Vulis, Michael

NEW ALGORITHMS FOR THE MULTI-DIMENSIONAL DFT

City University of New York PH.D. 1983

PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark __✓__.

1. Glossy photographs or pages _____
2. Colored illustrations, paper or print _____
3. Photographs with dark background _____
4. Illustrations are poor copy _____
5. Pages with black marks, not original copy _____
6. Print shows through as there is text on both sides of page _____
7. Indistinct, broken or small print on several pages ✓
8. Print exceeds margin requirements _____
9. Tightly bound copy with print lost in spine _____
10. Computer printout pages with indistinct print _____
11. Page(s) _____ lacking when material received, and not available from school or author.
12. Page(s) _____ seem to be missing in numbering only as text follows.
13. Two pages numbered _____. Text follows.
14. Curling and wrinkled pages ✓
15. Other _____

University
Microfilms
International

NEW ALGORITHMS FOR THE MULTI-DIMENSIONAL DFT

by

Michael Vulis

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy. The City University of New York.

- 1983 -

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfation of the dissertation requirements for the degree of Doctor of Philosophy.

04/21/1983 L. Auslander
Chairman of Examining Committee

04/21/1983 Alex Heller
Executive Officer

Alex Heller

A.T. Vasquez

R. Parikh
Supervisory Committee

The City University of New York

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my advisor, Professor L.Auslander. Without his constant encouragement and numerous suggestions this work would undoubtedly never have seen the light of day.

It would be totally impossible to thank all of those who have helped me carry out this research and (which was a much harder task) to have it written down; nevertheless, I am especially grateful to Dr. E.Feig, Prof. A.Heller, Prof. A.T.Vasquez and Dr. J.Cooley for their suggestions and to Ms. S.Persinger and Dr. C.Wajngurt for their help with the proof-reading.

Finally, I must express my sincere gratitude to the Government of the Union of Soviet Socialist Republics and Dean Z.Borevitch of LSU personally for making my life there intolerable and hence forcing me to leave their socialist paradise. Without them I would have never received as excellent an education as I did at the CUNY GC.

INTRODUCTION.

Over the last twenty years, a number of Finite Fourier algorithms has been created in an effort to reduce the number of data-dependent operations required to compute an arbitrary sized 'Transform'.

The Cooley-Tukey Fast Fourier Transform algorithm (FFT, see [1]), introduced over 15 years ago, requires O(Nlog(N)) operations rather than $O(N^2)$ (which will be necessary for the 'trivial' algorithm. performing a straightforward matrix multiplication) to effect a one-dimensional Discrete Fourier Transform (henceforth abbreviated as DFT) on n points (DFT(n:1)).

Some refining papers have been published on FFT during the subsequent decade and the Cooley-Tukey FFT algorithm is (and is likely to stay as) the most widely used and popular algorithm for the one-dimensional DFT. However, in 1976, FFT met with serious competition. Winograd Discrete Fourier Transform algorithm (WFTA, see [2]) radically decreases the number of multiplications relative to the FFT, sometimes at the expense of increased additions, and therefore improves the speed and precision of the Transform.

WFTA in its original form is an extremely efficient algorithm only for a few very special cases; it is designed

for DFT(p^s:1), where p is prime and both p and s are relatively small. Theoretically, the algorithm is supposed to work for any p and s, but in practice, numerical instability makes the use of WFTA impossible for p>13. Thus, in all existing implementations, an algorithm for DFT(n:1), using WFTA, will be constructed as follows: different WFTA will be used on different prime factors of n, and will be brought together, using one or another technique.

A few years later, an approach similar to WFTA, was tried for the multi-dimensional DFT (We mean the article due to L.Auslander, E.Feig and S.Winograd, see [3]). In this work, the authors constructed similar 'kernels' for DFT(p:n), where p is once again a small prime. These new kernels, once again, can be brought together to generate a multi-dimensional DFT algorithm on a rather large number of points along each axis. However, this generalization was not complete and no attempts to try to construct an algorithm for DFT(p^s:n) have ever been made.

In this work we will try to explore this case and will describe an algorithm for DFT(p^s:n), which is a certain generalization of the WFTA. Once more, the numerical instability, inherent in all algorithms, using WFTA ideas, will make the new algorithm suitable for only relatively small values of p and s; however, the techniques of combining the algorithms on different prime factors still can be used.

We will introduce the new algorithm first as an example. Chapter I will describe a sample DFT(9:2) algorithm, without going deeply into the theoretical details and/or the justification of the suggested construction. However, some remarks, linking this example with the subsequently described theory, will be provided. This Chapter will also include a sample block-scheme of the DFT(9:2) algorithm.

In Chapter II, we will introduce the underlying algebraic construction. All of the observations, made in Chapter I, will be extended to the general DFT(p^s:n) case. It will be further shown that WFTA DFT(p^s:1) and the algorithm for DFT(p:n) can be considered as special cases of the new algorithm and at the same time, as its subroutines. A sample block-scheme and summary will be supplied at the end of Chapter II.

Relatively short Chapters III and IV are 'Variations on a Theme'. We will introduce a different algorithm for DFT(p^2:n), first as an example (DFT(9:2), Chapter III) and then will justify it in Chapter IV. This second algorithm will be applicable only for DFT(p^2:n) and will combine the features of WFTA with those of the multi-dimensional FFT.

CONTENTS

CHAPTER I.

0. INTRODUCTION

In this Chapter, we present an example of a new algorithm for the Finite Fourier Transform on a n-dimensional data array with p^2 points along each axis, where p is a prime number and n and s are positive integers.

The example we are going to discuss is the case where n=2,s=2 and p=3, i.e. the 2-dimensional Fourier Transform on 9 by 9 points. The discussion of the general theory is presented in Chapter II. In this Chapter we tried to avoid any generality and hence the reader interested in seeing this algorithm as something more than just a magical sequence of calculations is referred to Chapter II. Some remarks tying the calculations with an underlying algebraic structure were inserted under the heading 'EXPLANATIONS'. They are clearly insufficient for reconstructing the algorithm for arbitrary p,n and s, but will be useful for those interested in both the algorithm and its underlying

structure. Readers, not interested in the theory involved, may skip the 'EXPLANATIONS'.

NOTATION

We will fix the following notation in this Chapter:

We denote by M=diag(M1,M2... Mq) the matrix

$$\begin{pmatrix} M1 & 0 & \cdots & 0 \\ 0 & M2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Mq \end{pmatrix}$$

and say that M is a block-diagonal matrix.

Analogously, we define M=cyc(M1,M2,.. Mq) as

$$\begin{pmatrix} M1 & M2 & \cdots & Mq \\ Mq & M1 & \cdots & Mq \\ \vdots & \vdots & \ddots & \vdots \\ M2 & M3 & \cdots & M1 \end{pmatrix}$$

and say that M is a cyclic or a circulant matrix.

Here q is any integer, and the Mi's are square matrices of the same size.

I. THE DESCRIPTION OF THE ALGORITHM

The input data for the Finite Fourier Transform on 9 by 9 points is given as a 9 by 9 array A(K,L); K,L=0,1,..8. Analogously the output is a 9 by 9 array $\hat{A}(\hat{K},\hat{L})$, $\hat{K},\hat{L}=0,1,..8$, where

$$\hat{A}(\hat{K},\hat{L}) = \sum_{K=0}^{8} \sum_{L=0}^{8} w^{K\hat{K}+L\hat{L}} A(K,L) \ , \ w = e^{2\pi i/9} \qquad (1)$$

The Fourier Transform is a linear transformation and hence can be written in a matrix form once we are given a way to order the input and output, i.e. once we define a linear order on the set of indices {(K,L)/ K,L=0,1,.. 8 }. The orderings for the input and output data will be presented in the TABLEs I and II respectively. These orderings are induced by a certain ring structure on the set of indices. This structure for the 9 by 9 case is discussed under 'EXPLANATIONS'. The reader is referred to Chapter II for the generalizations.

We rearrange the input data into the one-dimensional array B of length 81 as shown in the following table:

TABLE I.

B(0) = A(0,0)	B(27) = A(0,8)	B(54) = A(4,1)
B(1) = A(3,0)	B(28) = A(8,1)	B(55) = A(6,4)
B(2) = A(6,6)	B(29) = A(2,0)	B(56) = A(7,8)
B(3) = A(0,6)	B(30) = A(7,7)	B(57) = A(1,6)
B(4) = A(6,3)	B(31) = A(0,4)	B(58) = A(5,2)
B(5) = A(6,0)	B(32) = A(4,5)	B(59) = A(6,2)
B(6) = A(3,3)	B(33) = A(1,3)	B(60) = A(5,1)
B(7) = A(0,3)	B(34) = A(2,5)	B(61) = A(5,3)
B(8) = A(3,6)	B(35) = A(3,2)	B(62) = A(7,1)
B(9) = A(1,0)	B(36) = A(8,4)	B(63) = A(3,1)
B(10) = A(8,8)	B(37) = A(5,6)	B(64) = A(7,5)
B(11) = A(0,2)	B(38) = A(1,7)	B(65) = A(7,6)
B(12) = A(2,7)	B(39) = A(6,1)	B(66) = A(8,5)
B(13) = A(5,0)	B(40) = A(4,2)	B(67) = A(6,5)
B(14) = A(4,4)	B(41) = A(7,3)	B(68) = A(8,7)
B(15) = A(0,1)	B(42) = A(5,8)	B(69) = A(8,3)
B(16) = A(1,8)	B(43) = A(3,5)	B(70) = A(4,7)
B(17) = A(7,0)	B(44) = A(2,1)	B(71) = A(3,7)
B(18) = A(2,2)	B(45) = A(8,6)	B(72) = A(4,8)
B(19) = A(0,5)	B(46) = A(7,4)	B(73) = A(4,6)
B(20) = A(5,4)	B(47) = A(6,7)	B(74) = A(2,8)
B(21) = A(8,0)	B(48) = A(1,5)	B(75) = A(6,8)
B(22) = A(1,1)	B(49) = A(4,3)	B(76) = A(2,4)
B(23) = A(0,7)	B(50) = A(8,2)	B(77) = A(2,3)
B(24) = A(7,2)	B(51) = A(3,8)	B(78) = A(1,4)
B(25) = A(4,0)	B(52) = A(5,7)	B(79) = A(3,4)
B(26) = A(5,5)	B(53) = A(2,6)	B(80) = A(1,2)

We similarly rearrange the output:

TABLE II.

$\hat{B}(0) = \hat{A}(0,0)$	$\hat{B}(27) = \hat{A}(0,1)$	$\hat{B}(54) = \hat{A}(5,1)$
$\hat{B}(1) = \hat{A}(3,0)$	$\hat{B}(28) = \hat{A}(4,4)$	$\hat{B}(55) = \hat{A}(6,2)$
$\hat{B}(2) = \hat{A}(3,6)$	$\hat{B}(29) = \hat{A}(5,0)$	$\hat{B}(56) = \hat{A}(5,2)$
$\hat{B}(3) = \hat{A}(0,3)$	$\hat{B}(30) = \hat{A}(2,7)$	$\hat{B}(57) = \hat{A}(1,3)$
$\hat{B}(4) = \hat{A}(3,3)$	$\hat{B}(31) = \hat{A}(0,2)$	$\hat{B}(58) = \hat{A}(7,8)$
$\hat{B}(5) = \hat{A}(6,0)$	$\hat{B}(32) = \hat{A}(8,8)$	$\hat{B}(59) = \hat{A}(6,4)$
$\hat{B}(6) = \hat{A}(6,3)$	$\hat{B}(33) = \hat{A}(1,6)$	$\hat{B}(60) = \hat{A}(4,1)$
$\hat{B}(7) = \hat{A}(0,6)$	$\hat{B}(34) = \hat{A}(1,2)$	$\hat{B}(61) = \hat{A}(2,6)$
$\hat{B}(8) = \hat{A}(6,6)$	$\hat{B}(35) = \hat{A}(3,4)$	$\hat{B}(62) = \hat{A}(5,7)$
$\hat{B}(9) = \hat{A}(1,0)$	$\hat{B}(36) = \hat{A}(1,4)$	$\hat{B}(63) = \hat{A}(3,8)$
$\hat{B}(10) = \hat{A}(4,5)$	$\hat{B}(37) = \hat{A}(2,3)$	$\hat{B}(64) = \hat{A}(8,2)$
$\hat{B}(11) = \hat{A}(0,4)$	$\hat{B}(38) = \hat{A}(2,4)$	$\hat{B}(65) = \hat{A}(4,3)$
$\hat{B}(12) = \hat{A}(7,7)$	$\hat{B}(39) = \hat{A}(6,8)$	$\hat{B}(66) = \hat{A}(1,5)$
$\hat{B}(13) = \hat{A}(2,0)$	$\hat{B}(40) = \hat{A}(2,8)$	$\hat{B}(67) = \hat{A}(6,7)$
$\hat{B}(14) = \hat{A}(8,1)$	$\hat{B}(41) = \hat{A}(4,6)$	$\hat{B}(68) = \hat{A}(7,4)$
$\hat{B}(15) = \hat{A}(0,8)$	$\hat{B}(42) = \hat{A}(4,8)$	$\hat{B}(69) = \hat{A}(8,6)$
$\hat{B}(16) = \hat{A}(5,5)$	$\hat{B}(43) = \hat{A}(3,7)$	$\hat{B}(70) = \hat{A}(2,1)$
$\hat{B}(17) = \hat{A}(4,0)$	$\hat{B}(44) = \hat{A}(4,7)$	$\hat{B}(71) = \hat{A}(3,5)$
$\hat{B}(18) = \hat{A}(7,2)$	$\hat{B}(45) = \hat{A}(8,3)$	$\hat{B}(72) = \hat{A}(5,8)$
$\hat{B}(19) = \hat{A}(0,7)$	$\hat{B}(46) = \hat{A}(8,7)$	$\hat{B}(73) = \hat{A}(7,3)$
$\hat{B}(20) = \hat{A}(1,1)$	$\hat{B}(47) = \hat{A}(6,5)$	$\hat{B}(74) = \hat{A}(4,2)$
$\hat{B}(21) = \hat{A}(8,0)$	$\hat{B}(48) = \hat{A}(8,5)$	$\hat{B}(75) = \hat{A}(6,1)$
$\hat{B}(22) = \hat{A}(5,4)$	$\hat{B}(49) = \hat{A}(7,6)$	$\hat{B}(76) = \hat{A}(1,7)$
$\hat{B}(23) = \hat{A}(0,5)$	$\hat{B}(50) = \hat{A}(7,5)$	$\hat{B}(77) = \hat{A}(5,6)$
$\hat{B}(24) = \hat{A}(2,2)$	$\hat{B}(51) = \hat{A}(3,1)$	$\hat{B}(78) = \hat{A}(8,4)$
$\hat{B}(25) = \hat{A}(7,0)$	$\hat{B}(52) = \hat{A}(7,1)$	$\hat{B}(79) = \hat{A}(3,2)$
$\hat{B}(26) = \hat{A}(1,8)$	$\hat{B}(53) = \hat{A}(5,3)$	$\hat{B}(80) = \hat{A}(2,5)$

EXPLANATIONS. The DFT(9:2) is indexed by pairs of indices (K,L) where $0<K,L<8$. Let R be the ring of Gaussian integers modulo 9, i.e. the set of numbers (K+iL), where $i^2=-1$ and K and L are integers 0,1,..8, and the addition and the multiplication are the regular complex addition and multiplication followed by taking the residue modulo 9. Thus we can identify the set of pairs (K,L) with R, by setting $(K,L)\longleftrightarrow K+iL$. We will sometimes write A(K+iL) instead of A(K,L). The reader is referred to the Sections I-II of Chapter II for the definition of the ring R for the general case.

It is not hard to see that R contains exactly 9 zero divisors. They are the elements K+iL with K and L divisible by 3. The reader will observe that in TABLEs I and II we listed all the indices starting with 0, followed by 8 non-zero zero divisors (indices of B and $\hat{B}$, 1 through 8) and finished with data indexed by invertible elements of R. We refer the reader to Chapter II for details and explanations.

We rewrite the equations (1) as follows:

$$\hat{A}(0,0) = \sum_{K=0}^{8}\sum_{L=0}^{8} A(K,L), \tag{2}$$

$$\hat{A}(\hat{K},\hat{L}) = \sum_{K=0}^{8}\sum_{L=0}^{8} w^{K\hat{K}}{}_{w}{}^{L\hat{L}} A(K,L) =$$

$$\sum_{K=0}^{8}\sum_{L=0}^{8} A(K,L) + \sum_{K=0}^{8}\sum_{L=0}^{8} (w^{K\hat{K}}{}_{w}{}^{L\hat{L}} - 1)A(K,L) =$$

$$\hat{A}(0,0) + \sum_{K=0}^{8}\sum_{L=0}^{8} (w^{K\hat{K}}{}_{w}{}^{L\hat{L}} - 1)A(K,L)$$

Hence

$$\hat{A}(\hat{K},\hat{L}) - \hat{A}(0,0) = \sum_{K=0}^{8}\sum_{L=0}^{8} (w^{K\hat{K}}{}_{w}{}^{L\hat{L}} - 1)A(K,L). \tag{3}$$

We substitute the one-dimensional arrays B and $\hat{B}$ in place of A and $\hat{A}$ and rewrite the equations (3) in the following matrix form:

$$\hat{B}' - \hat{A}(0,0) = F \cdot B', \tag{4}$$

where F is an 80 by 80 matrix,

B' and $\hat{B}'$ are the vectors of length 80,

B'={B(i);i=1,..80};

$\hat{B}' = \{\hat{B}(i); i=1,..80\};$

After performing all of the necessary calculations, one sees that the matrix F has the following block-structure:

O	M	M	M	M	M	M	M	M	M
M									
M	C1			C2			C3		
M									
M									
M	C3			C1			C2		
M									
M									
M	C2			C3			C1		
M									

Let C be the 72x72 matrix containing the blocks C1,C2

and C3; C=cyc(C1,C2,C3). We term C the core of the FFT on 9x9 points. Let $w=e^{2\pi i/9}$, w is a primitive 9-th root of 1. Then the blocks are:

$M=cyc(w^3-1,w^6-1,0,w^6-1,w^6-1,w^3-1,0,w^3-1)$

$C1=cyc(w^1-1,w^8-1,0,w^2-1,w^5-1,w^4-1,0,w^1-1,w^7-1,w^2-1,0,$
$w^5-1,w^8-1,w^1-1,0,w^7-1,w^4-1,w^5-1,0,w^8-1,w^2-1,w^7-1,0,w^4-1)$

$C2=cyc(w^1-1,w^2-1,w^3-1,w^8-1,w^5-1,w^1-1,w^6-1,w^4-1,w^7-1,$
$w^5-1,w^3-1,w^2-1,w^8-1,w^7-1,w^6-1,w^1-1,w^4-1,w^8-1,w^3-1,$
$w^5-1,w^2-1,w^4-1,w^6-1,w^7-1)$

$C3=cyc(w^1-1,w^5-1,w^6-1,w^5-1,w^5-1,w^7-1,w^3-1,w^7-1,w^7-1,$
$w^8-1,w^6-1,w^8-1,w^8-1,w^4-1,w^3-1,w^4-1,w^4-1,w^2-1,w^6-1,$
$w^2-1,w^2-1,w^1-1,w^3-1,w^1-1)$

EXPLANATIONS. We observe that the core block C is the one indexed by elements of the unit group of the ring R. The blocks equal to M are indexed by the elements of the unit group U and the elements of D. Finally, the zero block in the top left corner of the matrix F is indexed only by the zero divisors. We observe that the entries of the block C are numbers w^k-1 (with k varying), whereas the elements of M can be written as $w^{3k}-1$ (with k varying). Carrying the analogy one step further, we say that the elements of the zero block are $w^{9k}-1$.

