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

Ъy

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.

2

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

Convolution occurs in many applications. Computationally, it is more convenient to use the <u>cyclic</u> convolution x*y, defined by

(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 \underline{x} and \underline{y} . Computing $\underline{x^*y}$ directly requires n^2 multiplications. Using the fast Fourier transform (see [1], [2], [3], [4]), $\underline{x^*y}$ can be computed with n[3log 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 $\underline{x^*y}$ 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 <u>circulant</u> or <u>cyclic</u> matrix over R is a matrix of the form:

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

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

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

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,...,n-1, only n(n-1)/2more multiplications are needed to compute $x \cdot A(y)$, giving a total of n(n+1)/2 multiplications.

<u>REMARK 1</u>. The standard algorithm for computing $x_{1}A(y)$ 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. <u>REMARK 2</u>. 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 $2x^2$ circulants can be computed with 2 multiplications (and 6 additions/subtractions) by

$$\begin{aligned} x_0 y_0 + x_1 y_1 &= \frac{1}{2} [(x_0 + x_1)(y_0 + y_1) + (x_0 - x_1)(y_0 - y_1)] \\ x_0 y_1 + x_1 y_0 &= \frac{1}{2} [(x_0 + x_1)(y_0 + y_1) - (x_0 - x_1)(y_0 - y_1)]. \end{aligned}$$

DEFINITION. Let $n = n_1 \dots n_k$ be a factorization of n. An (n_1, \dots, n_k) <u>super-circulant</u> matrix is defined inductively as follows: for k=1 it is just an nXn 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 is an (n_1, \dots, n_{k-1}) super-circulant.

SUPER-CIRCULANT LEMMA (Nicholson and Zalcstein [5]). If $n = n_1 \cdots n_k$ with n_i, n_j relatively prime for $i \neq j$ ($(n_i, n_j) = 1$), then there is a permutation matrix P such that for any nXn 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 $0 \le j \le n-1$, and for p = 1, 2, ..., 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 $j \rightarrow (j_i, j_2, ..., j_k)$ is one-to-one. Thus it is easy to see that the map $j \rightarrow j_i + j_2 n_1 + j_3 n_1 n_2 + \cdots + j_k n_1 n_2 \cdots n_{k-1}$ is one-to-one and, indeed, a permutation of the set $\{0, 1, ..., n-1\}$. This permutation gives the desired permutation matrix P, as we will now prove.

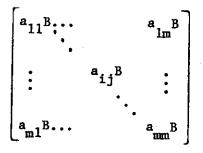
For m > 0, let Q_m be the mXm permutation matrix

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

representing the cyclic permutation

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

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



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 $j_1 + j_2 n_1 + \cdots + j_k n_1 \cdots n_{k-1}$ into $(j_1+1) + (j_2+1)n_1 + \cdots + (j_k+1)n_1 \cdots n_{k-1}$, where $'j_p+1'$ means addition modulo n_p . It is then straightforward to verify that

$$P^{-1}Q_{n}P = Q_{n_{1}} \otimes Q_{n_{2}} \otimes \cdots \otimes Q_{n_{k}}$$
(2)

Let A(x) be an nxn circulant. Then

$$A(x) = \sum_{j=0}^{n-1} x_j q_n^j, \text{ where } q_n^0 = I_n, \text{ the nxn identity matrix.}$$

Thus, applying (2), we get

$$P^{-1}A(\mathbf{x}) P = \sum_{j=0}^{n-1} x_j (Q_{n_1} \otimes \cdots \otimes Q_{n_k})^j$$
$$= \sum_{j=0}^{n-1} x_j (Q_{n_1}^j \otimes \cdots \otimes Q_{n_k}^j)$$
$$= \sum_{j=0}^{n-1} x_j Q_{n_1}^{j_1} \otimes \cdots \otimes Q_{n_k}^{j_k}$$
(3)

