INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the original text directly from the copy submitted. Thus, some dissertation copies are in typewriter face, while others may be from a computer printer.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyrighted material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is available as one exposure on a standard 35 mm slide or as a 17″ × 23″ black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. 35 mm slides or 6″ × 9″ black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI
Accessing the World's Information since 1938

300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

Order Number 8801760

Sparse matrix factorizations for fast symmetric Fourier transforms

Seguel, Jaime, Ph.D.

City University of New York, 1987

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

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. Dissertation contains pages with print at a slant, filmed as received ✓
16. Other _____

_____

_____

SPARSE MATRIX FACTORIZATIONS FOR FAST SYMMETRIC FOURIER TRANSFORMS

by

JAIME SEGUEL

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

1987

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

Sept 23' 87
date

L. Auslander
Chairman of Examining Committee

Sept 23' 87
date

A. T. Vasquez
Executive Officer

L. Auslander

A. T. Vasquez

Supervisory Committee

Table of contents

Introduction.

Several problems in science and engineering demand extensive computation of large size discrete Fourier transforms (DFT). One way to satisfy this demand is to expand the processor performance. Another way, is to choose cleverly designed algorithms: that is, essentially, ways of organizing the computations so that the number of operations required is minimized.

The design of DFT algorithms can be traced historically to the times of Gauss (1805) [H-J-B] and the principal discoveries of efficient computing methods involved, among others, authors as Runge, Danielson and Lanczos [D-L], Thomas [T], Good [G], Cooley and Tuckey [C-T] and Winograd [W].

The introduction in 1965 of the fast Fourier transform algorithm (FFT) by Cooley and Tuckey is considered to be a turning point in DFT computing methods. They showed that the DFT can be calculated using $NlogN$ operations instead of N^2. The FFT algorithm remains the most widely used method of computing the DFT despite the presentation in 1976, by Winograd, of an algorithm in which by computing DFTs as convolutions, a theoretical reduction over the FFT is achieved. Winograd's work also showed that an important factor in obtaining lower computational bounds for DFT algorithms is the use of the underlying mathematical structure of finite rings.

Further reductions in the DFT computational burden might be obtained in cases in which the input data sequence contains structured redundancies. A pioneering work in that direction is found in an article by Ten Eyck [T]. The Ten Eyck method calculates the DFT of a sequence having redundancies due to crystallographic symmetries by computing FFTs on subsequences containing all the necessary input information. This method is restricted to certain crystallographic symmetries since the essential input sequence that remains after the elimination of the redundancies does not always admit a partition into lines of data as required to compute on them with FFT's. This restriction is common in the problem of the elimination of input data redundancies in the DFT computation. The reduction in size of the original DFT matrix needs to be complemented with the design of fast methods to compute with the reduced matrix.

The purpose of this work is to present new algorithms computing the DFT for each of the following classes of symmetric sequences:

1.- Sequences satisfying: $x(n) = x(-n)$;

2.- Two-dimensional sequences satisfying: $x(n_1, n_2) = x(-n_1, n_2)$;

3.- Two-dimensiomal sequences satisfying: $x(n_1, n_2) = x(-n_1, -n_2)$;

4.- Two-dimensional sequences satisfying: $x(n_1, n_2) = x(n_2, n_1)$;

5.- Three-dimensional sequences satisfying:

$$\begin{aligned} x(n_1, n_2, n_3) &= x(-n_1, -n_2, n_3) \\ &= x(n_1, -n_2, -n_3) \\ &= x(-n_1, n_2, -n_3) \end{aligned}$$

where n, n_1, n_2, $n_3 \in Z/N$, and N is the product of two disctint odd primes.

The DFT computation of sequences having this type of symmetries is common in problems of structure determination by x-ray crystallography, [L-P]; DFT computations on sequences satisfying $x(n) = x(-n)$ are also extensively used in the solution of boundary-value problems in partial differential equations [H] , [S].

The new algorithms proposed here are derived by eliminating the redundant computations from a suitable DFT matrix representation, obtained by means of ring-theoretical techniques. This matrix representations always admit a factorization as a product of an integral matrix times a block diagonal complex matrix; factorization that was first proposed, for the one-dimensional DFT matrix, by Tolimieri [To].

The use of this DFT representations and their factoring formulas in the elimination of redundant computations is two folded. On one hand they provide algorithms based on preprocessing the symmetric sequence through additions and subtractions into a new sequence, which can then be transformed using FFTs and diagonal matrices. Hence, the post processing step, that appears in most of the existing fast algorithms computing the DFT of a symmetric sequences, has been eliminated. On the other hand, each one of the two factors in the above mentioned DFT factorization, naturally decompose into blocks indexed by the orbits of the action of a group G on the indexing ring of the original DFT matrix, providing the blocks with computationally desirable structures.

In all the cases considered in this work a group G can be chosen in such a way that the automorphisms describing the redundancies in the input DFT sequence map G-orbits onto G-orbits. Furthermore, G can be chosen so that the automorphisms either map one G-orbit onto a different one, or act on a G-orbit as multiplication times -1. In the first case the reduced block is either a skew-circulant or a tensor product of skew-circulant matrices while in the second case the reduced block turn out to be either a skew-circulant matrix, a tensor product of skew-circulant matrices or a block-Hankel matrix that decompose into skew-circulant blocks. Every skew-circulat matrix admits a sparse matrix factorization as the product of DFTs and diagonal matrices, (see Appendix). As for block-Hankel matrices, two different factoring formulas are presented in the first section (Proposition 1 and Proposition 2). Through this formulas the scheme of computing basically with FFTs and diagonal matrices is reocuperated at the cost of pre and post additions, in the first formula, and permutations, in the second one.

Although the implementation of this algorithms is not discussed here, their expression as tensor products can be actually used to generate code and explore its possible vectorization or parallelization.

1.- Factorization Methods For Block-Hankel Matrices

In this section we present two different sparse matrix factorization formulas for linear combinations of tensor products of Hankel matrices. The factors encountered are either skew-circulant matrices, permutation matrices or sparse matrices whose entries are zeroes or ones.

The aim of these factoring formulas is the reduction of the multiplicative complexity (i.e. the number of multiplications required to compute with the matrix) of the original matrix.

1.1.-Block-Hankel matrices and a first factoring formula

We first set the basic definitions and adopt some notational conventions.

All matrices considered in this work are complex matrices. An $n \times m$ matrix A having entries $a(k,l)$ will be denoted by :

$$A = (a(k,l)) \tag{1.1.1}$$

followed by the specification of the domains of k and l. In general it will be said that A is indexed in $R \times S$ if k ranges on R and l ranges on S. If needed, the notation

$$A = {}_{R}^{S}\left(a(k,l)\right) \tag{1.1.2}$$

will be used as an alternative to (1.1.1).

Special matrices such as column, row or diagonal matrices will be denoted as in (1.1.1) but with the extra indication of the symbols col, row and diag preceeding the matrrix brackets.

The transpose of A is denoted ${}^{t}A$ and $\overline{A}$ will denote the matrix whose entries are the complex conjugates of the entries of A.

The following symbols will always stand for the same matrices:

$$I_N \tag{1.1.3}$$

will denote the $N \times N$ identity matrix,

$$\tilde{I}_N = (a(k,l)) \tag{1.1.4}$$

will denote the $N \times N$ matrix whose entries are:

$$a(k,l) = \begin{cases} 1 & \text{if} \quad \mathrm{k+l=N} \\ 0 & \text{otherwise.} \end{cases}$$

Such a matrix is called the $N \times N$ off-diagonal identity.

(1.1.5) $$K_N$$

will stand for the $N \times 1$ column matrix whose entries are ones, and

(1.1.6) $$S_N = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

will denote the $N \times N$ shift operator.

The word block preceding the matrix bracket in (1.1.1) indicates that the entries of A are given in terms of block matrices. However, if no ambiguities arise, the word block will be avoided for simplicity.

The notations block-col, block-row and block-diag have the obvious meanings.

Let $A = (\, a(k,l)\,)$ be an $N \times N$ matrix, with $N = RQ$. Consider the following blocks in A

(1.1.7) $$A(k,l) = (\, a(n + kQ, m + lQ)\,)$$

$0 \leq k, l \leq R-1, 0 \leq n, m \leq Q-1$. Such a decomposition of A will be called the (R,Q)-*block decomposition of* A.

It is worth noticing that both the (R,Q) and the (Q,R) block decompositions of A exist as soon as $N = RQ$ but they are not equal unless $R = Q$.

The main tool in describing the properties of the block structured matrices is the *tensor or Kronecker product* of matrices, which is defined as follows :

Let

(1.1.8) $$A = (\, a(k,l)\,)$$

be an $N_1 \times N_2$ matrix and let B be an $M_1 \times M_2$ matrix. The tensor product of A and B, denoted by $A \otimes B$ is defined to be the matrix

(1.1.9) $$A \otimes B = block\,(\, a(k,l)B\,)$$

The tensor product is a bilinear operator on the space of $N_1M_2 \times N_2M_2$ matrices satisfying the two following extra properties

(1.1.10) $$^t(A \otimes B) = {}^tA \otimes {}^tB$$

(1.1.11) $$(A \otimes B)(C \otimes D) = AC \otimes BD$$

the last one for matrices of appropriate sizes.

An $N \times N$ *Hankel* matrix is a square matrix $A = (a(k,l))$, satisfying:

$$a(k,l) = a(k',l')$$

if $k + l = k' + l'$.

The set of all $N \times N$ complex Hankel matrices forms a complex vector space. A basis for this space is given by the Hankel matrices having ones in the $(k+1) - th$ off-diagonal and zeroes everywhere else. We denote this matrices by :

(1.1.12) $$H_k{}^{(N)}.$$

An important subspace of this vector space is the one formed by the skew-circulant matrices. An $N \times N$ skew-circulant matrix has the following general form:

(1.1.13) $$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{N-1} \\ a_1 & a_2 & & \dots & a_0 \\ a_2 & & & \dots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{N-1} & a_0 & a_1 & \dots & a_{N-2} \end{pmatrix}.$$

A standard notation for this matrix is :

(1.1.14) $$\mathrm{sc}(a_0, \dots, a_{N-1}) \quad \text{or} \quad \mathrm{sc}(a_k), \quad 0 \le k \le N-1$$

and clearly A is expressable as:

(1.1.15) $$A = a_{N-1} H_{N-1}{}^{(N)} + \sum_{k=0}^{N-2} a_k (H_k{}^{(N)} + H_{k+N}{}^{(N)}).$$

The most relevant property of skew-circulant matrices in the context of this work is the fact that they can be diagonalized by the discrete Fourier transform (DFT) matrix. The N-point DFT matrix is defined as :

(1.1.16) $$F(N) = (\omega^{kl})$$

$0 \leq k, l \leq N-1$; where $\omega = exp(\frac{2\pi i}{N})$ and the diagonalization of an $N \times N$ skew-circulant matrix A by $F(N)$ is expressed in the formula:

$$A = F(N)^{-1} D F(N)^{-1} \tag{1.1.17}$$

where D is an $N \times N$ diagonal matrix. See the appendix for details.

An (R,Q)-*Hankel* matrix is an $RQ \times RQ$ matrix $A = (a(k,l))$, which under (R,Q)-block decomposition satisfies:

$$A(k,l) = A(k',l')$$

whenever $k+l = k'+l'$. Therefore A is (R,Q)-Hankel if and only if it can be written as

$$A = \sum_{k=0}^{R-2} H_k{}^{(R)} \otimes A_k \tag{1.1.18}$$

where A_k is a $Q \times Q$ matrix for every k, $0 \leq k \leq R-2$.

In other words the space of all (R,Q)-Hankel matrices is the tensor product of the space of the $R \times R$ Hankel matrices times the space of the $Q \times Q$ complex matrices. A whole class of block structured matrices arises by taking successive tensor products of spaces of Hankel matrices. In general a matrix will be said to be $(R_1, \ldots, R_n, Q)$-*Hankel* if it is a member of the tensor product vector space of the $R_i \times R_i$-Hankel matrices $(i = 1, \ldots, n)$, times the vector space of the $Q \times Q$ matrices. Such a matrix is expressable as :

$$A = \sum_{k_1=0}^{R_1-2} \cdots \sum_{k_n=0}^{R_n-2} H_{k_1}{}^{(R_1)} \otimes \ldots \otimes H_{k_n}{}^{(R_n)} \otimes A(k_1, \ldots, k_n) \tag{1.1.19}$$

where $A(k_1, \ldots, k_n)$ is a $Q \times Q$ block for each $(k_1, \ldots, k_n) \in Z/R_1 \times \ldots \times Z/R_n$.

In what follows a formula for the factorization of matrices of the form of A in (1.1.19) is proposed. The core of our factoring method is illustrated in the following example: let

$$A = \begin{pmatrix} A_0 & A_1 & [0] \\ A_1 & [0] & A_2 \\ [0] & A_2 & A_3 \end{pmatrix} \tag{1.1.20}$$

where A_i, $0 \leq i \leq 3$ are $Q \times Q$ matrices and $[0]$ represents the $Q \times Q$ null matrix.

Now

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \otimes A_0 + \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \otimes A_1 + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \otimes A_2 + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes A_3 \tag{1.1.21}$$

$$= (I_3 \otimes A_0)(H_0{}^{(3)} \otimes I_Q) + (I_3 \otimes A_1)(H_1{}^{(3)} \otimes I_Q) + (I_3 \otimes A_2)(H_3{}^{(3)} \otimes I_Q) + (I_3 \otimes A_3)(H_4{}^{(3)} \otimes I_Q)$$

$$= \begin{pmatrix} I_3 \otimes I_Q & I_3 \otimes I_Q & I_3 \otimes I_Q & I_3 \otimes I_Q \end{pmatrix} \begin{pmatrix} I_3 \otimes A_0 & & & \\ & I_3 \otimes A_1 & & \\ & & I_3 \otimes A_2 & \\ & & & I_3 \otimes A_3 \end{pmatrix} \begin{pmatrix} H_0{}^{(3)} \otimes I_Q \\ H_1{}^{(3)} \otimes I_Q \\ H_3{}^{(3)} \otimes I_Q \\ H_4{}^{(3)} \otimes I_Q \end{pmatrix}$$

$$= [\begin{pmatrix} I_3 & I_3 & I_3 & I_3 \end{pmatrix} \otimes I_Q] \begin{pmatrix} I_3 \otimes A_0 & & & \\ & I_3 \otimes A_1 & & \\ & & I_3 \otimes A_2 & \\ & & & I_3 \otimes A_3 \end{pmatrix} [\begin{pmatrix} H_0{}^{(3)} \\ H_1{}^{(3)} \\ H_3{}^{(3)} \\ H_4{}^{(3)} \end{pmatrix} \otimes I_Q].$$

Consider the block-column matrix:

$$\begin{pmatrix} H_0{}^{(3)} \\ H_1{}^{(3)} \\ H_3{}^{(3)} \\ H_4{}^{(3)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{1.1.22}$$

the elimination of null rows in (1.1.22) gives:

$$\begin{pmatrix} \tilde{I}_1 & & \\ \tilde{I}_2 & & \\ & \tilde{I}_2 & \\ & \tilde{I}_1 & \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{pmatrix}. \tag{1.1.23}$$

When applied to the bottom equation in (1.1.21) this elimination of null rows propagates affecting the left factors in each tensor product. After writing all the corresponding reductions we get the factoring formula:

$$A = [\begin{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \end{pmatrix} \otimes I_Q] \begin{pmatrix} A_0 & & & \\ & I_2 \otimes A_1 & & \\ & & I_2 \otimes A_2 & \\ & & & A_3 \end{pmatrix} \tag{1.1.24}$$

$$\left[\begin{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\end{pmatrix}\\\begin{pmatrix}1&0&0\\0&0&1\end{pmatrix}\\\begin{pmatrix}0&1&0\\0&0&1\end{pmatrix}\end{pmatrix}\otimes I_Q\right].$$

Notice that, as in (1.1.23),

$$\text{(1.1.25)}\qquad \left(\begin{pmatrix}1\\0\\0\end{pmatrix}\ \begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix}\ \begin{pmatrix}0&0\\1&0\\0&1\end{pmatrix}\ \begin{pmatrix}0\\0\\1\end{pmatrix}\right) = \begin{pmatrix}I_1 & I_2 & & \\ & & I_2 & I_1\end{pmatrix}.$$

Consider now the $(3,Q)$-Hankel matrix:

$$\text{(1.1.26)}\qquad A = \begin{pmatrix}A_0&A_1&A_2\\A_1&A_2&A_3\\A_2&A_3&A_4\end{pmatrix}.$$

Expressing A as

$$\text{(1.1.27)}\qquad A = \begin{pmatrix}A_2&A_2&A_2\\A_2&A_2&A_2\\A_2&A_2&A_2\end{pmatrix}+\begin{pmatrix}A_0-A_2&A_1-A_2&[0]\\A_1-A_2&[0]&A_3-A_2\\[0]&A_3-A_2&A_4-A_2\end{pmatrix}$$

$$= \left(\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}\otimes A_2\right)+\begin{pmatrix}A_0-A_2&A_1-A_2&[0]\\A_1-A_2&[0]&A_3-A_2\\[0]&A_3-A_2&A_4-A_2\end{pmatrix}$$

$$= (I_3\otimes I_Q \quad I_3\otimes I_Q)\begin{pmatrix}\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}\otimes A_2 & \\ & \begin{pmatrix}A_0-A_2&A_1-A_2&[0]\\A_1-A_2&[0]&A_3-A_2\\[0]&A_3-A_2&A_4-A_2\end{pmatrix}\end{pmatrix}\begin{pmatrix}I_3\otimes I_Q\\I_3\otimes I_Q\end{pmatrix},$$

using the identities:

$$\text{(1.1.28)}\qquad \begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}\otimes A_2 = \begin{pmatrix}1\\1\\1\end{pmatrix}(1\ \ 1\ \ 1)\otimes A_2 = [\begin{pmatrix}1\\1\\1\end{pmatrix}\otimes I_Q]A_2[(1\ \ 1\ \ 1)\otimes I_Q],$$

and the formula (1.1.24), we obtain :

$$\text{(1.1.29)}\qquad A = \left(\left(\begin{pmatrix}1\\1\\1\end{pmatrix}\ \begin{pmatrix}1\\0\\0\end{pmatrix}\ \begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix}\ \begin{pmatrix}0&0\\1&0\\0&1\end{pmatrix}\ \begin{pmatrix}0\\0\\1\end{pmatrix}\right)\otimes I_Q\right)$$

$$\begin{pmatrix} A_2 & & & & \\ & A_0 - A_2 & & & \\ & & I_2 \otimes (A_1 - A_2) & & \\ & & & I_2 \otimes (A_3 - A_2) & \\ & & & & A_4 - A_2 \end{pmatrix}$$

$$\left(\begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \end{pmatrix} \otimes I_Q \right)$$

$$= \quad (M(3) \otimes I_Q)\, E_3(A)\, (L(3) \otimes I_Q).$$

Clearly all the steps followed for the above shown $(3, Q)$-Hankel matrix factorization are generalizable to any (R, Q)-Hankel matrix. The general forms of the factor matrices $E_R(A), M(R)$ and $L(R)$ as well as their characteristics can be drawn from a direct observation of the above shown example. As a matter of fact

(1.1.30)

$$E_R(A) \quad = \quad \begin{pmatrix} A_{R-1} & & \\ & block - diag\,(\, I_{k+1} \otimes [A_k - A_{R-1}]) & \\ & & block - diag\,(\, I_{R-k-1} \otimes [A_{k+R} - A_{R-1}]) \end{pmatrix}$$

$0 \leq k \leq R-2$. Therefore $E_R(A)$ is an $(R(R-1)+1)Q \times (R(R-1)+1)Q$ block diagonal matrix.

