A NOTE ON FAST CYCLIC CONVOLUTION

by

Y. Zalcstein

Computer Science Department
Carnegie-Mellon University
Pittsburgh, Pennsylvania

December 8, 1970

This work was supported by the Advanced Research Projects Agency of the Office of the Secretary of Defense (F44620-70-C-0107) and is monitored by the Air Force Office of Scientific Research.

ABSTRACT

This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires $n(n_1+1)\ldots(n_k+1)/2^k$ multiplications for the convolution of two n-vectors, where $n = n_1\ldots n_k$ is a factorization of n into factors which are pairwise relatively prime.

INDEX TERMS

convolution, cyclic matrix, super-circulant matrix

Let $\underset{\sim}{x} = (x_0, x_1, \ldots, x_{n-1})$ and $\underset{\sim}{y} = (y_0, y_1, \ldots, y_{n-1})$ be two n-vectors and let $\underset{\sim}{x} *' \underset{\sim}{y}$ be the convolution of $\underset{\sim}{x}$ and $\underset{\sim}{y}$ which is an n-vector whose k-th component is $(\underset{\sim}{x} *' \underset{\sim}{y})_k = \sum_{i=0}^{k} x_i y_{k-i}$, $k = 0, 1, \ldots, n-1$.

Convolution occurs in many applications. Computationally, it is more convenient to use the cyclic convolution $\underset{\sim}{x} * \underset{\sim}{y}$, defined by

$$\left(\sum_{i-0}^{n-1} x_i y_{n-i}, \sum_{i=0}^{n-1} x_i y_{1-i}, \ldots, \sum_{i=0}^{n-1} x_i y_{j-i}, \ldots, \sum_{i=0}^{n-1} x_i y_{n-1-i} \right) \quad (1)$$

(addition of subscripts modulo n). For example, the finite Fourier transform can only be applied to a cyclic convolution (see Ref. [1]). Any convolution can be reduced to a cyclic convolution by adjoining a sufficient number of zeros to the vectors $\underset{\sim}{x}$ and $\underset{\sim}{y}$. Computing $\underset{\sim}{x} * \underset{\sim}{y}$ directly requires n^2 multiplications. Using the fast Fourier transform (see [1], [2], [3], [4]), $\underset{\sim}{x} * \underset{\sim}{y}$ can be computed with $n[3\log n + 1]$ complex multiplications. The Fourier transform (and à fortiori the fast Fourier transform) does not exist in rings that do not contain a "sufficient" number of primitive roots of unity (see Nicholson [3]). The purpose of this note is to point out a method for computing $\underset{\sim}{x} * \underset{\sim}{y}$ using less than n^2 multiplications that works over an arbitrary commutative ring. In particular, a ring which occurs often in applications and in which Fourier transforms do not exist is the ring of integers modulo m for m composite.

Let R be a commutative ring. A circulant or cyclic matrix over R is a matrix of the form:

$$A(\underset{\sim}{x}) = \begin{bmatrix} x_0 & x_1 \cdots & x_{n-1} \\ x_{n-1} & x_0 \cdots & x_{n-2} \\ \vdots & \vdots \ddots & \vdots \\ x_1 & x_2 \cdots & x_0 \end{bmatrix}$$

i.e., $(A(\underset{\sim}{x}))_{ij} = x_{j-i}$ (subtraction modulo n), $i,j = 0,1,\ldots n-1$, where $\underset{\sim}{x} = (x_0,x_1,\ldots,x_{n-1})$ is an n-vector. The convolution $\underset{\sim}{x}*\underset{\sim}{y}$ is easily seen to be the first row of $A(\underset{\sim}{x}).A(\underset{\sim}{y})$ (matrix multiplication). The product of two circulants is a circulant. Thus $A(\underset{\sim}{x}).A(\underset{\sim}{y})$ is determined by its first row which is $\underset{\sim}{x}*\underset{\sim}{y} = \underset{\sim}{x}.A(\underset{\sim}{y})$.

LEMMA 1. The product $\underset{\sim}{x}.A(\underset{\sim}{y})$ can be computed using $n(n+1)/2$ multiplications.

PROOF. For all i and j, there exists k such that $j \equiv k-i \pmod n$; thus for $i \neq j$, both $x_i y_j$ and $x_j y_i$ appear in $\sum_{i=0}^{n-1} x_i y_{k-i}$. Applying the identity

$$x_i y_j + x_j y_i = x_i y_i + x_j y_j - (x_i - x_j)(y_i - y_j),$$

after computing the n products $x_i y_i$, $i=0,1,\ldots,n-1$, only $n(n-1)/2$ more multiplications are needed to compute $\underset{\sim}{x}.A(\underset{\sim}{y})$, giving a total of $n(n+1)/2$ multiplications.

REMARK 1. The standard algorithm for computing $\underset{\sim}{x}.A(\underset{\sim}{y})$ requires $n(n-1)$ additions. It is easy to see that the method of lemma 1 requires $\frac{5}{2}n(n-1)$ additions and subtractions. Thus a saving of $n(n-1)/2$ multiplications has been achieved at the expense of extra $\frac{3}{2}n(n-1)$ additions/subtractions.