EXPLANATIONS. At this point let us analyze the structure of R somewhat deeper. The group of units U of R contains 72 elements. U can be factored as a product of a cyclic subgroup $G \cong Z_8$ and a subgroup

$H \cong H_0 \oplus H_1$, where $H_0 \cong H_1 \cong Z_3$. Here G is generated by the element x=2+7i; the elements h_0=4 and h_1=1+3i generate H_0 and H_1 respectively. Further, let y=xh_0, G'=G $\oplus$ $H_0 \cong Z_{24}$ is the subgroup generated by y. Then every element of U can be uniquely written as $y^j h_0{}^k$ for some j=0,1,.. 23 and k=0,1,2. The reader is referred to Theorem 3 of Chapter II for details of the structure of the unit group for the general case. Thus, the group of units can be lexicographically ordered. We observe that the choice of B(9),B(10),...B(80) in TABLE I is is generated by this lexicographical ordering. Let T be the isomorphism of the additive structure of R, R^+, given by the following rule: T(a+bi)= a-bi . In other words, T is the complex conjugation on R. The reader may find the generalization in Chapter II, Section V. We observe the following properties of T, which can be easily proven:

1). Let <a,b>=$a_1b_1+a_2b_2$, where a=a_1+ia_2 and b=b_1+ib_2. Then <Ta,b>=Re(ab).

2) In the matrix form, T given by the following 2x2 matrix:

$$\begin{vmatrix} 1 & 0 \\ 0 & 8 \end{vmatrix}$$

Thus we observe:

B(9) = A(T(1))

B(10) = A(T(y))

B(11) = A(T(y^2))

....

B(32) = A(T(y^{23}))

B(33) = A(T(h_1))

$B(34) = A(T(yh_1))$

....

$B(56) = A(T(y^{23}h_1))$

$B(57) = A(T(h_1^{2}))$

$B(58) = A(T(yh_1^{2}))$

....

$B(80) = A(T(y^{23}h_1^{2}))$

The ordering on the output (TABLE II) is constructed in a similar manner: We use $y^{-1}=4+5i$ and $h_1^{-1}=1+6i$ instead of y and h_1. Thus,

$\hat{B}(9) = \hat{A}(1)$

$\hat{B}(10) = \hat{A}(y^{-1})$

$\hat{B}(11) = \hat{A}(y^{-2})$

....

$\hat{B}(32) = \hat{A}(y^{-23})$

$\hat{B}(33) = \hat{A}(h_1^{-1})$

$\hat{B}(34) = \hat{A}(y^{-1}h_1^{-1})$

....

$\hat{B}(56) = \hat{A}(y^{-23}h_1^{-1})$

$\hat{B}(57) = \hat{A}(h_1^{-2})$

$\hat{B}(58) = \hat{A}(y^{-1}h_1^{-2})$

....

$\hat{B}(80) = \hat{A}(y^{-23}h_1^{-2})$

The order on B(1),... B(8) and $\hat{B}(1),\ldots \hat{B}(8)$ is also far from being arbitrary: it is not hard to see that any zero divisors of R can be uniquely written as $3x^j$ for some j=0,1,.. 8 (cf. Chapter II, Lemma 2). We have:

$B(1) = A(T(3))$	$\hat{B}(1) = \hat{A}(3)$
$B(2) = A(T(3x))$	$\hat{B}(2) = \hat{A}(3x^{-1})$
$B(3) = A(T(3x^2))$	$\hat{B}(3) = \hat{A}(3x^{-2})$
....	....
$B(8) = A(T(3x^7))$	$\hat{B}(8) = \hat{A}(3x^{-7})$

Theorem 4 of Chapter II describes the nature of the action of the unit group on the set of the zero divisors for the general case.

We observe that the block C1 has some periodicity features: the entries equal to 0 are repeated after three different entries. At the same time the entries, equal to w^3-1 or w^6-1, occuring in the blocks C2 and C3, have the same "periodicity" and occupy the same positions as zeroes in the first block. This kind of phenomenon will allow us to factor the blocks and holds for p different from 3.

We write:

$C1 = Q1,$

$C2 = Q2 + R2,$

$C3 = Q3 + R3,$

where

$Q2=cyc(w^1-1,w^2-1,0,w^8-1,w^5-1,w^1-1,0,w^4-1,w^7-1,w^5-1,0,w^2-1,$
$w^8-1,w^7-1,0,w^1-1,w^4-1,w^8-1,0,w^5-1,w^2-1,w^4-1,0,w^7-1)$

$Q3=cyc(w^1-1,w^5-1,0,w^5-1,w^7-1,w^7-1,0,w^7-1,w^7-1,w^8-1,0,w^8-1,$
$w^8-1,w^4-1,0,w^4-1,w^4-1,w^2-1,0,w^2-1,w^2-1,w^1-1,0,w^1-1)$

$R2=cyc(0,0,w^3-1,0,0,0,w^6-1,0,0,0,w^3-1,0,0,0,w^6-1,0,0,0,$
$w^3-1,0,0,0,w^6-1,0)$

R3=cyc(0,0,w^6-1,0,0,0,w^3-1,0,0,0,w^6-1,0,0,0,w^3-1,0,0,0,
w^6-1,0,0,0,w^3-1,0)

EXPLANATIONS. As the reader can see, we collected the entries containing w^3 and w^6 in the blocks R2 and R3. The entries of C. containing the 9-th primitive roots of 1 are collected in Q1, Q2 and Q3. This technique is generalized in the Section IX of Chapter II.

As we will soon see, the blocks R1,R2,Q1,Q2 and Q3 can be "nicely" factored.

It is not hard to see that

Q1 = S1 x D1

Q2 = S1 x D2

Q3 = S1 x D3, where

S1=cyc(w^1-1,0,0,0,w^5-1,0,0,0,w^7-1,0,0,0,w^8-1,0,0,0,
w^4-1,0,0,0,w^2-1,0,0,0)

D1=cyc(1,0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0)

D2=cyc(1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)

D3=cyc(1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1)

EXPLANATIONS. The reader will observe that the entries equal to 1, occuring in the matrices D1,D2 and D3, occupy the same positions as the entries w-1 in the matrices Q1, Q2 and Q3. This phenomenon is explained in Sections X and XI, Chapter II.

Then

$$Q = \begin{Vmatrix} Q1 & Q2 & Q3 \\ Q3 & Q1 & Q2 \\ Q2 & Q3 & Q1 \end{Vmatrix} = \begin{Vmatrix} S1xD1 & S1xD2 & S1xD3 \\ S1xD3 & S1xD1 & S1xD2 \\ S1xD2 & S1xD3 & S1xD1 \end{Vmatrix} =$$

$$= \begin{Vmatrix} S1 & & \\ & S1 & \\ & & S1 \end{Vmatrix} \times \begin{Vmatrix} D1 & D2 & D3 \\ D3 & D1 & D2 \\ D2 & D3 & D1 \end{Vmatrix} = SxD$$

Here the matrix D contains only zeroes and ones and hence the multiplication by D involves no essential multiplications.

Let P1 be the permutation, given by the following substitution table:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17	23	6	12	18	24

Let $\overline{\overline{P1}}$ be the matrix of the permutation P1.

Then $\overline{\overline{P1}} \times Sx \overline{\overline{P1}}^{-1} = diag(C9,C9,C9,C9)$, where C9 is

$$\begin{Vmatrix} w^1-1 & w^5-1 & w^7-1 & w^8-1 & w^4-1 & w^2-1 \\ w^2-1 & w^1-1 & w^5-1 & w^7-1 & w^8-1 & w^4-1 \\ w^4-1 & w^2-1 & w^1-1 & w^5-1 & w^7-1 & w^8-1 \\ w^8-1 & w^4-1 & w^2-1 & w^1-1 & w^5-1 & w^7-1 \\ w^7-1 & w^8-1 & w^4-1 & w^2-1 & w^1-1 & w^5-1 \\ w^5-1 & w^7-1 & w^8-1 & w^4-1 & w^2-1 & w^1-1 \end{Vmatrix}$$

EXPLANATIONS. The matrix C9, described above, is nothing else than the core matrix of DFT(9·1), as defined in [2]. As shown in the Section XI of Chapter II, the cores of one-dimensional transforms on p^r points for $r<s$ always occur as subroutines whenever we compute $DFT(p^s \cdot n)$. We will encounter the core of DFT(3·1) as an essential component of blocks R2 and R3.

Then

Q =P4 x diag(C9,C9,C9,C9,C9,C9,C9,C9,C9,C9,C9,C9) xP5xD, (5)

for some permutation matrices P4 and P5.

We will now similarly factor the blocks R2 and R3. We observe that

R2 = S2 x D4

R3 = S2 x D5, where

S2=cyc(w^3-1,0,0,0,0,0,0,0,0,0,0,0,w^6-1,0,0,0,0,0,0,0,0,0,0,0)

D4=cyc(0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0)

D5=cyc(0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0)

EXPLANATIONS. Once more, we observe that the ones in D4 and D5 are not arbitrary; they correspond to the entries equal to w^3-1 in respectively R2 and R3.

Hence

$$R = \begin{vmatrix} 0 & R2 & R3 \\ R3 & 0 & R2 \\ R2 & R3 & 0 \end{vmatrix} = \begin{vmatrix} 0 & S2xD4 & S2xD5 \\ S2xD5 & 0 & S2xD4 \\ S2xD4 & S2xD5 & 0 \end{vmatrix} =$$

$$= \begin{vmatrix} S2 & 0 & 0 \\ 0 & S2 & 0 \\ 0 & 0 & S2 \end{vmatrix} \times \begin{vmatrix} 0 & D4 & D5 \\ D5 & 0 & D4 \\ D4 & D5 & 0 \end{vmatrix}$$

Once more, the matrix D´ containing D4 and D5 has only zeroes and ones and hence multiplying by it would require no essential multiplications.

At the same time, the block S2 can be further transformed as follows·

Let $\bar{P2}$ be the permutation, given by the following substitution table·

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11	23	12	24

Let $\overline{P2}$ be the matrix of the permutation P2.

Then $\overline{P2} \times S \times \overline{P2}^{-1}$ = diag(C3,C3,C3,C3,C3,C3,C3,C3,C3,C3,C3,C3), where

$$C3 = \begin{vmatrix} w^3-1 & w^6-1 \\ w^6-1 & w^3-1 \end{vmatrix}$$

We observe that the matrix C3 is the core of the one-dimensional DFT(3·1) as given in [2].

THE OUTSIDE BLOCK.

We are going to apply to the outside block M a factorization similar to the ones we used for the core.

EXPLANATIONS. The reader, familiar with [3], may observe that the matrix M is nothing else than the core of DFT(3:2), as defined in [3]. The factorization we are about to apply to M is nothing else than the essense of the factorization in [3]. The necessary justification of the factorization can be found in [3] or Chapter II. A different and perhaps more interesting question is the following:

In the first place. why do we find the core of DFT(3:2) as a submatrix of M? Section VII of Chapter II provides the answer to it. It further shows that for $s \geq 2$ we are bound to encounter all of the cores of DFT(p^r:n) ($r \leq s$) as submatrices of the matrix of DFT(p^s:n).

We write

M = M1 x M2, where

M1 = cyc(w^3-1,0,0,0,w^6-1,0,0,0,0)

M2 = cyc(1,0,0,0,0,1,0,1)

Once more. if $\overline{P3}$ is the permutation matrix of the permutation

1	2	3	4	5	6	7	8
1	5	2	6	3	7	4	8

then $\overline{P3} \times M1 \times \overline{P3}^{-1}$ = cyc(C3,C3.C3,C3).

EXPLANATIONS. We remark that the core of DFT(3·1) is now encountered as an essential component of DFT(3:2).

We can observe now that all of the multiplications used in this algorithm are concentrated in the blocks C3 and C9. Hence we will need two subroutines: one to multiply a vector of length 2 by the 2 by 2 matrix C3, and the other to multiply a vector of length 6 by the 6 by 6 matrix C9.

The matrices C3 and C9 are not arbitrary: they are the cores of DFT(3·1) and DFT(9:1) as defined in [2]. Thus the two mentioned subroutines are exactly the ones used in the Winograd's 1-dimensional algorithms.

II. SUMMARY OF THE ALGORITHM.

We conclude this Chapter with a brief step-by-step scheme of the algorithm.

STEP 1. Calculate the sum of the elements of A(K,L) and store it at A(0,0).

STEP 2. Store the data B(2),B(3)... B(8) as a one-

dimensional array BN1 of length 8 (cf. Table I).

STEP 3. Store B(9),B(10),..B(80) as a one-dimensional array of length 72. We term it BC.

STEP 4. Multiply BC by the 72x72 matrix D. This step does not involve any essential multiplications; we perform only additions (576 operations). We apply the permutation P1 to the output and store the results into the one-dimensional array BC1.

STEP 5. Multiply BC by the 72x72 matrix D'. This step does not involve any actual multiplications; we perform only additions (360 operations). We apply the permutation P2 to the output and store the results into the one-dimensional array BC2.

STEP 6. We calculate the sums

B(10)+B(18)+B(26)+B(34)+B(42)+B(50)+B(58)+B(66)+B(74)

B(11)+B(19)+B(27)+B(35)+B(43)+B(51)+B(59)+B(67)+B(75)

.....

B(17)+B(25)+B(33)+B(41)+B(49)+B(57)+B(65)+B(73)+B(81).

This step involves 64 additions. We store the output into the one-dimensional array BN2 of length 8.

STEP 7. We multiply the array BN1 by the matrix N2 and apply the permutation P3 to the output. We store the results back into the array BN1. This step involves 16 additions.

STEP 8. We multiply the array BN2 by the matrix N2 and apply the permutation P3 to the output. We store the results back into the array BN2. This step involves 16 additions.

STEP 9. We multiply the array BN1 by the matrix

diag(C3,C3,C3,C3). We apply the permutation $P3^{-1}$ to the output and store the results back into BN1. This step involves four calls of the subroutine I (see below).

STEP 10. We multiply the array BN2 by the matrix diag(C3,C3,C3,C3). We apply the permutation $P3^{-1}$ to the output and store the results back into BN2. This step involves four calls of the subroutine I (see below).

STEP 11. We multiply the array BC1 by the block-diagonal matrix of size 72x72 with 12 blocks equal to C9. This step requires 12 calls of the Subroutine II (see below). We apply the permutation $P1^{-1}$ to the output and store the results back into BC1.

STEP 12. We multiply the array BC2 by the block-diagonal matrix of size 72x72 with 36 blocks equal to C3. This step requires 36 calls of the subroutine I. We apply the permutation $P2^{-1}$ to the output and store the results back into BC2.

STEP 13. We add the arrays BC1 and BC2 and store the output into the array BC. This step requires 72 additions.

STEP 14. We make further additions as follows:

BC(1)=BC(1)+BN1(1),BC(9)=BC(9)+BN1(1),.. BC(65)=BC(65)+BN1(1)

BC(2)=BC(2)+BN1(2),BC(10)=BC(10)+BN1(2),.. BC(66)=BC(66)+BN1(2)

BC(8)=BC(8)+BN1(8),BC(16)=BC(16)+BN1(8),.. BC(72)=BC(72)+BN1(8)

This step involves 72 additions.

STEP 15. Using the Table II we assign the data in the array BN2 to the A(3,0)=B(1);A(3,6)=B(2);... A(6,6)=B(8). We take values for B(9)=A(1,0),... B(80)=A(2,5) from the array BC.

SUBROUTINE I. Computes the product of the 2x2 matrix C3 with an input vector of length 2.

SUBROUTINE II. Computes the product of the 6x6 matrix C9 with an input vector of length 6.

Remark. The given block-scheme should not be considered as a block-scheme of an actual computer program. The STORE instructions in the scheme are chosen mostly for the understanding of the reader, not for efficient use of storage.

CHAPTER II.

0. INTRODUCTION.

In this Chapter we present a new algorithm for the Discrete Fourier Transform on a multi-dimensional data array with p^s points along each axis, where p is a prime number and $s \geq 1$.

The algorithm we are going to introduce is closely connected with algorithms due to S.Winograd for the one-dimensional Fourier Transform on a power of a prime number of data (DFT(p^s:1), cf. [2]), and with the algorithm due to L.Auslander, E.Feig and S.Winograd which computes the n-dimensional Transform on data with p points along each axis, p being a prime number (DFT(p:n), cf. [3]). The new algorithm is a generalization of the two mentioned above and includes the algorithm for DFT(p^2:n), presented in Chapter I as a subcase.

We will refer to these cases as case [2],[3] and [I] of a general algorithm.

We will show further how more general cases sometimes use more primitive ones as steps or subroutines in an algorithm.

PRELIMINARY REMARKS AND NOTATION.

We reserve the letter "p" for a prime number. If s is a positive integer, we will often write q instead of p^s. In this research, the word "ring", whenever used, means "a commutative ring with 1". Similarly, "group" always means an abelian group. Further, all algebraic objects are assumed to be finitely generated.

Next, we will say briefly "Fourier Transform" instead of "one- or multi- dimensional Discrete Fourier Transform".

In the course of the construction, we will often encounter matrix equations which contain permutation matrices. An example will be an equation $B \otimes A = P_1 (A \otimes B) P_2$ In order to simplify the notation, we will avoid writing down the permutation matrices explicitly. Thus, we will write the last equation as $B \otimes A \simeq A \otimes B$. Although this simplification is convenient in this research, in the actual programming of these algorithms great care must be taken with the permutations.

I. DFT(P^S:N) - MULTIPLICATION STRUCTURE.

Let us outline the first steps of the construction.

Readers, familiar with Winograd's algorithm ([2]) may recall that the multipicative structure of the ring Zq, $q=p^s$, played an essential role in the course of the construction of the algorithm for DFT(q:n).

Similarily, in [3], the authors use the multiplicative structure of the finite field with $r=p^n$ elements, F_r, to construct an algorithm for the multi-dimensional DFT(p:n).

We are going to define a certain ring with p^{sn} elements. As the reader will see, both Zq and F_r can be considered as special cases of the new ring.

Let us begin by reviewing some basic definition and facts.

Definition. A commutative ring R is said to be a local ring if R possesses unique maximal ideal.

Example. The only ideal in a field is the zero ideal. Thus the zero ideal of a field is the unique maximal ideal, and hence any field is a local ring.

Example. The ring Zq, $q=p^s$, contains exactly s ideals: $(0)\subset(p^{s-1})\subset..\subset(p)$. Among them only (p) is a maximal ideal. Thus the ring Zq is local.

Let N be the unique maximal ideal in a local ring R. Then R/N is a field, so called residue field of the local ring R.

Since R possesses only one maximal ideal, its residue field is unique. The quotient map $R \longrightarrow R/N$ will be called the residue map of the local ring R.