On the other hand motivated by relations (1.1.23) and (1.1.25) we define the general blocks: $I_k^{(U)}$ (respectively: $I_k^{(L)}$) to be the $R \times k$ matrices whose upper (respectively: lower) $k \times k$ block is I_k and the rest null; and the general blocks $\tilde{I}_k^{(l)}$ (respectively: $\tilde{I}_k^{(r)}$) as the $k \times R$ matrix whose first left (respectively: right) $k \times k$ block is $\tilde{I}_k$ and the rest null. Now :

(1.1.31) $$M(R) \quad = \quad block\,(\, K_R \quad block\,(\, I_k^{(U)}\,) \quad block\,(\, I_k^{(L)}\,)\,)$$

$0 \leq k \leq R-2$ and

(1.1.32) $$L(R) \quad = \quad block\left({}^{t}K_R \quad block\left(\tilde{I}_k^{(l)}\right) \quad block\left(\tilde{I}_k^{(r)}\right)\right)$$

$0 \leq k \leq R-2$. Therefore $M(R)$ is an $R \times (R(R-1)+1)$ matrix, while $L(R)$ is an $(R(R-1)+1) \times R$ matrix. The factoring formula for A is :

(1.1.33). $$A \quad = \quad [M(R) \otimes I_Q]\, E_R(A)\, [L(R) \otimes I_Q]$$

The first factoring formula, stated and proved below, is a slight modification of (1.1.33)

PROPOSITION 1:

Let A be an (R,Q)-Hankel matrix such that all the $Q \times Q$ blocks of its (R,Q)-block decomposition, are skew-circulant blocks. Then:

(1.1.34) $$A \quad = \quad [I_R \otimes F(Q)^{-1}]\, [M(R) \otimes I_Q]\, \Delta\, [L(R) \otimes I_Q]\, [I_R \otimes F(Q)^{-1}],$$

where Δ is an $(R(R-1)+1)Q$ diagonal matrix.

Proof of Proposition 1:

Since each $Q \times Q$ block in the (R,Q)-block decomposition of A is skew-circulant, the matrix $E_R(A)$ consists of $(R(R-1)+1)$ skew-circulant blocks of dimension $Q \times Q$ in its main diagonal. Hence there exist a $Q(R(R-1)+1)$ diagonal matrix Δ such that :

(1.1.35) $$E_R(A) \quad = \quad [I_{R(R-1)+1} \otimes F(Q)^{-1}]\Delta[I_{R(R-1)+1} \otimes F(Q)^{-1}].$$

Now:

(1.1.36)
$$\begin{aligned} [M(R) \otimes I_Q][I_{R(R-1)+1} \otimes F(Q)^{-1}] &= [I_R M(R) \otimes F(Q)^{-1} I_Q] \\ &= [I_R \otimes F(Q)^{-1}][M(R) \otimes I_Q] \end{aligned}$$

and similarly:

(1.1.37)
$$\begin{aligned} [I_{R(R-1)+1} \otimes F(Q)^{-1}][L(R) \otimes I_Q] &= L(R)I_R \otimes I_Q F(Q)^{-1} \\ &= [L(R) \otimes I_Q][I_R \otimes F(Q)^{-1}] \end{aligned}$$

The Proposition follows after replacing this equation in formula (1.1.33).‖

Formula (1.1.33) is generalizable to $(R_1, \ldots, R_n, Q)$- Hankel matrices through a nesting procedure which is the natural generalization of what it is shown below in the case of (R_1, R_2, Q)-Hankel matrices.

Let A be an (R_1, R_2, Q)-Hankel matrix; then A is, in particular, an (R_1, R_2Q)-Hankel matrix and so formula (1.1.33) gives

$$A = [M(R) \otimes I_{R_2Q}]\, E_R(A)\, [L(R_1) \otimes I_{R_2Q}]. \tag{1.1.38}$$

Each block in the main diagonal of E_{R_1}, being the result of linear combinations of (R_2, Q)-Hankel matrices, is on its own an (R_2, Q)-Hankel matrix. Let $A(k)$ $1 \leq k \leq R_1(R_1 - 1) + 1$ denote each of these blocks. Then, again by (1.1.33):

$$A(k) = [M(R_2) \otimes I_Q]\, E_{R_2}(A(k))\, [L(R_2) \otimes I_Q], \tag{1.1.39}$$

therefore

$$\begin{aligned} A &= [M(R_1) \otimes I_{R_2Q}]\, [block - diag\,(A(k))]\, [L(R_1) \otimes I_{R_2Q}] \\ &= [M(R_1) \otimes I_{R_2Q}]\, [I_{R_1(R_1-1)+1} \otimes M(R_2) \otimes I_Q]\, [block - diag\,(E_{R_2}(A(k)))] \qquad (1.1.40) \\ &= [I_{R_1(R_1-1)+1} \otimes L(R_2) \otimes I_Q]\, [L(R_1) \otimes I_{R_2Q}], \end{aligned}$$

but

$$\begin{aligned} &[M(R_1) \otimes I_{R_1Q}]\, [I_{R_1(R_1-1)+1} \otimes M(R_2) \otimes I_Q] \\ &= [M(R_1) \otimes I_{R_2} \otimes I_Q]\, [I_{R_1(R_1-1)+1} \otimes M(R_2) \otimes I_Q] \qquad (1.1.41) \\ &= M(R_1) \otimes M(R_2) \otimes I_Q \end{aligned}$$

and similarly:

$$(1.1.42) \qquad [I_{R_1(R_1-1)+1} \otimes L(R_2) \otimes I_Q][L(R_1) \otimes I_{R_2Q}] = L(R_1) \otimes L(R_2) \otimes I_Q.$$

So, if we denote by $E_{R_2} \circ E_{R_1}(A)$ the block diagonal matrix resulting from applying the operation E_{R_2} to each block in $E_{R_1}(A)$, we get:

$$(1.1.43) \qquad A = [M(R_1) \otimes M(R_2) \otimes I_Q][E_{R_2} \circ E_{R_1}(A)][L(R_1) \otimes L(R_2) \otimes I_Q].$$

Hence, in general, for an $(R_1, \ldots, R_n, Q)$-Hankel matrix A we have the factoring formula:

$$(1.1.44) \qquad A = [M(R_1) \otimes \ldots \otimes M(R_n) \otimes I_Q][E_{R_n} \circ \ldots \circ E_{R_1}(A)][L(R_1) \otimes \ldots \otimes L(R_n) \otimes I_Q]$$

and if each $Q \times Q$ block in the $(R_1, \ldots, R_n, Q)$-block decomposition of A is skew-circulant we get the following generalization of the formula stated in Proposition 1:

$$(1.1.45) \qquad A = [I_{R_1 \ldots R_n} \otimes F(Q)^{-1}][M(R_1) \otimes \ldots \otimes M(R_n)]\,\Delta\,[L(R_1) \otimes \ldots \otimes L(R_n)][I_{R_1 \ldots R_n} \otimes F(Q)^{-1}],$$

where Δ is a $Q\prod_{i=1,\ldots,n}(R_i(R_i-1)+1)$ diagonal matrix.

Formula (1.1.45) plays a crucial role in reducing the size of Δ for (R,Q)-Hankel matrices in which $R = \prod_{i=1,\ldots,n} R_i$. In order to see that we first observe two simple facts :

Observation 1:

If A is an (R,Q)-Hankel matrix and $R = \prod_{i=1,\ldots,n} R_i$ then A is also an $(R_1, \ldots R_l, Q\prod_{k=l+1,\ldots,n} R_k)$-Hankel matrix, for any $0 \leq l \leq n$. Indeed, it is easy to see that if the off-diagonals formed by the $Q \times Q$ blocks are constant, so are the off-diagonals formed by $(Q\prod_{k=l+1\ldots n} R_k) \times (Q\prod_{k=l+1,\ldots,n} R_k)$ blocks.

Observation 2:

If $R = R_1R_2$, with $R_1 \geq 1$ and $R_2 \geq 1$ then:

$$(1.1.46) \qquad R(R-1)+1 \quad \geq \quad [R_1(R_1-1)+1][R_2(R_2-1)+1].$$

Indeed, if $R_1, R_2 \geq 1$, then obviously

(1.1.47) $$R_1R_2 + 1 \geq R_1 + R_2,$$

but this inequality implies:

(1.1.48) $$(R_1 + R_2)(R_1R_2 + 1) \geq (R_1 + R_2)^2,$$

which on its turn gives:

$$\begin{aligned} R(R-1)+1 &= R_1^2R_2^2 - R_1R_2 + 1 \\ (1.1.49) \qquad &\geq (R_1^2R_2^2 - R_1R_2 + 1) + (R_1 + R_2)^2 - (R_1 + R_2)(R_1R_2 + 1) \\ &= [R_1(R_1 - 1) + 1][R_2(R_2 - 1) + 1]. \end{aligned}$$

Therefore if formula (1.1.45) is used with a full decomposition of R into multiplicative factors, the size of the diagonal matrix achieves a minimun.

On the other hand, both formulas (1.1.34) and (1.1.45) require the same number of additions. In order to see this, let's consider the case $R = R_1R_2$. For a given matrix A, let:

$$\alpha(A)$$

be the number of additions required to compute with A,

$$c(A)$$

be the number of columns in A, and

$$r(A)$$

be the number of rows in A. Then:

(1.1.50) $$\alpha(A \otimes B) = c(A)\alpha(B) + r(B)\alpha(A).$$

Now, for a given R:

$$c(M(R)) \quad = \quad r(L(R)) \quad = R(R-1)+1,$$

$$r(M(R)) \quad = \quad c(L(R)) \quad = R,$$

$$\alpha(M(R)) \quad = \quad R(R-1)$$

and

$$\alpha(L(R)) \quad = \quad R-1.$$

Therefore, if $R = R_1 R_2$, the total number of additions in formula (1.1.45) is given by:

$$(1.1.51) \quad Z \quad = \quad [c(M(R_1))\alpha(M(R_2)) + r(M(R_2))\alpha(M(R_1))] + [c(L(R_1)\alpha(L(R_2)) + r(L(R_2))\alpha(L(R_1))].$$

A straight coputation shows that $Z \quad = \quad \alpha(M(R)) + \alpha(L(R))$.

1.2.- Factoring formula based on skew-circulant factors

As pointed out in the introduction, some block-Hankel matrices appear as a result of the elimination of redundant computations induced in the DFT matrix by symmetries in the input data. These block-Hankel matrices are always expressable as the tensor of a Hankel matrix times a skew-circulant one, where the Hankel factor comes from the elimination of three quarters of a skew-circulant matrix of even size. A typical situation is illustrated below:

Let

$$C = sc(c_0, c_1, c_2, c_3) \tag{1.2.1}$$

if we denote by

$$C_1 = \begin{pmatrix} c_0 & c_1 \\ c_1 & c_2 \end{pmatrix} \tag{1.2.2}$$

and

$$C_2 = \begin{pmatrix} c_2 & c_3 \\ c_3 & c_4 \end{pmatrix} \tag{1.2.3}$$

then we get

$$\begin{aligned} C &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes C_1 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes C_2 \\ &= I_2 \otimes C_1 + \tilde{I}_2 \otimes C_2 \end{aligned} \tag{1.2.4}$$

Consider another skew-circulant matrix of even size, like the 6×6 matrix B:

$$B = sc(b_0, b_1, b_2, b_3, b_4, b_5) = \begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix} \tag{1.2.5}$$

Our problem is the factorization of:

$$C_1 \otimes \begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix} + C_2 \otimes \begin{pmatrix} B_2 & B_1 \\ B_1 & B_2 \end{pmatrix} \tag{1.2.6}$$

Now

$$\begin{pmatrix} B_2 & B_1 \\ B_1 & B_2 \end{pmatrix} = S_6^3 \begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix}$$

(1.2.7)

$$= \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_3\right) \begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix}$$

$$= (\tilde{I}_2 \otimes I_3)B$$

Hence

(1.2.8)

$$C_1 \otimes \begin{pmatrix} B_1 & B_2 \\ B_2 & B_1 \end{pmatrix} + C_2 \otimes \begin{pmatrix} B_2 & B_1 \\ B_1 & B_2 \end{pmatrix} =$$

$$\left(C_1 \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes I_3 + C_2 \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_3\right)(I_2 \otimes B)$$

Defining :

(1.2.9)

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes I_3$$

we express (1.2.8) as:

(1.2.10)

$$(P[(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes C_1 + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes C_2) \otimes I_3]^t P)(I_2 \otimes B)$$

$$= P(C \otimes I_3)^t P(I_2 \otimes B)$$

Several variations of (1.2.6) will be found in coming sections but through suitable permutation they all will be proved to be tractable by the formula stated and proved below in Proposition 2. Let's first set some notations: the symbol

(1.2.11)

$$P(n, m)$$

will stand for the permutation matrix of size nm defined by:

(1.2.12) $$P(n,m)\, f_{ml+j} \;=\; f_{nj+l}$$

where $0 \le l \le n-1, 0 \le j \le m-1$ and f_k represents the k-th canonical vector. Notice that:

(1.2.13) $$^{t}P(n,m) \;=\; P(m,n)$$

and for an $n \times n$ matrix A and an $m \times m$ matrix B

(1.2.14) $$P(n,m)\,(A \otimes B)\,P(m,n) \;=\; B \otimes A$$

We also define the $l \times l$ permutation matrix

(1.2.15) $$R(l) \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

PROPOSITION 2:

Let r_k, $0 \le k \le n$ be a collection of even numbers. Let C be an $r_0 \times r_0$ skew-circulant matrix whose $(2, \frac{r_0}{2})$-block decomposition is:

(1.2.16) $$C \;=\; \begin{pmatrix} C_1 & C_2 \\ C_2 & C_1 \end{pmatrix}$$

For each r_k, $k \ge 1$ let J_{r_k} represent either I_{r_k} or $S_{r_k}^{\frac{r_k}{2}}$ and denote by:

(1.2.17) $$I \;=\; I_{r_1} \otimes \dots \otimes I_{r_n}$$

and

$$S = J_{r_1} \otimes \ldots \otimes J_{r_n} \tag{1.2.18}$$

Assuming that there exist a number $m > 0$ of numbers r_k for which $J_{r_k} = S_{r_k}^{\frac{r_k}{2}}, k \geq 1$, a permutation matrix P can be found such that:

$$C_1 \otimes I + C_2 \otimes S = P(I_m \otimes C \otimes I')^t P \tag{1.2.19}$$

where

$$I' = I_{(r_1 \ldots r_n)2^{-m}} \tag{1.2.20}$$

Proof of proposition 2 :

Let $t_q = \pi(r_k)$ be a permutation on $(r_k : k \geq 1)$ such that $J_{t_q} = S_{t_q}^{\frac{t_q}{2}}, 1 \leq q \leq m$.

Relative to π we can find a permutation matrix P_1 consisting of tensor products of matrices of the type of $P(n,m)$ and identities such that:

$$C_1 \otimes I + C_2 \otimes S$$

$$= P_1 \left(C_1 \otimes I_{t_1} \otimes \ldots \otimes I_{t_m} \otimes I_{t_{m+1}} \otimes \ldots \otimes I_{t_n} + C_2 \otimes S_{t_1}^{\frac{t_1}{2}} \otimes \ldots \otimes S_{t_m}^{\frac{t_m}{2}} \otimes I_{t_{m+1}} \otimes \ldots \otimes I_{t_n}\right)^t P_1 \tag{1.2.21}$$

$$= P_1 \left[\left(C_1 \otimes I_2 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes I_2 \otimes I_{\frac{t_m}{2}} + C_2 \otimes \tilde{I}_2 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes \tilde{I}_2 \otimes I_{\frac{t_m}{2}}\right) \otimes I_{t_{m+1}} \otimes \ldots \otimes I_{t_n} \right]^t P_1$$

Let P_2 be the permutation matrix , of the type of P_1, such that :

$$[C_1 \otimes I_2 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes I_2 \otimes I_{\frac{t_m}{2}} + C_2 \otimes \tilde{I}_2 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes \tilde{I}_2 \otimes I_{\frac{t_m}{2}}][I_{t_{m+1}} \otimes \ldots \otimes I_{t_n}]$$

$$= P_2[(I_2 \otimes \ldots \otimes I_2 \otimes C_1 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes I_{\frac{t_m}{2}} + \tilde{I}_2 \otimes \ldots \otimes \tilde{I}_2 \otimes C_2 \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes I_{\frac{t_m}{2}}) \otimes I_{t_{m+1}} \otimes \ldots \otimes I_{t_n}]^t P_2 \tag{1.2.22}$$

$$= P_2[(I_2 \otimes \ldots \otimes I_2 \otimes C_1 + \tilde{I}_2 \otimes \ldots \otimes \tilde{I}_2 \otimes C_2) \otimes I_{\frac{t_1}{2}} \otimes \ldots \otimes I_{\frac{t_m}{2}} \otimes I_{t_{m+1}} \otimes \ldots \otimes I_{t_n}]^t P_2$$

$$= P_2[(I_{2m} \otimes C_1 + \tilde{I}_{2m} \otimes C_2) \otimes I']^t P_2$$

Finally :

$$I_{2m} \otimes C_1 + \tilde{I}_{2m} \otimes C_2$$

(1.2.23)
$$= [R(2m) \otimes I_{\frac{r_0}{2}}] \begin{pmatrix} \begin{pmatrix} C_1 & C_2 \\ C_2 & C_1 \end{pmatrix} & & \\ & \ddots & \\ & & \begin{pmatrix} C_1 & C_2 \\ C_2 & C_1 \end{pmatrix} \end{pmatrix} {}^t[R(2m) \otimes I_{\frac{r_0}{2}}]$$

$$= [R(2m) \otimes I_{\frac{r_0}{2}}] [I_m \otimes C] [R(2m) \otimes I_{\frac{r_0}{2}}]$$

Hence if:

(1.2.24)
$$P_3 = R(2m) \otimes I_{\frac{r_0}{2}} \otimes I'$$

we get:

(1.2.25)
$$P_3 (I_m \otimes C \otimes I') {}^t P_3 = (I_{2m} \otimes C_1 + \tilde{I}_{2m} \otimes C_2) \otimes I'$$

Therefore

(1.2.26)
$$P (I_m \otimes C \otimes I') {}^t P = C_1 \otimes I + C_2 \otimes S$$

where

(1.2.27)
$$P = P_1 P_2 P_3.$$

2.- Even DFT

An N-point even sequence is a real or complex sequence $x = (x(n))$ satisfying:

$$x(n) = x(-n); \quad n \in Z/N.$$

Any algorithm designed to compute the DFT of an N-point even sequence taking advantage of the above stated relation is called an even DFT algorithm.

A fast 2^k-point even DFT algorithm, based on FFT's, is presented in [R]. This algorithm, originated in [C-L-W], computes the DFT of a real N-point even sequence, for a number N divisible by 4. The computation is done in three steps: first the even sequence is pre-processed into a $N/2$ sequence, then it is transformed through a $N/2$-point FFT and finally post-processed to obtain the DFT of the original even sequence.

In this section, using ring theoretical methods, we derived a two-steps (pre-processing and transforming) fast algorithm to compute the p_1p_2-point even DFT, with p_1 and p_2 two different primes. All the techniques used here will be either repeated or generalized in coming sections.

2.1.- Ring-theoretical structures and a DFT factorization

We first summarize some facts about the ring structure of Z/N and derive from them our basic factorization formula for the N-point DFT matrix. This factorization formula is due to Richard Tolimieri, and it first appears for a 15-point DFT matrix in [To].

For a positive integer N the symbol Z/N will denote the ring of integers modulo N. The subset of Z/N

$$U(N) \quad = \quad \{n \in Z/N : (n, N) = 1\} \tag{2.1.1}$$

where (n, N) denotes the greatest common divisor of n and N; is a group under ring multiplication. This group is called the group of units of Z/N.

For odd primes p, $U(p^l)$ is cyclic. In particular $U(p)$ is cyclic of order $p-1$. The groups $U(2^l)$ are cyclic for $l = 1, 2$, but not for $l \geq 3$ in which case decompose as the direct product of two cyclic groups.

For a composite number $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ it is possible to reduce congruence modulo N to a system of simpler congruences by applying the *Chinese Remainder Theorem* , which determines the ring isomorphism :

(2.1.2) $$f : Z/N \longrightarrow Z/p_1^{\alpha_1} \times \ldots \times Z/p_k^{\alpha_k}$$

$$f(n) \quad = \quad (n_1, \ldots, n_k) \quad ; \quad n_j \equiv n \pmod{p_j^{\alpha_j}}$$

where the ring structure in $Z/p_1^{\alpha_1} \times \ldots \times Z/p_k^{\alpha_k}$ is given by the direct sum of the rings $Z/p_j^{\alpha_j}, 1 \leq j \leq k$.

