

# FFT-like factorizations using group theory

*Steven Delvaux*      *Marc Van Barel*

*Report TW481, December 2006*



Katholieke Universiteit Leuven  
Department of Computer Science  
Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

# FFT-like factorizations using group theory

*Steven Delvaux*      *Marc Van Barel*

*Report TW 481, December 2006*

Department of Computer Science, K.U.Leuven

## Abstract

The Fast Fourier Transform (FFT) is based on an important factorization of the Fourier matrix  $F_n$  into a product of sparse matrices. In this paper, we demonstrate the existence of a set of FFT-like factorizations for an arbitrary Kronecker product of Fourier matrices  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$ . We show that there exists such a factorization for any chain of nested subgroups of the Abelian group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . The classical FFT will then be a special case of this scheme. However, the construction of FFT-like factorizations will allow a lot of freedom. This will allow to construct factorizations which cannot be obtained by simply inserting the classical FFT of each of the Kronecker factors of  $F$ . It will also be shown that the FFT-like factorizations of the matrix  $F$  can be brought into correspondence with the partitions of  $F$  into nested grids of rank-one blocks.

**Keywords :** Fourier matrix, Kronecker product, FFT, group theory, rank-one submatrix.

**AMS(MOS) Classification :** Primary : 42A99, Secondary : 15A69, 15A03, 15A23.

# FFT-like factorizations using group theory

Steven Delvaux <sup>\*</sup>, Marc Van Barel <sup>\*</sup>

15th December 2006

## Abstract

The Fast Fourier Transform (FFT) is based on an important factorization of the Fourier matrix  $F_n$  into a product of sparse matrices. In this paper, we demonstrate the existence of a set of FFT-like factorizations for an arbitrary Kronecker product of Fourier matrices  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$ . We show that there exists such a factorization for any chain of nested subgroups of the Abelian group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . The classical FFT will then be a special case of this scheme. However, the construction of FFT-like factorizations will allow a lot of freedom. This will allow to construct factorizations which cannot be obtained by simply inserting the classical FFT of each of the Kronecker factors of  $F$ . It will also be shown that the FFT-like factorizations of the matrix  $F$  can be brought into correspondence with the partitions of  $F$  into nested grids of rank-one blocks.

**Keywords:** Fourier matrix, Kronecker product, FFT, group theory, rank-one submatrix.

**AMS subject classifications:** 42A99, 15A69, 15A03, 15A23.

## 1 Introduction

This paper is a continuation of the authors' work on Fourier matrices and Kronecker products, and their relations with low rank submatrices and sparse matrix factorizations. Let us start with some definitions.

---

<sup>\*</sup>Department of Computer Science, Katholieke Universiteit Leuven, Celestijnenlaan 200A, B-3001 Leuven (Heverlee), Belgium. email: {Steven.Delvaux,Marc.VanBarel}@cs.kuleuven.be.

The research was partially supported by the Research Council K.U.Leuven, project OT/05/40 (Large rank structured matrix computations), Center of Excellence: Optimization in Engineering, by the Fund for Scientific Research–Flanders (Belgium), G.0455.0 (RHPH: Riemann-Hilbert problems, random matrices and Padé-Hermite approximation), G.0423.05 (RAM: Rational modelling: optimal conditioning and stable algorithms), and by the Belgian Programme on Interuniversity Poles of Attraction, initiated by the Belgian State, Prime Minister's Office for Science, Technology and Culture, project IUAP V-22 (Dynamical Systems and Control: Computation, Identification & Modelling). The scientific responsibility rests with the authors.

For  $A \in \mathbb{C}^{m \times p}$  and  $B \in \mathbb{C}^{n \times q}$ , define the *Kronecker product* of  $A$  and  $B$  as the block matrix

$$A \otimes B = \begin{bmatrix} a_{0,0}B & \dots & a_{0,p-1}B \\ \vdots & & \vdots \\ a_{m-1,0}B & \dots & a_{m-1,p-1}B \end{bmatrix}. \quad (1)$$

For  $n \in \mathbb{N} \setminus \{0\}$ , define the *Fourier matrix* of size  $n$  as  $F_n = \frac{1}{\sqrt{n}}[\omega^{ij}]_{i,j=0}^{n-1}$ , where  $\omega = \exp(2\pi\mathbf{i}/n)$  with  $\mathbf{i} := \sqrt{-1}$ .

The following property is well-known:

$$(AB) \otimes (CD) = (A \otimes C)(B \otimes D),$$

which is valid when the matrix products  $AB$  and  $CD$  are well-defined.

Let us now summarize some of the findings of our earlier work on Fourier matrices. In [2] we described a set of rank-one submatrices of a Fourier matrix with order a power of a prime number  $F_{p^m}$ , and we showed how these submatrices are an indication of a more intrinsic factorization of the matrix  $F_{p^m}$ , namely the well-known Cooley-Tukey FFT-factorization [5, 1].

In [3], we described a set of rank-one submatrices of a general Kronecker product of Fourier matrices

$$F = F_{n_1} \otimes \dots \otimes F_{n_k}. \quad (2)$$

We showed that such submatrices can be constructed in a nested form, and that they can be brought in correspondence with the chains of nested subgroups of the Abelian group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ .

It is then natural to ask if these rank-one submatrices of the matrix  $F$  in (2) are also a reflection of an underlying FFT-like factorization. This will be the subject of the present paper.

This paper is organized as follows. Section 2 provides some basic definitions from group theory and linear algebra. Section 3 contains the main theorem of this paper, involving FFT-like factorizations of a Kronecker product of Fourier matrices  $F$ . It will be shown that such factorizations can be obtained for any chain of nested subgroups of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . Section 4 deals with the intimate relation between the FFT-like factorizations of the matrix  $F$ , and the partitions of  $F$  into nested grids of rank-one blocks. Finally, some conclusions are provided in Section 5.