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 $n_i x n_i$ circulant for i = 1, 2, ..., k, then $C_1 \otimes ... \otimes C_k$ 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 $P^{-1}A(x) P$ 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 $f: N \rightarrow N$, where N is the set of positive integers such that for any commutative ring R, the product of two nxn circulants can be computed with f(n) multiplications. Then, if $n = n_1 \dots n_k$, with the n_i 's relatively prime in pairs, the product of two nxn circulants can be computed with $f(n_1) \dots f(n_k)$ 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 <u>commutative</u> 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 $f(n_1)...f(n_k)$ scalar multiplications. Thus the total number of scalar multiplications required is $f(n_1)...f(n_k)f(n_{k+1})$. This proves the lemma. By lemma 1, we can take f(n) = n(n+1)/2; thus we get the following: PROPOSITION. Let $n = n_1 \cdots n_k$ with $(n_i, n_j) = 1$ for $i \neq j$. Then the product of two nxn circulants and thus the convolution of two n-vectors can be computed using $n(n_1+1) \cdots (n_k+1)/2^k$ 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.

-7-

REFERENCES

- W. M. Gentleman and G. Sande, "Fast Fourier Transforms for Fun and Profit,"<u>Proc. 1966 Fall Joint Computer Conference</u>, <u>AFIPS</u>, v. <u>29</u>, 563-578.
- [2] J. W. Cooley, P. A. W. Lewis and P. D. Welch, "The Fast Fourier Transform and Its Applications," <u>IEEE Trans. Education</u>, E-12, 27-34, March, 1969.
- [3] P. J. Nicholson, <u>Algebraic Theory of the Finite Fourier Transform</u>, Ph.D. thesis, Department of Operations Research, Stanford University, March, 1969.
- [4] R. R. Stoner, <u>A Flexible Fast Fourier Transform Algorithm</u>, Army Electronics Command, Fort Huachuca, Arizona, report ECOM-6046 (CFSTI AD 696 431) August, 1969.
- [5] P. J. Nicholson and Y. Zalcstein, <u>Super-circulant Matrices and the</u> <u>Fast Fourier Transform</u>, to appear.
- [6] J. Landin, <u>An Introduction to Algebraic Structures</u>, Allyn and Bacon, Boston, 1969.
- [7] R. Bellman, <u>Introduction to Matrix Analysis</u>, McGraw-Hill, New York, 1960.