Let E_j denote the element in $Z/p_1^{\alpha_1} \times \ldots \times Z/p_k^{\alpha_k}$ having a one in the $j-th$ coordinate and zeroes everywhere else. Let

(2.1.3) $$e_j \quad = \quad f^{-1}(E_j); \quad j = 1, \ldots, k$$

Then $\{e_j : j = 1, \ldots, k\}$ forms a system of idempotent elements in $Z/(p_1^{\alpha_1} \ldots p_k^{\alpha_k})$, that is:

(2.1.4) $$e_j^2 \quad = \quad e_j; \quad j = 1, \ldots, k$$

(2.1.5) $$e_r e_s \quad = \quad 0; \quad r \neq s$$

(2.1.6) $$\sum_{j=1}^{k} e_j \quad = \quad 1$$

The system of idempotent elements determines the inverse image of the ring isomorphism f in the following sense:

(2.1.7) $$\sigma(n_1, \ldots, n_k) \quad = \quad f^{-1}(n_1, \ldots, n_k) \quad = \quad n \iff n = \sum_{j=1}^{k} n_j e_j$$

A crucial equation derived from the above listed facts is :

(2.1.8) $$\begin{aligned} \omega^{kl} &= \omega^{\sigma(k_1,k_2)\sigma(l_1,l_2)} \\ &= \omega^{(k_1e_1+k_2e_2)(l_1e_1+l_2e_2)} \\ &= \omega^{k_1l_1e_1}\omega^{k_2l_2e_2} \end{aligned}$$

Since

(2.1.9) $$e_1 \equiv 0 \ (mod\ p_2), \quad e_2 \equiv 0 \ (mod\ p_1)$$

we get

(2.1.10) $$\omega_1 \quad = \quad \omega^{e_1} \quad = \quad [exp(\frac{2\pi i}{p_1})]^{r_1}$$

(2.1.11) $$\omega_2 \quad = \quad \omega^{e_2} \quad = \quad [exp(\frac{2\pi i}{p_2})]^{r_2}$$

for some $1 \leq r_1 \leq p_1 - 1$ and $1 \leq r_2 \leq p_2 - 1$. Therefore ω_1 and ω_2 are respectively p_1 and p_2 roots of the unity. In particular

(2.1.12) $$\sum_{k_1=1}^{p_1-1} \omega_1^{k_1} \quad = \quad \sum_{k_2=1}^{p_2-1} \omega_2^{k_2} \quad = \quad -1$$

The action of $U = U(p_1p_2)$ decomposes Z/p_1p_2 into four orbits of the form $nU = \{nu : n \in U\}$. This orbits are isomorphically mapped onto $Z/p_1 \times Z/p_2$ via σ. Precisely we have :

(2.1.13) $$0U \xrightarrow{\sigma} O_0 = \{(0,0)\}$$

(2.1.14) $$e_1U \xrightarrow{\sigma} O_1 = U(p_1) \times \{0\}$$

(2.1.15) $$e_2U \xrightarrow{\sigma} O_2 = \{0\} \times U(p_2)$$

(2.1.16) $$U \xrightarrow{\sigma} O_3 = U(p_1) \times U(p_2)$$

So each U-orbit is either a cyclic group or the direct product of two cyclic groups. Furthermore if g_1 is the generator of $U(p_1)$ and g_2 is a generator of $U(p_2)$ we can endow O_1 , O_2 and O_3 with the orders induced by the bijections:

(2.1.17) $$n \in \{0, \ldots, p_1 - 2\} \longrightarrow (g_1^n, 0) \in O_1$$

(2.1.18) $$m \in \{0, \ldots, p_2 - 2\} \longrightarrow (0, g_2^m) \in O_2$$

(2.1.19) $$(n, m) \in \{0, \ldots, p_1 - 2\} \times \{0, \ldots, p_2 - 2\} \longrightarrow (g_1^n, g_2^m) \in O_3$$

where the source sets in (2.1.17) and (2.1.18) carry their natural orders while the source set in (2.1.19) follows the natural lexicographic order.

The partition of Z/p_1p_2 into U-orbits produces the decomposition of the matrix $F(p_1p_2)$ into blocks of the form:

(2.1.20) $$M(r, s) = \left(\omega^{\sigma^{-1}(k_1,k_2)\sigma^{-1}(l_1,l_2)}\right) = \left(\omega_1^{k_1l_1}\omega_2^{k_2l_2}\right)$$

$(k_1, k_2) \in O_r$ and $(l_1, l_2) \in O_s$. Considering the above defined orders for the U-orbits, equation (2.1.20) becomes

(2.1.21) $$M(r, s) = \left(\omega_1^{k_1l_1}\right) \otimes \left(\omega_2^{k_2l_2}\right)$$

Now, according to the values of the indices r and s we have:

(2.1.22) $$k_1 = \begin{cases} 0 & \text{if} \quad \mathrm{r} = 0, 2 \\ g_1^n & \text{otherwise} \end{cases}$$

(2.1.23) $$l_1 = \begin{cases} 0 & \text{if} \quad \mathrm{s} = 0, 2 \\ g_1^{n'} & \text{otherwise} \end{cases}$$

(2.1.24) $$k_2 = \begin{cases} 0 & \text{if} \quad \mathrm{r} = 0, 1 \\ g_2^m & \text{otherwise} \end{cases}$$

(2.1.25) $$l_2 = \begin{cases} 0 & \text{if} \quad \mathrm{r} = 0, 1 \\ g_2^{m'} & \text{otherwise} \end{cases}$$

and therefore :

$$(2.1.26)\qquad (\omega_1^{k_1 l_1}) = \begin{cases} (1) \quad \text{if} \quad r = 0,2 \quad \text{and} \quad s = 0,2 \\ {}^t K_{p_1-1} \quad \text{if} \quad r = 0,2 \quad \text{and} \quad s = 1,3 \\ K_{p_1-1} \quad \text{if} \quad r = 1,3 \quad \text{and} \quad s = 0,2 \\ sc\left(\omega_1^{g_1^n}\right), 0 \le n \le p_1 - 2 \quad \text{if} \quad r = 1,3 \quad \text{and} \quad s = 1,3 \end{cases}$$

$$(2.1.27)\qquad (\omega_2^{k_2 l_2}) = \begin{cases} (1) \quad \text{if} \quad r = 0,1 \quad \text{and} \quad s = 0,1 \\ {}^t K_{p_2-1} \quad \text{if} \quad r = 0,1 \quad \text{and} \quad s = 2,3 \\ K_{p_2-1} \quad \text{if} \quad r = 2,3 \quad \text{and} \quad s = 0,1 \\ sc\left(\omega_2^{g_2^m}\right), 0 \le m \le p_2 - 2 \quad \text{if} \quad r = 2,3 \quad \text{and} \quad s = 2,3 \end{cases}$$

From formula (2.1.12) we get :

$$(2.1.28)\qquad K_{p_1-1} = sc\left(\omega_1^{g_1^n}\right)(-K_{p_1-1}) \quad 0 \le n \le p_1 - 2$$

and

$$(2.1.29)\qquad K_{p_2-1} = sc\left(\omega_2^{g_2^m}\right)(-K_{p_2-1}) \quad 0 \le m \le p_2 - 2$$

Hence the different cases shown in equations (2.1.16) and (2.1.17) are respectively expressable as :

$$(2.1.30)\qquad (\omega_1^{k_1 l_1}) = \begin{cases} (1)(1) \\ (1)\,{}^t K_{p_1-1} \\ sc\left(\omega_1^{g_1^n}\right)(-K_{p_1-1}) \\ sc\left(\omega_1^{g_1^n}\right) I_{p_1-1} \end{cases}$$

and

$$(2.1.31)\qquad (\omega_2^{k_2 l_2}) = \begin{cases} (1)(1) \\ (1)\,{}^t K_{p_2-1} \\ sc\left(\omega_2^{g_2^m}\right)(-K_{p_2-1}) \\ sc\left(\omega_2^{g_2^m}\right) I_{p_2-1} \end{cases}$$

and so, defining the following auxiliary matrices

$$B_1(r) = \begin{cases} (1) & \text{if } r = 0,2 \\ sc\left(\omega_1^{g_1^n}\right) & \text{if } r = 1,3 \end{cases} \tag{2.1.32}$$

$$B_2(r) = \begin{cases} (1) & \text{if } r = 0,1 \\ sc\left(\omega_2^{g_2^m}\right) & \text{if } r = 2,3 \end{cases} \tag{2.1.33}$$

$$A_1(r,s) = \begin{cases} (1) & \text{if } r = 0,2 \text{ and } s = 0,2 \\ {}^tKp_1 - 1 & \text{if } r = 0,2 \text{ and } s = 1,3 \\ -K_{p_1-1} & \text{if } r = 1,3 \text{ and } s = 0,2 \\ I_{p_1-1} & \text{if } r = 1,3 \text{ and } s = 1,3 \end{cases} \tag{2.1.34}$$

$$A_2(r,s) = \begin{cases} (1) & \text{if } r = 0,1 \text{ and } s = 0,1 \\ {}^tKp_2 - 1 & \text{if } r = 0,1 \text{ and } s = 2,3 \\ -K_{p_2-1} & \text{if } r = 2,3 \text{ and } s = 0,1 \\ I_{p_2-1} & \text{if } r = 2,3 \text{ and } s = 2,3 \end{cases} \tag{2.1.35}$$

we can express the blocks $M(r,s)$ as :

$$M(r,s) = B_1(r)A_1(r,s) \otimes B_2(r)A_2(r,s) = (B_1(r) \otimes B_2(r))\ [A_1(r,s) \otimes A_2(r,s)] \tag{2.1.36}$$

Let's simplify the above written formula by defining :

$$B_r = \begin{cases} (1) & \text{if } r = 0 \\ sc\left(\omega_1^{g_1^n}\right) & \text{if } r = 1 \\ sc\left(\omega_2^{g_2^m}\right) & \text{if } r = 2 \\ B_1 \otimes B_2 & \text{if } r = 3 \end{cases} \tag{2.1.37}$$

and

(2.1.38) $$A_{r,s} = A_1(r,s) \otimes A_2(r,s)$$

then

(2.1.39) $$M(r,s) = B_r A_{r,s}$$

and since the factors B_r are independent from the index s we get the following DFT factorization :

(2.1.40) $$F_U(p_1p_2) = B(p_1p_2)\, A(p_1p_2)$$

$$= \begin{pmatrix} B_0 & & & \\ & B_1 & & \\ & & B_2 & \\ & & & B_3 \end{pmatrix} \begin{pmatrix} A_{0,0} & A_{0,1} & A_{0,2} & A_{0,3} \\ A_{1,0} & A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,0} & A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,0} & A_{3,1} & A_{3,2} & A_{3,3} \end{pmatrix}$$

2.2.- 35-point even DFT

In this section we derive a fast algorithm to compute the DFT of a 35-point even sequence. The use of the factoring formulas proposed in sections 1.1 and 1.2 as well as the basic ideas whose variations will repeatedly appear in the coming sections, are highlighted. Some notational conventions adopted here will be used in the rest of this work.

We assume $p_1 = 5$ and $p_2 = 7$. According to the nomenclature adopted in section 2.1 we have :

(2.2.1) $$e_1 = 21$$

(2.2.2) $$e_2 = 15$$

The group of units is

(2.2.3) $$U = \{1, 26, 11, 6, 16, 31, 8, 33, 18, 13, 23, 3, 29, 19, 4, 34, 9, 24, 22, 12, 32, 27, 2, 17\}$$

and the U-orbits , beside U itself, are :

(2.2.4) $$0U = \{0\}$$

(2.2.5) $$21U = \{21, 28, 14, 7\}$$

(2.2.6) $$15U = \{15, 5, 25, 20, 30, 10\}$$

The elements $g_1 = 3$ and $g_2 = 5$ generate the groups of units $U(5)$ and $U(7)$ respectively. We use them in conjuction with the ring isomorphism σ to identify the U-orbits with the following ordered two-dimensional sets:

(2.2.7) $$0U \xrightarrow{\sigma} O_0 = \{(0,0)\}$$

(2.2.8) $$21U \xrightarrow{\sigma} O_1 = \{(1,0), (3,0), (4,0), (2,0)\}$$

(2.2.9) $$15U \xrightarrow{\sigma} O_2 = \{(0,1),(0,5),(0,4),(0,6),(0,2),(0,3)\}$$

(2.2.10)
$$\begin{aligned} U \xrightarrow{\sigma} O_3 = \{&(1,1),(1,5),1,4),(1,6),(1,2),(1,3),\\ &(3,1),(3,5),(3,4),(3,6),(3,2),(3,3),\\ &(4,1),(4,5),(4,4),(4,6),(4,2),(4,3),\\ &(2,1),(2,5),(2,4),(2,6),(2,2),(2,3)\} \end{aligned}$$

The ordering given to O_1,O_2 and O_3 are those established in (2.1.17) – (2.1.19). Consequently we get the blocks:

(2.2.11) $$B_1 = sc\,(\omega_1, \omega_1^3, \omega_1^4, \omega_1^2)$$

and

(2.2.12) $$B_2 = sc\,(\omega_2, \omega_2^5, \omega_2^4, \omega_2^6, \omega_2^2, \omega_2^3)\,;$$

here

(2.2.13) $$\omega_1 = [exp(\frac{2\pi i}{5})]^3 \quad \text{and} \quad \omega_2 = [\exp(\frac{2\pi \mathrm{i}}{7})]^3.$$

A 35-point sequence $x = [x(n)]$, $n \in Z/35$ is called even if it satisfies:

(2.2.14) $$x(n) = x(-n)\,,\ n \in Z/35$$

The equality :

(2.2.15) $$-1U = U$$

implies that each U-orbit is mapped onto itself by the action defined by the multiplication by -1. Therefore the restriction of x to a U-orbit contains one half of redundant data (except by the orbit 0U). Using the isomorphism σ to identify $x(n)$ and $x(\sigma(n))$, we get precisely :

(2.2.16) $$x(1,0) = x(4,0)$$

$$x(3,0) = x(2,0)$$

in x restricted to O_1,

(2.2.17)
$$x(0,1) = x(0,6)$$
$$x(0,5) = x(0,2)$$
$$x(0,4) = x(0,3)$$

in x restricted to O_2 and

(2.2.18)
$$x(1,1) = x(4,6)$$
$$x(1,5) = x(4,2)$$
$$x(1,4) = x(4,3)$$
$$x(1,6) = x(4,1)$$
$$x(1,2) = x(4,5)$$
$$x(1,3) = x(4,4)$$
$$x(3,1) = x(2,6)$$
$$x(3,5) = x(2,2)$$
$$x(3,4) = x(2,3)$$
$$x(3,6) = x(2,1)$$
$$x(3,2) = x(2,5)$$
$$x(3,3) = x(2,4)$$

in x restricted to O_3.

If x^1, x^2 and x^3 denote the restrictions of x to O_1, O_2 and O_3 respectively, then from equations (2.2.16) – (2.2.18) we get:

(2.2.19) $$x^1 = S_4^2\ x^1$$

(2.2.20) $$x^2 = S_6^3\ x^2$$

(2.2.21) $$x^3 = (S_6^3 \otimes S_4^2)\ x^3$$

Therefore proving that the matrix :

$$S(35) = \begin{pmatrix} (1) & & & \\ & S_4^2 & & \\ & & S_6^3 & \\ & & & S_4^2 \otimes S_6^3 \end{pmatrix} \tag{2.2.22}$$

commutes with A(35) and B(35) independently is equivalent to proving that in both cases the output sequence of an even sequence is also an even sequence. The proof of $B(35)S(35) = S(35)B(35)$ is an easy consequence of the following observations:

Let

$$C_1 = \begin{pmatrix} \omega_1 & \omega_1^3 \\ \omega_1^3 & \omega_1^4 \end{pmatrix} \tag{2.2.23}$$

and let

$$C_2 = \begin{pmatrix} \omega_2 & \omega_2^5 & \omega_2^4 \\ \omega_2^5 & \omega_2^4 & \omega_2^6 \\ \omega_2^4 & \omega_2^6 & \omega_2^2 \end{pmatrix} \tag{2.2.24}$$

Now for i=1,2

$$B_i = \begin{pmatrix} C_i & \tilde{C}_i \\ \tilde{C}_i & C_i \end{pmatrix} \tag{2.2.25}$$

Hence in general :

$$B_i = I_2 \otimes C_i + \tilde{I}_2 \otimes \tilde{C}_i \tag{2.2.26}$$

On the other hand, if N is an even number, the matrix $S_N^{N/2}$ is of the following general form :

$$S_N^{N/2} = \tilde{I}_2 \otimes I_{N/2} \tag{2.2.27}$$

Therefore

$$\begin{aligned} S_4^2 B_1 &= (\tilde{I}_2 \otimes I_2)(I_2 \otimes C_1 + \tilde{I}_2 \otimes \tilde{C}_1) \\ &= \tilde{I}_2 \otimes C_1 + I_2 \otimes \tilde{C}_1 \\ &= (I_2 \otimes C_1 + \tilde{I}_2 \otimes \tilde{C}_1)(\tilde{I}_2 \otimes I_2) \\ &= B_1 S_4^2 \end{aligned} \tag{2.2.28}$$

Similarly:

$$S_6^3 B_2 = B_2 S_6^3 \tag{2.2.29}$$

As for $S(35)A(35) = A(35)S(35)$, it is enough to observe that

$$S_N^{N/2}(-K_N) = -K_N \tag{2.2.30}$$

and

$$^tK_N S_N^{N/2} = {}^tK_N \tag{2.2.31}$$

It is now clear that an essential input and output data sequence for each one of $A(35)$ and $B(35)$ can be chosen to be indexed by the same fundamental region for the action $n \longrightarrow -1n$ on $Z/35$. Furthemore since -1 acts on each U-orbit the union of the fundamental regions for these actions form a fundamental region for the whole action.