## 2 Basic definitions and notations

In this section we provide some basic definitions and notations from group theory and multilinear algebra to be used throughout this paper.

We denote by  $\mathbb{Z}_n$  the Abelian group  $\mathbb{Z}_n := \{0, \dots, n-1\}$ , with group operation defined by the addition modulo  $n$ . We denote by  $\mathbb{Z}_m \times \mathbb{Z}_n$  the direct product (cartesian product) group, i.e., the set of couples  $(i_1, i_2)$  with  $i_1 \in \mathbb{Z}_m$

and  $i_2 \in \mathbb{Z}_n$ , with group operation defined by the componentwise addition in  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$ , respectively.

The row indices of the matrix  $A \otimes B$  in (1) can be naturally labeled by means of the direct product group  $\mathbb{Z}_m \times \mathbb{Z}_n$ , while the column indices of this matrix can be naturally labeled by means of the direct product group  $\mathbb{Z}_p \times \mathbb{Z}_q$ . This allows to reformulate the definition of Kronecker product as follows:

$$(A \otimes B)_{i_1, i_2; j_1, j_2} := a_{i_1, j_1} b_{i_2, j_2}, \quad (3)$$

where  $(i_1, i_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$ ,  $(j_1, j_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$  parameterize the rows and columns of (1), respectively.

Similarly, the row indices of the matrix  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$  in (2) can be naturally labeled by means of the direct product group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , and similarly for the columns\*. This allows to reformulate the definition of  $F$  in (2) as follows:

$$F(\mathbf{g}, \mathbf{h}) = \frac{1}{\sqrt{n}} \omega_{n_1}^{g_1 h_1} \dots \omega_{n_k}^{g_k h_k}, \quad (4)$$

where the multi-indices  $\mathbf{g} := (g_1, \dots, g_k)$ ,  $\mathbf{h} := (h_1, \dots, h_k) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  parameterize the rows and columns of  $F$ , respectively, where  $n := n_1 \dots n_k$ , and with  $\omega_k = \exp(2\pi\mathbf{i}/k)$  denoting the  $k$ th root of unity.

We will often find it convenient to abbreviate (4) using the compact notation

$$\omega_{n_1}^{g_1 h_1} \dots \omega_{n_k}^{g_k h_k} =: \boldsymbol{\omega}^{\mathbf{g} \cdot \mathbf{h}}. \quad (5)$$

For example, consider the submatrix of  $F_3 \otimes F_3$  involving the rows labeled by the double indices  $(0, 0)$ ,  $(1, 2)$ ,  $(2, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ , and the columns labeled by the double indices  $(0, 0)$ ,  $(1, 1)$ ,  $(2, 2) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ . The position of this submatrix is shown in Figure 1.

$$F_3 \otimes F_3 = \begin{array}{|c|c|c|} \hline \otimes & \otimes & \otimes \\ \hline & & \\ \hline \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes \\ \hline \end{array}$$

Figure 1: The figure shows the submatrix of  $F_3 \otimes F_3$  whose elements are labeled via the multi-indices mentioned in the text. The entries of the submatrix are shown highlighted.

Note that the submatrix of Figure 1 can be expressed as

$$\frac{1}{\sqrt{9}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad (6)$$

---

\*In fact, this connection is even tighter: the matrix  $F$  is known to be a realization of the so-called *character table* of the Abelian group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  [4].

since for example  $\omega^{(1,2)\cdot(1,1)} := \omega_3^{1\cdot1}\omega_3^{2\cdot1} = \omega_3^3 = 1$ , and similarly for the other entries.

More generally, we have the following definition.

**Definition 1** (*Orthogonality:*) We say  $\mathbf{g}, \mathbf{h} \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  to be orthogonal, denoted  $\mathbf{g} \perp \mathbf{h}$ , if

$$\omega^{\mathbf{g}\cdot\mathbf{h}} = 1. \quad (7)$$

Here we used the notation of (5).

Here are some notions related to the concept of orthogonality. Let  $G$  be a subgroup of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . The *annihilator*

$$H := G^\perp \subset \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$$

is defined as the set of all elements  $\mathbf{h}$  for which  $\mathbf{h} \perp \mathbf{g}$ , for all  $\mathbf{g} \in G$ .

It is known from a theory called *Pontryagin duality* [4] that the annihilator of  $G$  is itself a group, which is isomorphic to the quotient group<sup>†</sup>

$$H \cong (\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k})/G.$$

In particular, it follows that  $|G| \cdot |H| = n$  with  $n := n_1 \dots n_k$ .

Since orthogonality is a symmetric relation, we will sometimes refer to a subgroup  $G$  and its annihilator  $H$  as a pair of *annihilating subgroups*. For example, an obvious pair of annihilating subgroups in  $\mathbb{Z}_3 \times \mathbb{Z}_3$  is given by  $G = \{(0, 0), (1, 0), (2, 0)\}$ ,  $H = \{(0, 0), (0, 1), (0, 2)\}$ . A less obvious pair of annihilating subgroups is given here by  $G = \{(0, 0), (1, 2), (2, 1)\}$ ,  $H = \{(0, 0), (1, 1), (2, 2)\}$ : see (6).

Given  $\mathbf{g} = (g_1, \dots, g_k)$ ,  $\mathbf{h} = (h_1, \dots, h_k) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , we say that  $\mathbf{g} < \mathbf{h}$  if there exists an index  $l$  such that  $g_i = h_i$  for all  $i = 1, \dots, l$ , and  $g_{l+1} < h_{l+1}$ . This is the so-called *lexicographical ordering* on  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ .

An alternative interpretation of the lexicographical ordering is as follows. To an element  $\mathbf{g} = (g_1, \dots, g_k) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , one can associate the number

$$g_1 n_2 \dots n_k + \dots + g_{k-1} n_k + g_k \in \mathbb{Z}_n. \quad (8)$$

Using this identification, the lexicographical ordering on  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  corresponds precisely to the usual ordering of integers in  $\mathbb{Z}_n$ . Note that this identification (8) was already implicitly used in (3), (4).

Given a permutation  $P$  of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , the *associated matrix* of  $P$  is defined as the matrix whose  $\mathbf{j}$ th column contains an entry 1 on its  $P(\mathbf{j})$ th position, and zeros elsewhere. We will use the same symbol  $P$  to denote both the permutation and its associated matrix.

We define the *image* of a permutation  $P$  of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  to be the tuple  $(P(\mathbf{g}_1), \dots, P(\mathbf{g}_n))$ , where  $\mathbf{g}_1, \dots, \mathbf{g}_n$  are the subsequent elements of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , ordered lexicographically such that  $\mathbf{g}_i < \mathbf{g}_j$  if  $i < j$ . We can then state the following definition.

<sup>†</sup>Recall that for an inclusion of Abelian groups  $G \subset G_0$ , the quotient group  $G_0/G$  is defined as the set of all the cosets  $g_0 + G := \{g_0 + g \mid g \in G\}$ , with  $g_0 \in G_0$ . The group operation is defined in the obvious way.

**Definition 2** (*Permutations sorting modulo or anti-modulo a subgroup*.) Given a subgroup  $G \subseteq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , and a permutation  $P$  of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . Define the image of  $P$  as described in the paragraphs above. We say the permutation  $P$  to

- sort the indices modulo  $G$  if the image of  $P$  can be subdivided into the form  $q_1 + G, \dots, q_{|Q|} + G$ .
- sort the indices anti-modulo  $G$  if the image of  $P$  can be subdivided into the form  $g_1 + Q, \dots, g_{|G|} + Q$ .

Here we denoted with  $Q$  a set of representants for the quotient group  $(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k})/G$ . We also assumed a certain order on the sets  $G, Q$ . (This may be the lexicographical ordering, but another order could be used as well).

For example, for the subgroup  $G = \{0, 3\} \subset \mathbb{Z}_6$ , the permutation  $P_1 : 0, 1, 2, 3, 4, 5 \mapsto \mathbf{0}, \mathbf{3}, 1, 4, 2, 5$  sorts the indices modulo  $G$ , while the permutation  $P_2 : 0, 1, 2, 3, 4, 5 \mapsto \mathbf{0}, 1, 2, \mathbf{3}, 4, 5$  sorts the indices anti-modulo  $G$ . Note that the elements of  $G$  were indicated in boldface.

As a second example, consider the subgroup  $G = \{(0, 0), (1, 1)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2$ . Then the permutation  $P_1 : (0, 0), (0, 1), (1, 0), (1, 1) \mapsto (\mathbf{0}, \mathbf{0}), (\mathbf{1}, \mathbf{1}), (0, 1), (1, 0)$  sorts the indices modulo  $G$ , while the permutation  $P_2$  with image  $(\mathbf{0}, \mathbf{0}), (0, 1), (\mathbf{1}, \mathbf{1}), (1, 0)$  sorts the indices anti-modulo  $G$ .

We note that Definition 2 is non-standard. We will need it to obtain compact descriptions of certain permutation matrices  $P$  in what follows.

### 3 FFT and chains of nested subgroups

In this section we state a theorem concerning the existence of FFT-like factorizations for a Kronecker product of Fourier matrices  $F$ . This section is organized as follows. In Subsection 3.1 we state the main result, and we illustrate it for several examples. In Subsection 3.2 we consider the proof of the main theorem.

#### 3.1 FFT-like factorizations: statement of the main theorem

In this subsection we state the main result of this paper. The proof of this theorem is deferred to Subsection 3.2, but we will already illustrate it for some special cases.

We need to introduce a little bit more terminology. Recall that  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  denotes the cartesian product set, with group operation defined by the componentwise *addition* in each of the  $\mathbb{Z}_{n_i}$ . It is a well-known fact that any finite Abelian group  $G$  is isomorphic to such a direct product of cyclic<sup>‡</sup> groups:

$$G \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_p}. \quad (9)$$

<sup>‡</sup>Recall that a group  $G$  is called *cyclic* if it is spanned by a single element  $g \in G$ . This means that  $G = \text{grp}\{g\}$ , where  $\text{grp}\{g\}$  denotes the smallest subgroup of  $G$  containing the element  $g$ . The element  $g$  is then called a *generator* for the group  $G$ .

(We used here indices  $m_1, \dots, m_p$  instead of  $n_1, \dots, n_k$ , since the latter will have a fixed meaning in what follows.) We define then the corresponding Kronecker product of Fourier matrices as

$$F_G := F_{m_1} \otimes \dots \otimes F_{m_p}. \quad (10)$$

Note that this definition is only well-determined if the choice of the factors  $\mathbb{Z}_{m_l}$  in the above decomposition (9) is fixed<sup>§</sup>, but this will be clear from the context in what follows.

In what follows, we will use the notation  $\prod_{i=1}^k A_i$  to denote the matrix product  $A_1 \dots A_k$ . Here it is assumed that the dimensions of the matrices  $A_i$  are compatible.