REMARK 2. By imposing restrictions on the ring R, one can obtain refinements of lemma 1. For example, if the characteristic of R is not divisible by 2, the product of two 2×2 circulants can be computed with 2 multiplications (and 6 additions/subtractions) by

$$x_0y_0 + x_1y_1 = \frac{1}{2}[(x_0+x_1)(y_0+y_1) + (x_0-x_1)(y_0-y_1)]$$

$$x_0y_1 + x_1y_0 = \frac{1}{2}[(x_0+x_1)(y_0+y_1) - (x_0-x_1)(y_0-y_1)].$$

DEFINITION. Let $n = n_1 \dots n_k$ be a factorization of n. An $(n_1,\dots,n_k)$ super-circulant matrix is defined inductively as follows: for k=1 it is just an n×n circulant. An $(n_1,\dots,n_k)$ super-circulant S is a block matrix whose blocks follow a circulant pattern:

$$S = \begin{bmatrix} B_0 & B_1 \cdots & B_{n_k-1} \\ B_{n_k-1} & B_0 \cdots & B_{n_k-2} \\ \vdots & \vdots & \vdots \\ B_1 & B_2 & B_0 \end{bmatrix}$$

such that each B_i is an $(n_1,\dots,n_{k-1})$ super-circulant.

SUPER-CIRCULANT LEMMA (Nicholson and Zalcstein [5]). *If $n = n_1 \dots n_k$ with n_i, n_j relatively prime for $i \neq j$ ($(n_i,n_j) = 1$), then there is a permutation matrix P such that for any n×n circulant matrix A, $P^{-1}AP$ is an $(n_1,\dots,n_k)$ super-circulant.*

PROOF. The proof uses the idea of "coordinatizing" the dimension n, in the spirit of the derivation of the fast Fourier transform.

For $0 \leq j \leq n-1$, and for $p = 1,2,\ldots,k$, let j_p be the smallest positive integer congruent to j mod n_p. Since the n_p's are relatively prime, in pairs, it follows from the Chinese remainder theorem ([6], p. 97) that the map $j \to (j_1, j_2, \ldots, j_k)$ is one-to-one. Thus it is easy to see that the map $j \to j_1 + j_2 n_1 + j_3 n_1 n_2 + \ldots + j_k n_1 n_2 \ldots n_{k-1}$ is one-to-one and, indeed, a permutation of the set $\{0,1,\ldots,n-1\}$. This permutation gives the desired permutation matrix P, as we will now prove.

For $m > 0$, let Q_m be the $m \times m$ permutation matrix

$$\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ \vdots & & & & 1 \\ 1 & 0 & & & 0 \end{bmatrix}$$

representing the cyclic permutation

$$(0\ 1\ 2 \ldots (m-1)) \quad \text{on} \quad \{0,1,\ldots,m-1\}.$$

Recall the definition of the Kronecker product of two matrices (Ref. [7]): If A is an $m \times m$ matrix, the <u>Kronecker</u> or <u>tensor</u> product $A \otimes B$ is the $mn \times mn$ matrix

$$\begin{bmatrix} a_{11}B \ldots & & a_{1m}B \\ \vdots & \ddots & \\ \vdots & a_{ij}B & \vdots \\ & & \ddots \\ a_{m1}B \ldots & & a_{mm}B \end{bmatrix}$$

The Kronecker product is associative. Also, it is easy to see that the Kronecker product of permutation matrices is a permutation matrix.

Furthermore, the permutation represented by $Q_{n_1} \otimes Q_{n_2} \otimes \cdots \otimes Q_{n_k}$ can be described in "coordinatized" form as follows: it maps $j_1 + j_2 n_1 + \ldots + j_k n_1 \ldots n_{k-1}$ into $(j_1{+}1) + (j_2{+}1)n_1 + \ldots + (j_k{+}1)n_1 \ldots n_{k-1}$, where '$j_p{+}1$' means addition modulo n_p. It is then straightforward to verify that

$$P^{-1} Q_n P = Q_{n_1} \otimes Q_{n_2} \otimes \cdots \otimes Q_{n_k} \tag{2}$$

Let $A(\underset{\sim}{x})$ be an $n \times n$ circulant. Then

$$A(\underset{\sim}{x}) = \sum_{j=0}^{n-1} x_j Q_n^j, \quad \text{where } Q_n^0 = I_n, \text{ the } n \times n \text{ identity matrix.}$$

Thus, applying (2), we get

$$P^{-1} A(\underset{\sim}{x})\, P = \sum_{j=0}^{n-1} x_j (Q_{n_1} \otimes \cdots \otimes Q_{n_k})^j$$

$$= \sum_{j=0}^{n-1} x_j (Q_{n_1}^j \otimes \cdots \otimes Q_{n_k}^j) \tag{3}$$

$$= \sum_{j=0}^{n-1} x_j \, Q_{n_1}^{j_1} \otimes \cdots \otimes Q_{n_k}^{j_k} \tag{4}$$