Lemma 1. Let N be a maximal ideal of R that is nilpotent. Then N is the unique maximal ideal of R and so, by definition, R is a local ring.

Proof. Let a be an noninvertible element of the ring which is not contained in N. Then (a) is an ideal, properly contained in R. Because N is a maximal ideal, $(a)+N=R$. Hence there exist elements $b \in (a)$ and $n \in N$, such that $b+n=1$. Since n is a nilpotent element, there exists $k>0$, such that $n^k=0$. Hence

$$1=1^k=b^k+\ldots+kbn^{(k-1)}+0=b(b^{(k-1)}+\ldots+kn^{(k-1)}),$$

or b is invertible. Hence $(a)=R$, and N is the only maximal ideal in R.

We next review a few basic facts about polynomial extensions of rings.

1). Let R be a ring and I be an ideal in R. Then I[u] is a subring of R[u] and

$$R[u]/I[u] \cong (R/I)[u].$$

2). Let $f(u) \in R[u]$. It is not hard to see that the set $I' = \{g(u) \in I[u] \mid g(u) \text{ is divisible by } f(u)\}$ is an ideal in I[u]. Let $I[u]/\langle f(u)\rangle = I[u]/I'$. Then

$$\frac{(R[u]/\langle f(u)\rangle)}{(I[u]/\langle f(u)\rangle)} \cong \frac{(R/I)[u]}{\langle f'[u]\rangle}$$

where $f'[u]$ is the image of $f(u)$ in $R/I[u]$.

3). Let $N \subset R$ be a nilpotent ideal. Then N[u] is a nilpotent

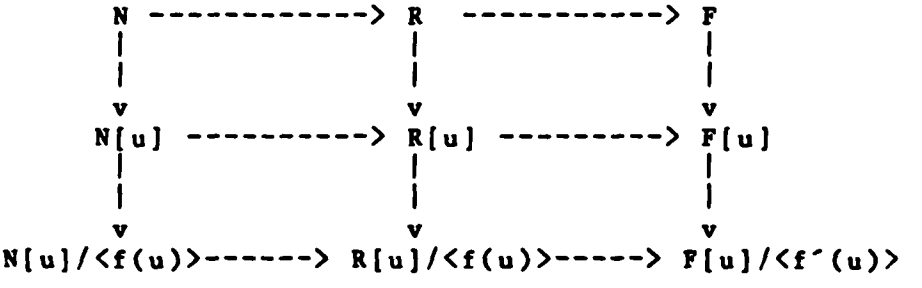
ideal in R[u].

Let F be a field, and f´ an irreducible polynomial over F. Then F[u]/<f´(u)> is a finite field. We are going to replace F by a local commutative ring R and look at some specific polynomial extensions of R.

Since the polynomial ring over a general local ring is not a unique factorization domain, it does not make sense to talk about an irreducible polynomial over a local ring. To overcome this difficulty, we introduce the following

Definition. Let R be a local ring with the maximal ideal N and the residue field F. Let $\pi : R \to F$ is the residue map; we extend it to a homomorphism $\pi[u]: R[u] \to F[u]$ by letting $(\pi[u])(u)=u$. We say that $f \in F[u]$ is a locally irreducible polynomial iff $f' = (\pi[u])(f) \in F[u]$ is an irreducible polynomial over F and $\deg_F(f') = \deg_R(f)$.

Consider the following commutative diagram, where $f \in R[u]$ and f is a locally irreducible polynomial.



Then

Lemma 2.

$R[u]/\langle f(u)\rangle = \overline{R}$ is a local ring with the maximal nilpotent ideal $\overline{N} = N[u]/\langle f(u)\rangle$ and the residue field $\overline{F} = F[u]/\langle f(u)\rangle$.

Proof.

Let $\overline{N} = N[u]/\langle f(u)\rangle = N+uN+u^2N+\ldots+u^{(n-1)}N$, where n is the degree of f. We observe that $\overline{N}$ is a nilpotent ideal in $R[u]/\langle f(u)\rangle$. We will verify that $\overline{N}$ is a maximal ideal by showing that $\overline{R}/\overline{N}$ is a field, and the lemma will follow from Lemma 1 above.

By (2), $\overline{R}/\overline{N} = (R/N)[u]/\langle f'[u]\rangle$. We have required f' to be an irreducible polynomial over $F = R/N$. Hence we have $\overline{R}/\overline{N} = F[u]/\langle f'[u]\rangle$, which is a field.

Remark. It is not hard to show that if F possesses an irreducible polynomial of degree n, then R has a locally irreducible polynomial of the same degree. Indeed, let f' be irreducible over F, deg(f')=n. Let $f\in R[u]$, deg(f)=n, be such that $(\pi[u])(f)=f'$. Then, by definition, f is locally irreduclible over R.

It is well known that for any $n \geq 1$ there is an irreducible polynomial of degree n over Zp; thus the ring Zq has locally irreducible polynomials of any given degree.

We can now consider the following diagram:

DIAGRAM I.

$$\begin{array}{ccc} Zq[u]/\langle f(u)\rangle & \xrightarrow{\pi^n} & Zp[u]/\langle f(u)\rangle \\ \downarrow \varphi^s & & \downarrow \varphi \\ Zq & \xrightarrow{\pi} & Zp \end{array}$$

Here π and π^n are projections of the local rings Zq and $Zq[u]/\langle f(u)\rangle$ on their residue fields. The map φ^s is defined as follows: elements of $Zq[u]/\langle f(u)\rangle$ are classes of polynomials congruent modulo f(u). For each such class there is exactly one representative of degree less than n. We

identify each class with this representative and define φ^s as projection of the representative on its constant term. We define φ analogously. It is straightforward to verify that the DIAGRAM I is commutative.

We observe that φ and φ^s are not ring homomorphisms, while π and $\bar{\pi}^n$ are. By a slight abuse of notation, we are going to write π instead of π^n and φ instead of φ^s.

NOTATION. For the rest of the discussion we fix n and the polynomial f. In order to shorten the notation, we set $Zq(n) = Zq[u]/\langle f(u)\rangle = Zq+Zq\cdot u+\ldots+ Zq\cdot u^{(n-1)}$ and $Zp(n)=Zp^1(n) = Zp[u]/\langle f'(u)\rangle$. Obviously, $Zp(n) = F_r$, $r=p^n$ We will always use the letter 'u' to denote the coset of u in $Zq[u]/\langle f(u)\rangle$.

II. Zq(N) - ADDITIVE STRUCTURE.

Let A be a complex function on the additive group of $Zq\oplus Zq\oplus\ldots\oplus Zq$. Recall that the DFT(q:n) is given by the following equation:

$$\hat{A}(a_0,a_1,\ldots a_{n-1})= \sum_{b_i=0;\, i=0,1\ldots n-1}^{q-1} w^{\left(\sum_{i=0}^{n-1} a_i b_i\right)} A(b_0,b_1,\ldots b_{n-1}), \quad (1)$$

where a_i ranges from 0 to q-1 for i=0,1,... n-1 and $w=e^{2\pi i/q}$

Additively, Zq(n) is a direct sum of n copies of the group Zq. Thus the additive group of the ring, $(Zq(n))^+$, is exactly the group on which we are doing the Transform. We

rewrite the equation (1) as follows:

$$\hat{A}(a) = \sum_{b \in Zq(n)} w^{(\sum_{i=0}^{n-1} a_i b_i)} \cdot A(b), \qquad (2)$$

for all $a \in (Zq(n))^{+}$. Here, in the notation of Section I, a_i is the i-th coefficient of the polynomial $a(u) = \sum_{i=0}^{n-1} a_i u^i \in Zq(n)$. We further write $\langle a,b \rangle = \sum_{i=0}^{n-1} a_i b_i$ Then, (2) is the same as

$$A(a) = \sum_{b \in Zq(n)} w^{\langle a,b \rangle} A(b) \qquad (3)$$

Our next goal is to link the bilinear form $\langle \ , \ \rangle$ with the multiplicative structure of Zq(n).

III. Zq(N) - MULTIPLICATIVE STRUCTURE REVISITED.

The ring Zq(n) was constructed as a polinomial extension of Zq. The maximal nilpotent ideal of Zq is (p), the set of elements, divisible by p. Thus, by Lemma 2, the maximal nilpotent ideal of Zq(n) is $(p)+(p)u+\ldots (p)u^{(n-1)}$. We will also denote it by (p). (p) consists exactly of the non-invertible elements of Zq(n). As (p) contains $p^{(s-1)n}$ elements, the group of units, U(Zq(n)), is of order $p^{sn} - p^{(s-1)n} = p^{(s-1)n}(p^n-1)$.

We observe that the map $\pi : Zq(n) \to Zp(n)$ projects U(Zq(n)) onto U(Zp(n)). The latter group is cyclic of order p^n-1, hence the former has to contain a cyclic subgroup of order divisible by p^n-1. As the order of U(Zq(n)) is $p^{(s-1)n}(p^n-1)$, U(Zq(n)) contains exactly one subgroup of order

p^n-1.

We denote this subgroup by $G = G^s$ and let x be one of its generators. We further define $H^s=1+(p)\subset Zq(n)$. It is easy to verify that H^s is a subgroup of U(Zq(n)), and the order of H^s is $p^{(s-1)n}$

Notation. The letters 'G', 'H' and 'x' will be reserved for the objects now defined.

Theorem 3. The group of units of the ring Zq(n) is isomorphic to the direct sum of the subgroups H^s and G^s Further, H is isomorphic to the direct sum of n copies of Z_p.

Proof. We recall that $Zq(n)=Zq[u]/\langle f(u)\rangle$, for some locally irreducible f. For i=0,1,.. n-1, let $h_i=1+pu^i$. We claim the following:

(1) For every i=0,1,.. n-1, h_i has order $p^{(s-1)}$.

(2) The elements h_i's satisfy the following "independence" condition:

$$(h_i)^{a_i} = 1 \implies p^{(s-1)} | a_i \text{ for every } i. \qquad (4)$$

The proofs of (1) and (2) are straightforward, while lengthy, exercises in elementary algebra, whose details we leave to the reader.

Let us now define

$$H^s(i)= gr(h_i), \qquad (5)$$

where gr(...) stands for the subgroup spanned by elements in the parentheses.

(1) and (2) are equivalent to the statement that

$H^s = \bigoplus H^s(i)$, and the order of $H^s(i)$ is $p^{(s-1)}$. Because the latter number is relatively prime to the order of G^s, $U(Zq(n)) = G^s \oplus H^s$.

Example [2]. Let n=1. Then $U(Zq) \cong Z_{(p-1)} \oplus Z_{p^{s-1}}$. is cyclic of order $p^{(s-1)}(p-1) = \Phi(q)$, where Φ is Euler's Phi function.

Example [3]. Let s=1. Here $U(Zp(n)) = Z_{p^n-1}$, the cyclic group of units of a finite field.

Example [I]. Let s=2. $U(Zq(n)) = Z_{p^n-1} \oplus (\bigoplus_{i=0}^{n-1} Zp)$. We observe that $H^2 \cong (Zp(n))^+$ and the isomorphism is given explicitly by $z \in Zp(n) \rightarrow 1+pz$. Here $(1+pz_1)(1+pz_2)=1+p(z_1+z_2)$.

IV. THE ZERO DIVISORS OF $Z_q(N)$.

We observe that Zq(n) contains the following family of ideals:

$$0=(p^s) \subset (p^{(s-1)}) \subset \ldots \subset (p^2) \subset (p) \subset Zq(n). \qquad (6)$$

Here $(p^k)=(p)^k$ and (p^k) contains $p^{(s-1)n}$ elements for every k. We define D^k as the set-theoretical difference $(p)^k-(p)^{k+1}$; notice that D^k contains exactly those elements which are divisible by p^k, but not by $p^{(k+1)}$. D^k contains $p^{(s-k)n} - p^{(s-k-1)n} = p^{(s-k-1)}(p^n-1)$ elements. Notice that $D^k = U(Zq(n))$, and for k>0, D^k contains only zero divisors.

We will now introduce a few more subgroups of U(Zq(n)). Let

$$H^{s,k} = 1+(p^k) \subset Zq(n).$$

We observe that $H^{s,1} = H^s$. Further, the subgroups $H^{s,k}$ (with $k>0$ varying) form a sequence, analogous to (6). We have:

$$\{1\}=H^{s,s}\subset H^{s,s-1}\subset\ldots\subset H^{s,1}\subset H^{s,0}=Zq(n). \qquad (7)$$

For $k>0$, $H^{s,k}$ is a subgroup of $U(Zq(n))$.

Remark. Similarly to H^s, $H^{s,k}$ is composed of subgroups $H^{s,k}(i)$, where $H^{s,k}(i) = gr(1+p^k u^i)$. It is not hard to show that

1) For every i,

$$\begin{array}{ccccccc} H^{s,s}(i) & \subset & H^{s,s-1}(i) & \subset & \ldots & & H^{s,1}(i) \\ \cap & & \cap & & & & \cap \\ H^{s,s} & \subset & H^{s,s-1} & \subset & \ldots & & H^{s,1} \end{array}$$

2) For every i and k, $H^{s,k}(i) = \{z^p \mid z\in H^{(k-1)}(i)\}$.

The proof of 2) is another lengthy exercise in elementary algerba. We leave the details to the reader.

The order of $H^{s,k}$ is $p^{(s-k)n}$. Hence, the order of the quotient group $H^{s,1}/H^{s,s-k} = \{1+(p)\}/\{1+(p)^{s-k}\}$ is $p^{(s-1)n-(s-s+k)n} = p^{(s-k-1)n}$. Let $G_k = G^s \oplus (H^{s,1}/H^{s,s-k})$. The order of G_k is $(p^n-1)p^{(s-k-1)n}$.

The unit group $U(Zq(n))$ acts on D^k via ring multiplication, i.e., for every $g\in U(Zq(n))$ and $d\in D^k$ $(g,d)\to gd\in D^k$. We next observe that for any $d\in D^k$ and g_1, $g_2\in U(Zq(n))$ such that $g_1 g_2^{-1}\in H^{s,s-k}$, $g_1 d = g_2 d$. (Indeed, if $g=g_1 g_2^{-1}\in H^{s,s-k}$, $g=1+p^{s-k}a$ for some a; $d=p^k b$ for some $b\in Zq$; hence $gd=(1+p^{s-k}a)p^k b=d$, and the assertion follows). Thus we can say that the group $G_k = G\oplus(H^{s,1}/H^{s,s-k})$ acts on D^k by the following rule: for every $g\in G_k$, $d\in D^k$, $(g,d)\to g\cdot d = g'd$, where g' is any of the preimages of g in $G^s\oplus H^{s,1}$. The next theorem will

expose the nature of this action.

Theorem 4. Let all notation be as above. For every $d_1, d_2 \in D^k$ there is one and only one $g \in G_k$ such that $g \cdot d_1 = d_2$, i.e. the action of G_k on D^k is simply transitive.

Proof. We prove the uniqueness first. Let $g_i(p^k a) = p^k b$ for $i=1,2$, where $g_1, g_2 \in G^s \oplus H^s$ Then $g_1^{-1} g_2 (p^k a) = p^k a$ and $(g_1^{-1} g_2 - 1) p^k a = 0$. The last statement implies that $g_1^{-1} g_2 \in H^{s, s-k}$ and hence the images of g_1 and g_2 in G_k coincide, which proves the uniqueness.

We discuss the existence next. Recall that the orders of D^k and G_k are the same and hence (by uniqueness) the set $G_k d_1$ also has the same order for any $d_1 \in D^k$. Further, $G_k d_1$ is a subset of D^k. Hence $G_k d_1$ must coincide with D^k and the existence follows.

Corollary. Every nonzero element of the ring Zq(n) can be uniquely written as product $p^k x^{\bar{k}} h_0^{k_0} h_1^{k_1} \ldots h_{n-1}^{k_{n-1}}$, where $k=0,1,\ldots s-1$, $\bar{k}=0,1,\ldots p^n-2$, and $k_j=0,1,\ldots p^{(s-1)}-1$ for $j=0,1,\ldots n-1$.

Proof. Let $S(k) = \{(\bar{k}, k_0, k_1, \ldots k_{n-1}) \mid \bar{k}=0,1,\ldots p^n-2, k_i=0,1,\ldots p^{(s-1)}-1 \text{ for } i=0,1,\ldots n-1\}$. Let $Exp^k : S(k) \to Zq(n)$, $Exp^k(\bar{k}, k_0, \ldots k_{n-1}) = x^{\bar{k}} h_0^{k_0} \ldots h_{n-1}^{k_{n-1}}$. Finally, let $D(k) = Exp^k(S(k))$. We observe that

1). $D(k) \subset D^k$ (see the definition of D^k).

2). The number of elements of S(k) is the same as that of D^k Thus, in order to proof that $D(k) = D^k$, we must show that Exp^k is one-to-one on S(k); it follows from the Theorem 4. To finish the proof, we recall that $Zq(n) = \bigcup_{k=0}^{s} D^k$ (see

Section III).

Example [2]. Let n=1. We can choose f(u)=u-1. Then $H^{s,1} \cong Z_p$ and so $H^{s,1}$ is cyclic. If we specify s=p=3, we can list explicitly the algebraic objects discussed above:

(1) = Z^{27}

(3) = { 0, 3, 6, 9, 12, 15, 18, 21, 24 }

(9) = { 0, 9, 18 }

(27) = { 0 }

D^0 = $U(Z_{27})$

D^1 = { 3, 6, 12, 15, 21, 24 }

D^2 = { 9, 18 }

D^3 = { 0 }

The group of units is cyclic and we can choose 2 as a generator:

$U(Z_{27})$ = { 1,2,4,8,16,5,10,20,13,26,25,23,19,11,22,17,7,14}

$H^{3,1}$ = { 1,4,16,10,13,25,19,22,7}

$H^{3,2}$ = { 1,10,19 }

$H^{3,3}$ = { 1 }

G = { 1, 26 }

Here $(H^{3,1}/H^{3,2}) \oplus G$ acts on D^1 in the sense of Lemma 3;

$(H^{3,1}/H^{3,1}) \oplus G \cong G$ acts on D^2

Example [I]. Choose n=2,p=3,s=2. The polynomial $f(u)=u^2+1$ is locally irreducible over Z_9 The ring $Z_9(2)$ contains 81 elements.

Here:

D^0 = $U(Z_9(2))$

D^1 = {3,3+3u,6u,3+6u,6,6+6u,3u,6+3u}

$D^2 = \{ 0 \}$

$G = \{1, 2+2u, 8u, 2+7u, 8, 7+7u, u, 7+2u\}$

$H^{2,1} = H^{2,1}(0) \oplus H^{2,1}(1) = \{1,4,7\} \oplus \{1, 1+3u, 1+6u\}$

$H^{2,2} = \{ 1 \}$

$(H^{2,1}/H^{2,1}) \oplus G$ acts on D^1 in the sense of Lemma 3.

V. AN AUTOMORPHISM OF $Z_q(N)$.

Theorem 5. There exist an automorphism T of the additive group of the ring Zq(n), such that the following equation holds:

$$< Ta, b > = \varphi(ab), \qquad (8)$$

where φ is as it was defined in Section I, for any $a, b \in Zq(n)$.

