPGA

Above shows the basic steps involved in implementation. The initial design entry of may be VHDL, schematic or Boolean expression. The optimization of the Boolean expression will be carried out by considering area or speed.

ADVANTAGES

The following are the advantages of the FPGA technology.

- Reduced time to market.
- Lower non-recurring engineering costs.
- Reprogrammable.

APPLICATIONS

The following are the applications of the FPGA technology.

- FPGA can be applied to a very wide range of applications including: random logic, integrating multiple SPLDs, device controllers, communication encoding and filtering, small to medium sized with SRAM blocks.
- Prototyping of designs later to be implemented in gate arrays. Prototyping might be possible using only a single large FPGA (which corresponds to a small gate array in terms of capacity).
- Emulation of entire hardware systems.

CONCLUSION

Here with polynomial matrix multiplication will be performed by using cyclic convolution with reduced power and efficiency than conventional ones. Cyclic

convolution is most efficient technique for reducing the power and number of iterations.

FUTURE SCOPE

- In this the 4x4 convolution and the data width is 4 bits shown. The convolution can be done for NXN and the width can be extended to N bits.
- And also use different type of convolution thermos for reducing the number of iterations.
- Use some power reduce technique to control the power dissipation also.

OUTPUT RESULT:

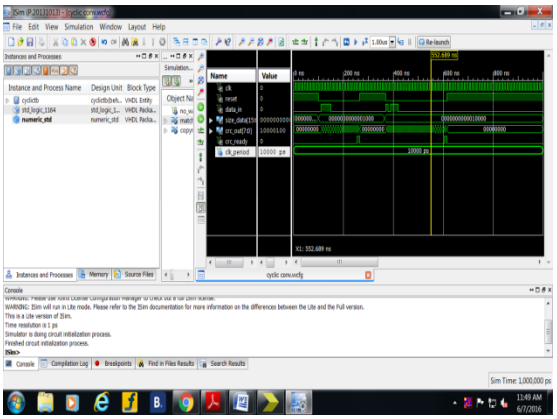


FIG: 2. OUT PUT

REFERENCES

[1] G.H. Golub and C. F. Van Loan, Matrix Computations, John Hopkins University Press, Baltimore, MD, USA, 1996.

[2] R. H. Lambert, M. Joho, and H. Mathis, ―Polynomial Singular Values for Number of Wideband Source Estimation and Principal Components Analysis,‖ in International Conference on Independent Component Analysis, 2001, pp. 379–383.

[3] S. Redif, J. G. McWhirter, P. Baxter, and T. Cooper, ―Robust Broadband Adaptive Beam forming via Polynomial Eigen values,‖ in IEEE OCEANS Conference, 2006, pp. 1–6.

[4] P. P. Vaidyanathan, ―Theory of Optimal Ortho normal Sub band Coders,‖ IEEE Transactions on Signal Processing, vol. 46, no. 6, pp. 1528–1543, June 1998.

[5] S. Redif, S. Weiss, and J. G. Mc Whirter, ―An Approximate Polynomial Matrix Eigen value Decomposition Algorithm for Para-Hermitian Matrices,‖ in IEEE International Symposium on Signal Processing and Information Technologies, 2011, pp. 421–425.

[6] S. Y. Kung, Y. Wu, and X. Zhang, ―Bezout Space-Time Pre coders and Equalizers for MIMO Channels,‖ IEEE Transactions on Signal Processing, vol. 50, no. 10, pp. 2499–2541, October 2002.

[7] J. Foster, J. G. McWhirter, S. Lambotharan, I. Proudler, M. Davies, and J. Chambers, ―Polynomial Matrix QR Decomposition and Iterative Decoding of Frequency Selective MIMO Channels,‖ IET Signal Processing, vol. 6, no. 7, pp. 704–712, September 2012.

[8] J. G. McWhirter, P. D. Baxter, T. Cooper, S. Redif, and J. Foster, ―An EVD Algorithm for Para-Hermitian Polynomial Matrices,‖ IEEE Transactions on Signal Processing, vol. 55, no. 5, pp. 2158–2169, May 2007.

[9] S. Redif, S. Weiss, and J. G. McWhirter, ―Design of FIR Para unitary Filter Banks for Sub band Coding using a Polynomial Eigen value Decomposition,‖ IEEE Transactions on Signal Processing, vol. 59, no. 11, pp. 5253–5264, December 2011.