Line (3) follows from the matrix identity $(A \otimes B) . (C \otimes D) = (A.C) \otimes (B.D)$, while line (4) follows from the identity $Q_p^p = I_p$ for all p. If C_i is an $n_i \times n_i$ circulant for $i = 1,2,\ldots k$, then $C_1 \otimes \cdots \otimes C_k$ is an

$(n_1,\ldots,n_k)$ super-circulant. Finally, a linear combination of $(n_1,\ldots n_k)$ super-circulants is an $(n_1,\ldots,n_k)$ super-circulant. Thus $P^{-1}A(\underset{\sim}{x})\,P$ is an $(n_1,\ldots,n_k)$ super-circulant and the lemma is proved. (A more conceptual proof appears in [5].)

As a consequence of the super-circulant lemma we obtain the following:

SPEED-UP LEMMA. *Suppose there is a function* $f\colon N \to N$, *where* N *is the set of positive integers such that for any commutative ring* R, *the product of two* $n \times n$ *circulants can be computed with* $f(n)$ *multiplications. Then, if* $n = n_1 \ldots n_k$, *with the* n_i*'s relatively prime in pairs, the product of two* $n \times n$ *circulants can be computed with* $f(n_1)\ldots f(n_k)$ *multiplications.*

PROOF. By the super-circulant lemma it suffices to consider multiplication of two $(n_1,\ldots,n_k)$ super-circulants. The proof is by induction on k. The assertion is trivially true for $k=1$. Assume that it is true for k and let S_1,S_2 be two $(n_1,\ldots,n_k,n_{k+1})$ super-circulants. Let R_k be the set of all $(n_1,\ldots,n_k)$ super-circulants over R. It is easy to see that R_k is a *commutative* ring, under matrix addition and multiplication. S_1 and S_2 can be considered $n_{k+1} \times n_{k+1}$ circulants over R_k. Thus S_1S_2 can be computed using $f(n_{k+1})$ multiplications in R_k. Further, by the induction hypothesis each multiplication in R_k requires $f(n_1)\ldots f(n_k)$ scalar multiplications. Thus the total number of scalar multiplications required is $f(n_1)\ldots f(n_k)f(n_{k+1})$. This proves the lemma.

By lemma 1, we can take $f(n) = n(n+1)/2$; thus we get the following:

PROPOSITION. _Let_ $n = n_1 \dots n_k$ _with_ $(n_i, n_j) = 1$ _for_ $i \neq j$. _Then the product of two_ $n \times n$ _circulants and thus the convolution of two n-vectors can be computed using_ $n(n_1+1)\dots(n_k+1)/2^k$ _scalar multiplications._

REMARK. It is easy to see that the factorization minimizing the number of multiplications by our method is the complete factorization of n into prime-power factors.

REFERENCES

[1] W. M. Gentleman and G. Sande,"Fast Fourier Transforms for Fun and Profit,"Proc. 1966 Fall Joint Computer Conference, AFIPS, v. 29, 563-578.

[2] J. W. Cooley, P. A. W. Lewis and P. D. Welch, "The Fast Fourier Transform and Its Applications," IEEE Trans. Education, E-12, 27-34, March, 1969.

[3] P. J. Nicholson, Algebraic Theory of the Finite Fourier Transform, Ph.D. thesis, Department of Operations Research, Stanford University, March, 1969.

[4] R. R. Stoner, A Flexible Fast Fourier Transform Algorithm, Army Electronics Command, Fort Huachuca, Arizona, report ECOM-6046 (CFSTI AD 696 431) August, 1969.

[5] P. J. Nicholson and Y. Zalcstein, Super-circulant Matrices and the Fast Fourier Transform, to appear.

[6] J. Landin, An Introduction to Algebraic Structures, Allyn and Bacon, Boston, 1969.

[7] R. Bellman, Introduction to Matrix Analysis, McGraw-Hill, New York, 1960.

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Department of Computer Science Carnegie-Mellon University Pittsburgh, Pennsylvania 15213	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP

3. REPORT TITLE

A NOTE ON FAST CYCLIC CONVOLUTION

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Scientific Interim

5. AUTHOR(S) (First name, middle initial, last name)

Y. Zalcstein

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
December 1970	8	7

8a. CONTRACT OR GRANT NO. F44620-70-C-0107 b. PROJECT NO. A0827-5 c. 61101D d.	9a. ORIGINATOR'S REPORT NUMBER(S) 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
TECH, OTHER	Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209

13. ABSTRACT

This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires $n(n_1+1)\ldots(n_k+1)/2^k$ multiplications for the convolution of two n-vectors, where $n = n_1\ldots n_k$ is a factorization of n into factors which are pairwise relatively prime.

DD FORM 1 NOV 65 1473

Security Classification

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT

Security Classification