Proof. Let C be the companion matrix of the polynomial f over Zq. Then the mapping $\sum_{i=0}^{n-1} a_i u^i \longrightarrow \sum_{i=0}^{n-1} a_i C^i = a(C)$ is a matrix representation of Zq(n) in M(Zq;n), the set of all endomorphisms of n-dimensional vector space over Zq. Notice that the first column of a(C) is $(a_0, a_1, \ldots a_{n-1})^t$, i.e. $a = \sum_{i=0}^{n-1} (a(C))_{i+1,1} u^i$ (We are using subscripts to denote the entries of a matrix.) Let

$$T(a) = \sum_{i=0}^{n-1} (a(C))_{1,i+1} u^i \qquad (9)$$

Then, clearly, T is an additive endomorphism of Zq(n).

T also satisfies the equation (8), because

$$\langle T(a), b \rangle = \sum_{i=0}^{n-1} (T(a))_i b_i = \sum_{i=0}^{n-1} (a(C))_{1,1+i} \cdot (b(C))_{1+i,1} = \sum_{i=1}^{n} (a(C))_{1,i} \cdot (b(C))_{i,1} = (a(C)b(C))_{1,1} = ((ab)(C))_{1,1} = (ab)_0 = \varphi(ab)$$

In order to complete the proof we have to show that T is bijective. Assume otherwise. Let $a \neq 0$, $a \in Ker(T)$. This is equivalent to the first row of the matrix a(C) containing only zeroes. Clearly, then, a(C) is not an invertible matrix and hence $a \notin U(Zq(n))$. Further, a is not one of the elements $p, p^2, p^3, \ldots p^{(s-1)}$, since $p^k(C)$ contains a nonzero leading entry. By Lemma 3 there exists an element $g \in G \oplus H^{s,1}$ such that $ag = p^k$ for some k. Then:

$$(p^k(C))_{1,1} = \sum_{i=1}^{n} (a(C))_{1,i} (g(C))_{i,1} = 0,$$

and we obtain a contradiction. This proves that T is an injection; that T is a surjection follows from the finite dimensionality of the vector space.

Example [1]. In the one-dimensional case T degenerates into the identity map.

Remark. We now state without proof a few elementary properties of T.

Lemma 6.

(1) $\varphi(a) = \varphi(T(a))$, for any $a \in Zq(n)$.

(2) $T(D^k) = D^k$, for every k.

(3) If we specify the basis $(1, u, u^2, \ldots u^{n-1})$, then T is given by a symmetric block-diagonal matrix with two blocks: the first one is the 1 x 1 identity matrix and the other is an (n-1) by (n-1) matrix.

Using the fact that T is a bijection, we can rewrite the

equations (3) as follows:

$$\hat{A}(T(b)) = \sum_{a\in Z_q(n)} w^{<Tb,a>} A(a) = \tag{10}$$

$$= \sum_{a\in Z_q(n)} w^{\varphi(ab)} A(a)$$

Let us rewrite the equations (10) further. The first entry of the output, $\hat{A}(T(0))=\hat{A}(0)=\sum_{a\in Z_q(n)} w^{\varphi(0)}\cdot A(a)=\sum_{a\in Z_q(n)} A(a)$. Then if $B(b)=\hat{A}(T(b))-\hat{A}(0)$ for $b\in Zq(n)$, we obtain

$$B(b)= \sum_{a\in Z_q(n)} w^{\varphi(ab)}\cdot A(a)- \sum_{a\in Z_q(n)} A(a)= \tag{11}$$

$$\sum_{a\in Z_q(n)}{}'(w^{\varphi(ab)}-1)A(a)= \sum_{a\in Z_q(n)}{}' W^s(ab)A(a), \text{ where}$$

$$W^s(t)=w^{\varphi(t)}-1. \tag{12}$$

Remark. We will often view W^s as a complex valued function on R.

From now on our task will be the computation of the numbers B(b) for all $b\in Zq(n)$; the values $\hat{A}(b)$ can be reconstructed as follows:

$$\hat{A}(b) = B(T^{-1}(b))+\hat{A}(0) \tag{13}$$

$\hat{A}(0)$ in turn can be computed using $p^{sn}-1$ additions.

The advantage of subtracting 1 from our coefficients lies in the number of additions we are to perform; if the number $w^{\varphi(ab)}=1$, we decrease the amount of additions by 1, since $W^s(ab)=0$: if $w^{(ab)}\neq 1$, we actually gain nothing but also lose nothing. At the same time the price we pay is $2(p^{sn}-1)$ additions. We perform $p^{sn}-1$ of them, while calculating A(0), and $p^{sn}-1$ more adding A(0) to the B(b) for all $b\neq 0$.

Let us keep in mind that on the last stage of the

algorithm we will have to perform the permutation T; for now, however, we drop the T and thus simplify the notation.

VI. DFT(Q:N) - STEPS OF THE ALGORITHM.

Let us subdivide the sums in (11) as follows:

$$B(b) = \sum_{K=0}^{S} \left(\sum_{a \in D^K} W^s(ab)A(a) \right), \text{ for all } b \in Zq(n). \qquad (14)$$

We say that the problem of calculating of the sums $B_{L,K}(b) = \sum_{a \in D^K} (W^s(ab))A(a)$ for all $b \in D^L$ is the (L,K)-th step of the algorithm. Clearly, once we have performed all the (L,K)-th steps for K,L=0,1,.. s, only additions are necessary in order to complete the algorithm.

Remark. This breaking up of the algorithm onto steps will in matrix notation be equivalent to the breaking of a matrix onto subblocks. The examples below will illustrate this statement.

Remark. Notice that the (s,K)-th step and (K,s)-th steps of the algorithm require no calculations. This is because $\sum_{a \in D^K} W^s(0 \cdot a)A(a) = \sum_{a \in D^K} (w^0 - 1)A(a) = 0$.
Similarly, the (K,s)-th step is the calculation of $\sum_{a \in D^s} W^s(ab)A(a)$ for all $b \in D^L$. We have $\sum_{a=0} W^s(ab)A(a) = W^s(0)A(0) = 0$.

Example [2]. Let p=3,s=2,n=1. S.Winograd in [2] ordered the input and output of DFT(9:1) and wrote the Transform in the following matrix form:

<u>DIAGRAM II.</u>

$$
\begin{Vmatrix} B(0) \\ \hline B(3) \\ B(6) \\ \hline B(1) \\ B(2) \\ B(4) \\ B(8) \\ B(7) \\ B(5) \end{Vmatrix}
=
\left\Vert \begin{array}{c|cc|cccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & w^3-1 & w^6-1 & w^3-1 & w^6-1 & w^3-1 & w^6-1 \\
0 & 0 & 0 & w^6-1 & w^3-1 & w^6-1 & w^3-1 & w^6-1 & w^3-1 \\ \hline
0 & w^3-1 & w^6-1 & w^1-1 & w^2-1 & w^4-1 & w^8-1 & w^7-1 & w^5-1 \\
0 & w^6-1 & w^3-1 & w^5-1 & w^1-1 & w^2-1 & w^4-1 & w^8-1 & w^7-1 \\
0 & w^3-1 & w^6-1 & w^7-1 & w^5-1 & w^1-1 & w^2-1 & w^4-1 & w^8-1 \\
0 & w^6-1 & w^3-1 & w^8-1 & w^7-1 & w^5-1 & w^1-1 & w^2-1 & w^4-1 \\
0 & w^3-1 & w^6-1 & w^4-1 & w^8-1 & w^7-1 & w^5-1 & w^1-1 & w^2-1 \\
0 & w^6-1 & w^3-1 & w^2-1 & w^4-1 & w^8-1 & w^7-1 & w^5-1 & w^1-1
\end{array} \right\Vert
\times
\begin{Vmatrix} A(0) \\ \hline A(3) \\ A(6) \\ \hline A(1) \\ A(2) \\ A(4) \\ A(8) \\ A(7) \\ A(5) \end{Vmatrix}
$$

where $w^9=1$.

The nine submatrices, highlighted in the DIAGRAM II, correspond to the nine (L,K) steps of the algorithm for K,L=0,1,2. Readers unfamiliar with Winograd's work, may be surprised to notice that the submatrices, corresponding to our (L,K) steps, have rather special forms. Thus, for example, the submatrix of the step (1,1) contains only zeroes. This observation will be made more precise in Lemma 5.

<u>Example</u> [3]. Let $p=3, n=2, s=1$ and $f(u)=u^2+1$. The element $1+u=x$ generates the group of units $U(Z_3(2))$. We rewrite the DFT(3·2) in the following matrix form:

DIAGRAM IV.

$$\begin{pmatrix} B(0) \\ \hline B(x^6) \\ B(x^7) \\ B(x^6) \\ B(x^5) \\ B(x^4) \\ B(x^3) \\ B(x^2) \\ B(x^1) \end{pmatrix} = \left(\begin{array}{c|cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & w^1-1 & w^1-1 & 0 & w^1-1 & w^2-1 & w^2-1 & 0 & w^2-1 \\ 0 & w^2-1 & w^1-1 & w^1-1 & 0 & w^1-1 & w^2-1 & w^2-1 & 0 \\ 0 & 0 & w^2-1 & w^1-1 & w^1-1 & 0 & w^1-1 & w^2-1 & w^2-1 \\ 0 & w^2-1 & 0 & w^2-1 & w^1-1 & w^1-1 & 0 & w^1-1 & w^2-1 \\ 0 & w^2-1 & w^2-1 & 0 & w^2-1 & w^1-1 & w^1-1 & 0 & w^1-1 \\ 0 & w^1-1 & w^2-1 & w^2-1 & 0 & w^2-1 & w^1-1 & w^1-1 & 0 \\ 0 & 0 & w^1-1 & w^2-1 & w^2-1 & 0 & w^2-1 & w^1-1 & w^1-1 \\ 0 & w^1-1 & 0 & w^1-1 & w^2-1 & w^2-1 & 0 & w^2-1 & w^1-1 \end{array}\right) \times \begin{pmatrix} A(0) \\ \hline A(x^0) \\ A(x^1) \\ A(x^2) \\ A(x^3) \\ A(x^4) \\ A(x^5) \\ A(x^6) \\ A(x^7) \end{pmatrix}$$

where $w^3=1$.

The four highlighted submatrices correspond to the (L,K)-th steps of the algorithm for K,L=0,1. We observe that the 8x8 submatrix, connected with the (0,0) step, has circulant form. Further, as we will see later, it can be factored as a product of two other matrices, a fact which is essential for the new algorithm.

VII. (L,K)-TH STEP - DEFICIENCY.

Definition. We say that the number K+L is the deficiency of the step (L,K).

As we will shortly see, the deficiency of the step says a lot about the step itself.

Lemma 7. For K and L such that $K+L \geq s$, the (L,K)-th step

requires no arithmetic operations.

Proof. Let us consider $W^s(ab), a \in D^k, b \in D^L$. Then $a=p^k a'$, $b=p^L b'$ for some $a', b' \in Zq(n)$. Hence $W^s(ab)=W^s(p^{K+L}a'b')=W^s(0)=0$ and the lemma follows.

We will assume next that $0 \leq K+L < s$.

We will show that all the steps with deficiency greater than zero can be reduced to steps of $DFT(p^r;n)$ with $r<s$.

As we have observed in Theorem 4, any element a of D^k can be uniquely written as $p^k g$, where $g \in G_k = G^s \oplus (H^{s,1} / H^{s,s-k})$. Let $A'' = H^{s,s-k-L} / H^{s,s-k}$, $B'' = H^{s,s-k-L} / H^{s,s-L}$. Here A" is a subgroup of G_k and B" is a subgroup of G_L. Let $C'' = G \oplus (H^{s,1} / H^{s,s-k-L})$. Then $G_k/A'' = G_L/B'' = C''$. We further define

$$C = \{ g^i h_0^{i_0} h_1^{i_1} \ldots h_{n-1}^{i_{n-1}} \;/\; 0 \leq i < p^n - 1, \; 0 \leq i_j < p^{s-k-L-1} \text{ for } j=0,1,\ldots n-1 \}.$$

Then C is a set of representatives of cosets of A" in G_k. At the same time C is a set of representatives of cosets of B" in G_L. Thus for any $k,L=0,1\ldots s$ we can uniquely write an element a of D^k as $a = p^k a' a''$, where $a' \in C$ and $a'' \in A''$. Analogously, any element b of D^L can be uniquely written as

$p^L b' b''$, where $b' \in C$ and $b'' \in B$.

Then we observe that

$$ab = p^k a'a'' \cdot p^L b'b'' = a'b' \cdot p^{K+L} a''b'' = p^{K+L} a'b' \qquad (15)$$

The last equation follows from the earlier observation that $p^j(1+p^j t)=p^j$ for $j+j \geq s$.

Thus the product ab does not depend on a" and b".

Remark. Let K=L=0.

Here A" and B" are trivial subgroups and C"= U(Zq(n)). At the same time, whenever K>0 or L>0, C" is a proper quotient group of the unit group.

We now return to the algorithm.

Definition. We denote by $E_{m,n}$ the m by n matrix with all entries 1 and let $E_m = E_{m,m}$.

Let us consider the equations for the (L,K)-th step. We are to compute (see equations 11 and 14):

$$B_{L,K}(b) = \sum_{a \in D^K} W^s(ab)A(a) \text{ for all } b \in D^L, \qquad (16)$$

or, in the matrix form,

$$B_{L,K} = M^s_{L,K} \times A_k, \qquad \text{where} \qquad A_k = \{A(t) \mid t \in D^k\},$$

$B_{L,K}=\{B_{L,K}(t) \mid t\in D^L\}$, and $M_{L,K}=\{ W^s(ab) \mid, a\in D^k, b\in D^L\}$. Let $B_{L,K}(b',b'') = B_{L,K}(b)$, $A_k(a',a'')=A_k(a)$, where a',a'',b' and b'' are as defined above. We rewrite the equations (16) as follows:

$$B_{L,K}(b',b'') = \sum_{a''\in A''}\sum_{a'\in C'} W^s(ab)A(a',a'') = \sum_{a'\in C'} W^s(p^{K+L}a'b')((\sum_{a''\in A''} A(a',a''), \tag{17}$$

for all $b''\in B''$ and $b'\in C$.

Thus we obtain:

$$M^s_{L,K}=\bar{M}^s_{L,K} \otimes E_{p^L,p^k} , \tag{18}$$

where $\bar{M}^s_{L,k}$ is the square $(p^n-1)p^{(s-k-L-1)}$ by $(p^n-1)p^{(s-k-L-1)}$ matrix with entries $W^s(p^{K+L}a'b')$, indexed by elements a',b' of C.

The equations (17) do not depend on the the choice of the representatives a',b' and thus we can say that the matrix $\bar{M}^s_{L,K}$ is indexed by elements of C".

One immediately observes that the matrix $\bar{M}^s_{L,K}$ does not depend on K or L separately, but only on their sum.

Example [2]. The submatrices, corresponding to the steps (1,0) and (0,1) of the algorithm are both built from 2x2 block C_3, where

$$C_3 = \begin{vmatrix} w^3-1 & w^6-1 \\ w^6-1 & w^3-1 \end{vmatrix},$$

where $w^9=1$.

The matrix C_3 also occurs in the DFT(3:1), where it corresponds to the (0,0)-step.

We will shortly see the reason for this.

We are going to compare the matrices $\bar{M}^s_{L,K}$ obtained for different values of s. Let $\bar{\pi}$ be the quotient map $Zq(n) \longrightarrow Zq(n)/(p^{K+L}) \cong Z_{p^{s-K-L}}(n)$. The restriction of $\bar{\pi}$ on C is a bijection between C and $U(Z_{p^{s-K-L}}(n))$.

Lemma 8.

$$W^s(p^{K+L}a'b') = W^{s-K-L}(\bar{\pi}(a')\bar{\pi}(b')), \qquad (19)$$

for every $a',b' \in C$.

Proof. Recall thet $w=e^{2\pi i/q}$, let further $v=w^{p^{K+L}}$. We observe that for $a,b \in Zq(n)$ such the $\bar{\pi}(a)=\bar{\pi}(b)$ we have $v^{\bar{\pi}(a)}=v^{\bar{\pi}(b)}=v^a$. (Here the exponents are considered as integers; it is easy to see that there is no ambiguity). Hence, $W^s(p^{K+L}a'b')=w^{p^{K+L}\varphi(a'b')}-1=v^{\varphi(a'b')}-1=v^{a'b'}-1$ $= W^{s-K-L}(\bar{\pi}(a')\bar{\pi}(b'))$, which concludes the proof.

Corollary.

$$\bar{M}^s_{L,K} = M^{s-k-L}_{0,0}$$

Let us summarize this discussion in the following

Theorem 9. The (L,K)-th step of DFT(q:n) is equivalent (up to additions) to the (0,0)-th step of DFT(p^{s-k-L} :n).

Proof. Equation (17) shows that in order to multiply a vector by $M^{s}_{L,K}$, we have to perform some additions and then multiply the shorter vector by the matrix $\bar{M}^{s}_{L,K}$. As we saw in Lemma 8, the latter matrix is the one which corresponds to (0,0)-th step of DFT(p^{s-k-L} :n), which completes the proof.

Remark. Let us look at the practical aspects of Theorem 9. Assume that we are given subroutines for computing DFT(p^{k}:n) for k=1,2,.. s-1. Then in order to compute DFT(p^{s}:n) we have to perform all (L,K)-th steps of the latter problem; our subroutines will handle all of these steps but one, namely (0,0). Thus we see that the computer program for calculating DFT(p^{s}:n) will be built from "standard" blocks. We will see that these blocks are actually subroutines for computing of Winograd's core of 1-dimensional transform.

From now on, we will concentrate our attention on the (0,0)-th step. We will also call it the core step of the algorithm.

Let us introduce some more notation.

Let $y=xh_0$. Then y generates the subgroup $G' = G^{s} \oplus H^{s}(0)$ of order $p^{(s-1)}(p^{n}-1)$. Let $H' = \bigoplus_{i=1}^{n-1} H^{s}(i)$. Then $U(Zq(n)) = G' \oplus H'$. Every element t of the group of units U(Zq(n)) can be written uniquely as $t=y^{k}h$, where $k=0,1,..p^{(s-1)}(p^{n}-1)-1$ and $h \in H'$; $h = h_1^{k_1} .. h_{n-1}^{k_{n-1}}$ for some $k_1,k_2,.. k_{n-1} = 0,1,..p^{(s-1)}-1$. We rewrite the equations (17) for the core step.

$$B_{0,0}(y^L h_1^{L_1} h_2^{L_2} \dots h_{n-1}^{L_{n-1}}) = \tag{20}$$
$$\sum_{K=0}^{p^{s-1}(p^s-1)-1} \sum_{K_i=0}^{p^{s-1}-1} W^s(y^{L+k} h_1^{L_1+K_1} \dots h_{n-1}^{L_{n-1}+K_{n-1}}) A(y^K h_1^{K_1} \dots h_{n-1}^{K_{n-1}})$$

or, shorter,

$$B_{0,0}(y^L h) = \sum_{K=0}^{p^{s-1}(p^s-1)-1} \sum_{h' \in H'} W^s(y^{K+L} h h') A(y^K h')$$

We now introduce one more permutation. Let I map the group of units to itself, sending each element into its multiplicative inverse. We rewrite the equations (20) as

$$B_c(y^L h_1^{L_1} \dots h_{n-1}^{L_{n-1}}) = B_{0,0}(I(y^L h_1^{L_1} \dots h_{n-1}^{L_{n-1}})) = \tag{21}$$
$$= \sum_{K=0}^{p^{s-1}(p^s-1)-1} \sum_{K_i=0}^{p^{s-1}-1} W^s(y^{k-L} h_1^{k_1-L_1} \dots h_{n-1}^{k_{n-1}-L_{n-1}}) \quad x$$
$$A(y^k h_1^{k_1} \dots h_{n-1}^{k_{n-1}}).$$

or, in the matrix form,

$$B_c = M_c A_c. \tag{22}$$

We will show now that the matrix M_c is connected with a representation of a certain group algebra.