**Theorem 3** (*FFT-like factorizations:*) *Let  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$  be a matrix as in (2). Consider a chain of nested subgroups of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ :*

$$\{0\} = G_0 \subset G_1 \subset \dots \subset G_{L-1} \subset G_L, \quad (11)$$

with  $G_L = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . Denote the corresponding chain of annihilators by

$$H_0 \supset H_1 \supset \dots \supset H_{L-1} \supset H_L = \{0\}. \quad (12)$$

Then there exist permutations

$$\begin{cases} P_1: \text{sorting simultaneously anti-modulo each of the } G_l, \\ P_2: \text{sorting simultaneously modulo each of the } H_l, \end{cases}$$

such that the matrix  $P_1^T F P_2$  decomposes as

$$P_1^T F P_2 = \prod_{l=1}^L (I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|}) D_l, \quad (13)$$

where each  $I_k$  denotes the identity matrix of size  $k$ ,  $k \in \mathbb{N}$ , where each  $D_l$  denotes a suitable unitary diagonal matrix, with  $D_L := I$ , and where the notation  $F_{G_l/G_{l-1}}$  is defined according to (10), assuming a given identification of the quotient group  $G_l/G_{l-1}$  as in the right hand side of (9).

The proof of Theorem 3 is deferred to Subsection 3.2.

For the remainder of this subsection, we will restrict ourselves to describing some special cases of Theorem 3. First we will show that the factorization (13) generalizes the classical FFT factorization.

To this end, let us first consider the case of the Fourier matrix  $F_{p^m}$  with  $p$  prime. The Abelian group associated to this matrix equals  $\mathbb{Z}_{p^m}$ . We can choose then the chain of subgroups (11) of  $\mathbb{Z}_{p^m}$  as follows:

$$\{0\} \subset \mathbb{Z}_p \subset \dots \subset \mathbb{Z}_{p^{m-1}} \subset \mathbb{Z}_{p^m},$$

---

<sup>§</sup>The nonuniqueness of the decomposition  $G \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_p}$  follows since (i)  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$  whenever  $m$  and  $n$  are coprime, and (ii)  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_n \times \mathbb{Z}_m$ . This is intimately related to the fact that the corresponding character tables satisfy (i)  $F_{mn} = P_1^T (F_m \otimes F_n) P_2$  for certain permutations  $P_1, P_2$  [5, page 195], and (ii) we have the general identity  $A \otimes B = P_3^T (B \otimes A) P_4$  for certain permutations  $P_3, P_4$  [5, page 84].

where we chose  $L = m$ , and where we used the canonical inclusions  $\mathbb{Z}_{p^l} \subset \mathbb{Z}_{p^{l+1}}$  for each  $l$ . Note that we have here all the quotient groups cyclic of the form  $\mathbb{Z}_{p^{l+1}}/\mathbb{Z}_{p^l} \cong \mathbb{Z}_p$ .

The permutation  $P_1$  sorting anti-modulo each of the subgroups  $\mathbb{Z}_{p^l}$  can now be chosen to be the identity operator, while the permutation  $P_2$  sorting modulo each of the annihilators  $\mathbb{Z}_{p^{m-l}}$  can be chosen to be the so-called *digit-reversing permutation*  $P_{p^m}$  (as defined in Definition 9). The factorization (13) becomes

$$FP_{p^m} = \prod_{l=1}^m (I_{p^{l-1}} \otimes F_p \otimes I_{p^{m-l}}) D_l,$$

which is nothing but the well-known Cooley-Tukey FFT-factorization [5]. One could even further specify the value of each of the unitary diagonal matrices  $D_l$  in the above expression by using the information in the proof of Theorem 3, see Section 3.2, but we will not do this here.

More generally, a series of Cooley-Tukey FFT-factorizations is known for the Fourier matrix  $F_n$  with  $n$  arbitrary [5, Chapter 2]. Each such factorization can be obtained from a chain of subgroups

$$\{0\} = \mathbb{Z}_{k_0} \subset \mathbb{Z}_{k_1} \subset \dots \subset \mathbb{Z}_{k_{L-1}} \subset \mathbb{Z}_{k_L} = \mathbb{Z}_n,$$

for a suitable sequence of integers  $k_l$ , with  $k_l$  a divisor of  $k_{l+1}$  for each  $l$ . The corresponding expression for the Cooley-Tukey FFT-factorization is exactly the same as for the case of  $F_{p^m}$  described above, except that the role of the digit-reversing permutation  $P_{p^m}$  should now be replaced by a more general *index-reversing permutation*  $P_{k_1, \dots, k_L}$  (as defined in Definition 10):

$$FP_{k_1, \dots, k_L} = \prod_{l=1}^m (I_{k_{l-1}} \otimes F_{k_l/k_{l-1}} \otimes I_{n/k_l}) D_l.$$

We will now provide another series of examples. To this end, we note that (13) can be used to provide us with a set of nontrivial *automorphisms* of the matrix  $F$ , i.e., equalities of the form  $P_1^T F P_2 = F$  where  $P_1, P_2$  are nontrivial permutations. This will follow from the freedom that we have in the choice of certain generators. (This will become clear in Section 3.2, see Lemma 6). Briefly, this will allow us in certain cases to choose each of the diagonal matrices  $D_l$  in (13) equal to the identity, so that the factorization (13) becomes then

$$\begin{aligned} P_1^T F P_2 &= \prod_{l=1}^L (I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|}) \\ &= (F_{G_1/G_0} \otimes I)(I \otimes F_{G_2/G_1} \otimes I) \dots (I \otimes F_{G_L/G_{L-1}}) \\ &= F_{G_1/G_0} \otimes F_{G_2/G_1} \otimes \dots \otimes F_{G_{L+1}/G_L}, \end{aligned} \quad (14)$$

which is again a Kronecker product of Fourier matrices.