We choose :

$$O_0^+ = \{(0,0)\} \tag{2.2.32}$$

$$O_1^+ = \{(1,0),(3,0)\} \tag{2.2.33}$$

$$O_2^+ = \{(0,1),(0,5),(0,4)\} \tag{2.2.34}$$

$$O_3^+ = \{(1,1),(1,5),(1,4),(1,6),(1,2),(1,3),(3,1),(3,5),(3,4),(3,6),(3,2),(3,3)\} \tag{2.2.35}$$

The fundamental arithmetic operations required to compute with essential sequences are represented in what we call a *fundamental matrix.*

We consider first the fundamental blocks in $B(35)$. For $r = 1, 2$ we have:

$$B_r = \begin{array}{c} \\ O_r^+ \\ -O_r^+ \end{array} \begin{array}{c} \begin{array}{cc} O_r^+ & -O_r^+ \end{array} \\ \begin{pmatrix} C_r & \bar{C}_r \\ \bar{C}_r & C_r \end{pmatrix} \end{array} \tag{2.2.36}$$

on the border of the matrix we have written the indexing sets of the corresponding sub-blocks. Now with respect to the output sequence the fundamental operations are represented in:

$$\begin{array}{cc} & \begin{matrix} O_r^+ & -O_r^+ \end{matrix} \\ O_r^+ & \begin{pmatrix} C_r & \bar{C}_r \end{pmatrix} \end{array} \tag{2.2.37}$$

and the elimination of input redundancies gives the fundamental block:

$$B_r^+ = \begin{matrix} O_r^+ \\ O_r^+ \end{matrix} \begin{pmatrix} \\ C_r + \bar{C}_r \end{pmatrix} \tag{2.2.38}$$

In particular:

$$B_1^+ = \begin{pmatrix} \omega_1 + \omega_1^4 & \omega_1^3 + \omega_1^2 \\ \omega_1^3 + \omega_1^2 & \omega_1^4 + \omega_1 \end{pmatrix} = sc(\omega_1 + \omega_1^4, \omega_1^3 + \omega_1^4) \tag{2.2.39}$$

and

$$B_2 = sc(\omega_2 + \omega_2^6, \omega_2^5 + \omega_2^2, \omega_2^4 + \omega_2^3) \tag{2.2.40}$$

The fundamental matrix derived from B_3 presents a different structure. The partition of O_3 as $O_3^+ \cup -O_3^+$ gives:

$$\begin{array}{cc} & \begin{matrix} O_3^+ & -O_3^+ \end{matrix} \\ \begin{matrix} O_3^+ \\ -O_3^+ \end{matrix} & \begin{pmatrix} C_1 \otimes B_2 & \bar{C}_1 \otimes \bar{B}_2 \\ \bar{C}_1 \otimes \bar{B}_2 & C_1 \otimes B_2 \end{pmatrix} \end{array} \tag{2.2.41}$$

This matrix is similar to B_3 and the fundamental block derived from it clearly equals the one derived from B_3. This block is

$$B_3^+ = \begin{matrix} O_3^+ \\ O_3^+ \end{matrix} \begin{pmatrix} \\ C_1 \otimes B_2 + \bar{C}_1 \otimes B_2 \end{pmatrix} \tag{2.2.42}$$

B_3^+ is a $(2,6)$-Hankel matrix. Since B_2 and $\bar{B}_2$ are skew-circulant matrices, the 6×6 blocks in the $(2,6)$-block decomposition of B_3^+ are skew-circulant and so both Propositions 1 and 2 can be applied. Proposition 1 gives

$$B_3^+ = [I_2 \otimes F(6)^{-1}][M(2) \otimes I_6] \Delta [L(2) \otimes I_6][I_2 \otimes F(6)^{-1}] \tag{2.2.43}$$

Notice that Δ is a 18×18 diagonal matrix. Proposition 2 yields

$$B_3^+ = P(B_1 \otimes I_3)P(I_2 \otimes B_2) \tag{2.2.44}$$

where P is the permutation matrix $P(2,2) \otimes I_3$. If D_1 and D_2 are the diagonal matrices such that: $B_1 = F(4)\, D_1\, F(4)$ and $B_2 = F(6) D_2 F(6)$ then we get

$$B_3^+ = P[(F(4)^{-1} \otimes I_3)\,(D_1 \otimes I_3)\,(F(4)^{-1} \otimes I_3)]\,P\,[(I_2 \otimes F(6)^{-1})\,(I_2 \otimes D_2)\,(I_2 \otimes F(6)^{-1})] \tag{2.2.45}$$

Iin this formula all the factors are 12×12 matrices.

We compute now the fundamental blocks in $A(35)$. Originally

$$A(35) = \begin{pmatrix} (1) & {}^tK_4 & {}^tK_6 & {}^tK_4 \otimes {}^t K_6 \\ -K_4 & I_4 & -K_4 \otimes K_6 & I_4 \otimes {}^t K_6 \\ -K_6 & {}^tK_4 \otimes (-K_6) & I_6 & {}^tK_4 \otimes I_6 \\ K_4 \otimes K_6 & I_4 \otimes (-K_6) & (-K_4) \otimes I_6 & I_4 \otimes I_6 \end{pmatrix} \tag{2.2.46}$$

In order to get a better structured fundamental matrix we replade the fundamental set O_3^+ by another fundamental set:

$$O_3' = \{(1,1),(1,5),(1,4),(3,1),(3,5)(3,4),(4,1),(4,5),(4,6)(4,4),(2,1),2,5),(2,4)\} \tag{2.2.47}$$

Notice that if x' denotes the restriction of a symmetric sequence x to O_3' then

$$x^3 = (P(2,2) \otimes I_3)\ \mathrm{x}' \tag{2.2.48}$$

Restricting the row indexing set of $A(35)$ to $O_0^+ \cup O_1^+ \cup O_2^+ \cup O_3'$ yields

$$\begin{pmatrix} (1) & {}^tK_4 & {}^tK_6 & {}^tK_4 \otimes {}^tK_6 \\ -K_2 & (1\,0) \otimes I_2 & -K_2 \otimes {}^tK_6 & (1\ 0) \otimes I_2 \otimes {}^t K_6 \\ -K_3 & -{}^tK_4 \otimes K_3 & (1\ 0) \otimes I_3 & {}^tK_4 \otimes (1\ 0) \otimes I_3 \\ K_4 \otimes K_3 & -I_4 \otimes K_3 & -K_4 \otimes (1\ 0) \otimes I_3 & I_4 \otimes (1\ 0) \otimes I_3 \end{pmatrix} \tag{2.2.49}$$

$$= \begin{pmatrix} \begin{pmatrix} (1) & {}^tK_4 \\ -K_2 & (1\,0)\otimes I_2 \end{pmatrix} & \begin{pmatrix} (1) & {}^tK_4 \\ -K_2 & (1\,0)\otimes I_2 \end{pmatrix} \otimes {}^tK_6 \\ \begin{pmatrix} (1) & {}^tK_4 \\ -K_4 & I_4 \end{pmatrix} \otimes (-K_3) & \begin{pmatrix} (1) & {}^tK_4 \\ -K_4 & I_4 \end{pmatrix} \otimes (1\,0)\otimes I_3 \end{pmatrix}$$

$$= \begin{pmatrix} \begin{pmatrix} (1) & {}^tK_4 \\ -K_2 & (1\,0)\otimes I_2 \end{pmatrix} & \\ & \begin{pmatrix} (1) & {}^tK_4 \\ -K_4 & I_4 \end{pmatrix} \otimes I_3 \end{pmatrix} \begin{pmatrix} I_5 & I_5 \otimes {}^t K_6 \\ I_5 \otimes (-K_3) & I_5 \otimes (1\,0)\otimes I_3 \end{pmatrix}$$

$$= M_1 M_2$$

The row indexing set of M_1 is already restricted to a fundamental region but its column indexing set is: $O_0 \cup O_1 \cup O_2^+ \cup O_3'$, hence the block indexed by O_1 is yet to be reduced. This reduction only affects :

$$\begin{pmatrix} (1) & {}^tK_4 \\ -K_2 & (1\,0)\otimes I_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{2.2.50}$$

which produces the fundamental block:

$$\begin{pmatrix} (1) & 2^tK_2 \\ -K_2 & I_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \tag{2.2.51}$$

The fundamental matrix derived from M_1 is

$$M_1^+ = \begin{pmatrix} \begin{pmatrix} 1 & 2 & 2 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{pmatrix} \tag{2.2.52}$$

The row indexing set of M_2 is $O_0^+ \cup O_1 \cup O_2^+ \cup O_3'$, its restriction to $O_0 \cup O_1^+ \cup O_2^+ \cup O_3'$ produces

$$\begin{pmatrix} \begin{pmatrix} 1 & \\ & (1\,0)\otimes I_2 \end{pmatrix} & \begin{pmatrix} 1 & \\ & (1\,0)\otimes I_2 \end{pmatrix} \otimes {}^t K_6 \\ I_5 \otimes K_3 & I_5 \otimes (1\,0)\otimes I_3 \end{pmatrix} \tag{2.2.53}$$

The column indexing set of this matrix has not been reduced yet. Consider first the column block indexed by O_1

$$
\begin{array}{c}
\begin{matrix} (1,0) & (3,0) & (4,0) & (2,0) \end{matrix} \\
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
-K_3 & & & \\
 & -K_3 & & \\
 & & -K_3 & \\
 & & & -K_3
\end{pmatrix}
\end{array}
\tag{2.2.54}
$$

The fundamental block derived from (2.2.54) is:

$$
\begin{array}{c}
\begin{matrix} (1,0) & (3,0) \end{matrix} \\
\begin{pmatrix}
0 & 0 \\
1 & 0 \\
0 & 1 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
-K_3 & \\
 & -K_3 \\
-K_3 & \\
 & -K_3
\end{pmatrix}
\end{array}
\tag{2.2.55}
$$

The block whose column is indexed by O_2 is of the form

(2.2.56)

$$\begin{array}{c} \begin{matrix} (0,1) & (0,5) & (0,4) & (0,6) & (0,2) & (0,3) \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

So the fundamental block is of the form :

(2.2.57)

$$\begin{array}{c} \begin{matrix} (0,1) & (0,5) & (0,4) \end{matrix} \\ \begin{pmatrix} 2 & 2 & 2 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Finally the block corresponding to the column indexing set O_3 is of the form :

(2.2.58)

$$\begin{array}{c} \{1\}\times U(6) \quad \{3\}\times U(6) \quad \{4\}\times U(6) \quad \{2\}\times U(6) \\ \begin{pmatrix} 0\ldots & \ldots & \ldots & \ldots 0 \\ {}^tK_6 & & & \\ & {}^tK_6 & & \\ 0\ldots & \ldots & \ldots & \ldots 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0\ldots & \ldots & \ldots & \ldots 0 \\ (1\ 0)\otimes I_3 & & & \\ & (1\ 0)\otimes I_3 & & \\ & & (1\ 0)\otimes I_3 & \\ & & & (1\ 0)\otimes I_3 \end{pmatrix} \end{array}$$

The fundamental block is obtained by the additions of the sub-blocks indexed in $\{n\}\times\{1,5,4\}$ plus the sub-blocks indexed by $\{-n\}\times\{6,2,3\}$. The result is the block with column indexing set O_3'

(2.2.59)

$$\begin{pmatrix} 0\ldots & \ldots & \ldots & \ldots 0 \\ {}^tK_3 & & {}^tK_3 & \\ & {}^tK_3 & & {}^tK_3 \\ 0\ldots & \ldots & \ldots & \ldots 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0\ldots & \ldots & \ldots & \ldots 0 \\ I_3 & & & \\ & I_3 & & \\ & & I_3 & \\ & & & I_3 \end{pmatrix}$$

Summarizing, the final form of the fundamental matrix in M_2 is:

(2.2.60)

$$M_2^+ = \begin{pmatrix} I_3 & \begin{pmatrix} 2 & \\ & I_2 I_2 \end{pmatrix} \\ \begin{pmatrix} 1 & \\ & I_2 \\ & I_2 \end{pmatrix} \otimes (-K_3) & I_5 \otimes I_3 \end{pmatrix}$$

2.3.- p_1p_2-point even DFT

The generalization of the 35-point even DFT to a p_1p_2 -point even DFT follows after the the observation of a few facts.

Consider first a symmetric sequence x defined in Z/p_1p_2, p_1 and p_2 two different primes, and let x^0, x^1, x^2 and x^3 denote the restrictions of x to O_0, O_1, O_2 and O_3, that is:

$$x^0 = [x(0,0)] \tag{2.3.1}$$

$$x^1 = [x(g_1^n,0)] \quad 0 \le n \le p_1 - 2 \tag{2.3.2}$$

$$x^2 = [x(0,g_2^m)] \quad 0 \le m \le p_2 - 2 \tag{2.3.3}$$

$$x^3 = [x(g_1^n,g_2^m)] \quad 0 \le n \le p_1 - 2,\ 0 \le m \le p_2 - 2 \tag{2.3.4}$$

the condition of x being symmetric is equivalent to the following conditions on the restricted sequences

$$x(g_1^n,0) = x(g_1^{n+\frac{p_1-1}{2}},0) \quad 0 \le n \le p_1 - 2 \tag{2.3.5}$$

$$x(0,g_2^m) = x(0,g_2^{m+\frac{p_2-1}{2}}) \quad 0 \le m \le p_2 - 2 \tag{2.3.6}$$

$$x(g_1^n,g_2^m) = x(g_1^{n+\frac{p_1-1}{2}},g_2^{m+\frac{p_2-2}{2}}) \quad 0 \le n \le p_1 - 2 \quad \text{and} \quad 0 \le \mathrm{m} \le \mathrm{p}_2 - 2 \tag{2.3.7}$$

Now, in general, for an even number N and an N-point sequence $y = [y(n)]$, the action on y of the shift operator raised to the $\frac{N}{2}$ power is given by:

$$[y(n+\frac{N}{2})] = S_N^{\frac{N}{2}}\,[y(n)] \tag{2.3.8}$$

and so the equations:

$$x^1 = S_{p_1-1}^{\frac{p_1-1}{2}}\,x^1 \tag{2.3.9}$$

(2.3.10) $$x^2 = S_{p_2-1}^{\frac{p_2-1}{2}} x^2$$

(2.3.11) $$x^3 = (S_{p_1-1}^{\frac{p_1-1}{2}} \otimes S_{p_2-1}^{\frac{p_2-1}{2}}) x^3$$

are the generalization of equations (2.2.16) – (2.2.18).

The fact that the operator:

(2.3.12) $$S(p_1p_2) = \begin{pmatrix} (1) & & & \\ & S_{p_1-1}^{\frac{p_1-1}{2}} & & \\ & & S_{p_2-1}^{\frac{p_2-1}{2}} & \\ & & & S_{p_1-1}^{\frac{p_1-1}{2}} \otimes S_{p_2-1}^{\frac{p_2-1}{2}} \end{pmatrix}$$

commutes with $B(p_1p_2)$ and $A(p_1p_2)$ follows from the general arguments already given in section 2.2 .

The fundamental regions for the action of -1 on the sets O_r r=1,2,3 are described as

(2.3.13) $$O_1^+ = U(p_1)^+ \times \{0\}$$

(2.3.14) $$O_2^+ = \{0\} \times U(p_2)^+$$

(2.3.15) $$O_3^+ = U(p_1)^+ \times U(p_2)$$

where

(2.3.16) $$U(p_1)^+ = \{g_1^n : 0 \leq n < \frac{p_1 - 1}{2}\}$$

(2.3.17) $$U(p_2)^+ = \{g_2^m : 0 \leq m < \frac{p_2 - 1}{2}\}$$

Let C_r, $r = 1, 2$ be the sub-block in B_r obtained by restricting the column and row indexing sets of B_r to O_r. This is :

(2.3.18) $$C_r = (\omega_r^{g_r^{n+m}}) \qquad 0 \leq n, m < \frac{p_r - 1}{2}$$

Then

$$(2.3.19) \qquad B_r = \begin{matrix} \\ O_r^+ \\ -O_r^+ \end{matrix} \begin{matrix} \begin{matrix} O_r^+ & -O_r^+ \end{matrix} \\ \begin{pmatrix} C_r & \bar{C}_r \\ \bar{C}_r & c_r \end{pmatrix} \end{matrix}$$

and so the fundamental derived from B_r is

$$(2.3.20) \qquad B_r^+ = \begin{matrix} \\ O_r^+ \end{matrix} \begin{matrix} \begin{matrix} O_r^+ \end{matrix} \\ \begin{pmatrix} C_r + \bar{C}_r \end{pmatrix} \end{matrix} = \left(\omega_r^{g_r^{n+m}} + \omega_r^{-g_r^{n+m}}\right)$$

In general an $N \times N$ Hankel matrix $A = (a(k,l))$ is skew-circulant if it satisfies :

$$(2.3.21) \qquad a(k,l) = a(k',l'), \quad \text{whenever} \quad \mathrm{k'+l'+N = k+l}$$

hence, to show the skew-circulancy of $B_r^+ \quad r = 1,2$, we take $n+m = n'+m'+(p_r - 1/2)$ and compare the (n,m) and (n',m') entries. Since

$$(2.3.22) \qquad g_r^{(p_r-1)/2} = -1$$

we have that

$$(2.3.23) \qquad \omega_r^{g_r^{n+m}} = \omega_r^{-g_r^{n'+m'}}$$

and therefore the (n,m) entry $\omega_r^{g_r^{n+m}} + \omega_r^{-g_r^{n+m}}$ is trivially equal to the (n',m') entry.

As for the structure of B_3^+ we consider:

$$(2.3.24) \qquad B_3 =$$

$$\begin{pmatrix} I_{p_1-1/2} \otimes I_{p_2-1} & \\ & I_{p_1-1/2} \otimes S_{p_2-1}^{\frac{p_2-1}{2}} \end{pmatrix} \begin{pmatrix} C_1 \otimes B_2 & \bar{C}_1 \otimes \bar{B}_2 \\ \bar{C}_1 \otimes \bar{B}_2 & C_1 \otimes B_2 \end{pmatrix} \begin{pmatrix} I_{p_1-1/2} \otimes I_{p_2-1} & \\ & I_{p_1-1/2} \otimes S_{p_2-1}^{\frac{p_2-1}{2}} \end{pmatrix}$$

the factor:

$$(2.3.25) \qquad \begin{array}{c} \\ O_3^+ \\ -O_3^+ \end{array} \begin{array}{c} \begin{array}{cc} O_3^+ & -O_3^+ \end{array} \\ \begin{pmatrix} C_1 \otimes B_2 & \bar{C}_1 \otimes \bar{B}_2 \\ \bar{C}_1 \otimes \bar{B}_2 & C_1 \otimes B_2 \end{pmatrix} \end{array}$$

produces the same fundamental matrix as B_3 and that is :

$$(2.3.26) \qquad \begin{array}{rcl} & & O_3^+ \\ B_3^+ & = & O_3^+ \left(C_1 \otimes B_2 + \bar{C}_1 \otimes B_2 \right) \end{array}$$

this matrix is a $(\frac{p_1-1}{2}, p_2 - 1)$-Hankel matrix with skew-circulant $(p_2 - 1) \times (p_2 - 1)$ blocks and so it satisfies the hypothesis of either one of proposition 1 or proposition 2.

3.- Two-dimensional symmetric sequences

This section is mainly dedicated to show the use of the factorization formulas proved in section 1 in the design of fast algorithms computing the two-dimensional DFT of certain classes of symmetric sequences.

A new DFT matrix representation based on the action of a subgroup of the group of units is introduced. This new DFT representation is motivated by the fact that even though the U-orbits are mapped onto U-orbits by the automorphism with respect to which the sequences are invariant, the group of units does not provide the fundamental matrices with any computationally desirable structure.

3.1.- Sequences invariant under $\phi(n_1, n_2) = (-n_1, n_2)$

The two-dimensional N-point discrete Fourier transform is the operator acting on the space of N^2-point complex sequences represented by

$$F(N:2) = (\omega^{<\vec{m},\vec{n}>}) \tag{3.1.1}$$

where $<,>$ denotes the usual dot product and $\vec{m}$ and $\vec{n}$ range over $Z/N \times Z/N$.

The set $Z/N \times Z/N$ is endowed with the ring structure of the direct sum of its components and so its group of units is $U = U(N) \times U(N)$. As before, we consider $N = p_1p_2$, p_1 and p_2 two different primes. The U-orbits on $Z/p_1p_2 \times Z/p_1p_2$ are subsets of the form of

$$aU(p_1p_2) \times bU(p_1p_2) \tag{3.1.2}$$

where a and b are either 0, or the idempotents e_1, e_2 or 1. Using the isomorphism induced by the chinese remainder theorem each U-orbit is identified with a set of the form:

$$O_i \times O_j \tag{3.1.3}$$

$0 \leq i, j \leq 3$. The DFT blocks produced by the partition of the indexing ring $Z/p_1p_2 \times Z/p_1p_2$ into U-orbits are of the following general form

$$M(r_1, r_2, s_1, s_2) = (\omega^{m_1n_1}\omega^{m_2n_2})$$

$$= (\omega^{m_1n_1})(\omega^{m_2n_2}) \tag{3.1.4}$$

$$= M(r_1, s_1) \otimes M(r_2, s_2)$$

where $\vec{m} = (m_1, m_2) \in O_{r_1} \times O_{r_2} \quad \vec{n} = (n_1, n_2) \in O_{s_1} \times O_{s_2}$. Now:

$$M(r_1, r_2, s_1, s_2) = B_{r_1} A_{r_1,s_1} \otimes B_{r_2} A_{r_2 s_2}$$

(3.1.5)

$$= (B_{r_1} \otimes B_{r_2})\,(A_{r_1,s_1} \otimes A_{r_2,s_2})$$

yields the matrix representation of the two-dimensional DFT :

$$F_U(p_1p_2 : 2) = block - diag(B_{r_1} \otimes B_{r_2})\, block(A_{r_1,s_1} \otimes A_{r_2,s_2})$$

(3.1.6)

$$= B(p_1p_2 : 2)\, A(p_1p_2 : 2)$$

$0 \leq r_1, r_2, s_1, s_2 \leq 3$.