VIII. DFT(Q:N) - GROUP ALGEBRAS AND SHIFT OPERATOR.

We start this section with some general observations.

Let A be a finite (abelian) group. We are given a decomposition of A as a direct product of cyclic subgroups

A_i, i=1,...N. Let $A_i = gr(a_i)$, let m_i be the order of a_i. Thus we can take A as the set of N-tuples $(j_1, j_2, \ldots j_N)$, where $0 \leq j_i < m_i$ We consider A to be lexicographically ordered.

Let R be a ring. The set of all functions X:A-->R can be given an algebraic structure, called a group algebra R[A], which is canonically isomorphic to $\bigotimes_{i=1}^{N} R[A_i]$.

Let us consider $R[A_i]$. We define a representation of A_i in $M(R,m_i)$ by mapping a_i to S_{m_i}, where S_{m_i} is the m_i by m_i matrix

$$\begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{vmatrix}$$

Then $R[A_i]$ is represented as the algebra generated in $M(R,m_i)$ by S_{m_i}. For any given $X \in R[A_i]$, the image of X in $M(R,m_i)$, denoted as $\overline{X}$, is the matrix $||X(a^{-1}b)||_{a,b \in A}$.

Let us give two examples.

First, if X(1)=1 and X(a)=0 for a=1, $\overline{X}$ is exactly the shift operator matrix S_{m_i}.

Second, if we define X(a)=1 for all a, $\overline{X} = \sum_{j=1}^{m_i} S_{m_i}^{j}$ is a matrix, containing only ones. We have denoted it by E_{m_i}.

Analogously, we define the representation of R[A] by mapping $X \longrightarrow \overline{X} = ||X(a^{-1}b)||_{a,b \in A}$. Then the matrix X is an element of the tensor product of algebras;

$\overline{X} = \sum_{a \in A} (\bigotimes_{i=1}^{N} S_{m_i}^{j_i}) X(a)$, where $a = \prod_{i=1}^{N} a_i^{j_i}$.

<u>Remark</u>. The reader who is not satisfied with the brevity of this discussion is referred to [6] for more detailed exposition.

For our purposes it is sufficient to observe that if we set R=$\mathbb{C}$, the field of complex numbers, A=U(Zq(n)) and X=W^s (We now consider W^s as a function from U(Zq(n)) to $\mathbb{C}$), then the matrix M_c belongs to the tensor product of algebras $\mathbb{C}[H^s(1)] \otimes \ldots \otimes \mathbb{C}[H^s(n-1)] \otimes \mathbb{C}[G^s]$ and hence can be written as

$$M_c = \sum_{i_j=0}^{p^{s-1}-1} \sum_{i=0}^{p^{s-1}(p^n-1)-1} S^{i}_{p^{s-1}} \otimes S^{i_2}_{p^{s-1}} \ldots S^{i_{n-1}}_{p^{s-1}} \otimes S^{i}_{p^{s-1}(p^n-1)} \; W^s(h_1^{i_1} h_2^{i_2} \ldots y^{i}). \tag{23}$$

Let us introduce some additional notation. Let $r=p^{(s-1)}$ be the order of the generators h_i. Let $\alpha=p^{(s-1)}(p^n-1)$, the order of the generator y. Further, if h is an element of $H' = \bigoplus H^s(i)$, we define $S_r(h)$ as the tensor product $\bigotimes_{i=1}^{n-1} S_r^{j_i}$, where $h=\prod_{i=1}^{n-1} h_i^{j_i}$. Equation (23) can now be written as

$$M_c = \sum_{h\in H'} \sum_{i=0}^{\alpha-1} S_r(h) \otimes S^i_\alpha \cdot W^s(hy^i). \tag{24}$$

IX. THE CORE - PRIMITIVE ROOTS AND REPETITIONS.

Let us define the mappings W_k: Zq(n)-->C as follows:

$$W_k(g) = \begin{cases} W^s(g), & \text{if } (1+W^s(g))^{s-k} = 1 \\ & \text{and } (1+W^s(g))^{s-k-1} \neq 1. \\ 0, & \text{otherwise.} \end{cases}$$

We observe that $W^s = \sum_{k=0}^{s} W_k$. Further, we define

$$M_k = \sum_{h\in H'} \sum_{i=0}^{\alpha-1} S_r(h) \otimes S^i W_k(y^i h). \tag{25}$$

Then by (24) we have

$$M_c = \sum_{k=0}^{s} M_k \qquad (26)$$

We are going to handle the matrices M_k separately.

Let us further limit our field of attention. We define, for every $h \in H'$,

$$M_k(h) = \sum_{i=0}^{d-1} S^i W^s(hy^i). \qquad (27)$$

Then we obtain:

$$M_k = \sum_{R \in H'} Sr(h) \otimes M_k(h) \qquad (28)$$

As we will see in Section XI, for $k>0$ $M_k(h)$ can be always decomposed as the tensor product $E_{p^{s-k}} \otimes N_k(h)$ for some matrix $N_k(h)$. Before doing this we will outline the remaining steps of the construtions.

We are going to factor the blocks $N_k(h)$ in section XI. In order to do this we are going to need to get some additional information about the structure of the ring Zq(n). The section X will be devoted to this. Later, in section XI, we will extend the factorization to the core itself.

X. $Z_q(N)$ - CONSTANT ELEMENTS.

As the reader recalls, we constructed the ring Zq(n) as a polynomial extension of Zq, using a locally irreducible polynomial f. Thus, we may consider Zq as a subring of Zq(n). We call the elements of this subring constants. The alternative way of defining the constants is the following

Definition. An element $z=\sum_{i=0}^{n-1} z_i u^i \in Zq(n)$ is termed a constant, if $z_i=0$ for all $i>0$. Further, z is termed an almost constant iff $p|z_i$ for all $i>0$.

The multiplicative group of all invertible constants is clearly a subgroup of $U(Zq(n))$. In this section we are going to find out which of the subgroups $H^s(i)$ and G^s may contain invertible constants. As we will see later, this information is crucial for the construction of the core algorithm.

Let us first look at the residue field $Zp(n)=Zp[u]/\langle f'(u)\rangle$. The following lemma can be found in algebra textbooks (cf.[5]):

Lemma 10. If x is a generator of U(F), where F is the finite field with p^n elements, then the invertible constants of the field F are exactly the elements $x^{k\sigma}$, where $\sigma=(p^n-1)/(p-1)$, $k=0,1,.. p-2$.

In the next few lemmas we will extend this result to Zq(n).

Lemma 11. G^s does not contain any almost constants, which are not constants, i.e. for every element $a=\sum_{i=0}^{n-1} a_i u^i \in G^s$ ($p|a_i$ for $i>0$) => ($a_i=0$ for $i>0$).

Proof. Let an almost constant element $\sum_{i=0}^{n-1} a_i u^i$ belong to the subgroup G of order p^n-1. Then

$$(\sum_{i=0}^{n-1} a_i u^i)=(a_0+\sum_{i=1}^{n-1} pa'_i u^i) \qquad (29)$$

The right hand side of (30) is equal to its p^{sn}'th power, since it is an element of G^s and the order of G^s divides $(p^{sn}-1)$.

Thus,
$\sum_{i=0}^{n-1} a_i u^i = (a_0 + p(\sum_{i=1}^{n-1} a'_i u^i))^{p^{ns}}$
We evaluate the expression in the right hand side and observe that all binomial coefficients except that of $a_0^{(p^{ns})}$ are divisible by p^s. Hence,
$(\sum_{i=0}^{n-1} a_i u^i) = a_0^{(p^{ns})}$, which is constant. We equate the coefficients of the different powers of u and see that the elements $a'_j = 0$, $j = 1,2,..p-1$, which concludes the proof.

Remark. We observe that the rings Zq and Zq(n) both contain $\Phi(p^s) = p^{(s-1)}(p-1)$ invertible constants.

Lemma 12. x^k is constant if and only if k is divisible by $\gamma = (p^n-1)/(p-1)$.

Proof. We are going to show that x^γ is a constant in Zq(n). Let $\bar{x}$ be the image of x in Zp(n). Then $\bar{x}$ is a non-zero element of the finite field, and hence $\bar{x}^\gamma$ is a constant in the field. Lifting $\bar{x}^\gamma$ back into Zq(n) we observe that x^γ is an almost constant element. By Lemma 11 we conclude that x^γ is a ring constant. All elements $x^{k\gamma}$ for k varying are also constants. There are exactly p-1 of them. We observe that the subgroup $H^s(0)$ consists exclusively of constants and contains exactly $p^{(s-1)}$ elements. Altogether we accounted for all $(p-1)p^{(s-1)}$ invertible constants.

We summarize the results in the following

Theorem 13. All invertible constants of the ring are elements of the form $x^i h_0^j$, where i is divisible by $\gamma = (p^n-1)/(p-1)$. Furthermore, if $y = xh_0$, then y^γ generates the subgroup of the constants.

XI. $M_K(H)$ - FACTORIZATION.

We are ready now to undertake the factorization of the blocks $M_k(h)$. We will first obtain a few properties of the mappings W_k (Lemmas 14,15,16) and then will obtain the factorization of $M_k(h)$ in Theorem 17. We will continue in use of the notation that $\gamma=(p^n-1)/(p-1)$ and $\alpha=(p^n-1)p^{(s-1)}$

Lemma 14. Let $m\in Z$, $z=y^m$ is a constant. Then

$1+W^s(zy^ih)=(1+W^s(y^ih))^z$.

Proof. $W^s(zh))+1=w^{\varphi(hy^iz)}=w^{z\varphi(hy^i)}=(W^s(y^ih)+1)^z$

Lemma 15. Let $t\in Zq(n)$; $1+W^s(t)$ be a primitive p^{s-k}-th root of 1. Let $z=y^m$ as in Lemma 14. Then $1+W_k(zt)$ runs over all primitive p^{s-k}-th roots of unity as m runs over $0,1,\ldots p^{s-k-1}(p-1)-1$

Proof follows from the previous lemma.

Let $\alpha_\kappa=(p^n-1)p^{s-k-1}$ for $k=0,1,\ldots s-1$. We observe that α_κ always divides α and $\alpha=\alpha_0$.

Lemma 16.

$$W_k(hy^i)=W_k(hy^{i+\alpha_\kappa}) \qquad (30)$$

Proof. We have to consider two cases. First, we assume that both $1+W_k(hy^i)$ and $1+W_k(hy^iy^{\alpha_\kappa})$ are not p^{s-k}-th primitive roots of 1. Then both $W_k(hy^i)$ and $W_k(hy^iy^{\alpha_\kappa})$ are zero and the proof follows. We now assume that $1+W_k(hy^i)$ is a primitive p^{s-k}-root of 1. Then $W_k(hy^i)=0$ and $\varphi(hy^i)=p^kt$ for some integer t, not divisible by p. We want to show that $\varphi(hy^i-hy^iy^{\alpha_\kappa})=0$. Here $y^{\alpha_\kappa}=x^{\alpha_\kappa}h_0^{\alpha_\kappa}=h_0^{\alpha_\kappa}$. Let $hy^i=p^kt+\sum_{j=1}^{s-1}a_ju^j$.

Then $\varphi(hy^i y^{\alpha_\kappa}) = \varphi(p^k t h_0^{\alpha_\kappa} + h_0^{\alpha_\kappa} \sum_{j=1}^{n-1} a_j y^j)$. We observe that $p^k h_0^{\alpha_\kappa} = p^k h^{p^{s-k-1}(p^n-1)} = p^k$ and hence $\varphi(hy^i y^{\alpha_\kappa}) = \varphi(hy^i)$, which concludes the proof in this case. The last possibility is that $1+W_k(hy^i y^{\alpha_\kappa})$ is a p^{s-k}-th primitive root. The proof is analagous to the previous case.

We now combine the results of 13,14 and 15 into the following key Theorem:

Theorem 17. The matrix $M_k(h)$ can be factored as a tensor product of a α_κ by α_κ matrix $N_k(h)$ by E_{p^κ}, where $N_k(h) = \sum_{i=0}^{\alpha_\kappa - 1} S^i_\alpha W_k(hy^i)$.

Proof.

Using Lemma 16, we can rewrite the definition of $M_k(h)$ as follows:

$$M_k(h) = \sum_{i=0}^{\alpha-1} W_k(hy^i) \cdot S^i_\alpha = \tag{31}$$

$$\sum_{j=0}^{p^\kappa-1} \sum_{i=0}^{\alpha_\kappa-1} W_k(hy^i) S^{i+j\alpha_\kappa}_\alpha = \sum_{j=0}^{p^\kappa-1} \sum_{i=0}^{\alpha_\kappa-1} W_k(hy^i) S^i_{\alpha_\kappa} \otimes S^j_{p^\kappa} =$$

$$\sum_{i=0}^{\alpha_\kappa-1} S^i_{\alpha_\kappa} W_k(hy^i) \otimes \sum_{j=0}^{p^\kappa-1} S^j_{p^\kappa} =$$

$$\sum_{i=0}^{\alpha_\kappa-1} S^i_{\alpha_\kappa} \cdot W_k(hy^i) \otimes E_{p^\kappa} .$$

Let $N_k(h) = \sum_{i=0}^{\alpha_\kappa-1} S^i_{\alpha_\kappa} W_k(hy^i)$. Thus we obtain:

$$M_k(h) = N_k(h) \otimes E_{p^\kappa} , \tag{32}$$

which concludes the proof.

Remark. The previous Theorem is trivial for the case k=0. For k>0, however, it allows us to greatly reduce the amount of calculation performed. We recall the fact that the number of multiplications necessary to perform the

multiplication of a square NxN matrix A by an arbitrary vector V of length N is same as in multiplication of an NQ by NQ matrix $A \bullet E_Q$ by an arbitrary vector of length NQ. We will see now that the matrix $N_k(h)$ can be further decomposed.

$N_K(H)$ - FURTHER DECOMPOSITION.

We are now going to present $N_k(h)$ as a product of two matrices. Each of them will have a rather specific form (see Theorem 19). The decomposition we are about to obtain will allow us to substantially reduce the amount of performed calculations.

We recall that

$$N_k(h)=\sum_{i=0}^{\alpha_k-1} W_k(hy^i)S^i_{\alpha_k}, \text{ where } \alpha_k=(p^n-1)p^{s-k-1} \qquad (33)$$

Let $\beta_k=(p-1)p^{s-k-1} = \Phi(p^{s-k})$. For $L=0,1,\dots \beta_k-1$ we define the sets $B_L=\{j=0,1,..\ \alpha_k-1 \mid W_k(hy^j)=W^s(p^k y^{L\delta'})\}$. We also define $B=\{j=0,1,\dots\alpha_k-1 \mid W_k(hy^j)=0\}$. Then

$$B\cup\bigcup_{L=0}^{\beta_k-1} B_L=\{0,1,\dots \alpha_k-1\}. \qquad (34)$$

We next define the matrices $Q_L(h)=\sum_{j\in B_L} S^j_{\alpha_k}$, $Q(h)=\sum_{j\in B} S^j_{\alpha_k}$. Then we obtain the following

Lemma 18. $Q_L(h)=S^{L\delta'}_{\alpha_k}Q_0(h)$.

The proof follows from Lemma 16.

We now decompose the blocks $N_k(h)$. The following theorem is of the key importance for the algorithm.

Theorem 19.

1) The $\alpha_k \times \alpha_k$ matrix $N_k(h)$ can be presented as $Q_0(h)C''_k$, where $Q_0(h)$ contains only zeros and ones and C''_k is the matrix $\sum_{L=0}^{p_k-1} W_k(p^k y^{\delta L}) S_{\alpha_k}^{\delta L}$.

2) Further, $C''_k = I \otimes C_{p^{s-k}}$, where $C_{p^{s-k}}$ is the core matrix of $DFT(p^{s-k}:1)$.

Proof of the assertion 1).

$$N_k(h) = \sum_{L=0}^{p_k-1} W_k(p^k y^{L\delta'}) Q_L(h) + 0 \times Q(h) = \qquad (35)$$

$$\sum_{L=0}^{p_k-1} W_k(p^k y^{L\delta'}) S_{\alpha_k}^{L\delta'} Q_0(h) = Q_0(h) \cdot \sum_{L=0}^{p_k-1} W_k(p^k y^{L\delta'}) S_{\alpha_k}^{L\delta'} = Q_0(h) C''_k.$$

The matrix C''_k in the last equation does not depend on h. We delay the proof of the assertion 2) in order to bring in a few remarks.

Remark. C''_k and $Q_0(h)$ both belong to the same commutative group algebra and hence commute.

The matrices $Q_0(h)$ contain only zeros and ones (cf. with the example below), and hence do not affect the multiplicative complexity. At the same time, most of the entries of the matrix C''_k turn out to be zeros.

Example [3]. The 8x8 block on the DIAGRAM IV, which corresponds to the core step of DFT(3:2) can be factored as product $Q \times C''_k$, where Q is

$$\begin{Vmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{Vmatrix}$$

And S" is

$$\begin{Vmatrix} w^1-1 & 0 & 0 & 0 & w^2-1 & 0 & 0 & 0 \\ 0 & w^1-1 & 0 & 0 & 0 & w^2-1 & 0 & 0 \\ 0 & 0 & w^1-1 & 0 & 0 & 0 & w^2-1 & 0 \\ 0 & 0 & 0 & w^1-1 & 0 & 0 & 0 & w^2-1 \\ w^2-1 & 0 & 0 & 0 & w^1-1 & 0 & 0 & 0 \\ 0 & w^2-1 & 0 & 0 & 0 & w^1-1 & 0 & 0 \\ 0 & 0 & w^2-1 & 0 & 0 & 0 & w^1-1 & 0 \\ 0 & 0 & 0 & w^2-1 & 0 & 0 & 0 & w^1-1 \end{Vmatrix}$$

where $w=e^{2\pi i/3}$.

In this example we are given only one matrix $N_k(h)$, so we are not able to demostrate very much. The example of DFT(9·2) which contains different blocks and different factorizations, can be found in Chapter I.

We observe that the matrix $C_0''=I_4 \otimes C_3$, where C_3 is the the core matrix of DFT(3:1).

Proof of the assertion 2).