We give now some examples of automorphisms of the matrix  $F$ , i.e., factorizations for which (14) equals precisely the given matrix  $F$ . For the present

examples, we will restrict ourselves to simply observing in an empirical way such a set of automorphisms.

As a first example of this type, consider  $H := \{0, 1, 2\} \subseteq \mathbb{Z}_3$ , with annihilator  $G = \{0\}$ . We have then the automorphism

$$F_3([\mathbf{0}, 2, 1], [\mathbf{0}, \mathbf{2}, \mathbf{1}]) = F_3.$$

Here we denoted the matrix  $P_1^T F_3 P_2$  using a matlab-style notation<sup>¶</sup>.

Note that we have ordered here the elements of  $H$  in a nontrivial way, as  $0, 2, 1$ . Corresponding to the permutation of the columns  $P_2$  which is induced by this ordering of the elements of  $H$ , we have then constructed a permutation of the rows  $P_1$  such that  $P_1^T F_3 P_2 = F_3$ . This is a special case of a general mechanism which will be described in Lemma 6.

As a second example of this type, recall that the subgroups  $H := \{(0, 0), (1, 1), (2, 2)\}$ ,  $G := \{(0, 0), (1, 2), (2, 1)\}$  of  $\mathbb{Z}_3 \times \mathbb{Z}_3$  are annihilating. One can now check the automorphism

$$(F_3 \otimes F_3)([(\mathbf{0}, \mathbf{0}), (1, 0), (2, 0), (\mathbf{2}, \mathbf{1}), (0, 1), (1, 1), (\mathbf{1}, \mathbf{2}), (2, 2), (0, 2)], [(\mathbf{0}, \mathbf{0}), (\mathbf{1}, \mathbf{1}), (\mathbf{2}, \mathbf{2}), (0, 1), (1, 2), (2, 0), (0, 2), (1, 0), (2, 1)]) = F_3 \otimes F_3. \quad (15)$$

Note that again, we have chosen here a fixed ordering for the elements of  $H$  occurring in the permutation  $P_2$ . Corresponding to this choice of ordering of  $P_2$ , we have then constructed a permutation of the rows  $P_1$  (which is then completely determined) such that  $P_1^T (F_3 \otimes F_3) P_2 = F_3 \otimes F_3$ <sup>||</sup>.

We should stress that such automorphisms-like factorizations of the matrix  $F$ , thus for which each of the unitary diagonal matrices  $D_l$  in (13) equals the identity, are only possible under certain conditions on the chain of subgroups (11). This will be one of the topics of the next subsection (more precisely, see Lemma 6).

### 3.2 FFT-like factorizations: proof of the main theorem

In this subsection we come to the proof of Theorem 3. Incidentally, this will lead to some more detailed information about the permutations  $P_1, P_2$  and the unitary diagonal matrices  $D_l$  involved in the statement of this theorem. The reader should of course reacquaint familiarity with the statement of this theorem.

We will first prove Theorem 3 under the assumption that each quotient group  $G_l/G_{l-1} \cong H_{l-1}/H_l$  is cyclic, and of order  $m_l$ , say, for certain  $m_l \in \mathbb{N}$ . (For the

<sup>¶</sup>Matlab is a registered trademark of The MathWorks, Inc.

<sup>||</sup>For the present example (and the previous one), the existence of a suitable permutation  $P_1$  can in fact be anticipated from standard group representation theory. The reason is that the permutation  $P_2$  corresponds here to a *group isomorphism*  $f : G \rightarrow H$ , with  $G = H = \mathbb{Z}_3 \times \mathbb{Z}_3$ . It is known that such an isomorphism induces a one-to-one correspondence between the characters of  $G$  and  $H$ . This one-to-one correspondence induces then the existence of a permutation  $P_1$  such that the corresponding character tables satisfy  $P_1^T F_G P_2 = F_H$ . However, we will deal with more general situations as well, for which we are not aware of such a group representation-based explanation.

general case, see further in this subsection.) Hence

$$G_l/G_{l-1} \cong H_{l-1}/H_l \cong \mathbb{Z}_{m_l}. \quad (16)$$

Denote then with

$$\begin{cases} \mathbf{g}_l \text{ a generator of } G_l \text{ over } G_{l-1}, \\ \mathbf{h}_l \text{ a generator of } H_{l-1} \text{ over } H_l. \end{cases} \quad (17)$$

Here with  $\mathbf{g}$  being a generator of  $B$  over  $A$ , we mean that  $A \subset B$ ,  $\mathbf{g} \in B$  and  $B = \text{grp}\{A, \mathbf{g}\}$ , where we use the notation  $\text{grp}\{V\}$  to denote the smallest subgroup of  $B$  containing all the elements of  $V$ .

Consider now arbitrary  $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . The above construction allows to decompose these elements in a unique way as

$$\begin{cases} \mathbf{a} = a_1 \mathbf{g}_1 + \dots + a_L \mathbf{g}_L, & \text{with each } a_l \in \mathbb{Z}_{m_l}, \\ \mathbf{b} = b_1 \mathbf{h}_1 + \dots + b_L \mathbf{h}_L, & \text{with each } b_l \in \mathbb{Z}_{m_l}. \end{cases} \quad (18)$$

Here we use the notation  $a\mathbf{g}$  with  $a \in \mathbb{N}$  to denote the sum of  $a$  copies of  $\mathbf{g}$ , i.e.,  $\mathbf{g} + \dots + \mathbf{g}$ .

The idea is now to consider  $(a_1, \dots, a_L)$  and  $(b_1, \dots, b_L)$  as *multi-indices* for the rows and columns of a multilevel decomposition of  $F$ , respectively.