We will consider the elimination of redundant computations induced on $F_U(p_1p_2 : 2)$ by an input sequence satisfying :

(3.1.7) $$x(n_1, n_2) = x(-n_1, n_2) = x(\phi(n_1, n_2))$$

$(n_1, n_2) \in Z/p_1p_2 \times Z/p_1p_2$. Such a sequence will be called ϕ-symmetric. The automorphism ϕ acts on each U-orbit mapping

(3.1.8) $$O_i \times O_j \xrightarrow{\phi} -O_i \times O_j$$

hence a fundamental region for the ϕ-action on $Z/p_1p_2 \times Z/p_1p_2$ is given by the set

(3.1.9) $$\bigcup_{0 \leq i,j \leq 3} O_i^+ \times O_j$$

Let's denote by x^{ij} the restriction of x to $O_i \times O_j$ and let

(3.1.10) $$S(i) = \begin{cases} (1) & \text{if} \quad i = 0 \\ S_{p_1-1}^{\frac{p_1-1}{2}} & \text{if} \quad i = 1 \\ S_{p_2-1}^{\frac{p_2-1}{2}} & \text{if} \quad i = 2 \\ S(1) \otimes S(2) & \text{if} \quad i = 3 \end{cases}$$

(3.1.11)
$$I(i) = \begin{cases} (1) & \text{if} \quad i = 0 \\ I_{p_1-1} & \text{if} \quad i = 1 \\ I_{p_2-1} & \text{if} \quad i = 2 \\ I_{(p_1-1)(p_2-1)} & \text{if} \quad i = 3 \end{cases}$$

then x is ϕ-symmetric, for every $0 \leq i, j \leq 3$ if and only if:

(3.1.12)
$$x^{ij} \quad = \quad (S(i) \otimes I(j))\, x^{ij}$$

Now using results obtained in section 2

(3.1.13)
$$[S(r_1) \otimes I(r_2)]\, [A_{r_1,s_1} \otimes A_{r_2,s_2}] = [A_{r_1,s_1} \otimes A_{r_2,s_2}]\, [S(s_1) \otimes I(s_2)]$$

and

(3.1.14)
$$[S(r_1) \otimes I(r_2)]\, [B_{r_1} \otimes B_{r_2}] = [B_{r_1} \otimes B_{r_2}]\, [S(r_1) \otimes I(r_2)]$$

This proves that both of $B(p_1p_2 : 2)$ and $A(p_1p_2 : 2)$ preserve ϕ-symmetric sequences.

In order to get the fundamental blocks derived from $B(p_1p_2 : 2)$ we consider first the matrices of the form $B_{r_1} \otimes B_{r_2}$ with $0 \leq r_1 \leq 2$ and $0 \leq r_2 \leq 3$. The general form of these blocks is

(3.1.15)
$$\begin{array}{c} \\ O_{r_1}^+ \times O_{r_2} \\ (-O_{r_1}^+) \times O_{r_2} \end{array} \begin{array}{c} \begin{array}{cc} O_{r_1}^+ \times O_{r_2} & (-O_{r_1}^+) \times O_{r_2} \end{array} \\ \begin{pmatrix} C_{r_1} \otimes B_{r_2} & \tilde{C}_{r_1} \otimes B_{r_2} \\ \tilde{C}_{r_1} \otimes B_{r_2} & C_{r_1} \otimes B_{r_2} \end{pmatrix} \end{array}$$

Hence the fundamental blocks are of the form

(3.1.16)
$$\begin{array}{c} \\ O_{r_1} \times O_{r_2} \end{array} \begin{array}{c} \begin{array}{c} O_{r_1}^+ \times O_{r_2} \end{array} \\ \left((C_{r_1} + \tilde{C}_{r_1}) \otimes B_{r_2} \right) \end{array} \quad = \quad B_{r_1}^+ \otimes B_{r_2}$$

If $r_1 = 3$ then the original block is of the form

$$
\begin{array}{c} \\ O_3^+ \times O_r \\ (-O_3^+) \times O_r \end{array}
\begin{array}{c}
\begin{array}{cc} O_3^+ \times O_r & (-O_3^+) \times O_r \end{array} \\
\begin{pmatrix} C_1 \otimes B_2 \otimes B_r & \bar{C}_1 \otimes \bar{B}_2 \otimes B_r \\ \bar{C}_1 \otimes \bar{B}_2 \otimes B_r & C_1 \otimes B_2 \otimes B_r \end{pmatrix}
\end{array}
\tag{3.1.17}
$$

and so the general form of the fundamental blocks is

$$
\begin{array}{c} \\ O_3 \times O_r \end{array}
\begin{array}{c}
\begin{array}{c} O_3 \times O_r \end{array} \\
\left([C_1 \otimes B_2 + \bar{C}_1 \otimes \bar{B}_2] \otimes B_r \right)
\end{array}
= \quad B_3^+ \otimes B_r
\tag{3.1.18}
$$

In order to compute the fundamental blocks derived from $A(p_1p_2 : 2)$ we consider the partition of each matrix $A_{k,l}$ as:

$$
A_{k,l} = \begin{array}{c}
\begin{array}{cc} O_l^+ & (-O_l^+) \end{array} \\
\begin{array}{c} O_k^+ \\ (-O_k^+) \end{array}
\begin{pmatrix} A_{k,l}^1 & A_{k,l}^2 \\ A_{k,l}^3 & A_{k,l}^4 \end{pmatrix}
\end{array}
\tag{3.1.19}
$$

for $k, l \neq 0$ and

$$
A_{k,0} = \begin{array}{c}
\begin{array}{c} O_0^+ \end{array} \\
\begin{array}{c} O_k^+ \\ -O_k^+ \end{array}
\begin{pmatrix} A_{k,0}^1 \\ A_{k,0}^3 \end{pmatrix}
\end{array}
\tag{3.1.20}
$$

if $l = 0$ and $k \neq 0$ and

$$
A_{0,l} = O_0^+ \begin{array}{c}
\begin{array}{cc} O_l^+ & -O_l^+ \end{array} \\
\begin{pmatrix} A_{0,l}^1 & A_{0,l}^2 \end{pmatrix}
\end{array}
\tag{3.2.21}
$$

if $k = 0$ but $l \neq 0$

The general form of the fundamental blocks is now clearly seen to be

$$
\begin{cases} (A_{r_1,s_1}^1 + A_{r_1,s_1}^2) \otimes A_{r_2,s_2} & \text{if} \quad s_1 \neq 0 \\ A_{r_1,0}^1 \otimes A_{r_2,s_2} & \text{otherwise} \end{cases}
\tag{3.1.22}
$$

3.2.-**Sequences invariant under $\psi(n_1, n_2) = (-n_1, -n_2)$**

For a ψ-invariant or ψ-symmetric sequence we mean a $(p_1p_2)^2$-point sequence satisfying:

$$x(n_1, n_2) \quad = \quad x(\psi(n_1, n_2)) \quad = \quad x(-n_1, -n_2) \tag{3.2.1}$$

The automorphism ψ maps each of the sets $O_i \times O_j$ onto itself. This mapping is described by

$$O_i \times O_j \xrightarrow{\psi} (-O_i) \times (-O_j) \tag{3.2.2}$$

A ψ-fundamental region on $Z/p_1p_2 \times Z/p_1p_2$ is given by the union of the ψ-fundamental regions on each of the sets $O_i \times O_j$. These fundamental regions are

$$\begin{cases} O_0 \times O_j^+ & \text{if} \quad 0 \leq \mathrm{j} \leq 3 \\ O_i^+ \times O_j & \text{if} \quad 1 \leq \mathrm{i} \leq 3 \quad \text{and} \quad 0 \leq \mathrm{j} \leq 3 \end{cases} \tag{3.2.3}$$

As before, a ψ-symmetric sequence is characterized by its invariance under the action of an operator. Indeed: a sequence x is

ψ-symmetric, if and only if:

$$(S(i) \otimes S(j))\, x^{ij} \quad = \quad x^{ij} \tag{3.2.4}$$

$S(k)$ and x^{ij} as defined in section 3.1 .

Using arguments already invoked in previous sections we conclude that the operator:

$$S' \quad = \quad block - diag(S(i) \otimes S(j)) \tag{3.2.5}$$

commutes with both of $B(p_1p_2 : 2)$ and $A(p_1p_2 : 2)$. Therefore we derive our fundamental matrices from the blocks of $B(p_1p_2 : 2)$ and $A(p_1p_2 : 2)$ independently.

From $B(p_1p_2 : 2)$ we get

$$\begin{cases} B_j^+ & \text{if} \quad 0 \leq \mathrm{j} \leq 3 \quad \text{and} \quad \mathrm{i} = 0 \\ B_i^+ \otimes B_j & \text{if} \quad 1 \leq \mathrm{i} \leq 3 \quad \text{and} \quad 0 \leq \mathrm{j} \leq 3 \end{cases} \tag{3.2.6}$$

and in $A(p_1p_2 : 2)$ we find

$$
\begin{cases}
A^1_{k,l} + A^2_{k,l} & \text{if} \quad l = k = 0 \\
(A^1_{k,l} + A^2_{k,l}) \otimes A_{i,j} & \text{if} \quad k \neq 0 \quad \text{and} \quad l \neq 0 \\
A^1_{k,0} \otimes \begin{pmatrix} A^1_{i,j} + A^2_{i,j} \\ A^3_{i,j} + A^4_{i,j} \end{pmatrix} & \text{if} \quad l = 0 \\
(A^1_{0,l} + A^2_{0,l}) \otimes \begin{pmatrix} A^1_{i,j} & A^2_{i,j} \end{pmatrix} & \text{if} \quad k = 0
\end{cases}
\tag{3.2.7}
$$

3.3.- Another DFT matrix representation

In all the cases so far examined the action of the lexicographically ordered group of units provided a DFT representation suitable for the elimination of redundancies induced by the corresponding class of input sequences. The fact that the homomorphism with respect to which the sequence was invariant, mapped U-orbits onto U-orbits was clearly a necessary condition for the fundamental blocks to be either skew-circulant or tractable by Propositions 1 or 2. In this section we deal with an automorphism for which the above mentioned condition is not sufficient forcing so the presentation of a DFT matrix based on a finer action. An important feature of this new DFT representation is the fact that as well as in the previous ones, it also factors as the product of a block diagonal matrix times an integral matrix.

The automorphism of $Z/p_1p_2 \times Z/p_1p_2$ that motivates our new DFT matrix representation is

$$\xi(n_1, n_2) = (n_2, n_1) \quad n_1, n_2 \in Z/p_1p_2 \tag{3.3.1}$$

We first illustrate the deficiencies of the fundamental blocks derived from $F_U(p_1p_2 : 2)$ by considering the block in $F_U(p_1p_2)$ indexed by the U-orbit

$$e_1U(p_1p_2) \times e_1U(p_1p_2) \tag{3.3.2}$$

with $e_1 = 21$, $p_1 = 5$ and $p_2 = 7$. Through the chinese remainder theorem this orbit is identified with the cartesian product

$$U(5) \times \{0\} \times U(5) \times \{0\} = O_1 \times O_1 \tag{3.3.3}$$

The group $U(5)$ is ordered following the natural order of the powers of its generator: 3. (See (2.1.17)). Hence, we get:

$$U(5) = \{1, 3, 4, 2\} \tag{3.3.4}$$

The automorphism ξ acts on $O_1 \times O_1$. A ξ-fundamental region is

$$\begin{aligned} &\{(1,0,1,0),(1,0,3,0),(1,0,4,0),(1,0,2,0),\\ &(3,0,3,0),(3,0,4,0),(3,0,2,0),\\ &(4,0,4,0),(4,0,2,0),(2,0,2,0)\} \end{aligned} \tag{3.3.5}$$

This set is not expressable in terms of O_1^+ or O_1 as required to get well structured fundamental blocks. A way around this difficulty is provided by the subgroup of U

$$G = \{(3^n, 5^m, 3^n, 5^m) : 0 \leq n \leq 3,\ 0 \leq m \leq 5\} \tag{3.3.6}$$

G is fixed under the action of ξ, this is: $\xi(g) = g$ for every $g \in G$.

Consider the G-orbits

$$(1,0,1,0)G = \{(1,0,1,0),(3,0,3,0),(4,0,4,0),(2,0,2,0)\} \tag{3.3.7}$$

$$(1,0,3,0)G = \{(1,0,3,0),(3,0,4,0),(4,0,2,0),(2,0,1,0)\} \tag{3.3.8}$$

$$(1,0,4,0)G = \{(1,0,4,0),(3,0,2,0),(4,0,1,0),(2,0,3,0)\} \tag{3.3.9}$$

$$(1,0,2,0)G = \{(1,0,2,0),(3,0,1,0),(4,0,3,0),(2,0,4,0)\} \tag{3.3.10}$$

It is worth noticing that $(1,0,1,0)G$ is a cyclic group as well as the set:

$$\Gamma = \{(1,0,1,0),(1,0,3,0),(1,0,4,0),(1,0,2,0)\} \tag{3.3.11}$$

Indeed they are both isomorphic to $U(5)$ and there direct product is:

$$O_1 \times O_1 = \bigcup_{a \in \Gamma} aG = \Gamma G \tag{3.3.12}$$

The way ξ maps G-orbits onto G-orbits in $O_1 \times O_1$ as well as the way the orbits are affected by the ξ action can be described through the values of ξ in Γ. Consider

$$\xi(1,0,1,0) = (1,0,1,0) \quad , \tag{3.3.13}$$

$$\xi(1,0,3,0) = (3,0,1,0) = (1,0,2,0)(3,0,3,0) \tag{3.3.14}$$

and

$$\xi(1,0,4,0) = (4,0,1,0) = (1,0,4,0)(4,0,4,0) \tag{3.3.15}$$

In these equations we have factorized each ξ image as the product of an element in Γ times an element in $(1,0,1,0)G$. By looking at this expressions we conclude that the orbit $(1,0,1,0)G$ is fixed by ξ, the orbit $(1,0,3,0)G$ is mapped onto $(1,0,2,0)G$ and the orbit $(1,0,4,0)G$ gets mapped onto itself via

$$(1,0,4,0)G \xrightarrow{\xi} -1(1,0,4,0)G \tag{3.3.16}$$

Let

$$G_1^+ = \{(3^n, 5^m, 3^n, 5^m) : 0 \leq n \leq 1, \quad 0 \leq m \leq 5\} \tag{3.3.17}$$

From the above shown analysis, it follows that the union of the sets

$$(1,0,1,0)G, \quad (1,0,3,0)G, \quad (1,0,4,0)G_1^+ \tag{3.3.18}$$

forms a ξ-fundamental region. The first two sets in (3.3.18) are of the type of O_1 while the last one is structured as O_1^+.

Before stating the general form of the DFT representation based on the G-action, we want to use the already computed G-orbits to illustrate the factoring technique that allows its expression as the product of a complex block-diagonal matrix times an integral one.

The matrix of dot products among the elements in the G-orbits is:

(3.3.19)

	$(1,1)(3,3)(4,4)(2,2)$	$(1,3)(3,4)(4,2)(2,1)$	$(1,4)(3,2)(4,1)(2,3)$	$(1,2)(3,1)(4,3)(2,4)$
$(1,1)$	2 1 3 4	4 2 1 3	0 0 0 0	3 4 2 1
$(3,3)$	1 3 4 2	2 1 3 4	0 0 0 0	4 2 1 3
$(4,4)$	3 4 2 1	1 3 4 2	0 0 0 0	2 1 3 4
$(2,2)$	4 2 1 3	3 4 2 1	0 0 0 0	1 3 4 2
$(1,3)$	4 2 1 3	0 0 0 0	3 4 2 1	2 1 3 4
$(3,4)$	2 1 3 4	0 0 0 0	4 2 1 3	1 3 4 2
$(4,2)$	1 3 4 2	0 0 0 0	2 1 3 4	3 4 2 1
$(2,1)$	3 4 2 1	0 0 0 0	1 3 4 2	4 2 1 3
$(1,4)$	0 0 0 0	3 4 2 1	2 1 3 4	4 2 1 3
$(3,2)$	0 0 0 0	4 2 1 3	1 3 4 2	2 1 3 4
$(4,1)$	0 0 0 0	2 1 3 4	3 4 2 1	1 3 4 2
$(2,3)$	0 0 0 0	1 3 4 2	4 1 2 3	3 4 2 1
$(1,2)$	3 4 2 1	2 1 3 4	4 2 1 3	0 0 0 0
$(3,1)$	4 2 1 3	1 3 4 2	2 1 3 4	0 0 0 0
$(4,3)$	2 1 3 4	3 4 2 1	1 3 4 2	0 0 0 0
$(2,4)$	1 3 4 2	4 2 1 3	3 4 2 1	0 0 0 0

Hence the DFT block indexed on this G-orbits admits the decomposition:

(3.3.20)
$$\begin{pmatrix} B_1S_4 & B_1S_4^2 & B_1(-K_4\otimes^t K_4) & B_1S_4^3 \\ B_1S_4^2 & B_1(-K_4\otimes^t K_4) & B_1S_4^3 & B_1S_4 \\ B_1(-K_4\otimes^t K_4) & B_1S_4^3 & B_1S_4 & B_1S_4^2 \\ B_1S_4^3 & B_1S_4 & B_1S_4^2 & B_1(-K_4\otimes^t K_4) \end{pmatrix}$$

and so the factorization:

(3.3.21)
$$\begin{pmatrix} B_1 & & & \\ & B_1 & & \\ & & B_1 & \\ & & & B_1 \end{pmatrix} \begin{pmatrix} S_4 & S_4^2 & -K_4\otimes^t K_4 & S_4^3 \\ S_4^2 & -K_4\otimes^t K_4 & S_4^3 & S_4 \\ -K_4\otimes^t K_4 & S_4^3 & S_4 & S_4^2 \\ S_4^3 & S_4 & S_4^2 & -K_4\otimes^t K_4 \end{pmatrix}$$

Now, as it will be shown below, the whole DFT representation admits a similar factorization. Let's first define the group G:

$$G = \{(u, u) : u \in U(p_1 p_2) \times U(p_1 p_2)\} \tag{3.3.22}$$

With the help of the Chinese Remainder Theorem we identify:

$$G = \{(g_1^n, g_2^m, g_1^n, g_2^m) : 0 \leq n \leq p_1 - 2, \quad 0 \leq m \leq p_2 - 2\} \tag{3.3.23}$$

g_1 and g_2 denote generators of $U(p_1)$ and $U(p_2)$ respectively.

Let

$$G' = \{(1, 1, g_1^{n'}, g_2^{m'}) : 0 \leq n' \leq p_1 - 2, \quad 0 \leq m' \leq p_2 - 2\} \tag{3.3.24}$$

and

$$G'' = \{(g_1^{n''}, g_2^{m''}, 1, 1) : 0 \leq n'' \leq p_1 - 2, \quad 0 \leq m'' \leq p_2 - 2\} \tag{3.3.25}$$

Then G' and G'' are isomorphic to $U(p_1) \times U(p_2)$ and after identifying the group of units in $Z/p_1p_2 \times Z/p_1p_2$ with

$$U = \{(g_1^n, g_2^m, g_1^k, g_2^l) : 0 \leq n, k \leq p_1 - 2 \quad 0 \leq m, l \leq p_2 - 2\} \tag{3.3.26}$$

we easily see that

$$U = G'G = G''G \tag{3.3.27}$$

where the product between the groups is the direct product.