The matrix C_k'' is given by the following equation:

$$C_k''=\sum_{L=0}^{\beta_k-1} W_k(p^k y^{L\delta'}) S_{\alpha_k}^{L\delta} \qquad (36)$$

Here $y^{\delta'}$ is a generator of a multiplicative group of the ring Zq, which we will denote by $\bar{y}$. At the same time,

$$S_{\alpha_k}^{L\delta}=S_{\beta_k}^{L\delta'} \otimes I_{\gamma'} , \qquad (37)$$

Hence

$$C_k''=\sum_{L=0}^{\beta_k-1} W_k(\bar{y}^L) S_{\alpha_k}^{L\delta}=\left(\sum_{L=0}^{\beta_k-1} W_k(\bar{y}^L) S_{\beta_k}^{L}\right) \otimes I_{\delta'} = \qquad (38)$$

$$C_{p^{s-k}} \otimes I_{\delta'}$$

where

$$C_{p^{s-k}} = \sum_{L=0}^{\beta_k - 1} W_k(\bar{y}^L) S^L_{\beta_k} \quad , \text{ and } \beta_k = (p-1)p^{s-k-1} \qquad (39)$$

We compare the equations (39) and (24) and observe that the matrix $C_{p^{s-k}}$ corresponds to the core step of DFT(p^{s-k}:1). Thus for the second time in this algorithm we have found that the subroutines for the DFT on lower number of points come up as steps of the algorithm with higher number of points.

We conclude this part of discussion, bringing together the decomposition of $M_k(h)$:

$$M_k(h) = (Q_0(h)\ (C_{p^{s-k}} \otimes I_{\delta'}\ )) \otimes E_{p^k} \qquad (40)$$

XII. THE CORE - BRINGING PIECES TOGETHER.

The decomposition of M_k is given by equations (25) and (40) and we are going to bring them together. In order to do this we observe that the only term in the right hand side of (40) which depends on h is $Q_0(h)$.

Theorem 20. (The factorization of the core).

$M = \sum_{k=0}^{s-1} Q_k \bar{C}_k \otimes E_p$, where Q_k contains only zeros and ones and $\bar{C}_k \tilde{=} I_{\delta p^{(s-k)(n-1)}} \otimes C_{p^{s-k}}$.

Proof.

$$M_k = \sum_{h \in H'} S_{p^{s-k}}(h) \otimes (Q_0(h) \cdot (C_{p^{s-k}} \otimes I_\gamma)) \otimes E_{p^\kappa} = \qquad (41)$$

$$\left(\sum_{h \in H'} S_{p^{s-k}}(h) \otimes (Q_0(h) \cdot (C_{p^{s-k}} \otimes I_\gamma))\right) \otimes E_{p^\kappa} =$$

$$\left(\sum_{h \in H'} S_{p^{s-k}}(h) \otimes Q_0(h)\right) (I_{p^{(s-k)(n-1)}} \otimes C_{p^{s-k}} \otimes I_\gamma) \otimes E_{p^\kappa} =$$

$$Q_k \cdot \overline{C}_k \otimes E_p \quad , \text{ where}$$

$$Q_k = \sum_{h \in H'} S_{p^{s-k}}(h) \otimes Q_0(h),$$

$$\overline{C}_k = I_{p^{(s-k)(n-1)}} \otimes C_{p^{s-k}} \otimes I_\gamma =$$

$$P_k (I_{p^{(s-k)(n-1)}\gamma} \otimes C_{p^{s-k}}) P_k^{-1} = I_{\gamma p^{(s-k)(n-1)}} \otimes C_{p^{s-k}}.$$

Here the matrix Q_k contains only zeroes and ones, while the matrix $(I_{p^{(s-k)(n-1)}\gamma}) \otimes C_{p^{s-k}}$ has the block-diagonal shape and consists of $p^{(s-k)(n-1)}\gamma$ identical square blocks. Each of the blocks is a copy of the core matrix of $DFT(p^{s-k}:1)$.

This concludes the proof of Theorem 20.

CONCLUSION

We now bring together the pieces of the Algorithm.

It will proceed as follows:

1) We calculate $\hat{A}(0) = \sum_{a \in Z_q^{(n)}} A(a)$, as defined in (13) and (14).

2) Let $A_k = \{A(t) \mid t \in D^k\}$.

Let $M_C^s = Q_k \overline{C}_k \otimes E_{p^\kappa}$ as given in Theorem 20.

Let $M^{s}_{0,0} = I \cdot M^{s}_{c}$, where I is the permutation matrix of the inversion mapping I:U(Zq(n))-->U(Zq(n)) (see (21),(22)), let further

$M^{s}_{L,K} = \overline{M}^{s}_{L,K} \otimes E_{p^L, p^K} = M^{s-k-l}_{0,0} \otimes E_{p^L, p^K}$, as given in (18) and Lemma 8.

We calculate $B_{L,K} = M^{s}_{L,K} \cdot A_k$ for all K and L.

Remark. As we have shown in Lemma 7, for $K+L \geq s$ no calculations should be performed since then $M_{L,K}$ is a zero matrix.

3) We calculate the output of DFT(p^s:n):

$\hat{A}(b) = \hat{A}(0) + \sum_{K=0}^{S} B_{L,K}(T^{-1}(b))$, as given by (13) and (14).

XIII. SUMMARY.

1). In Section I we introduced the conception of a locally irreducible polynomial over a local ring. We further used this idea to define ring Zq(n), $q=p^s$, which combined the properties of a finite field with those of the ring of integers modulo p^k. We have shown in Section II that Zq(n) can be conveniently used to index DFT(p^s:n) and established the necessary notation.

2). We analyzed the algebraic structure of Zq(n) in Sections III and IV. Theorem 3 (Section III) describes the structure of the unit group of Zq(n) and Theorem 4 (Section IV) describes the structure of the set of zero

divisors of Zq(n) and the (multiplicative) action of of the unit group on it.

3). We linked the structures of Zq(n) as a ring and as a module (over Zq) in Section V. Thus we justified the reasons for bringing up the ring structure on the first place.

4). We factored the DFT(p^s:n) equations as collection of Steps, corresponding to different ideals of Zq(n) in Section VI. It was further shown that some of the steps will involve no calculations in the algorithm (cf.Lemma 7, Section VII), whereas the others can be reduced to the Core step equations of DFT(p^r:n), for some r<s (cf. Theorem 9, Section VII). By Core step we meant the step, corresponding to the unit group of Zq(n). Thus we have shown that the problem of evaluating DFT(p^s:n) can be reduced to the problems of multiplying of a vector by the core matrix of DFT(p^r;n) for r=1,...s. This problem was discussed in Sections VIII-XII.

5). We have observed in Section VIII that the core matrix M_c can be viewed as an element of a representation of a certain group algebra. This allowed us to further subdivide the problem into smaller ones (see Section IX). On the matrix language, we subdivided M_c into a collection of smaller blocks, corresponding to the different cosets of the unit group.

6). We analyzed the structure of a single block in Section XI. Some additional information about the ring Zq(n) was obtained in Section X: We found out how the

elements of the base ring Zq are distributed in Zq(n) (see Theorem 13). Using this information, we factored a single block in Section XI (Theorems 17 and 19).

7). Finally, we extended these factorizations to the core itself (Section XII, Theorem 20). Theorem 20 gives us the scheme for the algorithm; it also shows that all multiplications in $DFT(p^s;n)$ can be performed as part of the core steps of one-dimensional transforms $DFT(p^s:1)$. Efficient subroutines which handle these tasks had been written for 1-dimensional Winograd's algorithm and thus can be used for our algorithm.

8). The whole algorithm can be considered as a step in calculation of general multi-dimensional Discrete Transform, with number of points along each axis not necessary prime and number of points along different axes varying. One can obtain an algorithm for this kind of problem, incorporating the algorithms similar to one we described using different techniques.

APPENDIX: THE BLOCK-SCHEME OF THE ALGORITHM

We conclude this Chapter with a brief step-by-step scheme of the Algorithm. This block-scheme should not be considered as a computer program. Exact implementation of it will imply tremendous waste of storage and multiple unnecessary assignments, since the numerous intermediate arrays we introduce below are included mostly for the reader's convenience and not for the efficient use of storage.

The reader will observe that we will use elements of Zq(n) instead of subscripts. Thus,

$A(a_0,a_1,\dots a_{n-1}) = A(a)$, for $a=\sum_{i=0}^{n-1} a_i u^i \in Zq(n)$.

Further, we will consider some multi-dimensional arrays as one-dimensional. This equivalence will be done in PLI manner, rather than in FORTRAN's. Thus, the elements of some 2-dimensional 2x2 array M may be considered as a one-dimensional array {M(1,1),M(2,1),M(1,2),M(2,2)} of length 4.

Remark. Certain information about the indexation ring will be necessary to proceed with construction. Thus, we will assume that we performed the following computations:

1). We have found a locally irreducible polynomial $f \in Zq$, $deg(f)=n$.

2). We are able to reconstruct the subsets D^k of Zq(n), as defined in Section III.

3). We have found a generator x of subgroup G of U(Zq(n)).

4). We can order and list the elements of D^k as cosets under

the action of cyclic subgroups of G^s (see Theorem 4).
In other words, we are able to present any element of Zq(n) in the form given in Corollary of Theorem 4.
5). We are able to compute the values of permutations T (see Section V) and I (see Section VII).

INPUT: n-dimensional array A with p^s points along each axis.

OUTPUT: n-dimensional array A with p^s points along each axis.

=> STEP 1. Define constant Z as the sum of all entries of A, i.e. $Z=\sum_{a\in Z_q(n)} A(a)$.

=> STEP 2. For all k=0,1,.. s-1 define n-dimensional arrays Ak with $(p^n-1)p^{s-k-1}$ points along the first axis and p^{s-k-1} along any of the other axes. Store elements of A in Ak as follows:
for all $a\in D^k$, let $Ak(\bar{k},k_1,\ldots k_{n-1}) = A(p^k y^{\bar{k}} h_1^{k_1},\ldots h_{n-1}^{k_{n-1}}) = A(a)$. Thus for every k, Ak will contain exactly elements of D^k.

=> STEP 3. For all k,L=0,1,.. s-1 define n-dimensional arrays $B_{L,K}$. Let $B_{L,K}$ be an array of the same size as A_L ($B_{L,K}$ will contain the output from (L,K)-th step of the algorithm, see Sections VI and VII).

=> STEP 4. Perform STEPS 5-8 for all k=0,1,..s-1
l=0,1,..s-1: than proceed to STEP 9.

=> STEP 5. Define n-dimensional array $\bar{A}_{L,k}$ with $(p^n-1)p^{(s-k-L-1)}$ points along first axis and $p^{(s-k-L-1)}$ points along

other axes. Calculate and store sums as follows:

$\bar{A}_{L,K}(k,k_1,\ldots k_{n-1}) = \sum A_k(j,j_1,\ldots j_{n-1})$, where summation is taken over all n-tuples $(j,j_1,\ldots j_{n-1})$ such that for every $i=1,\ldots n-1$ $j_i \equiv k_i \pmod{p^{s-k-L-1}}$ and $\bar{j} \equiv \bar{k} \pmod{(p^n-1)p^{s-k-L-1}}$.

REMARK. Arrays $\bar{A}_{L,K}$ will be used as the input for the core step of $DFT(p^{s-k-L}:n)$. The output will be stored into arrays $\bar{B}_{L,K}$, which we will define next.

=> STEP 6. Define array $\bar{B}_{L,K}$ as a n-dimensional array of the same size as $\bar{A}_{L,K}$

=> STEP 7. Call SUBROUTINE $C(\bar{A}_{L,K},\bar{B}_{L,K},p,s-K-L,n)$ (This subroutine, described below, will compute the core step of the $DFT(p^{s-k-L}:n)$).

=> STEP 8. Store output $\bar{B}_{L,K}$ in array $B_{L,K}$ as follows:

Let $B_{L,K}(\bar{L},L_1,\ldots L_{n-1}) = \bar{B}_{L,K}(\bar{j},j_1,\ldots j_{n-1})$, where for every $i=1,\ldots n-1$ $L_i \equiv j_i \pmod{p^{s-k-L-1}}$ and $\bar{L} \equiv \bar{j} \pmod{(p^n-1)p^{s-k-L-1}}$.

REMARK. $B_{L,K}$ is the output from the (L,K)-th step of the algorithm, cf.(16).

=> STEP 9. Perform additions as follows: for every $L=0,1,\ldots s-1$ and $b \in D^L$, let

$\hat{A}(b) = Z + \sum_{K=0}^{s-1} B_{L,K}(\bar{L},L_1,\ldots L_{n-1})$, where $b = p^L y \bar{L} h_1^{L_1} \ldots h_{n-1}^{L_{n-1}}$.

=> STEP 10. Permute the output array A as follows: For every $a \in Zq(n)$, let

$A(a) = A(T^{-1}(a))$, where T is as defined in Section 5.

SUBROUTINE C(A,B,p,s,n).

This subroutine computes the core step of DFT(p^s:n).

INPUT: n-dimensional array A with $p^{(s-1)}(p^n-1)$ points along first axis and $p^{(s-1)}$ points along all others.

OUTPUT: n-dimensional array B of the same size.

=> STEP C1. Define arrays Ak for k=0,.. s-1 as exact copies of A.

=> STEP C2. Perform STEPS C3-C11 for all k=0,.. s-1. Then proceed to STEP C12.

=> STEP C3. Multiply array Ak by matrix Qk. Here Ak is considered as 1-dimensional array (see REMARK at the beginning of this Appendix). Matrix Q_k is defined in Section XII and contains only zeros and ones. Thus, this step will involve only additions.

We store the output back into Ak.

=> STEP C4. Apply permutation Pk to Ak (see proof of Theorem 20 for definition of Pk).

REMARK. As given in Theorem 20, we will have to multiply Ak by block-diagonal matrix C_k. This will be done in a loop.

=> STEP C5. Define arrays X,Y,Z. Let X be a one-dimensional array of length $p^{(s-1)}(p-1)$. Let Y and Z be one-dimensional arrays of length $(p-1)p^{s-k-1}$. Let $M=(p^n-1)p^{(s-1)(n-k)}/(p-1)$. Perform STEPS C6-C10 for all m=0,1,..M-1.

=> STEP C6. For all $i=1,..p^{(s-1)}(p-1)$ let

$X(i)=Ak(i+mp^{(s-1)}(p-1))$,

=> STEP C7. For all $i=1,..(p-1)p^{s-k-1}$ let

$Y(i)=\sum X(j)$, where summation is taken over all $j\equiv i$ (mod

$(p-1)p^{s-k-1}$).

=> STEP C8. Call SUBROUTINE W(Y,Z,p,s-k). (This subroutine computes the core step of one-dimensional DFT(p^{s-k},1)). Here Y is the input and Z is the output of the subroutine.

=> STEP C9. For all $i=1,..(p-1)p^{s-k}$ let

$X(i)=Z(j)$, where $i \equiv j \pmod{(p-1)p^{s-k-1}}$.

=> STEP C10. For all $i=1,...(p-1)p^{s-k}$ let

$Ak(i+m(p-1)p^{n(s-1)})=X(i)$.

=> STEP C11. Apply permutation Pk^{-1} to the array Ak.

=> STEP C12. Compute array B as follows: For every $i=1,2,..(p^n-1)p^{n(s-1)}$ let $B(i)=\sum_{K=0}^{s} Ak(i)$.

REMARK. On the last STEP of this subroutine we will view B as n-dimensional array indexed by elements of the unit group of Zq(n). Thus, let $B(a)=B(k,k_1,k_2,..\ k_{n-1})$ for $a=y^k h_1^{k_1}..h_{n-1}^{k_{n-1}}$

=> STEP C13. Apply the inverse permutation to array B (cf.(21)).

Let $B(a)=B(a^{-1})$ for all a.

REMARK. As the reader sees, we did not perform any multiplications in this subroutine. All multiplications are performed in Winograd's core subroutine W.

SUBROUTINE W(A,B,p,s).

This subroutine computes the core step of 1-dimensional DFT(p^s:1) as described in Winograd's works. (cf.[2]). Numerious papers describing efficient implementations of this subroutine have been published. See, for example, [4]).

CHAPTER III.

0. INTRODUCTION

We will now present one more algorithm for DFT(p^2:n), which uses the same ring structure for the indexation purposes. This other algorithm will be given first as an example (DFT(9:2)) and will be justified in the next Chapter. The notation which we are going to use will be compatible with Chapters I and II.

The reader will observe that the algorithm we are about to present will combine some features of Winograd type algorithm (cf.[2]) with construction, similar to the one appearing in the Cooley-Tukey algorithm (cf. [1]).

I. ANOTHER ALGORITHM FOR DFT(9:2).

The input data for the Finite Fourier Transform on 9 by 9

points is given as a 9 by 9 array A(K,L), where K,L=0,1,..8. Let us rearrange the data into the one-dimensional array B of length 81 as shown in the following table:

TABLE I.

B(0) = A(0,0)	B(27) = A(0,2)	B(54) = A(1,7)
B(1) = A(3,0)	B(28) = A(5,4)	B(55) = A(6,7)
B(2) = A(6,6)	B(29) = A(2,0)	B(56) = A(7,8)
B(3) = A(0,6)	B(30) = A(4,4)	B(57) = A(1,6)
B(4) = A(6,3)	B(31) = A(0,7)	B(58) = A(8,5)
B(5) = A(6,0)	B(32) = A(4,5)	B(59) = A(6,8)
B(6) = A(3,3)	B(33) = A(1,3)	B(60) = A(5,1)
B(7) = A(0,3)	B(34) = A(5,8)	B(61) = A(8,3)
B(8) = A(3,6)	B(35) = A(3,8)	B(62) = A(1,4)
B(9) = A(1,0)	B(36) = A(8,4)	B(63) = A(3,1)
B(10) = A(2,2)	B(37) = A(8,6)	B(64) = A(4,8)
B(11) = A(0,8)	B(38) = A(4,1)	B(65) = A(4,6)
B(12) = A(2,7)	B(39) = A(6,1)	B(66) = A(5,2)
B(13) = A(8,0)	B(40) = A(1,5)	B(67) = A(6,5)
B(14) = A(7,7)	B(41) = A(4,3)	B(68) = A(2,4)
B(15) = A(0,1)	B(42) = A(2,5)	B(69) = A(5,3)
B(16) = A(7,2)	B(43) = A(3,5)	B(70) = A(4,7)
B(17) = A(4,0)	B(44) = A(5,7)	B(71) = A(3,4)
B(18) = A(8,8)	B(45) = A(5,6)	B(72) = A(7,5)
B(19) = A(0,5)	B(46) = A(7,4)	B(73) = A(7,6)
B(20) = A(8,1)	B(47) = A(6,4)	B(74) = A(2,8)
B(21) = A(5,0)	B(48) = A(4,2)	B(75) = A(6,2)
B(22) = A(1,1)	B(49) = A(7,3)	B(76) = A(8,7)
B(23) = A(0,4)	B(50) = A(8,2)	B(77) = A(2,3)
B(24) = A(1,8)	B(51) = A(3,2)	B(78) = A(7,1)
B(25) = A(7,0)	B(52) = A(2,1)	B(79) = A(3,7)
B(26) = A(5,5)	B(53) = A(2,6)	B(80) = A(1,2)

Analogously we define a one-dimensional array $\hat{B}$ of length 81 which will correspond to the two-dimensional output $\hat{A}(K,L)$, where K,L=0,1,. 8, as follows:

TABLE II.