-8-

DOCUMENT CONTROL DATA - R & D DOCUMENT CONTROL DATA - R & D DOCUMENT CONTROL DATA - R & D DEFENDENT CONTROL CONTROL DE LA CONTRO	Security Classification						
<pre>1 OF CONVERTIGE COMPARE SUBJECT Construction of Computer Science Carnegie-Mellon University Pittaburgh, Pennsylvania 15213 - MCDEAT TITLE A NOTE ON FAST CYCLIC CONVOLUTION - Descharter were worth for a report and inclusive dates) Scientific Interim - Automit for annee and inclusive dates) Scientific Interim - Automit for annee and inclusive dates) F44620-70-C-0107 - MEDOAT TOTL A0827-5 61101D - - - - - - - - - - - - - - - - - - -</pre>	DOCUMENT CONT	COL DATA - R & D					
<pre>1 OF CONVERTIGE COMPARE SUBJECT Construction of Computer Science Carnegie-Mellon University Pittaburgh, Pennsylvania 15213 - MCDEAT TITLE A NOTE ON FAST CYCLIC CONVOLUTION - Descharter were worth for a report and inclusive dates) Scientific Interim - Automit for annee and inclusive dates) Scientific Interim - Automit for annee and inclusive dates) F44620-70-C-0107 - MEDOAT TOTL A0827-5 61101D - - - - - - - - - - - - - - - - - - -</pre>	(Security classification of title, body of abstract and indexing a	nnotation must be entered when the overall report is classifi	ed)				
Depail Links to Computer Size 12. Secure A NOTE ON FAST CYCLIC CONVOLUTION * Decomber 10x Notes (Type at report and Anchorse detex) Scientific Interim * ANOTE ON FAST CYCLIC CONVOLUTION * Decomber 10x Notes (Type at report and Anchorse detex) Scientific Interim * ANOTE ON FAST CYCLIC CONVOLUTION * Decomber 1970 * ANOTE ON FAST CYCLIC CONVOLUTION * Contract on GASH NO. F44620-70c-0107 * Report Tati December 1970 * Contract on GASH NO. F44620-70c-0107 * Report Tati December 1970 * Contract on GASH NO. F44620-70c-0107 * Report Note * Contract on GASH NO. F44620-70c-0107 * Report Note * Strinkeron Notes This document has been approved for public release and sale; its distribution is unlimited. * Strinkeron Notes The GASE OF Scientific Research 1400 Wilson Boulevard (SNMA) Arilington, Virginia 22209 * Notes of the convolution of two needed of the convolution of two needed of the convolution of two needed of the seconsed hore neatively prime.	1. ORIGINATING ACTIVITY (Corporate author)	28. REPORT SECURITY CLASSIFICAT	ION				
Carnegie-Wellon University Pittaburgh, Pennsylvania 15213 A NOTE ON FAST CYCLIC CONVOLUTION A DECONFINE NOTES (Type of report and inclusive dates) Scientific Interim C AVTORNEY (Type of report and inclusive dates) Scientific Interim Partation and the inclusive dates) Scientific Interim C AVTORNEY (The Network REPORT NUMBER(5) PAG20-7-5 6 611010 A D EXTORNEY NOTES This document has been approved for public release and sale; its distribution is unlimited. TH SOFTANCE TECH, OTHER This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires $(n_1+1)(n_k+1)/2^k$ multiplications for the convolution of two n-vectors, where n = n_1n_k is a factorization of n into factors which are pairwise relatively prime.	Department of Computer Science	UNCLASSIFIED	1				
Pitteburgh, Pennsylvania 15213 A NOTE ON FAST CYCLIC CONVOLUTION - OELECTIFICE NOTES (Type of report and inclusive dates) Scientific Interim - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT TALK - AUTOCOLL/For theme, middle influit. less nome) Y. Zalcstein - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers that may be escilated - REPORT NOUS (Any other numbers (Any other numbers that may be escilated - REPORT NOT NOT NOT NOT NOT NOT NOT NOT NOT NO		20. GROUP					
A NOTE ON FAST CYCLIC CONVOLUTION C. DESCRIPTIVE MOTE NO PAST CYCLIC CONVOLUTION C. COLLECTION C. COLLECTIO							
A NOTE ON PAST CYCLIC CONVOLUTION A DESCRIPTIVE MOTES (Type of report and influtive dates) Scientific Interim A AUTIONIS (First mame, addide initial: last name) A Contract of disket not B Contract not B Contract of disket							
Deschiptive voltes (Type of report and inclusive dates) Scientific Interim AutoONIS/(First name, addde inflict. Marforms) Y. Zalestein Aneoset 1970 B Consent too. P44620-70-0-0107 Ao827-5 Consent too. Ao827-5 Consent too. Ao827-5 This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. AutoONISCONSENCE and Consents This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. the unlimited of the convolution of two numbers (Any other numbers (SRMA) Arlington, Virginia 22209 the set of the convolution of two numbers (Any other numbers) is a factorization of n into factors which are pairwise relatively prime.	3. REPORT THLE		1				
Deschiptive voltes (Type of report and inclusive dates) Scientific Interim AutoONIS/(First name, addde inflict. Marforms) Y. Zalestein Aneoset 1970 B Consent too. P44620-70-0-0107 Ao827-5 Consent too. Ao827-5 Consent too. Ao827-5 This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. AutoONISCONSENCE and Consents This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. This document has been approved for public release and sale; its distribution is unlimited. the unlimited of the convolution of two numbers (Any other numbers (SRMA) Arlington, Virginia 22209 the set of the convolution of two numbers (Any other numbers) is a factorization of n into factors which are pairwise relatively prime.							