To see what this means, let us first recall some ideas behind the standard multilevel decomposition of the matrix  $F$ . Denote with  $\mathbf{e}_l \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  the standard basis vector which is zero except for its  $l$ th component, where it has an entry 1. Then we have that (using the notations of Section 2)

$$\begin{aligned} & \frac{1}{\sqrt{n}} \left[ \omega^{(a_1 \mathbf{e}_1 + \dots + a_k \mathbf{e}_k) \cdot (b_1 \mathbf{e}_1 + \dots + b_k \mathbf{e}_k)} \right]_{a_1, \dots, a_k; b_1, \dots, b_k} \\ &= \frac{1}{\sqrt{n}} \left[ \omega^{(a_1 \mathbf{e}_1) \cdot (b_1 \mathbf{e}_1)} \dots \omega^{(a_k \mathbf{e}_k) \cdot (b_k \mathbf{e}_k)} \right]_{a_1, \dots, a_k; b_1, \dots, b_k} \\ &= \frac{1}{\sqrt{n}} \left[ \omega_{n_1}^{a_1 b_1} \dots \omega_{n_k}^{a_k b_k} \right]_{a_1, \dots, a_k; b_1, \dots, b_k} \\ &= F_{n_1} \otimes \dots \otimes F_{n_k}, \end{aligned} \quad (19)$$

where the first transition follows from the fact that the  $\mathbf{e}_l$  form an *orthogonal set*, i.e.,  $\mathbf{e}_i \perp \mathbf{e}_j$  whenever  $i \neq j$  (as defined in Definition 1), where the second transition follows since  $\omega^{\mathbf{e}_l \cdot \mathbf{e}_l} = \omega_{n_l}$  for all  $l$ , and where the last transition is nothing but the definition of Kronecker product.

Now in the present situation, we will not use the standard basis vectors  $\mathbf{e}_l$  anymore, but use instead the new basis vectors  $\mathbf{g}_l$  and  $\mathbf{h}_l$  constructed in (17) to parametrize the rows and columns in a multilevel decomposition of  $F$ , respectively. Formally, this corresponds to using the permutations

$$\mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}, \quad (20)$$

defined by

$$\begin{cases} P_1 : a_1 m_2 \dots m_L + \dots + a_{L-1} m_L + a_L \mapsto a_1 \mathbf{g}_1 + a_2 \mathbf{g}_2 + \dots + a_L \mathbf{g}_L, \\ P_2 : b_1 m_2 \dots m_L + \dots + b_{L-1} m_L + b_L \mapsto b_1 \mathbf{h}_1 + b_2 \mathbf{h}_2 + \dots + b_L \mathbf{h}_L. \end{cases} \quad (21)$$

Here the numbers on the left are assumed to be in *Euclidean division form*, i.e., we assume that  $a_l \in \mathbb{Z}_{m_l}$  for each  $l$ .

It is easy to see that the mappings  $P_1, P_2$  are *bijective*; see our earlier derivation of (18). To consider  $P_1, P_2$  as *permutations* on  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ , it suffices then to use the natural identification by means of lexicographical ordering of their domain  $\mathbb{Z}_n$  in (20) with  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ .

We should be aware that, in contrast to the  $\mathbf{e}_l$ , the new basis vectors  $\mathbf{g}_l$  and  $\mathbf{h}_l$  for the rows and columns do in general *not* form a biorthogonal system anymore. Indeed, the condition  $\mathbf{g}_i \perp \mathbf{h}_j$  is now only guaranteed to hold when  $i < j$ . The latter follows since for  $i < j$ , we have by construction that  $\mathbf{g}_i \in G_i \subset G_{j-1}$  and  $\mathbf{h}_j \in H_{j-1} = G_{j-1}^\perp$ ; see (17).

The fact that in general  $\mathbf{g}_i \not\perp \mathbf{h}_j$  when  $i > j$  will now cause some extra factors to appear in the multilevel decomposition of  $P_1^T F P_2$ :

$$\begin{aligned} & \frac{1}{\sqrt{n}} \omega^{(a_1 \mathbf{g}_1 + \dots + a_L \mathbf{g}_L) \cdot (b_1 \mathbf{h}_1 + \dots + b_L \mathbf{h}_L)} \\ &= \frac{1}{\sqrt{n}} \prod_{i,j} \omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)} \\ &= \frac{1}{\sqrt{n}} \prod_{i \geq j} \omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)}. \end{aligned} \quad (22)$$

Briefly, the fact that (22) still contains factors with  $i > j$  will cause  $P_1^T F P_2$  to be different from the simple Kronecker product form of (19), but instead to have the more complicated form involving the unitary diagonal matrices  $D_l$  in the right hand side of (13).

To prove this claim, suppose that we fix the first indices  $a_1, b_1$ . We can then refactorize (22) as follows:

$$\frac{1}{\sqrt{n}} \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \prod_{i \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_1 \mathbf{h}_1)} \prod_{i \geq j \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)},$$

or equivalently (distributing the factor  $\sqrt{n}$ )

$$\frac{1}{\sqrt{m_1}} \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \prod_{i \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_1 \mathbf{h}_1)} \frac{1}{\sqrt{n/m_1}} \prod_{i \geq j \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)}. \quad (23)$$

Suppose now that we keep the indices  $a_1, b_1$  fixed, while varying the indices  $a_2, \dots, a_L; b_2, \dots, b_L$ . The elements in (23) constitute then the submatrix

$$\begin{aligned} & \frac{1}{\sqrt{m_1}} \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \text{diag} \left( \prod_{i \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_1 \mathbf{h}_1)} \right)_{a_2, \dots, a_L} \\ & \frac{1}{\sqrt{n/m_1}} \left[ \prod_{i \geq j \geq 2} \omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)} \right]_{a_2, \dots, a_L; b_2, \dots, b_L}. \end{aligned} \quad (24)$$