$\hat{B}(0) = \hat{A}(0,0)$	$\hat{B}(27) = \hat{A}(0,5)$	$\hat{B}(54) = \hat{A}(2,5)$
$\hat{B}(1) = \hat{A}(3,0)$	$\hat{B}(28) = \hat{A}(1,8)$	$\hat{B}(55) = \hat{A}(6,4)$
$\hat{B}(2) = \hat{A}(3,3)$	$\hat{B}(29) = \hat{A}(5,0)$	$\hat{B}(56) = \hat{A}(5,7)$
$\hat{B}(3) = \hat{A}(0,6)$	$\hat{B}(30) = \hat{A}(8,8)$	$\hat{B}(57) = \hat{A}(1,6)$
$\hat{B}(4) = \hat{A}(3,6)$	$\hat{B}(31) = \hat{A}(0,4)$	$\hat{B}(58) = \hat{A}(1,4)$
$\hat{B}(5) = \hat{A}(6,0)$	$\hat{B}(32) = \hat{A}(8,1)$	$\hat{B}(59) = \hat{A}(6,8)$
$\hat{B}(6) = \hat{A}(6,6)$	$\hat{B}(33) = \hat{A}(1,3)$	$\hat{B}(60) = \hat{A}(4,8)$
$\hat{B}(7) = \hat{A}(0,3)$	$\hat{B}(34) = \hat{A}(4,1)$	$\hat{B}(61) = \hat{A}(8,3)$
$\hat{B}(8) = \hat{A}(6,3)$	$\hat{B}(35) = \hat{A}(3,8)$	$\hat{B}(62) = \hat{A}(8,5)$
$\hat{B}(9) = \hat{A}(1,0)$	$\hat{B}(36) = \hat{A}(1,5)$	$\hat{B}(63) = \hat{A}(3,1)$
$\hat{B}(10) = \hat{A}(7,7)$	$\hat{B}(37) = \hat{A}(8,6)$	$\hat{B}(64) = \hat{A}(5,1)$
$\hat{B}(11) = \hat{A}(0,8)$	$\hat{B}(38) = \hat{A}(5,8)$	$\hat{B}(65) = \hat{A}(7,6)$
$\hat{B}(12) = \hat{A}(7,2)$	$\hat{B}(39) = \hat{A}(6,1)$	$\hat{B}(66) = \hat{A}(7,1)$
$\hat{B}(13) = \hat{A}(8,0)$	$\hat{B}(40) = \hat{A}(8,4)$	$\hat{B}(67) = \hat{A}(6,2)$
$\hat{B}(14) = \hat{A}(2,2)$	$\hat{B}(41) = \hat{A}(7,3)$	$\hat{B}(68) = \hat{A}(1,2)$
$\hat{B}(15) = \hat{A}(0,1)$	$\hat{B}(42) = \hat{A}(1,7)$	$\hat{B}(69) = \hat{A}(2,3)$
$\hat{B}(16) = \hat{A}(2,7)$	$\hat{B}(43) = \hat{A}(3,2)$	$\hat{B}(70) = \hat{A}(2,8)$
$\hat{B}(17) = \hat{A}(7,0)$	$\hat{B}(44) = \hat{A}(7,8)$	$\hat{B}(71) = \hat{A}(3,7)$
$\hat{B}(18) = \hat{A}(4,4)$	$\hat{B}(45) = \hat{A}(2,6)$	$\hat{B}(72) = \hat{A}(8,7)$
$\hat{B}(19) = \hat{A}(0,2)$	$\hat{B}(46) = \hat{A}(8,2)$	$\hat{B}(73) = \hat{A}(4,6)$
$\hat{B}(20) = \hat{A}(4,5)$	$\hat{B}(47) = \hat{A}(6,7)$	$\hat{B}(74) = \hat{A}(4,7)$
$\hat{B}(21) = \hat{A}(2,0)$	$\hat{B}(48) = \hat{A}(2,1)$	$\hat{B}(75) = \hat{A}(6,5)$
$\hat{B}(22) = \hat{A}(5,5)$	$\hat{B}(49) = \hat{A}(4,3)$	$\hat{B}(76) = \hat{A}(7,5)$
$\hat{B}(23) = \hat{A}(0,7)$	$\hat{B}(50) = \hat{A}(7,4)$	$\hat{B}(77) = \hat{A}(5,3)$
$\hat{B}(24) = \hat{A}(5,4)$	$\hat{B}(51) = \hat{A}(3,5)$	$\hat{B}(78) = \hat{A}(5,2)$
$\hat{B}(25) = \hat{A}(4,0)$	$\hat{B}(52) = \hat{A}(4,2)$	$\hat{B}(79) = \hat{A}(3,4)$
$\hat{B}(26) = \hat{A}(1,1)$	$\hat{B}(53) = \hat{A}(5,6)$	$\hat{B}(80) = \hat{A}(2,4)$

The permutations presented in the Tables I and II are once again connected with the underlying ring structure and will be justified in the next Chapter.

The finite Fourier transform on 9x9 points is given by the following equations:

$$\hat{A}(\hat{K},\hat{L}) = \sum_{K=0}^{8}\sum_{L=0}^{8} w^{K\hat{K}} w^{L\hat{L}} A(K,L), \qquad (1)$$

where $\hat{K}$ and $\hat{L}$ range from 0 to 8 and $w = e^{2\pi i/9}$.

We will write the Finite Fourier transform operator in the matrix form as follows:

$$\hat{B} = F \times B, \qquad (2)$$

where F is an 81 by 81 matrix.

After writing out all the details one sees that the matrix F has the following block structure:

1	1	1	1	1	1	1	1	1	1	1
1	1	N	N	N	N	N	N	N	N	N
1	N	C11	C12	C13	C21	C22	C23	C31	C32	C33
1	N	C13	C11	C12	C23	C21	C22	C33	C31	C32
1	N	C12	C13	C11	C22	C23	C21	C32	C33	C31
1	N	C31	C32	C33	C11	C12	C13	C21	C22	C23
1	N	C33	C31	C32	C13	C11	C12	C23	C21	C22
1	N	C32	C33	C31	C12	C13	C11	C22	C23	C21
1	N	C21	C22	C23	C31	C32	C33	C11	C12	C13
1	N	C23	C21	C22	C33	C31	C32	C13	C11	C12
1	N	C22	C23	C21	C32	C33	C31	C12	C13	C11

Here the blocks Cij and N are 8 by 8 matrices, all blocks denoted by '1' contain only entries equal to 1.

Let C be the 72x72 matrix containing the blocks C11,

C12,.. C33. Then C=cyc(C1,C2,C3), where C1=cyc(C11,C12,C13), C2=cyc(C21,C22,C23), C3=cyc(C31,C32,C33). We will say that C is the core of the two-dimensional FFT on 9x9 points. Let $w = e^{2\pi i/9}$. Then the described blocks are:

$$N = cyc\,(w^3, w^6, 1, w^6, w^6, w^3, 1, w^3)$$

$$C11 = cyc\,(w^1, w^2, 1, w^2, w^8, w^7, 1, w^7)$$

$$C12 = cyc\,(w^4, w^8, 1, w^8, w^5, w^1, 1, w^1)$$

$$C13 = cyc\,(w^7, w^5, 1, w^5, w^2, w^4, 1, w^4)$$

$$C21 = cyc\,(w^1, w^5, w^3, w^8, w^8, w^4, w^6, w^1)$$

$$C22 = cyc\,(w^4, w^2, w^3, w^5, w^5, w^7, w^6, w^4)$$

$$C23 = cyc\,(w^7, w^8, w^3, w^2, w^2, w^1, w^6, w^7)$$

$$C31 = cyc\,(w^1, w^8, w^6, w^5, w^8, w^1, w^3, w^4)$$

$$C32 = cyc\,(w^4, w^5, w^6, w^2, w^5, w^4, w^3, w^7)$$

$$C33 = cyc\,(w^7, w^2, w^6, w^8, w^2, w^7, w^3, w^1)$$

We will now introduce a few more 8x8 matrices. We define:

$$D11 = C11 + C12 + C13 = 3 \cdot cyc(0, 0, 1, 0, 0, 0, 1, 0)$$

$$D12 = C11 + w^3 C12 + w^6 C13 = 3 \cdot cyc(0, w^2, 0, w^2, w^8, 0, 0, 0)$$

$$D13 = C11 + w^6 C12 + w^3 C13 = 3 \cdot cyc(w^1, 0, 0, 0, 0, w^7, 0, w^7)$$

$$D21 = C21 + C22 + C23 = 3 \cdot cyc(0, 0, w^3, 0, 0, 0, w^6, 0)$$

$$D22 = C21 + w^3 C22 + w^6 C23 = 3 \cdot cyc(0, w^5, 0, w^8, w^8, 0, 0, 0)$$

$$D23 = C21 + w^6 C22 + w^3 C23 = 3 \cdot cyc(w^1, 0, 0, 0, 0, w^4, 0, w^1)$$

$$D31 = C31 + C32 + C33 = 3 \cdot cyc(0, 0, w^6, 0, 0, 0, w^3, 0)$$

$$D32 = C31 + w^3 C32 + w^6 C33 = 3 \cdot cyc(0, w^8, 0, w^5, w^8, 0, 0, 0)$$

$$D33 = C31 + w^6 C32 + w^3 C33 = 3 \cdot cyc(w^1, 0, 0, 0, 0, w^1, 0, w^4)$$

Then if we define

$$D = (I_8 \bullet F_3 \bullet I_3) C (I_8 \bullet F_3^{-1} \bullet I_3), \qquad (3)$$

D = cyc(D1, D2, D3), where

$$Di = diag(Di1, Di2, Di3),\ i=1,2,3$$

We repeat this procedure once more. Let

$$E11 = D11 + D21 + D31 = 9\,cyc(0,0,0,0,0,0,0,0)$$

$$E21 = D11 + w^3 D21 + w^6 D31 = 9\,cyc(0,0,1,0,0,0,0,0)$$

$$E31 = D11 + w^6 D21 + w^3 D31 = 9\,cyc(0,0,0,0,0,0,1,0)$$

$$E12 = D12 + D22 + D32 = 9\,cyc(0,0,0,0,w^8,0,0,0)$$

$$E22 = D12 + w^3 D22 + w^6 D32 = 9\,cyc(0,0,0,w^2,0,0,0,0)$$

$$E32 = D12 + w^6 D22 + w^3 D32 = 9\,cyc(0,w^2,0,0,0,0,0,0)$$

$$E13 = D13 + D23 + D33 = 9\,cyc(w^1,0,0,0,0,0,0,0)$$

$$E23 = D13 + w^3 D23 + w^6 D33 = 9\,cyc(0,0,0,0,0,w^7,0,0)$$

$$E33 = D13 + w^6 D23 + w^3 D33 = 9\,cyc(0,0,0,0,0,0,0,w^7)$$

Then, if we define

$$E=(I_{24}\otimes F_3)xDx(I_{24}\otimes F_3^{-1}), \qquad (4)$$

$$E=diag(E11, E21, E31, E12, E22, E23, E13, E23, E33)$$

Combining (3) and (4), we obtain:

$$E=(I_{24}\otimes F_3)(I_8\otimes F_3\otimes I_3)C(I_8\otimes F_3^{-1}\otimes I_3)(I_{24}\otimes F_3^{-1}) \qquad (5)$$

and hence in order to calculate CxX, where X is a vector of length 72, one should calculate

$$(I_8\otimes F_3^{-1}\otimes I_3)(I_{24}\otimes F_3^{-1})E(I_{24}\otimes F_3)(I_8\otimes F_3\otimes I_3)V \qquad (6)$$

Here

$$(I_{24}\otimes F_3)(I_8\otimes F_3\otimes I_3) = (I_8\otimes I_3\otimes F_3)(I_8\otimes F_3\otimes I_3) = \qquad (7)$$

$$= I_8\otimes((F_3\otimes I_3)(I_3\otimes F_3)) = I_8\otimes F_3\otimes F_3$$

Then

$$C = (I_8\otimes F_3^{-1}\otimes F_3^{-1})E(I_8\otimes F_3\otimes F_3)V \qquad (8)$$

and we can use the algorithm described in [3] to calculate $F_3\otimes F_3$ and the inverse transform.

Thus the <u>core</u> step of the algorithm will have three

following stages:

1) We apply DFT(3:2) 8 times to the input 9-tuples (these 9-tuples will be described in Chapter IV).

2) We multiply an input vector of length 72 by matrix E.

3) We apply the inverse DFT(3:2) 8 times.

It is easy to see that the second stage will require 40 essential multiplications, while the first and the third will need $8N_3$ each, where N_3 is the number of essential multiplications, needed to compute DFT(3:2). Altogether we will need $40+16N_3$ essential multiplications for the core step.

The remaining part of the computations is connected with 8x8 block N, where

$$N = \mathrm{cyc}\,(w^3, w^6, 1, w^6, w^6, w^3, 1, w^3)$$

We observe that N is nothing else than the matrix of DFT(3:2) and hence the algorithm described in [3] will once more be applicable.

Thus the multiplication of N by a vector of length 8, which is to be done twice, requires N_3 multiplications. Altogether we have $40+18N_3$ multiplications. N_3 becomes 4 if we use the algorithm [3] and thus we conclude that the described DFT(9:2) algorithm will require 112 essential multiplications.

II. THE ALGORITHM FOR DFT(9:2): SUMMARY.

We conclude this section with a brief step-by-step scheme of the algorithm.

==> STEP 1. Calculate the sum of the elements of A(K,L) and store it at $\hat{A}(0,0)$.

==> STEP 2. Store B(2),B(3)... B(8) as a one-dimensional array BN1 of length 8 (cf. Table I).

==> STEP 3. Store B(9),B(10),..B(80) as a two-dimensional 9x8 array BC. The following diagram displays the distribution of the elements of A in the array BC.

TABLE III.

BC: \ J / I \	1	2	3	4	5	6	7	8
1	(1,0)	(2,2)	(0,8)	(2,7)	(8,0)	(7,7)	(0,1)	(7,2)
2	(4,0)	(8,8)	(0,5)	(8,1)	(5,0)	(1,1)	(0,4)	(1,8)
3	(7,0)	(5,5)	(0,2)	(5,4)	(2,0)	(4,4)	(0,7)	(4,5)
4	(1,3)	(5,8)	(3,8)	(8,4)	(8,6)	(4,1)	(6,1)	(1,5)
5	(4,3)	(2,5)	(3,5)	(5,7)	(5,6)	(7,4)	(6,4)	(4,2)
6	(7,3)	(8,2)	(3,2)	(2,1)	(2,6)	(1,7)	(6,7)	(7,8)
7	(1,6)	(8,5)	(6,8)	(5,1)	(8,3)	(1,4)	(3,1)	(4,8)
8	(4,6)	(5,2)	(6,5)	(2,4)	(5,3)	(4,7)	(3,4)	(7,5)
9	(7,6)	(2,8)	(6,2)	(8,7)	(2,3)	(7,1)	(3,7)	(1,2)

(The entries are the subscripts of the corresponding elements of A(K,L)).

Remark. One can see that the indices in any column of the Table III are the same modulo 3. This event enables us to

perform the transformation of the input data rather efficiently. We will give a justification in next Chapter.

==> STEP 4. We consider each column of BC as input data for the DFT(3:2) and perform the transform (Cf.[3] for an efficient algorithm). After this step is completed, we store the output back into BC. Then the first row of BC will contain the sums of the entries which were in each column before the Step 4. We store the first row of BC into a one-dimensional array BN2.

==> STEP 5. We multiply each row of BC by the corresponding block of the matrix E. Thus the first row is multiplied by E11 (which is zero matrix), the second by E21,.. the ninth by E33. As shown above, the multiplication by Eij is just multiplication by a constant, followed by a cyclic shift. The output is stored back into BC.

==> STEP 6. We apply inverse DFT(3:2) to each column of BC (cf. with the Step 4). The output is stored back into BC.

==> STEP 7. We multiply BN2 by the matrix N. As shown in [3], it can be done using only 4 multiplications. The output is saved as $\hat{B}(2),\ldots\hat{B}(8)$, or $\hat{A}(3,0),..\ \hat{A}(6,3)$ (cf. Table II).

==> STEP 8. We multiply BN1 by N and store the output back into BN1.

==> STEP 9. We add BN1 to each row of BC and store the outputs back into BC.

==> STEP 10. We unravel the data contained in the array BC and store it as $\hat{B}(9),\hat{B}(10),..\hat{B}(80)$, or $\hat{A}(1,0),\ldots\hat{A}(2,4)$ (cf.

Table II).

As will be shown in the next Chapter, the same scheme can be applied not only for $9=3^2$, but for any square of a prime number.

CHAPTER IV.

0. INTRODUCTION

In this Chapter we discuss a new algorithm for the n-dimensional Finite Fourier Transform on p^2 points along each axis, where p is a prime number ($DFT(p^2 \cdot n)$). This algorithm is logically based on the algebraic structures, presented in Chapter II. In order to avoid numerious repetitions we will restrict ourselves to the list of definitions and results from Chapter II used in this construction. The notation we are going to use is fully compatible with Chapter II. The reader interested in complete understanding of new algorithm is thereby urged to read this Chapter *after* a certain level of familiarity with Chapter II has been reached.

I. $Z_q(N)$, CASE $Q=P^2$

We have introduced Zq(n), $q=p^s$, in Section I of Chapter II. We will now recall the definitions in the notation adjusted for the case s=2.

We start with local ring Zq of integers modulo $q=p^2$, where p is a prime. Let $f \in Zq[u]$, deg(f)=n be a locally irreducible polynomial over Zq (cf. Chapter II, Section I). We define $Zq(n)=Zq[u]/\langle f(u)\rangle$. It was shown in Lemma 2, Chapter II, that Zq(n) is a local ring with the maximal nilpotent ideal (p) and the residue field $Zp[u]/\langle f'(u)\rangle$, where $f'(u) \in Zp[u]$ is the image of f(u) in Zp[u] under the canonical ring epimorphism $Zq[u] \to Zp[u]$.

We observe that Zq(n) contains p^{2n} elements. Amongst them, p^n are zero divisors, $p^{2n}-p^n$ are invertible. Let D be the set of all zero divisors different from 0; let U be the unit group of Zq(n). The structure of the group U is given by Theorem 3 of Chapter II. For $q=p^2$ we obtain:

Lemma 1.

Let $H=1+(p)$, for $i=0,1,..n-1$ let $H(i) = \{1+pku^i \mid k=0,1,..p-1\}$. Then H and H(i) are subgroups of U; for every i $H(i) \cong Zp$ and $H = \bigoplus_{i=0}^{n-1} H(i)$. Furthermore, $U = H \oplus G$, where G is a cyclic subgroup of order p^n-1.

The proof follows from Theorem 3 of Chapter II.

We will introduce the following notation: let x be one of

the generators of G. The elements $h_i=1+pu^i$ (i=0,1,..n-1) will generate subgroups H(i).

Thus, we can uniquely write any element of U as $h_0^{k_0}h_1^{k_1}\ldots h_{n-1}^{k_{n-1}}x^k$ for some $k_0,k_1,\ldots k_{n-1}=0,1,\ldots p-1$ and $k=0,1,..p^n-2$ (cf. Chapter II, Theorem).