Scientific Interim Y. Zalcstein 2. TOTAL NO. OF PAGES 2. NO. OF REFS December 1970 8 7 Scientific 7 7 Scientific 700 OF REFS 7 Scientific 8 7 Scientific 7 7 Sci	A NOTE ON FAST CYCLIC CONVOLUTION						
Scientific Interim Y. Zalcstein 2. TOTAL NO. OF PAGES 2. NO. OF REFS December 1970 8 7 Scientific 7 7 Scientific 700 OF REFS 7 Scientific 8 7 Scientific 7 7 Sci							
Y. Zalcstein A. REPORT DATE December 1970 St. CONTRACT ON CONTRAC	4. DESCRIPTIVE NOTES (Type of report and inclusive dates)						
Y. Zalcstein A. REPORT DATE December 1970 St. CONTRACT ON CONTRAC	Scientific Interim						
Y. Zalcstein Y. Zalcstein * REPORT DATE December 1970 F44620-70-C-0107 b. GRUCTION A0827-5 G1101D d December Conservation A0827-5 G1101D d Conservation Conservation A0827-5 Conservation G1101D d This document has been approved for public release and sale; its distribution is unlimited. The SUPPLEMENTARY MOTES TECH, OTHER 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.							
A. REPORT DATE 74. TOTAL NO. OF PAGES 76. NO. OF REFS December 1970 8 7 Id. CONTRACT ON GRANT NO. F4. OTAL NO. OF PAGES 7 F4. CONTRACT ON GRANT NO. F4. OTAL NO. OF PAGES 7 F4. CONTRACT ON GRANT NO. F4. OTAL NO. OF PAGES 7 F4. CONTRACT ON GRANT NO. F4. OTAL NO. OF PAGES 7 F4. OTAL TO NO. OF GRANT NO. F4. OTAL NO. OF PAGES 7 F4. OTAL TO NO. F4. OTAL NO. OF PAGES 7 F4. OTAL TO. F4. OTAL TO. F4. OTAL TO. A0827-5 5 5 5 61101D 5 5 5 A0827-5 5 5 5 61101D 5 5 5 7 This document has been approved for public release and sale; 11 11 SUPPLEMENTARY NOTES 12. SPONSORING MILITARY ACTIVITY A11 GUENTARY NOTES 14. OF OTCE OFFICE OF Scientific Research 1400 Wilson Boulevard (SRMA) A11 Ington, Virginia 22209 11 AMPLEMENTARY NOTES 14.00 Wilson Boulevard 7 14.00 Wilson Boulevard 14.01 / 2 ^k							
Becember 1970 8 7 10. CONTRACT ON GRANT NO. F44620-70-C-0107 b PROJECT NO. A0827-5 GillolD 94. ORIGINATON'S REPORT NUMBER(S) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 7. 10. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss distribution is unlimited. 11. SUPPLEMENTARY NOTES 12. SPONSORING MULTARY ACTIVITY 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.	Y. Zalcstein						
Becember 1970 8 7 10. CONTRACT ON GRANT NO. F44620-70-C-0107 b PROJECT NO. A0827-5 GillolD 94. ORIGINATON'S REPORT NUMBER(S) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 7. 10. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss distribution is unlimited. 11. SUPPLEMENTARY NOTES 12. SPONSORING MULTARY ACTIVITY 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.							
Becember 1970 8 7 10. CONTRACT ON GRANT NO. F44620-70-C-0107 b PROJECT NO. A0827-5 GillolD 94. ORIGINATON'S REPORT NUMBER(S) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 4. 95. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss report) 7. 10. OTHER REPORT NO(S) (Any other numbers that may be sealfared miss distribution is unlimited. 11. SUPPLEMENTARY NOTES 12. SPONSORING MULTARY ACTIVITY 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.							
December 1070 FGCONTACTOR GRANTNO. F44620-70-C-0107 b PROJECT NOIGS (Any other numbers that may be said/gred diff report) G1101D d. d. </td <td></td> <td></td> <td></td>							
F44620-70-C-0107 A0827-5 61101D at To Distainaution statement Tis document has been approved for public release and sale; its distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MCLITARY ACTIVITY Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 TH ARSTHACT 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.							
 b. PROJECT HO. AO827-5 G1101D a. Distribution statement tis distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MULTARY ACTIVITY Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13. Anstract This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires n(n₁+1)(n_k+1)/2^k multiplications for the convolution of two n-vectors, where n = n₁n_k is a factorization of n into factors which are pairwise relatively prime. 	BA, CONTRACT OR GRANT NO.	94. ORIGINATOR'S REPORT NUMBER(S)					
 b. PROJECT HO. AO827-5 G1101D a. Distribution statement tis distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MULTARY ACTIVITY Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13. Anstract This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires n(n₁+1)(n_k+1)/2^k multiplications for the convolution of two n-vectors, where n = n₁n_k is a factorization of n into factors which are pairwise relatively prime. 	F44620-70-C-0107						
61101D a. 10 Distribution statement This Report No(8) (Any other numbers that may be sailgned this report) 11 SUPPLEMENTATION STATEMENT This document has been approved for public release and sale; its distribution is unlimited. 11 SUPPLEMENTARY NOTES 12 SPONSORING MILITARY ACTIVITY TECH, OTHER 12 SPONSORING MILITARY ACTIVITY Ariington, Virginia 22209 11 ANSTRACT 12 SPONSORING MILITARY ACTIVITY 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.			1				