Recal now that  $a_1, b_1$  are the ‘dominant’ indices in the multilevel decomposition of  $P_1^T FP_2$ , see (21). It follows then from (24) that the  $(a_1, b_1)$ th *block entry* of  $P_1^T FP_2$  is of the form

$$s_{a_1, b_1} D_{b_1} T,$$

where  $S, T$  are fixed matrices (the matrix  $T$  is *fixed* since it is the same for each choice of  $a_1, b_1$ , i.e., for each block entry of  $P_1^T FP_2$ ), and where  $D_{b_1}$  is a certain diagonal matrix depending on the index  $b_1$ , but not on  $a_1$ . The proof of (13) can then be finished by means of a recursive application of the following two lemmas.  $\square$

**Lemma 4** *Let  $S, T$  be given matrices. Suppose that we have given a matrix  $M$  with  $(i, j)$ th block entry given by  $s_{i, j} D_j T$ , where  $D_j$  is a certain diagonal matrix, depending only on  $j$ . More specifically,*

$$M = \begin{bmatrix} s_{0,0} D_0 T & \cdots & s_{0, n-1} D_{n-1} T \\ \vdots & & \vdots \\ s_{m-1,0} D_0 T & \cdots & s_{m-1, n-1} D_{n-1} T \end{bmatrix}.$$

Then we have that

$$M = (S \otimes I) D (I \otimes T), \quad (25)$$

for the diagonal matrix  $D = \text{diag}(D_0, \dots, D_{n-1})$ .

PROOF. The matrix  $S \otimes I$  equals

$$S \otimes I = \begin{bmatrix} s_{0,0} I & \cdots & s_{0, n-1} I \\ \vdots & & \vdots \\ s_{m-1,0} I & \cdots & s_{m-1, n-1} I \end{bmatrix}.$$

On the other hand, we have  $D(I \otimes T) = \text{diag}(D_0, \dots, D_{n-1}) \text{diag}(T, \dots, T) = \text{diag}(D_0 T, \dots, D_{n-1} T)$ . The result follows now immediately.  $\square$

We need also the following, more technical lemma.

**Lemma 5** *Under the assumptions of (16) and (17), let us assume that the generator  $\mathbf{h}_l$  of  $H_{l-1}$  over  $H_l$  has been fixed. Then we can choose the generator  $\mathbf{g}_l$  of  $G_l$  over  $G_{l-1}$  such that*

$$\omega^{\mathbf{g}_l \cdot \mathbf{h}_l} = \omega_{m_l}, \quad (26)$$

i.e., the  $m_l$ th root of unity. Hence

$$\frac{1}{\sqrt{m_l}} \left[ \omega^{(a_l \mathbf{g}_l) \cdot (b_l \mathbf{h}_l)} \right]_{\{a_l, b_l\}=0}^{m_l-1} = \frac{1}{\sqrt{m_l}} \left[ \omega_{m_l}^{a_l b_l} \right]_{\{a_l, b_l\}=0}^{m_l-1} = F_{m_l}, \quad (27)$$

i.e., the Fourier matrix of size  $m_l$ .

PROOF. Consider the map

$$f : G_l \rightarrow \mathbb{C}^\times : \mathbf{g}_l \mapsto \omega^{\mathbf{g}_l \cdot \mathbf{h}_l}, \quad (28)$$

where we use  $\mathbb{C}^\times$  to denote the set  $\mathbb{C} \setminus \{0\}$ , with group operation defined by the usual multiplication of complex numbers. This map  $f$  is a *group morphism*, in the sense that it is compatible with the respective group operations:  $f(\mathbf{g}_l + \tilde{\mathbf{g}}_l) = f(\mathbf{g}_l)f(\tilde{\mathbf{g}}_l)$ . It follows then from standard group theory that the image  $\text{Im}(f)$  must be a *subgroup* of  $\mathbb{C}^\times$ , more precisely

$$\text{Im}(f) \cong G_l / \text{Ker}(f), \quad (29)$$

where  $\text{Ker}(f) := f^{-1}(1)$  denotes the kernel of  $f$ .

We want now to characterize  $\text{Ker}(f)$ . Recalling that  $\mathbf{h}_l$  was chosen as a generator of  $H_{l-1}$  over  $H_l$ , it follows immediately from the definition (28) that

$$\text{Ker}(f) \supseteq H_{l-1}^\perp = G_{l-1}.$$

Substituting this in (29), we see that  $\text{Im}(f)$  must be isomorphic with a *subgroup* of

$$G_l / G_{l-1} \cong \mathbb{Z}_{m_l}. \quad (30)$$

We want to show now that  $\text{Im}(f)$  is actually isomorphic with the *full* group  $\mathbb{Z}_{m_l}$  in (30). Suppose thus by contradiction that  $\text{Im}(f)$  has order  $k < m_l$ . It follows then from the definition (28) that

$$1 = (\omega^{\mathbf{g}_l \cdot \mathbf{h}_l})^k = \omega^{\mathbf{g}_l \cdot (k\mathbf{h}_l)},$$

for all  $\mathbf{g}_l \in G_l$ . Hence  $k\mathbf{h}_l \in G_l^\perp = H_l$ . But since  $\mathbf{h}_l$  was chosen as a generator of  $H_{l-1}$  over  $H_l$ , and in view of (16), the latter is only possible if  $k = m_l$ .