On the other hand each set of the form $O_i \times O_j$ is a group on its own. The relation between $O_i \times O_j$ and the G-orbits contained in it can be described as follows

Let

$$\vec{\delta} = (\delta_1, \delta_2, \delta_3, \delta_4) \tag{3.3.28}$$

be any element in $Z/p_1 \times Z/p_2 \times Z/p_1 \times Z/p_2$ having either a one or a zero in each δ_k entry. Then the G-orbit

$$\vec{\delta}G = \{(\delta_1 g_1^n, \delta_2 g_2^m, \delta_3 g_1^n, \delta_4 g_2^m) : n, m\} \tag{3.3.29}$$

is a subgroup of the group of the form $O_i \times O_j$ given by

$$\delta_1 U(p_1) \times \delta_2 U(p_2) \times \delta_3 U(p_1) \times \delta_4 U(p_2) \tag{3.3.30}$$

If $\vec{\delta}_{ij}$ denotes the element $\vec{\delta}$ such that $\vec{\delta}_{ij}G$ is a subgroup of $O_i \times O_j$. Then the G-orbits contained in $O_i \times O_j$ are the cosets of the quotient group

$$O_i \times O_j / \vec{\delta}_{ij} G' \tag{3.3.31}$$

Thus groups $\vec{\delta}_{ij}G'$ and $\vec{\delta}_{ij}G^n$ can be chosen as set of representatives of the cosets. Having in mind the elimination of ξ redundant information we select

$$\vec{\delta}_{11}G' = \{(0, 1, 0, g_2^m) : m\} \tag{3.3.32}$$

$$\vec{\delta}_{13}G' = \{(0, g_2^m, 1, 1) : m\}$$

$$\vec{\delta}_{31}G^n = \{(1, 1, 0, g_2^m) : m\}$$

$$\vec{\delta}_{22}G' = \{(1, 0, g_1^n, 0) : n\}$$

$$\vec{\delta}_{23}G' = \{(1, 0, g_1^n, 1) : n\}$$

$$\vec{\delta}_{32}G^n = \{(g_1^n, 1, 1, 0) : n\}$$

$$\vec{\delta}_{33}G' = \{(1, 1, g_1^n, g_2^m) : n, m\}$$

We write in a separate list the elements $\vec{\delta}_{ij}$ for which $\vec{\delta}_{ij}G = O_i \times O_j$.

$$\vec{\delta}_{00} = (0, 0, 0, 0) \tag{3.3.33}$$

$$\vec{\delta}_{01} = (0,0,0,1)$$

$$\vec{\delta}_{02} = (0,0,1,0)$$

$$\vec{\delta}_{03} = (0,0,1,1)$$

$$\vec{\delta}_{10} = (0,1,0,0)$$

$$\vec{\delta}_{12} = (0,1,1,0)$$

$$\vec{\delta}_{20} = (1,0,0,0)$$

$$\vec{\delta}_{21} = (1,0,0,1)$$

$$\vec{\delta}_{30} = (1,1,0,0)$$

We will usually refer to this sets as the indexing sets of the G-orbits.

The DFT representation based on G-orbits is the matrix built from the blocks of the form

(3.3.34) $$M(\vec{a},\vec{b}) = (\omega^{<\vec{m},\vec{n}>})$$

where $\vec{a}$ and $\vec{b}$ range on the above defined indexing sets and $\vec{m} \in \vec{a}G$ and $\vec{n} \in \vec{b}G$. Let $\vec{a} = (a_1, a_2, a_3, a_4)$ and $\vec{b} = (b_1, b_2, b_3, b_4)$, then

(3.3.35) $$\vec{m} = (u_1 a_1 e_1 + u_2 a_2 e_2, u_1 a_3 e_1 + u_2 a_4 e_2)$$

$$\vec{n} = (v_1 b_1 e_1 + v_2 b_2 e_2, v_1 b_3 e_1 + v_2 b_4 e_2)$$

Here u_1 and v_1 are either in $U(p_1)$ or are equal to 0, while u_2 and v_2 are either in $U(p_2)$ or equal to 0. In any case:

(3.3.36) $$\omega^{<\vec{m},\vec{n}>} = \omega^{(a_1b_1+a_3b_3)u_1v_1e_1+(a_2b_2+a_4b_4)u_2v_2e_2} = \omega_1^{(a_1b_1+a_3b_3)u_1v_1}\omega_2^{(a_2b_2+a_4b_4)u_2v_2}$$

Let Q_1 be 0 if $a_1b_1 + a_3b_3 \equiv 0 \ (mod p_1)$ or the power of g_1 such that $g_1^{Q_1} \equiv a_1b_1 + a_3b_3 \ (mod p_1)$ otherwise. Let Q_2 be 0 if $a_2b_2 + a_4b_4 \equiv 0 \ (mod p_2)$ or the power of g_2 such that $g_2^{Q_2} \equiv a_2b_2 + a_4b_4 \ (mod p_2)$ otherwise.

Since

$$(3.3.37)\qquad \begin{cases} u_1 = 0 \Longleftrightarrow (a_1, a_3) = (0,0) \\ v_1 = 0 \Longleftrightarrow (b_1, b_3) = (0,0) \\ u_2 = 0 \Longleftrightarrow (a_2, a_4) = (0,0) \\ v_2 = 0 \Longleftrightarrow (b_2, b_4) = (0,0) \end{cases}$$

we have

$$(3.3.38)\qquad (\omega_1^{(a_1b_1+a_3b_3)u_1v_1}) = \begin{cases} (1) \quad u_1 = 0 \quad v_1 = 0 \\ (1)\,{}^tK_{p_1-1} \quad \text{if} \quad u_1 = 0, \quad v_1 \neq 0 \\ B_1(-K_{p_1} \otimes {}^tK_{p_1-1}) \quad \text{if} \quad u_1 \neq 0, v_1 \neq 0, Q_1 = 0 \\ B_1(-Kp_1) \quad \text{if} \quad u_1 \neq 0, v_1 = 0 \\ B_1 S_{p_1-1}^{Q_1} \quad \text{if} \quad u_1 \neq 0. v_1 \neq 0, Q_1 \neq 0 \end{cases}$$

$$(3.3.39)\qquad (\omega_2^{(a_2b_2+a_4b_4)u_2v_2}) = \begin{cases} (1) \quad \text{if} \quad u_2 = 0, v_2 = 0 \\ (1)\,{}^tK_{p_2-1} \quad \text{if} \quad u_2 = 0, v_2 \neq 0 \\ B_2(-K_{p_2-1}) \quad \text{if} \quad u_2 \neq 0, v_2 = 0 \\ B_2(-K_{p_2-1} \otimes {}^tK_{p_2-1}) \quad \text{if} \quad u_2 \neq 0, v_2 \neq 0, Q_2 = 0 \\ B_2 S_{p_2-1}^{Q_2} \quad \text{if} \quad u_2 \neq 0, v_2 \neq 0, Q_2 \neq 0 \end{cases}$$

Therefore

$$(3.3.40)\qquad M(\vec{a}, \vec{b}) \quad = \quad [B_1(\vec{a})) \otimes B_2(\vec{b})]\,[A_1(\vec{a}, \vec{b}) \otimes A_2(\vec{a}, \vec{b})]$$

where:

$$(3.3.41)\qquad B_1(\vec{a}) = \begin{cases} (1) \quad \text{if} \quad u_1 = 0 \\ B_1 \quad \text{if} \quad \text{otherwise} \end{cases},$$

$$(3.3.42)\qquad B_2(\vec{a}) = \begin{cases} (1) \quad \text{if} \quad u_2 = 0 \\ B_2 \quad \text{otherwise} \end{cases},$$

$$A_1(\vec{a},\vec{b}) = \begin{cases} (1) \quad \text{if} \quad u_1 = 0,\ v_1 = 0 \\ {}^tK_{p_1-1} \quad \text{if} \quad u_1 = 0,\ v_1 \neq 0 \\ -K_{p_1-1} \quad \text{if} \quad u_1 \neq 0,\ v_1 = 0 \\ -K_{p_1-1} \otimes {}^tK_{p_1-1} \quad \text{if} \quad u_1 \neq 0,\ v_1 \neq 0,\ Q_1 = 0 \\ S_{p_1-1}^{Q_1} \quad \text{if} \quad u_1 \neq 0,\ v_1 \neq 0,\ Q_1 \neq 0 \end{cases} \tag{3.3.43}$$

and

$$A_2(\vec{a},\vec{b}) = \begin{cases} (1) \quad \text{if} \quad u_2 = 0,\ v_2 = 0 \\ {}^tK_{p_2-1} \quad \text{if} \quad u_2 = 0,\ v_2 \neq 0 \\ -K_{p_2-1} \quad \text{if} \quad u_2 \neq 0,\ v_2 = 0 \\ -K_{p_2-1} \otimes {}^tK_{p_2-1} \quad \text{if} \quad u_2 \neq 0,\ v_2 \neq 0,\ Q_2 = 0 \\ S_{p_2-1}^{Q_2} \quad \text{if} \quad u_2 \neq 0,\ v_2 \neq 0,\ Q_2 \neq 0 \end{cases} \tag{3.3.44}$$

So the G based DFT matrix is given by

$$\begin{aligned} F_G(p_1p_2:2) =& [block-diag(B_1(\vec{a},\vec{b}) \otimes B_2(\vec{a},\vec{b})]\ [block(A_1(\vec{a},\vec{b}) \otimes A_2(\vec{a},\vec{b}))] \\ =& [block-diag(B_{\vec{a}})]\ \ [block(A_{\vec{a},\vec{b}})] \end{aligned} \tag{3.3.45}$$

3.4.-Sequences invariant under $\xi(n_1, n_2) = (n_2, n_1)$

An $(p_1 p_2)^2$-point sequence x is called ξ-invariant or ξ-symmetric if it satisfies:

$$x(n_1, n_2) = x(\xi(n_1, n_2)) = x(n_2, n_1) \tag{3.4.1}$$

We design here a fast algorithm computing the DFT of a ξ-invar iant sequence, that takes advantage of the relation (3.4.1).

We first prove the preservation of the ξ-symmetry by the operator $F_G(p_1 p_2 : 2)$. Let $\vec{m}$ and $\vec{n}$ be any two elements in $Z/p_1 p_2 \times Z/p_1 p_2$, then clearly

$$\begin{aligned} < \xi(\vec{m}), \vec{n} > &= < \vec{m}, \xi(\vec{n}) > \\ < \xi(\vec{m}), \xi(\vec{n}) > &= < \vec{m}, \vec{n} > \end{aligned} \tag{3.4.2}$$

So for $\vec{m} \in Z/p_1 p_2 \times Z/p_1 p_2$, and x ξ-symmetric

$$\begin{aligned} \hat{x}(\vec{m}) &= \sum_{\vec{n}} x(\vec{n}) \omega^{<\vec{m}, \vec{n}>} \\ &= \sum_{\vec{n}} x(\xi(\vec{n})) \omega^{<\vec{m}, \xi(\vec{n})>} \\ &= \sum_{\vec{n}} x(\vec{n}) \omega^{<\xi(\vec{m}), \vec{n}>} \\ &= \hat{x}(\xi(\vec{m})) \end{aligned} \tag{3.4.3}$$

Thus $F_G(p_1 p_2 : 2)$ preserves the ξ-symmetry. Consider now the computation:

$$y = [block - diag(B_{\vec{a}})]\, x \tag{3.4.4}$$

Let $\vec{m}$, $\vec{n} \in \vec{a}G$ where $\vec{a}$ is any of the indexing elements defined in section 3.3, then

$$\begin{aligned} y(\vec{m}) &= \sum_{\vec{n} \in \vec{a}G} x(\vec{n}) \omega^{<\vec{m}, \vec{n}>} \\ &= \sum_{\vec{n} \in \vec{a}G} x(\xi(\vec{n})) \omega^{<\xi(\vec{m}), \xi(\vec{n})>} \\ &= y(\xi(\vec{m})) \end{aligned} \tag{3.4.5}$$

This proves that $block - diag(B_{\vec{a}})$ also preserves the ξ symmetry. Therefore so does the matrix $block(A_{\vec{a},\vec{b}})$.

The indexing sets of the fundamental matrices are obtained by studying the action of ξ on the indexing set of the G-orbits defined in section 3.3. This action is naturally divided in two parts, the one determined by the elements $\vec{\delta}_{ij}$ with $i \neq j$ and the one determined by elements of the form $\vec{\delta}_{ii}$.

If $i \neq j$, ξ will send an element in $\vec{\delta}_{ij}G'$ into an element in $\vec{\delta}_{ji}G''$ and vice-versa. Hence a G-orbit indexed by an element in $\vec{\delta}_{ij}G'$ will be mapped onto a different G-orbit. Consequently, a subset of a ξ-fundamental region is given by any set of G-orbits indexed in a fundamental region for the ξ action on the first partition of the indexing set, that is the piece determined by δ_{ij}, with $i \neq j$.

The remaining piece of ξ-fundamental region on $Z/p_1p_2 \times Z/p_1p_2$ is determined with the help of the group structure of the corresponding subset of the G-orbits indexing set. We observe that: for any element $\vec{a} \in \vec{\delta}_{ii}G'$ there exists a (not necessarily unique) $g \in G$ such that :

$$\xi(\vec{a}) = (\vec{a})^{-1}g \tag{3.4.6}$$

Indeed, if $\vec{a} \in \vec{\delta}_{ii}$, then $\vec{a}$ is of the form

$$\vec{a} = (\delta_1, \delta_2, \delta_1 g_1^n, \delta_2 g_2^m) \tag{3.4.7}$$

where δ_1, δ_2 are either one or zero, then

$$\begin{aligned} \xi(\vec{a}) &= (\delta_1 g_1^n, \delta_2 g_2^m, \delta_1, \delta_2) \\ &= (\delta_1, \delta_2, \delta_1 g_1^{-n}, \delta_2 g_2^{-m})\,(g_1^n, g_2^m, g_1^n, g_2^m) \\ &= (\vec{a})^{-1}g \end{aligned} \tag{3.4.8}$$

By putting on g the conditions :

$$g_1^n = 1 \quad \text{whenever} \quad \delta_1 = 0 \tag{3.4.9}$$

and

$$g_2^m = 1 \quad \text{whenever} \quad \delta_2 = 0 \tag{3.4.10}$$

the element g in formula (3.4.6) becomes unique.

Formula (3.4.6) helps in describing the way the action of ξ modifies the G-orbits. Three main cases arise from our analysis:

Case 1:

Let $\vec{a}$ be the identity in $\vec{\delta}_{ii}G'$. In this case g is the identity in G and so ξ acts on $\vec{a}G$ as the identity map. The G-orbits corresponding to this case are

$$(1,0,1,0)G, \quad (0,1,0,1)G, \quad \text{and} \quad (1,1,1,1)\text{G} \tag{3.4.11}$$

and they, together with $(0,0,0,0)G$, form the subset of the fixed elements in the ξ-fundamental region.

Case 2:

If $\vec{a}$ is an element of order 2 in $\delta_{ii}G'$ then, since in general $\xi(\vec{ab}) = \xi(\vec{a})\xi(\vec{b})$

$$\xi(\vec{a})^2 = \xi(\vec{a})\xi(\vec{a}) = 1 \tag{3.4.12}$$

and since $\xi(\vec{a}) = (\vec{a})^{-1}g$ we have

$$1 = \xi(\vec{a}^2) = (\vec{a}^{-1})^2 g^2 = g^2 \tag{3.4.13}$$

Therefore

$$g = \begin{cases} (-1,1,-1,1) & \text{if} \quad \text{i} = 1 \\ (1,-1,1,-1) & \text{if} \quad \text{i} = 2 \\ (-1,-1,-1,-1) & \text{if} \quad \text{i} = 3 \end{cases} \tag{3.4.14}$$

and thus ξ restricted to $\vec{a}G$ is the map:

$$\vec{a}G \xrightarrow{\xi} -\vec{a}G \tag{3.4.15}$$

Notice that being $\vec{\delta}_{ii}G$ a cyclic group of even order $p_i - 1$ for $i = 1,2$ and the direct product of two cyclic groups of orders $p_1 - 1$ and $p_2 - 1$ for $i = 3$ we find one element of order two for $i = 1,2$ and three elements of order two for $i = 3$. They produce the following G-orbits:

$$
\begin{cases}
(1,0,-1,0)G & \text{if} \quad \mathrm{i}=1 \\
(0,1,0,-1)G & \text{if} \quad \mathrm{i}=2 \\
\text{if} \quad \mathrm{i}=3 \begin{cases} (1,1,-1,1)G \\ (1,1,1,-1)G \\ (1,1,-1,-1)G \end{cases}
\end{cases}
\tag{3.4.16}
$$

Therefore each orbit in this case contains a ξ-fundamental region. Let

$$
G_1^+ = \{(g_1^n, g_2^m, g_1^n, g_2^m) : 0 \leq n < \frac{p_1-2}{2},\ 0 \leq m \leq p_2-2\}
\tag{3.4.17}
$$

and

$$
G_2^+ = \{(g_1^n, g_2^m, g_1^n, g_2^m) : 0 \leq n \leq p_1-2,\ 0 \leq m < \frac{p_2-1}{2}\}
$$

A precise list of fundamental sets extracted from the above shown orbits is

$$
\begin{cases}
(1,0,-1,0)G_1^+ \\
(0,1,0,-1)G_2^+ \\
(1,1,-1,1)G_1^+ \\
(1,1,1,-1)G_1^+ \\
(1,1,-1,-1)G_1^+
\end{cases}
\tag{3.4.18}
$$

Case 3:

If $\vec{a}$ is neither the identity nor an element of order two in $\delta_{ii}G$, then $(\vec{a})^{-1} \neq \vec{a}$ and so ξ maps

$$
\vec{a}G \xrightarrow{\xi} (\vec{a})^{-1}gG \neq \vec{a}G
\tag{3.4.19}
$$

therefore none of the G-orbits gets mapped onto itself. A ξ- fundamental region is formed by

$$
\bigcup_{1 \leq m < \frac{(p_2-1)}{2}} (0,1,0,g_2^m)G \quad \text{if} \quad \mathrm{i}=1
\tag{3.4.20}
$$

(3.4.21) $$\bigcup_{1\le n<\frac{p_1-1}{2}} (1,0,g_1^n,0)G \quad \text{if} \quad i=2$$

(3.4.22) $$\bigcup_{1\le n<\frac{p_1-1}{2},\ 0\le m\le p_2-2} (1,1,g_1^n,g_2^m)G \quad \text{if} \quad i=3$$

We summarize and divide the ξ-fundamental region into the three following sections

(3.4.23) $$(0,0,0,0)G,\ (0,1,0,1)G,\ (1,0,1,0)G,\ (1,1,1,1)G$$

(3.4.24) $$\bigcup_{1\le m<\frac{p_2-1}{2}} (0,1,0,g_2^m)G,$$

$$\bigcup_{1\le n<\frac{p_1-1}{2}} (1,0,g_1^n,0)G,$$

$$\bigcup_{0\le m\le p_2-2,1\le n<\frac{p_1-1}{2}} (1,1,g_1^n,g_2^m)G,$$

$$\bigcup_{1\le m\le p_2-2} (1,1,0,g_2^m)G,$$

$$(0,0,0,1)G,\ (0,0,1,0)G,\ (0,0,1,1)G,\ (0,1,1,0)G$$

(3.4.25) $$(0,1,0,-1)G_2^+,\ (1,0,-1,0)G_1^+,\ (1,1,-1,1)G_1^+,\ (1,1,1,-1)G_1^+,\ (1,1,-1,-1)G_1^+$$

The fundamental matrix derived from $block-diag(B_{\vec{a}})$, when $\vec{a}G$ is any set in (3.4.23) is a block diagonal matrix whose main diagonal is formed by

(3.4.26) $$\begin{cases} (1) \quad on \quad (0,0,0,0)G \\ B_2 \quad on \quad (0,1,0,1)G \\ B_1 \quad on \quad (1,0,1,0)G \\ B_1 \otimes B_2 \quad on \quad (1,1,1,1)G \end{cases}$$

This piece of the fundamental matrix coincides with the original one since their indexing sets are fixed by the ξ action. We list now the fundamental blocks indexed in the sets in (3.4.24)

$$
(3.4.27)\qquad \begin{cases} I_{\frac{p_1-1}{2}-1}\otimes B_2 \quad on \quad \bigcup_{1\le m<\frac{p_2-1}{2}}(0,1,0,g_2^m)G \\ I_{\frac{p_1-1}{2}-1}\otimes B_1 \quad on \quad \bigcup_{1\le n<\frac{p_1-1}{2}}(1,0,g_1^n,0)G \\ I_{\frac{p_1-1}{2}-1}\otimes I_{p_2-1}\otimes B_1\otimes B_2 \quad on \quad \bigcup_{0\le m\le p_2-2,\ 1\le n<\frac{p_1-1}{2}}(1,1,g_1^n,g_2^m)G \\ I_{p_2-1}\otimes B_1\otimes B_2 \quad on \quad \bigcup_{0\le m\le p_2-2}(1.1.0.g_2^n)G \\ B_2 \quad on \quad (0,0,0,1)G \\ B_1 \quad on \quad (0,0,1,0)G \\ B_1\otimes B_2 \quad on \quad (0,0,1,1)G \quad and \quad ((0,1,1,0)G \end{cases}
$$

These fundamental blocks correspond to one half of the blocks in a section of the original matrix. The blocks are kept unaltered.

