A note on fast cyclic convolution

Y Zalcstein
Carnegie Mellon University

Follow this and additional works at: http://repository.cmu.edu/compsci
NOTICE WARNING CONCERNING COPYRIGHT RESTRICTIONS:
The copyright law of the United States (title 17, U.S. Code) governs the making of photocopies or other reproductions of copyrighted material. Any copying of this document without permission of its author may be prohibited by law.
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. This document has been approved for public release and sale; its distribution is unlimited.
ABSTRACT

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

INDEX TERMS

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

Convolution occurs in many applications. Computationally, it is more
convenient to use the cyclic convolution \( x^\ast y \), defined by

\[
(x^\ast y)_k = \sum_{i=0}^{n-1} x_i y_{(k-i) \mod n}, \quad k=0, 1, \ldots, n-1. 
\]

(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 \( x \) and \( y \). Computing
\( x^\ast y \) directly requires \( n^2 \) multiplications. Using the fast Fourier
transform (see [1], [2], [3], [4]), \( x^\ast y \) 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 \( x^\ast y \) 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:
The product of two circulants is a circulant. Thus \( A(x).A(y) \) is determined by its first row which is \( x^*y = x.A(y) \).

**LEMMA 1.** The product \( x.A(y) \) can be computed using \( n(n+1)/2 \) multiplications.

**PROOF.** For all \( i \) and \( j \), there exists \( k \) such that \( j = k - i \) (mod \( n \)); 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 \( x_i y_i \), only \( n(n-1)/2 \) more multiplications are needed to compute \( x.A(y) \), giving a total of \( n(n+1)/2 \) multiplications.

**REMARK 1.** The standard algorithm for computing \( x.A(y) \) requires \( n(n-1) \) additions. It is easy to see that the method of lemma 1 requires \( 5/2 n(n-1) \) additions and subtractions. Thus a saving of \( n(n-1)/2 \) multiplications has been achieved at the expense of extra \( 3/2 n(n-1) \) 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 2x2 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 \( n = n_1 \cdots n_k \) be a factorization of \( n \). An \((n_1, \ldots, n_k)\) super-circulant matrix is defined inductively as follows: for \( k = 1 \) it is just an \( n \times n \) circulant. An \((n_1, \ldots, n_k)\) super-circulant \( S \) is a block matrix whose blocks follow a circulant pattern:

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

such that each \( B_i \) is an \((n_1, \ldots, n_k)\) super-circulant.

SUPER-CIRCULANT LEMMA (Nicholson and Zalcstein [5]). If \( n = n_1 \cdots n_k \) with \( n_i, n_j \) relatively prime for \( i \neq j \), then there is a permutation matrix \( P \) such that for any \( n \times n \) circulant matrix \( A \), \( P^{-1}AP \) is an \((n_1, \ldots, n_k)\) 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 $j \mapsto (j_1,j_2,\ldots,j_k)$ is one-to-one. Thus it is easy to see that the map $j \mapsto j_1 + j_2 n_1 + j_3 n_1 n_2 + \ldots + j_k n_1 n_2 \cdots n_{k-1}$ 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

\[
\begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0
\end{bmatrix}
\]

representing the cyclic permutation

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

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

\[
\begin{bmatrix}
a_{11}B & \cdots & a_1B \\
\vdots & \ddots & \vdots \\
a_{i1}B & \cdots & a_{i\,m}B \\
\vdots & \ddots & \vdots \\
a_{m1}B & \cdots & a_{m\,m}B
\end{bmatrix}
\]
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

\[
\text{maps } j_1 + j_2 n_1 + \cdots + j_k n_1 \cdots n_{k-1} \text{ into } (j_1 + 1) + (j_2 + 1)n_1 + \cdots + (j_k + 1)n_1 \cdots n_{k-1},
\]

where \( 'j+p' \) 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 \( A(x) \) be an \( n \times n \) circulant. Then

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

Thus, applying (2), we get

\[
P^{-1} A(x) P = \sum_{j=0}^{n-1} x^j (Q_{n_1} \otimes \cdots \otimes Q_{n_k})^j
\]

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

\[
= \sum_{j=0}^{n-1} x^j Q_{n_1}^j \otimes \cdots \otimes Q_{n_k}^j \tag{4}
\]

Line (3) follows from the matrix identity \((A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)\), 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 \( P^{-1}A \xi P \) 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 \( f: \mathbb{N} \to \mathbb{N} \), where \( \mathbb{N} \) 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 \( n = n_1 \ldots n_k \) 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 \( n(n_1+1) \ldots (n_k+1)/2^k \) 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


A NOTE ON FAST CYCLIC CONVOLUTION

This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires \( n(n_1+1) \cdots (n_k+1)/2^k \) multiplications for the convolution of two \( n \)-vectors, where \( n = n_1 \cdots n_k \) is a factorization of \( n \) into factors which are pairwise relatively prime.
<table>
<thead>
<tr>
<th>KEY WORDS</th>
<th>LINK A</th>
<th>LINK B</th>
<th>LINK C</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE</td>
<td>WT</td>
<td>ROLE</td>
<td>WT</td>
</tr>
</tbody>
</table>

Security Classification