Similarly, any element of D can be uniquely written as px^k for some $k=0,..p^n-2$. (see Corollary after Theorem 4, Chapter II).

Let $a=\sum_{i=0}^{n-1}a_iu^i \in Zq(n)$, $b=\sum_{i=0}^{n-1}b_iu^i \in Zq(n)$. We define

$\langle a,b\rangle = \sum_{i=0}^{n-1}a_ib_i \in Zq$ and $\varphi(a)=a_0$

It was shown in Section V of Chapter II that there exists a bijective homomorphism T of the additive structure of Zq(n) such that the following equation holds for every $a,b \in Zq(n)$:

$\langle a,Tb\rangle = \varphi(ab)$.

(cf.Theorem 5,Chapter II).

We now obtained all the information necessary to start the construction of the algorithm.

II. DFT(Q·N) AND THE STEPS OF THE ALGORITHM.

The Discrete Fourier Transform DFT(p^2:n) is given by the following equations:

$$\hat{A}(j_0, j_1 \cdots j_{n-1}) = \sum_{i_\kappa=0, \kappa=0,1\ldots}^{p^2-1} w^{\sum_{\kappa=0}^{n-1} i_\kappa j_\kappa} A(i_0, i_1, \ldots i_{n-1}), \quad (1)$$

where $A, \hat{A} : Zq \oplus Zq \oplus \ldots \oplus Zq \longrightarrow \mathbb{C}$ and $w = e^{2\pi i/q}$.

For $a = \sum_{i=0}^{n-1} a_i u^i \in Zq(n)$ we will write $A(a) = A(a_0, \ldots a_{n-1})$ and $\hat{A}(a) = \hat{A}(a_0, \ldots a_{n-1})$ and we will consider A and $\hat{A}$ as functions from Zq(n) to C. Using the previously established notation, we rewrite the DFT equations (1) in the following form:

$$\hat{A}(b) = \sum_{a \in Z_q(n)} w^{\langle a,b \rangle} A(a) \quad (2)$$

Using defined mapping T, we will rewrite (2) once more:

$$B(b) = \hat{A}(T^{-1}b) = \sum_{a \in Z_q(n)} V(ab) \cdot A(a), \quad (3)$$

where $V(t) = w^{\varphi(t)}$; $V \cdot Zq(n) \dashrightarrow C$.

Following Section VI of Chapter II we will subdivide these equations onto "Steps". We rewrite (3):

$$B(0) = \sum_{a \in Z_q(n)} A(a) \quad (4)$$

$$B(b) = A(0) + \sum_{a \in D} V(ab)A(a) + \sum_{a \in U} V(ab)A(a),$$

for every $b \in D$.

$$B(b) = A(0) + \sum_{a \in D} V(ab)A(a) + \sum_{a \in U} V(ab)A(a),$$

for every $b \in U$.

Similarly to Section VI of Chapter II we will introduce

four Steps of the algorithm.

Let the (X,Y)-th Step of the algorithm be the problem of the evaluation of sums

$$B_{X,Y}(b) = \sum_{a \in Y} V(ab)A(a) \qquad (5)$$

for all $b \in X$, where X,Y=D or U. Thus we are to perform 4 Steps: (D,D), (D,U), (U,D) and (U,U) and to add up the results in order to evaluate (4).

Remark. Here our notation somewhat differs from the one used in Chapter II. We recall that W(a)=V(a)-1, where W was defined in Chapter II. Further, our four Steps correspond to Steps (1,1), (1.0), (0,1) and (0,0) as defined in Chapter II.

We observe that the (D,D) Step will require no essential multiplications. Indeed, every elements $a,b \in D$ can be written as $a=pa'$, $b=pb'$ for some $a',b' \in Zq(n)$. Hence, $V(ab)=V(p^2a'b')=V(0)=1$ and the equations (5) for (D,D) Step can be written as

$$B_{D,D}(b) = \sum_{a \in D} A(a), \text{ for all } b \in D. \qquad (6)$$

Remark. This result is just a consequence of much more general Lemma 7 of Chapter II.

In the next Section we will analyze the (D,U) and (U,D) Steps. They will be handled in almost the same way as it was done in Chapter II. The core or (U,U) Step will be discussed in Section 4, where some new techniques will be presented.

III. (D,U) AND (U,D) STEPS.

Let us rewrite the equations (5) for the (D,U) Step first. We recall that any element of D can be uniquely written as px^L for some $L=0,1,.. p^n-2$ and any element of U can be uniquely written as $x^k h$ for some $k=0,1,.. p^n-2$ and $h \in H$. Thus we are to calculate for all $L=0,1,.. p^n-2$

$$B_{D,U}(px^L) = \sum_{a \in U} V(px^L a)A(a) = \sum_{a \in U} V(px^L x^k h)A(hx^k) = \quad (7)$$

$$= \sum_{K=0}^{p^n-2} V(px^{K+L})\Big(\sum_{h \in H} A(hx^k)\Big).$$

Let $B'(L)=B_{D,U}(px^L)$ and $A'(K)=\sum_{h \in H} A(hx^k)$ for $K,L=0,1,.. p^k-2$. Let further

$M = ||v^{K+L}||$ ($K,L=0,1,.,. p^n-2$) be (p^n-1) by (p^n-1) matrix. Thus in order to evaluate (7) we have to evaluate the product $B'=MxA'$ for an arbitrary vector A'.

We will now similarly rewrite (5) for the (U,D) Step:

$$B_{U,D}(hx^k) = \sum_{a \in D} V(hx^k a)A(a) = \sum_{L=0}^{p^n-2} V(px^{K+L})A(px^L), \quad (8)$$

where $a=px^L$ and $b=hx^k$.

We define $A''(K)=A(px^k)$ for all $K=0,1,...p^n-1$ and $B''(L)=B_{U,D}(hx^L)$ for all $L=0,1,.. p^n-1$. (The right hand side does not depend on h, as shown in (8)). Thus, (U,D) Step is also reduced to the evaluation of $B''=MxA''$ and therefore is equivalent (up to a certain number of additions) to the (D,U) Step.

Remark. The reduction we applied to the (D,U) and (D,U) is discussed in details in Section VII, Chapter II. It further follows from there that M-1 can be permuted into the core matrix of DFT(p:n), using the inverse permutation on U (See Chapter II, Section IX). Note that by M-1 we understand the matrix obtained from M by subtracting 1 from every entry. The algorithm for the evaluation of DFT(p:n) is discussed in [2] and final Sections of Chapter II.

IV. (U,U) (OR CORE) STEP.

We now face the problem of the evaluation of

$$B_{U,U}(b) = \sum_{a \in U} V(ab)A(a) \qquad (9)$$

for all $b \in U$. Let $B_0(b) = B_{U,U}(b^{-1})$ for every element b of U. We rewrite (9) as

$$B_0(b) = \sum_{a \in U} V(ab^{-1})A(a) \qquad (10)$$

Every element $t \in U$ can be uniquely written as $h_0^{k_0} h_1^{k_1} \cdots h_{n-1}^{k_{n-1}} x^k$. We will induce an order on U by lexicographically ordering the (n+1)-tuples $(k_0, k_1, \ldots k_{n-1}, k)$. Thus we can now rewrite (10) in the following matrix form:

$$B = N \times A, \qquad (11)$$

where N is an $p^n(p^n-1)$ by $p^n(p^n-1)$ matrix. Repeating the argument from Chapter II, Section IX, we observe that N can be written as a sum of tensor products as follows:

$$N = \sum_{\kappa=0}^{p^n-2} \sum_{\kappa_i=0}^{p-1} S_{p^n-1}^{\kappa} \otimes \left(\bigotimes_{i=0}^{n-1} S_p^{k_i}\right) \times V(h_0^{k_0} h_1^{k_1} \cdots h_{n-1}^{\kappa_{n-1}} x^k) \qquad (12)$$

We recall that Fourier transform is the diagonalization operator for the Shift operator S; more precisely, if F_a is the matrix of DFT(a·1), then $F_a \otimes S_a \otimes F_a^{-1}$ is the diagonal matrix diag$(1, w^1, w^2, \ldots w^{a-1})$, where $w = e^{2\pi i/a}$. Let F be the matrix $(I_{p^n-1}) \otimes \left(\bigotimes_{i=0}^{n-1} F_p\right)$. We will partially diagonalize N, using F.

Lemma 2. Let $N' = F \otimes N \otimes F^{-1}$. Then:

1). N' is a block-diagonal matrix with p^n blocks, each of them being a $(p^n-1)\times(p^n-1)$ matrix.

2). Furthermore, these blocks are matrices

$$N(i_0, i_1, \ldots i_{n-1}) = \qquad (13)$$

$$\sum_{\kappa=0}^{p^n-2} \sum_{j_s=0, s=0,1..}^{n-1} w^{\left(\sum_{s=0}^{n-1} p i_s j_s\right)} V(x^k h_0^{j_0} \cdots h_{n-1}^{j_{n-1}}) \; S_{p^n-1}^{\kappa}$$

Proof. The proof follows from elementary properties of the tensor product.

The next theorem is of key importance and justifies the algorithm.

Theorem 3. Any of the circulant (p^n-1) by (p^n-1) matrices $N(i_0, i_1, \ldots i_{n-1})$ can be written as $w^a S_{p^n-1}^b$ for some $a = 0, 1, \ldots p^{2n}-1$ and $b = 0, 1, \ldots p^n-2$, where both a and b depend on $(i_0, i_1, \ldots i_{n-1})$.

Proof. Recall that the blocks $N(i_0, i_1, \ldots i_{n-1})$ are given by (13). We evaluate part of the right hand side of the latter equation as follows:

$$w\Big(\sum_{s=0}^{n-1} p j_s i_s\Big)_w \quad \Big(x^k \prod_{s=0}^{n-1} h_s^{j_s}\Big) = \tag{14}$$

$$w\Big(\sum_{s=0}^{n-1} p j_s i_s\Big)_w \quad \Big(x^k\Big(1+\sum_{s=0}^{n-1} p j_s u^s\Big)\Big) =$$

$$w\Big(\sum_{s=0}^{n-1} p j_s i_s\Big) + \Big(x^k\Big(1+\sum_{s=0}^{n-1} p j_s u^s\Big)\Big)$$

We rewrite the exponents as follows:

If $x^k = \sum_{t=0}^{n-1} a_t(k) u^t$, then

$$p\sum_{s=0}^{n-1} j_s i_s + \varphi\Big(x^k\Big(1+p\sum_{s=0}^{n-1} j_s u^s\Big)\Big) = \tag{15}$$

$$p\sum_{s=0}^{n-1} j_s i_s + \varphi\Big(\Big(\sum_{t=0}^{n-1} a_t(k) u^t\Big)\Big(1+p\sum_{s=0}^{n-1} j_s u^s\Big)\Big) =$$

$$\Big(\sum_{t=0}^{n-1} a_t(k) u^t\Big) + p\,\varphi\Big(\Big(\sum_{s=0}^{n-1} j_s i_s\Big) + \Big(\Big(\sum_{t=0}^{n-1} a_t(k) u^t\Big)\Big(\sum_{s=0}^{n-1} j_s u^s\Big)\Big) =$$

$$a_0(k) + p\,\varphi\Big(\Big(\sum_{s=0}^{n-1} j_s i_s\Big) + \Big(\sum_{s=0}^{n-1} j_s\Big(\sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)\Big) =$$

$$a_0(k) + p\,\varphi\Big(\sum_{s=0}^{n-1} j_s\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big).$$

Hence we can rewrite (13) as

$$M(i_0, i_1, \ldots i_{n-1}) = \tag{16}$$

$$\sum_{k=0}^{p^n-2} \sum_{j_s=0, s=0,1,\ldots}^{n-1} w^{a_0(k)}{}_w p\varphi\Big(\sum_{s=0}^{n-1} j_s\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)_{S^k_{p^n-1}} =$$

$$\sum_{k=0}^{p^n-2} w^{a_0(k)}\Big(\sum_{j_s=0, s=0,1,\ldots}^{n-1} {}_w p\varphi\Big(\sum_{s=0}^{n-1} j_s\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)\Big)_{S^k_{p^n-1}} =$$

$$\sum_{k=0}^{p^n-2} w^{a_0(k)}\Big(\sum_{j_s=0, s=0,1}^{n-1} {}_w p j_s \varphi\Big(\sum_{s=0}^{n-1} \Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)\Big)_{S^k_{p^n-1}} =$$

$$\sum_{k=0}^{p^n-2} w^{a_0(k)}\Big(\sum_{j_s=0}^{n-1} \prod_{s=0}^{n-1} {}_w p j_s \varphi\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)_{S^k_{p^n-1}} =$$

$$\sum_{k=0}^{p^n-2} w^{a_0(k)}\Big(\prod_{s=0}^{n-1} \sum_{j_s=0}^{n-1} {}_w p j_s \varphi\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big)\Big)_{S^k_{p^n-1}} =$$

We observe that $\sum_{j_s=0}^{n-1} {}_w p j_s \varphi\Big(i_s + \sum_{t=0}^{n-1} a_t(k) u^{t+s}\Big) = 0$, unless

$$\left(\sum_{t=0}^{n-1} a_t(k)u^{t+s}\right) = -i_s \text{ (modulo p)} \qquad (17)$$

Hence in order to prove the assertion we have to show that for fixed $i_0, i_1, \ldots i_{n-1}$ there is at most one k, such that (17) holds for all s=0,1... p-1.

Let us assume that (17) holds for k_1 and k_2. Then let $a_t = a_t(k_1) - a_t(k_2)$. We assume that

$$\varphi\left(\sum_{t=0}^{n-1} a_t u^{t+s}\right)(0) \equiv 0 \pmod{p} \text{ for every } s=0,1,.. p-1 \qquad (18)$$

We proceed with an informal induction: Let s=0. Then (18) implies that $\varphi(\sum_{t=0}^{n-1} a_t u^t) \equiv 0$, and hence $a_0 \equiv 0 \pmod{p}$. Next let s=1. Equation (18) implies that $\varphi(\sum_{t=0}^{n-2} a_t u^{t+1} + a_{n-1}\sum_{i=0}^{n-1}(-f_i u^i)) = 0 \pmod{p}$, where $f_0, f_1, .. f_{n-1}$ are the coefficients of the polynomial f(u) which has been used in the definition of the ring. The latter expression is equal to $a_{n-1}f_0$. As is easy to see, the coefficient f_0 has to be relatively prime to p, since otherwise the polynomial $f' = (\pi[u])(f)$ has less degree over Zq than f has over Zp. Therefore, $a_{n-1} \equiv 0 \pmod{p}$.

We will proceed with s=2,3,... and will analogously prove that $a_{(n-2)}, a_{(n-3)}, \ldots \equiv 0 \pmod{p}$. Thus we prove

that $a_t(k_1) \equiv a_t(k_2) \pmod p$ for every t. It implies that $\sum_{t=0}^{n-1} (a_t(k_1) - a_t(k_2)) u^t \equiv 0 \pmod p$. The left hand side is equal to $x^{k_1} - x^{k_2}$ and hence $x^{k_2}(x^{k_1-k_2} - 1) \in D$, where x^{k_2} is invertible. Therefore, $x^{k_1-k_2} \in 1+D=H$. We conclude that $x^{k_1-k_2}=1$, $k_1 \equiv k_2 \pmod{p^n-1}$, and the assertion follows.

Recall that (U,U)-step of the construction is given by equations (10)-(11). We will rewrite (11) now:

$$B_0 = (F^{-1} \otimes N' \otimes F) \times A_U \qquad (19)$$

Thus, (U,U)-step is subdivided into three stages:

1. Multiplication by the matrix $F = I_{p^n-1} \otimes (\bigotimes_{k=0}^{n-1} F_p)$.
2. Multiplication by the matrix N'.
3. Multiplication by the matrix $F^{-1} = I_{p^n-1} \otimes (\bigotimes_{k=0}^{n-1} F_p^{-1})$.

We observe that F is a tensor product of an identity matrix with the matrix of DFT(p:n); thus the algorithm of [3] can be conveniently used (p^n-1) times in the first stage. We will further mention that DFT(p:n) can be applied independently to the entries, indexed by different cosets of H in U. Similarly, we will use the inverse DFT(p:n) (p^n-1) times for the third stage. Certain number of multiplications (at most $p^n(p^n-1)$) will be performed in the second stage.

V. THE DATA TRANSFORMATIONS IN THE ALGORITHM.

As we have seen. the first stage of (U,U) step of the algorithm works independently on D and on the cosets of H in U. Further, (D,U) step also can be split onto DFT(p:n) calls using data indexed by different cosets of H. Finally, (U,D) step uses only data, indexed by elements of D. We observe that the multiplicative cosets of H are the additive cosets of D. The problem we face is how to extract the data indexed by a coset of D from an n-dimensional p^2 by p^2 by ... p^2 input array A.

First, we observe that the data, indexed by D itself, is collected into a lattice in A: D is indexed by $(i_0,i_1,\dots i_{n-1})$, where $p|i_j$ for every j. Analogously, the data indexed by a coset $a+D=a\circ H$ $(a\in U)$ is indexed by $(i_0,i_1,\dots i_{n-1})$, where i_j is congruent to the j-th coefficient of a modulo p.

Example. The Table III of Section III illustrates these lattices for the case p=3,n=2.

The lattice structure of input allows us to transform the data as follows:

We extract subarrays $A_{j_1}=\{A(i_0,i_1,\dots i_{n-1}),\ j_1=i_{n-1} \mod p\}$. Then each of the arrays A_{j_1}, $j_1=0,1,..p-1$, contains $p^{(n-1)}$ cosets of D. We consider the next index and subdivide A_{j_1} onto $A_{j_1 j_2}$, $j_2=0,1,..\ p-1$, et cetera.

Remark. We start with the last or the first index depending on the sequence of storing of the elements of an array used

by the software: it differs with the programming language. The output transformation will proceed analogously, as shown by the following

Lemma 4. T respects cosets of D, i.e. if a and b belong to the same coset of D, then so do T(a) and T(b).

Proof.

Let $b=a+pz$, for some $z \in Zq(n)$. Then $T(b)-T(a)=T(a+pz)-T(a)=T(a)+pT(z)-T(a)=pT(z)$, hence $T(b)=T(a)+pT(z)$, Q.E.D.

Remark. Extreme care should be exercised in the actual programming of this algorithm with respect to the permutations.

REFERENCES

[1] J.W.Cooley and J.W.Tukey. An algorithm for the Machine Calculation of Complex Fourier Series. Math. of Computations, Vol.19, No.90 (1965) 297-301

[2] S.Winograd. Arithmetic Complexity of Computations. CBMS-NSF Regional Conference Series in Applied Math. 1980

[3] L.Auslander E.Feig, S.Winograd. New Algorithms for the Multi-dimensional Discrete Fourier Transform. IBM Research Report.

[4] H.F.Silverman. An Introduction to Programming the Winograd Fourier Transform Algorithm (WFTA). IEEE Trans. ASSP, vol 25, April 1977, pp.152-165

[5] N.Jacobson, Lectures on Abstract Algebra, vol.III.

[6] L.Auslander, E.Feig, S.Winograd. Discrete Fourier Transforms: Something Old, Something New, Something Borrowed... IBM Research Report.