The remaining part of the fundamental matrix comes from orbits on which the action of ξ equals a multiplication times -1. The techniques for the block reduction are the same as in section 2. The result is the following

$$
(3.4.28)\qquad \begin{cases} B_1^+ \quad on \quad (0,1,0,-1)G \\ B_2^+ \quad on \quad (1,0,-1,0)G \\ B_3^+ \quad on \quad (1,1,-1,1)G,\ (1,1,1,-1)G \quad and \quad (1,1,-1,-1)G \end{cases}
$$

Before giving the general form of the fundamental blocks derived from $block(A_{\vec{a},\vec{b}})$ we observe a fact about shift operators.

Observation:

Let n be an even number, the

$$
(3.4.29)\qquad S_n=\begin{pmatrix} T_1 & R_1 \\ R_1 & T_1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\otimes T_1+\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\otimes R_1
$$

where T_1 and R_1 are $\frac{n}{2}\times\frac{n}{2}$ matrices of the following form:

$$
(3.4.30)\qquad T_1=\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}
$$

(3.4.31) $$R_1 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

From these formulas we conclude that: firstly

(3.4.32) $$S_n^Q = \begin{pmatrix} T_Q & R_Q \\ R_Q & T_Q \end{pmatrix}$$

and secondly

(3.4.33) $$T_1 + R_1 \quad = \quad S_{\frac{n}{2}}^r$$

We shall prove by induction on r that

(3.4.34) $$T_r + R_r = S_{\frac{n}{2}}^r$$

Assuming (3.4.34) for $r = k-1, \quad k \geq 2,$

(3.4.35) $$S_n^k = \begin{pmatrix} T_{k-1} & R_{k-1} \\ R_{k-1} & T_{k-1} \end{pmatrix} \begin{pmatrix} T_1 & R_1 \\ R_1 & T_1 \end{pmatrix}$$

$$= \begin{pmatrix} T_{k-1}T_1 + R_{k-1}R_1 & T_{k_1}R_1 + R_{k-1}T_1 \\ R_{k-1}T_1 + T_{k-1}R_1 & R_{k-1}R_1 + T_{k-1}T_1 \end{pmatrix}$$

$$= \begin{pmatrix} T_k & R_k \\ R_k & T_k \end{pmatrix}$$

hence

(3.4.36) $$T_k + R_k = (T_{k-1} + R_{k-1})\ (T_1 + R_1) = S_{\frac{n}{2}}^{k-1} S_{\frac{n}{2}}$$

These matrices, coming from reductions on powers of shift operators, are encountered in some of the computations of fundamental blocks performed on matrices of the type of $block(A_{\vec{a},\vec{b}})$.

The general formulas of fundamental blocks derived from $block(A_{\vec{a},\vec{b}})$ are easier to describe in the cases in which the column indexing orbit $\vec{b}G$ is either fixed (i.e. a member of the list (3.4.23)) or sent to a different orbit by the action of ξ (i.e. a member of the list (3.4.24)). Let's analyse first the case $\vec{b}G \in$ (3.4.23)

$$
(3.4.37)\qquad \begin{cases} A_{\vec{a},\vec{b}} & if \quad aG \in (3.4.23) \\ A_{\vec{a},\vec{b}} & if \quad \vec{a}G \in (3.4.24) \\ [(1\ 0) \otimes I_{\frac{p_1-1}{2}}]A_{\vec{a},\vec{b}} & if \quad \vec{a}G \in (3.4.25) \\ [(1\ 0) \otimes I_{\frac{p_2-1}{2}}]A_{\vec{a},\vec{b}} & if \quad \vec{a} = (0,1,0,-1) \\ [(1\ 0) \otimes I_{\frac{p_1-1}{2}(p_2-1)}]A_{\vec{a},\vec{b}} & if \quad \vec{a} = (1,1,-1,1),(1,1,1,-1),(1,1,-1,-1) \end{cases}
$$

Let's consider now $\vec{b}G \in (3.4.24)$

$$
(3.4.38)\qquad \begin{cases} A_{\vec{a},\vec{b}} + A_{\vec{a},xi(\vec{b})} & if \vec{a}G \in (3.4.23) \\ A_{\vec{a},\vec{b}} + A_{\vec{a},\xi(\vec{b})} & if \quad \vec{a}G \in (3.4.24) \\ [(1\ 0) \otimes I_{\frac{p_1-1}{2}}]\ [A_{\vec{a},\vec{b}} + A_{\vec{a},\xi(\vec{b})}] & if \quad \vec{a} = (1,0,-1,0) \\ [(1\ 0) \otimes I_{\frac{p_2-1}{2}}]\ [A_{\vec{a},\vec{b}} + A_{\vec{a},\xi(\vec{b})}] & if \quad \vec{a} = (0,1,0,-1) \\ [(1\ 0) \otimes I_{\frac{p_1-1}{2}(p_2-1)}]\ [A_{\vec{a},\vec{b}} + A_{\vec{a},\xi(\vec{b})}] & if \quad \vec{a} = (1,1,-1,1),(1,1,1,-1),(1,1,-1,-1) \end{cases}
$$

The description of the fundamental matrices whose columns are indexed by G-orbits in (3.4.25) requires the partition of the original matrix into blocks. Consider a column indexing orbit having $\vec{b}G_1^+ \cup (-\vec{b}G_1^+)$ as fundamental set. The following matrix corresponds to a column permutation of $A_{\vec{a},\vec{b}}$ and it clearly produces the same fundamental block as $A_{\vec{a},\vec{b}}$

$$
(3.4.39)\qquad \begin{array}{c} \\ \vec{a}G \end{array} \begin{array}{c} \begin{array}{cc} \vec{b}G_1^+ & -\vec{b}G_1^+ \end{array} \\ \begin{pmatrix} A_1^1(\vec{a},\vec{b}) \otimes A_2(\vec{a},\vec{b}) & A_1^2(\vec{a},\vec{b}) \otimes A_2'(\vec{a},\vec{b}) \end{pmatrix} \end{array}
$$

here

$$
(3.4.40)\qquad A_1^1(\vec{a},\vec{b}) = \begin{cases} (1) \\ -K_{p_1-1} \\ {}^tK_{\frac{p_1-1}{2}} \\ -K_{p_1-1} \otimes {}^tK_{\frac{p_1-1}{2}} \\ \begin{pmatrix} T_{Q_1} \\ R_{Q_1} \end{pmatrix} \end{cases}
$$

and

$$A_1^2(\vec{a},\vec{b}) = \begin{cases} (0) \\ (0)\otimes K_{p_1-1} \\ {}^tK_{\frac{p_1-1}{2}} \\ -K_{p_1-1}\otimes {}^tK_{\frac{p_1-1}{2}} \\ \begin{pmatrix} R_{Q_1} \\ T_{Q_1} \end{pmatrix} \end{cases} \tag{3.4.41}$$

and $A_2'(\vec{a},\vec{b}) = A_2(\vec{a},\vec{b})S_n^{\frac{n}{2}}$ with n equal to the number of columns in $A_2(\vec{a},\vec{b})$.

Let $A^+ = A_1^1(\vec{a},\vec{b})\otimes A_2(\vec{a},\vec{b}) + A_1^2(\vec{a},\vec{b})\otimes A_2'(\vec{a},\vec{b})$, then the fundamental blocks are

$$\begin{cases} A^+ \quad for \quad \vec{a}G \in (3.4.23),\ (3.4.24) \\ [(1\ 0)\otimes I_{\frac{p_1-1}{2}}]A^+ \\ [(1\ 0)\otimes I_{\frac{p_2-1}{2}}]A^+ \\ [(1\ 0)\otimes I_{\frac{p_1-1}{2}(p_2-1)}]A^+ \end{cases} \tag{3.4.42}$$

The fundamental set $(0,1,0,-1)G_2^+$ is the only one left in the previous analysis. Notice that

$A_1(\vec{a},(0,1,0,-1))$ is either (1) or $-K_{p_2-1}$ and so it is independent from the column indexing set. The matrix

$$\vec{a}G \begin{pmatrix} (0,1,0,-1)G_2^+ & -(0,1,0,-1)G_2^+ \\ A_1(\vec{a},(0,1,0,-1))\otimes A_2^1(\vec{a},(0,1,0,-1)) & A_1(\vec{a},(0,1,0,-1))\otimes A_2^2(\vec{a},(0,1,0,-1)) \end{pmatrix} \tag{3.4.43}$$

where

$$A_2^1 = \begin{cases} (1) \\ -K_{p_2-1} \\ {}^tK_{\frac{p_2-1}{2}} \\ -K_{p_2-1}\otimes {}^tK_{\frac{p_2-1}{2}} \\ \begin{pmatrix} T_{Q_2} \\ R_{Q_2} \end{pmatrix} \end{cases} \tag{3.4.44}$$

(3.4.45)
$$A_2^2(\vec{a},\vec{b}) = \begin{cases} (0) \\ (0)\otimes K_{p_2-1} \\ {}^tK_{\frac{p_2-1}{2}} \\ -K_{p_2-1}\otimes\ {}^tK_{\frac{p_2-1}{2}} \\ \begin{pmatrix} R_{Q_2} \\ T_{Q_2} \end{pmatrix} \end{cases}$$

Therefore if $A^{++} = A_1(\vec{a},(0,1,0,-1))\otimes[A_2^1(\vec{a},(0,1,0,-1))+A_2^2(\vec{a},(0,1,0,-1))]$, then the fundamental blocks are of the following general forms:

(3.4.46)
$$\begin{cases} A^{++} \quad if \quad \vec{a}G \in (3.4.2),\ (3.4.23) \\ [(1\ 0)\otimes I_{\frac{p_1-1}{2}}]A^{++} \quad if \quad \vec{a}=(1,0,-1,0) \\ [(1\ 0)\otimes I_{\frac{p_2-1}{2}}]A^{++} \quad if \quad \vec{a}=(0,1,0,-1) \\ [(1\ 0)\otimes I_{\frac{p_1-1}{2}(p_2-1)}]A^{++} \quad if \quad \vec{a}=(1,1,1,-1),\ (1,1,-1,1)\ (1,1,-1,-1) \end{cases}$$

4. A three dimensional symmetry

As in previous sections our main goal here is showing how the formulas proved in Propositions 1 and 2 can be applied to get sparse matrix factorizations for blocks of high multiplicative complexity that appear in fundamental matrices derived from the elimination of certain structured redundant computations from the DFT matrix.

4.1 Λ-fundamental regions

Let Λ be the group of automorphisms in $Z/p_1p_1 \times Z/p_1p_2 \times Z/p_1p_2$ given by the direct product of the groups generated by

$$\lambda_1(n_1, n_2, n_3) = (-n_1, -n_2, n_3) \tag{4.1.1}$$

$$\lambda_2(n_1, n_2, n_3) = (n_1, -n_2, -n_3) \tag{4.1.2}$$

Let $Z/p_1p_2 \times Z/p_1p_2 \times Z/p_1p_2$ be endowed with the ring structure of direct sum, and let U denote its group of units. Since $-1 \in U(p_1p_2)$

$$\lambda U = U \tag{4.1.3}$$

for all $\lambda \in \Lambda$ and so every element in Λ maps U-orbits onto U-orbits. Through the chinese remainder theorem isomorphism we establish a one-to-one correspondence between U-orbits and sets of the form $O_i \times O_j \times O_k$; $0 \leq i, j, k \leq 3$ and as before we look for a Λ-fundamental region expressable in terms of sets of the form O_l^+ and O_l. This is achieved by taking first a fundamental region for λ_1, selecting from it a subset having no more than one element from each λ_2-orbit and then selecting from this subset a set containing no more than one element from each λ_3-orbit, where $\lambda_3 = \lambda_1\lambda_2$.

Consider first the action of λ_1 on a set of the form $O_i \times O_j \times O_k$. This action can be represented as the mapping

$$O_i \times O_j \times O_k \xrightarrow{\lambda_1} -O_i \times -O_j \times O_k \tag{4.1.4}$$

a fundamental region for this action is

$$\begin{cases} \{0\} \times O_j^+ \times O_k & if \quad i = 0 \\ O_i^+ \times O_j \times O_k & if \quad i = 1,2,3 \end{cases} \tag{4.1.5}$$

the set $\{0\} \times O_j^+ \times O_k$ is mapped onto $\{0\} \times -O_j^+ \times O_k$ by λ_2 and so it contains just one element from each λ_2-orbit intersecting it. On the other hand

$$O_i^+ \times O_j \times O_k \xrightarrow{\lambda_2} O_i^+ \times -O_j \times -O_k = O_i^+ \times O_j \times O_k \tag{4.1.6}$$

that is λ_2 acts on $O_i^+ \times O_j \times O_k$. A fundamental region for this λ_2 action is

$$\begin{cases} O_i^+ \times \{0\} \times O_k^+ & if \quad j = 0 \\ O_i^+ \times O_j^+ \times O_k & if \quad j = 1,2,3 \end{cases} \tag{4.1.7}$$

So far the combined action of λ_1 and λ_2 produces the following fundamental sets

$$\begin{cases} \{0\} \times O_j^+ \times O_k & 0 \le j,k \le 3 \\ O_i^+ \times \{0\} \times O_k^+ & 1 \le i \le 3 \quad 0 \le k \le 3 \\ O_i^+ \times O_j^+ \times O_k & 1 \le i,j \le 3 \quad 0 \le k \le 3 \end{cases} \tag{4.1.8}$$

Since

$$\lambda_3(n_1,n_2,n_3) = (-n_1,n_2,-n_3) \tag{4.1.9}$$

an analysis similar to that one applied to λ_2 tells that the sets $O_i^+ \times \{0\} \times O_k^+$ and $O_i^+ \times O_j^+ \times O_k$ contain only one element from each λ_3-orbit intersecting them and that λ_3 acts on $\{0\} \times O_j^+ \times O_k$. The mapping corresponding to this latter action is:

$$\{0\} \times O_j^+ \times O_k \xrightarrow{\lambda_3} \{0\} \times O_j^+ \times -O_k \tag{4.1.10}$$

and so we get a new fundamental set

(4.1.11) $$\{0\} \times O_j^+ \times O_k^+ \quad 0 \leq j,k \leq 3$$

Summarizing, a A-fundamental region is given by the union of the sets listed below

(4.1.12) $$\{0\} \times O_j^+ \times O_k^+ \quad 0 \leq j,k \leq 3$$

and

(4.1.13) $$O_i^+ \times \{0\} \times O_k^+ \quad 1 \leq i \leq 3; \quad 0 \leq k \leq 3$$

and

(4.1.14) $$O_i^+ \times O_j^+ \times O_k \quad 1 \leq i,j \leq 3; \quad 0 \leq k \leq 3$$

4.2.- Λ-invariant sequences

A sequence x indexed in $Z/p_1p_2 \times Z/p_1p_2 \times Z/p_1p_2$ is said to be Λ-invariant or Λ- symmetric if

$$x(n_1, n_2, n_3) = x(\lambda(n_1, n_2, n_3)) \quad \text{for all} \quad \lambda \in \Lambda \tag{4.2.1}$$

The DFT matrix representation to be used for the incorporation of Λ-controlled redundancies is the natural generalization of $F(p_1p_2)$ to the three-dimensional case. Our building blocks are the matrices of the form

$$M((i_1, j_1, k_1), (i_2, j_2, k_2)) = (B_{i_1} \otimes B_{j_1} \otimes B_{k_1})\ (A_{i_1 i_2} \otimes A_{j_1, j_2} \otimes A_{k_1 k_2}) \tag{4.2.2}$$

and so the DFT matrix naturally factors as

$$F_U(p_1p_2 : 3) = block - diag(B_{i_1} \otimes B_{j_1} \otimes B_{k_1})\ \ block(Ai_1i_2 \otimes A_{j_1j_2} \otimes A_{k_1k_2}) \tag{4.2.3}$$

On the other hand a λ-symmetric sequence is invariant under each one of the following matrices

$$S(p_1p_2) \otimes S(p_1p_2) \otimes I_{p_1p_2} \tag{4.2.4}$$

$$S(p_1p_2) \otimes I_{p_1p_2} \otimes S(p_1p_2) \tag{4.2.5}$$

$$I_{p_1p_2} \otimes S(p_1p_2) \otimes S(p_1p_2) \tag{4.2.6}$$

Since each one of these matrices commutes with each of the factors of $F_U(p_1p_2 : 3)$ the factors of $F_U(p_1p_2 : 3)$ preserve λ- symmetries and therefore we obtain the fundamental DFT matrix by independently reducing each of them to fundamental matrices indexed on the Λ fundamental region formed by the sets in (4.1.12) – (4.1.14). Our reductive technique is similar to the one used in section 2.

Let C_i, $i = 0, \ldots, 3$ be the blocks defined in section 2. Consider first indexing sets of the form of $\{0\} \times O_j^+ \times O_k^+$, $0 \leq j, k \leq 3$. If the redundant output is eliminated we obtain a block of the following general form:

$$\begin{array}{c} \\ \{0\} \times O_j^+ \times O_k^+ \end{array} \begin{array}{c} \begin{array}{cccc} \{0\} \times O_j^+ \times O_k^+ & \{0\} \times -O_j^+ \times O_k^+ & \{0\} \times -O_j^+ \times -O_k^+ & \{0\} \times O_j^+ \times -O_k^+ \end{array} \\ \begin{pmatrix} C_j \otimes C_k & \bar{C}_j \otimes C_k & \bar{C}_j \otimes \bar{C}_k & C_j \otimes \bar{C}_k \end{pmatrix} \end{array} \tag{4.2.7}$$

thus, the elimination of input redundant data yields: aspect

$$\begin{array}{c} \\ \{0\} \times O_j^+ \times O_k^+ \end{array} \begin{array}{c} \begin{array}{c} \{0\} \times O_j^+ \times O_k^+ \end{array} \\ \begin{pmatrix} C_j \otimes C_k + \bar{C}_j \otimes C_k + \bar{C}_j \otimes \bar{C}_k + C_j \otimes \bar{C}_k \end{pmatrix} \end{array} \tag{4.2.8}$$

Recalling that $O_0 = \{0\}$ we draw from (4.2.8) the following sub-cases for the fundamental blocks

$$\begin{cases} (1) & if \quad j = k = 0 \\ B_j^+ & if \quad j \neq 0, \; k = 0 \\ B_k^+ & if \quad j = 0, \; k \neq 0 \end{cases} \tag{4.2.9}$$

If, on the other hand, $j \neq 0$ and $k \neq 0$ the matrix in (4.2.8) can be factored as

$$(C_j + \bar{C}_j) \otimes (C_k + \bar{C}_k) \tag{4.2.10}$$

Recalling that $C_l + \bar{C}_l = B_l^+$, we can express the fundamental blocks as:

$$B_j^+ \otimes B_k^+ \quad 1 \leq j, k \leq 3 \tag{4.2.11}$$

Each factor in this tensor product is either skew-circulant or suitable for the application of the sparse matrix factorization formulas of either one of Proposition 1 (page 10) or Proposition 2 (page 18).