61101D a. 10 Distribution statement This Report No(8) (Any other numbers that may be sailgned this report) 11 SUPPLEMENTATION STATEMENT This document has been approved for public release and sale; its distribution is unlimited. 11 SUPPLEMENTARY NOTES 12 SPONSORING MILITARY ACTIVITY TECH, OTHER 12 SPONSORING MILITARY ACTIVITY Ariington, Virginia 22209 11 ANSTRACT 12 SPONSORING MILITARY ACTIVITY 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	A0827-5						
a This document has been approved for public release and sale; its distribution is unlimited. TECH, OTHER TECH, OTHER 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.			e essigned				
 To Distribution STATEMENT This document has been approved for public release and sale; its distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MILITARY ACTIVITY AIT FORCE Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13 APSTRACT This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires n(n₁+1)(n_k+1)/2^k multiplications for the convolution of two n-vectors, where n = n₁n_k is a factorization of n into factors which are pairwise relatively prime. 	61101D	(his report)					
 To Distribution STATEMENT This document has been approved for public release and sale; its distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MILITARY ACTIVITY AIT FORCE Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13 APSTRACT This note presents a new algorithm for computing the cyclic convolution of two vectors over a commutative ring. The algorithm requires n(n₁+1)(n_k+1)/2^k multiplications for the convolution of two n-vectors, where n = n₁n_k is a factorization of n into factors which are pairwise relatively prime. 		· · · · · · · · · · · · · · · · · · ·					
This document has been approved for public release and sale; its distribution is unlimited. 11. SUPPLEMENTARY NOTES TECH, OTHER 12. SPONSORING MILITARY ACTIVITY AIT Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13. ANSTRACT 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.		I					
its distribution is unlimited. TECH, OTHER 12. SPONSORING MILITARY ACTIVITY Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13. APSIMACT 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.		c release and sale:	1				
11. SUPPLEMENTARY NOTES 12. SPONSORING MULITARY ACTIVITY TECH, OTHER Air Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13. APSTRACT 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.		e rereade and bare,					
TECH, OTHERAir Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 2220913 APSTRACTThis 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	its distribution is unimited.						
TECH, OTHERAir Force Office of Scientific Research 1400 Wilson Boulevard (SRMA) Arlington, Virginia 2220913 APSTRACTThis 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.							
TECH, OTHER 1400 Wilson Boulevard (SRMA) Arlington, Virginia 22209 13 APSIGACT 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	11. SUPPLEMENTARY NOTES						
Ariington, Virginia 22209 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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	TECH OTHER						
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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	inon, other						
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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.		Arlington, Virginia 22209					
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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	13 ABSTRACT						
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 $n = n_1n_k$ is a factorization of n into factors which are pairwise relatively prime.	This note presents a new algorithm for c	mputing the cyclic convolution of t	wo				
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.	-						
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.	vectors over a commutative ring. The al	gorithm requires $n(n_1+1)\dots(n_n+1)/2^{-1}$					
factorization of n into factors which are pairwise relatively prime.	-	-					
	multiplications for the convolution of t	vo n-vectors, where $n = n_1 \cdots n_k$ is a	•				
	factorization of n into factors which ar	pairwise relatively prime.					
DD FORM 1473	factorization of in finco factors which ar	s pullwide relucively prime.					
DD ^{FORM} 1473							
DD ^{FORM} 1473		· · · ·					
DD FORM 1473							
DD FORM 1473							
DD FORM 1473	1						
DD FORM 1473	1						
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473	1						
DD FORM 1473							
DD FORM 1473							
DD FORM 1473							
DD FORM 1473		······					
	DD FORM 1473						

-

.

,

•

Security Classification

Security Classifi	cation							
14.	KEY WORDS		LIN		LINKB		LINK C	
			ROLE	₩T	ROLE	₩ T	ROLE	WТ
					i			
								·
								•
								1
							[]	