A similar situation is found when formulating the fundamental blocks indexed in sets of the type $O_i^+ \times \{0\} \times O_k^+ \quad 1 \leq i \leq 3 \; 0 \leq k \leq 3$

Consider now indexing sets of the type $O_j^+ \times O_k^+ \times O_k$, $\quad 1 \leq i, j \leq 3, \;\; 0 \leq k \leq 3$. By eliminating the redundant outputs we get a block of the following general form:

(4.2.12)

$$\begin{array}{c} \\ O_i^+ \times O_j^+ \times O_k \\ O_i^+ \times O_j^+ \times O_k \end{array} \begin{array}{c} \begin{array}{cccc} O_i^+ \times O_j^+ \times O_k & -O_i^+ \times -O_j^+ \times O_k & O_i^+ \times -O_j^+ \times -O_k & -O_i^+ \times O_j^+ \times -O_k \end{array} \\ \begin{pmatrix} C_i \otimes C_j \otimes B_k & \bar{C}_i \otimes \bar{C}_j \otimes B_k & C_i \otimes \bar{C}_j \otimes \bar{B}_k & \bar{C}_i^+ \otimes C_j^+ \otimes \bar{B}_k \end{pmatrix} \end{array}$$

The following are the different cases of fundamental blocks derived from (4.2.12).

If $k = 0$ we clearly get the same blocks as in (4.2.9) and (4.2.10). As for $k \geq 1$ we observe that

(4.2.13)

$$\begin{aligned} &C_i \otimes C_j \otimes B_k + \bar{C}_i \otimes \bar{C}_j \otimes B_k + \bar{C}_i \otimes C_j \otimes \bar{B}_k + C_i \otimes \bar{C}_j \otimes \bar{B}_k \\ =&C_i \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_k] + \bar{C}_i \otimes [\bar{C}_j \otimes B_k + C_j \otimes \bar{B}_k] \end{aligned}$$

Let $I(k)$ and $S(k)$ be as defined in section 3 and let $I'(k)$ denote the identity matrix of one half the dimension of $I(k)$. Using the relation

(4.2.14)

$$S(k)\bar{B}_k = B_k$$

we obtain

(4.2.15)

$$[I'(j) \otimes S(k)]\,[\bar{C}_j \otimes B_k + C_j \otimes \bar{B}_k] = \bar{C}_j \otimes \bar{B}_k + C_j \otimes B_k$$

Therefore

(4.2.16)

$$\begin{aligned} &C_i \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_k] + \bar{C}_i \otimes [\bar{C}_j \otimes B_k + C_j \otimes \bar{B}_k] \\ =&(C_i \otimes I'(j) \otimes I(k))\,(I'(i) \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_r]) + (\bar{C}_i \otimes I'(j) \otimes S(k))\,(I'(k) \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_r]) \\ =&(C_i \otimes I'(j) \otimes I(k) + \bar{C}_i \otimes I'(j) \otimes S(k))\,(I'(i) \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_k]) \end{aligned}$$

The left factor in the bottom line of (4.2.16) clearly admits the factorization formula of Proposition 2 for $i = 1, 2$, as for $i = 3$, since $C_3 = C_1 \otimes B_2$ we get

(4.2.17)

$$\begin{aligned} &C_3 \otimes I'(j) \otimes I(k) + \bar{C}_3 \otimes I'(j) \otimes S(k) \\ =&C_1 \otimes B_2 \otimes I'(j) \otimes I(k) + \bar{C}_1 \otimes \bar{B}_2 \otimes I'(j) \otimes S(k) \\ =&(C_1 \otimes I_{p_2-1} \otimes I'(j) \otimes I(k) + \bar{C}_1 \otimes S_{p_2-1}^2 \otimes I'(j) \otimes S(k))\,(I_{\frac{p_1-1}{2}} \otimes B_2 \otimes I'(j) \otimes I(k) \end{aligned}$$

The left factor in the bottom line of (4.2.16) is also factorizable by the formula given in proposition 2. Let's consider now the right factor in the bottom line of (4.2.15) By factoring it as

$$
\begin{aligned}
&I'(i) \otimes [C_j \otimes B_k + \bar{C}_j \otimes \bar{B}_k] \\
&= I'(i) \otimes (C_1 \otimes I_{p_2-1} \otimes I(k) + \bar{C}_1 \otimes S^2_{p_2-1} \otimes S(k)) \; (I_{\frac{p_1-1}{2}} \otimes I_{p_2-1} \otimes B_K)
\end{aligned} \tag{4.2.18}
$$

The analysis splits again in two cases. If $j = 1, 2$ the factor $C_j \otimes I(k) + \bar{C}_j \otimes S(k)$ is clearly factorizable by the formula in proposition 2. If $j = 3$ then

$$
\begin{aligned}
&C_3 \otimes I(k) + \bar{C}_3 \otimes S(k) \\
&= C_1 \otimes B_2 \otimes I(k) + \bar{C}_1 \otimes \bar{B}_2 \otimes S(k) \\
&= (C_1 \otimes I_{p_2-1} \otimes I(k) + \bar{C}_1 \otimes S^2_{p_2-1} \otimes S(k)) \; (I_{\frac{p_1-1}{2}} \otimes I_{p_2-1} \otimes B_k)
\end{aligned} \tag{4.2.19}
$$

This left factor in the bottom equation of (4.2.19) satisfies the hypothesis of Proposition 2, so the whole expression admits a sparse matrix factorization.

Since the fundamental blocks indexed by sets of the form of $O_i^+ \times O_j^+ \times O_k$, under $(\frac{p_i-1}{2}, \frac{p_j-1}{2}, p_k - 1)$-block decomposition, present skew-circulant $(p_k - 1) \times (p_k - 1)$ blocks Proposition 1 also provides a sparse matrix factorization formula.

For a general description of the fundamental blocks derived from the matrix $block(A_{i_1,i_2} \otimes A_{j_1,j_2} \otimes A_{k_1,k_2})$ we use the matrices $A^t_{l_1,l_2}$, $0 \leq l_1, l_2 \leq 3$, $1 \leq t \leq 4$ defined in section 3. Our analysis splits again into three main cases

Case 1

If the row indexing set is $\{0\} \times O_j^+ \times O_k^+$ then we have

$$
(A^1_{j_1,j_2} + A^2_{j_1,j_2}) \otimes (A^1_{k_1,k_2} + A^2_{k_1,k_2}) \tag{4.2.20}
$$

if the column indexing set is $\{0\} \times O_{j_2}^+ \times O_{k_2}^+$

$$
A^1_{j_1,0} \otimes (A^1_{0,i_2} + A^2_{0,i_2}) \otimes (A^1_{k_1,k_2} + A^2_{k_1,k_2}) \tag{4.2.21}
$$

if the column indexing set is $O_{i_2}^+ \times \{0\} \times O_{k_2}^+$

(4.2.22) $(A^1_{0,i_2} \otimes A^1_{j_1,j_2} + A^2_{0,i_2} \otimes A^2_{j_1,j_2}) \otimes [A^1_{k_1k_2} A^2_{k_1,k_2}] + (A^1_{0,i_2} \otimes A^2_{j_1,j_2} + A^2_{0,i_2} \otimes A^1_{j_1,j_2}) \otimes [A^2_{k_1,k_2} A^1_{k_1,k_2}]$

if the column indexing set is $O^+_{i_2} \times O^+_{j_2} \times)_{k_2}$.

Case 2

If the row indexing set is $O^+_{i_1} \times \{0\} \times O^+_{k_1}$ then we have

(4.2.23) $$A_{i_1,0} \otimes (A^1_{0,j_2} + A^2_{0,j_2}) \otimes (A^1_{k_1,k_2} + A^2_{k_1,k_2})$$

if the column indexing set is $\{0\} \times O^+_{j_2} \times O^+_{k_2}$

(4.2.24) $$(A^1_{i_1,i_2} + A^2_{i_1,i_2}) \otimes (A^1_{k_1,k_2} + A^2_{k_1,k_2})$$

if the column indexing set is $O^+_{i_2} \times \{0\} \times O_{k_2}$

(4.2.25) $(A^1_{i_1,i_2} \otimes A^1_{0,j_2} + A^2_{i_1,i_2} \otimes A^2_{0,j_2}) \otimes [A^1_{k_1,k_2} A^2_{k_1,k_2}] + (A^1_{i_1,i_2} \otimes A^2_{0,j_2} + A^2_{i_1,i_2} \otimes A^1_{0,j_2}) \otimes [A^2_{k_1,k_2} A^1_{k_1,k_2}]$

if the column indexing set is $O^+_{i_2} \times O^+_{j_2} \times O_{k_2}$

Case 3

If the row indexing set is $O^+_{i_1} \times O^+_{j_1} \times O_{k_1}$ then we have

(4.2.26) $$A^1_{i_1,0} \otimes (A^1_{j_1,j_2} + A^2_{j_1,j_2}) \otimes (A^1_{k_1,k_2} + A^2_{k_1,k_2})$$

if the column indexing set is $\{0\} \times O^+_{j_2}$

(4.2.27) $$(A^1_{i_1,i_2} + A^2_{i_1,i_2}) \otimes A^1_{j_1} \otimes \begin{pmatrix} A^1_{k_1,k_2} + A^2_{k_1,k_2} \\ A^3_{k_1,k_2} + A^4_{k_1,k_2} \end{pmatrix}$$

if the column indexing set is $O^+_{i_2} \times \{0\} \times O^+_{k_2}$, and

(4.2.28) $(A^1_{i_1,i_2} \otimes A^1_{j_1,j_2} + A^2_{i_1,i_2} \otimes A^2_{j_1,j_2}) \otimes A_{k_1,k_2} + (A^1_{i_1,i_2} \otimes A^2_{j_1,j_2} + A^2_{i_1,i_2} \otimes A^1_{j_1,j_2}) \otimes A_{k_1,k_2} S(k_2)$

if the column indexing set is $O^+_{i_2} \times O^+_{j_2} \times O_{k_2}$.

Appendix: On the complexity of certain Toeplitz and Hankel matrices

The vector space of the $N \times N$ Hankel matrices was defined in section 1. The vector space of $N \times N$ Toeplitz matrices is closely related to it. As a matter of fact an $N \times N$ matrix A is called a Toeplitz matrix if there exists an $N \times N$ Hankel matrix B such that:

$$A = T_N B \tag{A.1}$$

where

$$T_N = \begin{pmatrix} 1 & \\ & \tilde{I}_{N-1} \end{pmatrix} \tag{A.2}$$

By the complexity of computing with a matrix A it is meant the minimal number of arithmetic operations that are necessary to compute $\vec{b} = A\vec{x}$.

The purpose of this appendix is to show that certain subspaces of either Toeplitz or Hankel matrices are composed by elements whose complexity is of the order of $N\ logN$. These subspaces are the (λ)-circulant matrices in the space of Toeplitz matrices and the (λ)-skew-circulant matrices in the space of Hankel matrices, where λ is a complex number. In section 1.1 we introduced the skew-circulant matrices as the subspace of Hankel matrices generated by

$$\{H_{N-1}^{(N)}\} \cup \{H_k^{(N)} + H_{N+k}^{(N)} : 0 \leq k < N-1\} \tag{A.3}$$

now we generalize this definition by calling (λ)-skew-circulant an $N \times N$ matrix A belonging to the space generated by

$$\{H_{N-1}^{(N)}\} \cup \{H_k^{(N)} + \lambda H_{N+k}^{(N)}\} \tag{A.4}$$

and saying that, in particular, if $\lambda = 1$ the matrix A is called skew-circulant. As a way of example, let's consider the case $N = 3$. In this case we have:

$$H_0^{(3)} + \lambda H_3^{(3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \lambda \\ 0 & \lambda & 0 \end{pmatrix}$$

$$H_1^{(3)} + \lambda H_4^{(3)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \tag{A.5}$$

$$H_2^{(3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

forms a basis for the subspace of the 3×3 (λ)-skew-circulant matrices

By a circulant matrix A we understand any element in the space generated by

$$\{T_N H_{N-1}^{(N)}\} \cup \{T_N(H_k^{(N)} + H_{k+N}^{(N)}) \ : \ 0 \leq k < N-1\} \tag{A.6}$$

Thus, the $N \times N$ circulant matrices form indeed a subspace of the space of $N \times N$ Toeplitz matrices. Furthermore they form an algebra. We can easily see this by observing that:

$$T_N H_{N-1}^{(N)} = S_N^{N-1}$$

$$T_N(H_k^{(N)} + H_{k+N}^{(N)}) = S_N^k \quad 0 \leq k < N-1 \tag{A.7}$$

and recalling that $\{S_N^k : 0 \leq k < N-1\}$ is a cyclic group under matrix product.

A (λ)-circulant matrix is any matrix in the space generated by

$$\{T_N H_{N-1}^{(N)}\} \cup \{T_N(H_k^{(N)} + \lambda H_{k+N}^{(N)}) : 0 \leq k < N-1\} \tag{A.8}$$

A (λ)-circulant matrix is denoted by

$$(\lambda) - c(a_0, \ldots, a_{N-1}) \tag{A.9}$$

where a_k : $0 \leq k \leq N-1$ is the coefficient of the k-th element in the basis $(A.8)$. Similarly, we denote a (λ)-skew-circulant matrix by

$$(A.10) \qquad (\lambda) - sc(a_0, \ldots, a_{N-1})$$

The relation between λ-circulant and λ-skew-circulant matrices and circulant and skew-circulant matrices is established as follows:

Let $\lambda = e^{i\alpha}$ and let $\theta = e^{\frac{-i\alpha}{N}}$. Then given $A = (\lambda) - sc(a_0, \ldots, a_{N-1})$, the matrix $B = sc(a_0, \theta a_1, \ldots, \theta^{N-1} a_{N-1})$ is such that:

$$(A.11) \qquad \begin{pmatrix} 1 & & & \\ & \theta & & \\ & & \ddots & \\ & & & \theta^{N-1} \end{pmatrix} A \begin{pmatrix} 1 & & & \\ & \theta & & \\ & & \ddots & \\ & & & \theta^{N-1} \end{pmatrix} = B$$

Indeed, if

$$(A.12) \qquad A = (a(k,l))$$

and

$$(A.13) \qquad B = (b(k,l))$$

and if $0 \leq k, l, k', l' < N$ and $k + l = k' + l' + N$. Then

$$\begin{aligned} b(k,l) &= \theta^{k+l} a(k,l) \\ &= \theta^{k'+l'+N} a(k,l) \\ &= [e^{\frac{-i\alpha}{N}}]^{k'+l'+N} e^{i\alpha} a(k',l') \qquad (A.14) \\ &= e^{\frac{-i\alpha(k'+l')}{N}} a(k',l') \\ &= b(k',l') \end{aligned}$$

Now, according to observation (2.3.21) B is skew-circulant, and thus $(A.11)$ follows.

Similarly we can prove that if $A = (\lambda) - c(a_0, \ldots, a_{N-1})$ then the matrix $B = c(\theta^{N-1}a_0, \ldots, \theta a_{N-2}, a_{N-1})$ is such that:

$$(A.15) \qquad \begin{pmatrix} 1 & & & \\ & \theta & & \\ & & \ddots & \\ & & & \theta^{N-1} \end{pmatrix} A \begin{pmatrix} \theta^{N-1} & & & \\ & \ddots & & \\ & & \theta & \\ & & & 1 \end{pmatrix} = B$$

The diagonalization of circulant and skew-circulant matrices by DFT's is proved now. Consider first the circulant matrix $A = c(a_0, \ldots, a_{N-1})$. Let $\vec{a} = (a_0, \ldots, a_{N-1})$ and let

$$(A.16) \qquad \begin{aligned} \hat{\vec{a}} &= F(N)\vec{a} \\ &= (\hat{a}_0, \ldots, \hat{a}_{N-1}) \end{aligned}$$

we will prove that

$$(A.17) \qquad \begin{pmatrix} \hat{a}_0 & & \\ & \ddots & \\ & & \hat{a}_{N-1} \end{pmatrix} = F(N)^{-1} A F(N)$$

Indeed, since clearly

$$(A.18) \qquad F(N)^{-1} S_N = (\omega^{-k(l-1)})$$

$0 \leq k, l \leq N-1$, then

$$(A.19) \qquad F(N)^{-1} S_N = (\omega^k \omega^{-kl}) = diag - (\omega^k)\ [F(N)]^{-1}$$

hence

$$(A.20) \qquad F(N)^{-1} S_N F(N) = diag - (\omega^k)$$

therefore, for $0 \leq j \leq N-1$

$$(A.21) \qquad F(N)^{-1} S_N^j F(N) = [F(N)^{-1} S_N F(N)]^j = diag - (\omega^{kj})$$

and since $A = \sum_{j=0}^{N-1} a_j S_N^j$ we get

$$
\begin{aligned}
F(N)^{-1}AF(N) &= \sum_{j=0}^{N-1} a_j F(N)^{-1} S_N^j F(N) \\
&= \sum_{j=0}^{N-1} a_j [diag - (\omega^{kj})] \\
&= diag - [\sum_{j=0}^{N-1} a_j \omega^{kj}] \\
&= diag - (\hat{a}_k)
\end{aligned}
\tag{A.22}
$$

On the other hand the relations:

$$F(N)^{-1}T_N = F(N) \tag{A.23}$$

and

$$T_N \; sc(a_0, \ldots, a_{N-1}) = c(a_0, \ldots, a_{N-1}) \tag{A.24}$$

yield, for the skew-circulant matrix $A = sc(a_0, \ldots, a_{N-1})$, the diagonalization formula:

$$F(N)AF(N) = diag - (\hat{a}_k) \tag{A.25}$$

Therefore the complexity of computing with (λ)-circulant and (λ)-skew-circulant matrices is of the order of $O(NlogN)$. Indeed by $(A.22)$ and $(A.25)$ it is sufficient to use the fast Fourier transform algorithm so as to perform the required calculations.

References

[C-T] Cooley,J.W. and Tukey,J.W. *"An algorithm for the machine calculation of complex Fourier series"*. Math. Comput., vol. 19, no. 2, pp 297-301.

[D] Davis,P.J. *Circulant Matrices.* Wiley, New York-Chichester-Brisbane. 1979.

[D-L] Danielson,G.C. and Lanczos,C. *"Some improvements in practical Fourier analysis and their application to x-ray scattering from liquids"* J. Franklin Inst., vol. 233, nos. 4 and 5, pp.365-380 and 435-452, April and May 1942.

[G] Good,I.J. *"The interaction algorithm and practical Fourier analysis"* J.R. Statist. Soc. B, vol 20, no. 2, pp 361-372, 1958.

[I-R] Ireland,K. and Rosen,M. *A Classical Introduction to Modern Number Theory"* Spring-Verlag, New York, 1982.

[R] Rabiner,L.R. *"On the use of symmetry in FFT computation"* IEEE ASSP, vol 27, no. 3, June 1979.

[T] Ten Eyck,L.F. Acta Crystallographica A29, pp. 183-191, 1973.

[H] Hockney,R.W.*" A fast direct solution of Poisson's equation using Fourier analysis "* J. Assoc. Compt. Mach. v. 12, 1965, pp 95-113

[H-J-B] Heideman,M.T., Johnson,D.H. and Burrus,C.S.*"Gauss and the History of the Fast Fourier Transform"* IEEE ASSP magazine, October 1984.

[L-P] Ladd,M.F.C., Palmer,R.A. *" Structure Determination by X-Ray Crystallography"*. Plenum Press. New York, Second Edition, 1985.

[S] Swarztrauber,P.N. *" Fast Poisson solvers"*. MAA Studies in Numerical Analysis, vol. 24 (G.H. Golub, ed.) , Math. Assoc. of America, 1984, pp 319-370.

[To] Tolimieri,R. " Implementing Fast Fourier Transform Algorithms ". To appear

[W] Winograd,S. *"On computing the discrete Fourier transform"* Proc. Nat. Acad. Sci. USA., vol.

73. no. 4, pp 1005-1006, April 1976.

[L] Lee,B.G. *" FCT- A fast cosine transform"* . Proc. IEEE ICASSP 1984, pp 28A.3.1.-28A.3.4.

[M] Makhoul,J. *"A fast cosine transform in one and two dimensions"*. IEEE Trans. Acoust. Speech, Signal Processing, vol. ASSP-28, pp27-34, 1980.

[H-W] Wang,Z., Hunt,B.R. *"The discrete cosine transform - a new version"*. Proc. IEEE ICASSP, Boston, MA, 1983, pp 1256-1259.