We conclude that  $\text{Im}(f)$  is isomorphic to the group  $\mathbb{Z}_{m_l}$  in (30). Since by construction  $\text{Im}(f)$  is a multiplicative subgroup of  $\mathbb{C}^\times$ , this is only possible if  $\text{Im}(f)$  equals the set of roots of unity  $\{\omega_{m_l}^k\}_{k=0}^{m_l-1}$ . In particular, we have  $\omega_{m_l} \in \text{Im}(f)$ , and hence by the definition (28) there exists a  $\mathbf{g}_l \in G_l$  satisfying the required condition (26).

To conclude the proof, we should then still show that the constructed  $\mathbf{g}_l$  must indeed be a generator of  $G_l$  over  $G_{l-1}$ . But this follows easily since if  $k\mathbf{g}_l \in G_{l-1}$  for some  $k$  with  $0 < k \leq m_l$ , then

$$1 = \omega^{(k\mathbf{g}_l) \cdot \mathbf{h}_l} = (\omega^{\mathbf{g}_l \cdot \mathbf{h}_l})^k = \omega_{m_l}^k,$$

whence  $k = m_l$ . □

Summarizing, we have now finished the proof of Theorem 3 in the case where each  $G_l / G_{l-1} \cong H_{l-1} / H_l \cong \mathbb{Z}_{m_l}$  is cyclic.

Let us now consider the case where

$$G_l / G_{l-1} \cong H_{l-1} / H_l \cong \mathbb{Z}_{m_l^1} \times \dots \times \mathbb{Z}_{m_l^p}, \quad (31)$$

for some  $P \in \mathbb{N}$ . (The superscripts in the above equation are used as *labels*, not powers.) Consider the natural basis for the right hand side of (31), i.e., the set of  $P$ -tuples  $\mathbf{e}_l^p$  which equal zero except for their  $p$ th component which is 1. Denote with  $\mathbf{h}_l^p$  a representant of  $\mathbf{e}_l^p$  in  $H_{l-1}$ , i.e., an element of  $H_{l-1}$  whose image under the natural map  $H_{l-1} \rightarrow H_{l-1}/H_l$  equals  $\mathbf{e}_l^p$ . It follows then for example that

$$\text{grp}\{H_l, \mathbf{h}_l^p\}/H_l \cong \mathbb{Z}_{m_l^p},$$

and

$$\text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\}/H_l \cong \bigotimes_{q \neq p} \mathbb{Z}_{m_l^q}$$

**Lemma 6** *Under the assumption of (31), assume that the generators  $\mathbf{h}_l^p$  of  $H_{l-1}$  over  $H_l$  have been fixed as described in the paragraphs above. Then we can choose a set of generators  $\mathbf{g}_l^p$  of  $G_l$  over  $G_{l-1}$  which form a biorthogonal basis with respect to the  $\mathbf{h}_l^p$ , in the sense that*

$$\mathbf{g}_l^p \perp \mathbf{h}_l^q, \quad (32)$$

whenever  $p \neq q$ , and moreover

$$\omega^{\mathbf{g}_l^p \cdot \mathbf{h}_l^p} = \omega_{m_l^p}, \quad (33)$$

for all  $p$ .

PROOF. The proof is similar to the proof of Lemma 5. Note first that the required biorthogonality conditions imply that  $\mathbf{g}_l^p$  must belong to the group

$$G_l^p := (\text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\})^\perp.$$

Consider now the group morphism

$$f : G_l^p \rightarrow \mathbb{C}^\times : \mathbf{g}_l^p \mapsto \omega^{\mathbf{g}_l^p \cdot \mathbf{h}_l^p}. \quad (34)$$

It follows then that

$$\text{Im}(f) \cong G_l^p / \text{Ker}(f),$$

where we have again the trivial inclusion  $\text{Ker}(f) \supseteq G_{l-1}$ . Thus we see that  $\text{Im}(f)$  is isomorphic to a *subgroup* of

$$\begin{aligned} G_l^p / G_{l-1} &:= (\text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\})^\perp / (H_{l-1})^\perp \\ &= (\text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\})^\perp / (\text{grp}_q\{H_l, \mathbf{h}_l^q\})^\perp \end{aligned} \quad (35)$$

$$\begin{aligned} &\cong \text{grp}_q\{H_l, \mathbf{h}_l^q\} / \text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\} \\ &\cong \mathbb{Z}_{m_l^p}, \end{aligned} \quad (36)$$

where the last transition follows by the choice of the  $\mathbf{h}_l^p$ .

We want now to show that  $\text{Im}(f)$  is actually isomorphic with the *full* group  $\mathbb{Z}_{m_l^p}$  in (36). Suppose thus by contradiction that  $\text{Im}(f)$  has order  $k < m_l^p$ . It follows then that for all  $\mathbf{g}_l^p \in G_l^p$ ,

$$1 = (\omega^{\mathbf{g}_l^p \cdot \mathbf{h}_l^p})^k = \omega^{\mathbf{g}_l^p \cdot (k\mathbf{h}_l^p)},$$

whence  $k\mathbf{h}_l^p \in (G_l^p)^\perp = \text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\}$ . Due to the choice of the  $\mathbf{h}_l^p$ , the latter is only possible if  $k = m_l^p$ .

We conclude that  $\text{Im}f$  is isomorphic with the group  $\mathbb{Z}_{m_l^p}$  in (36). Since by construction  $\text{Im}(f)$  is a multiplicative subgroup of  $\mathbb{C}$ , it follows then easily from the definition (34) that there exists a  $\mathbf{g}_l^p \in G_l^p$  satisfying the required condition (33). By construction of  $G_l^p$ , the required biorthogonality conditions (32) are then also satisfied.

To finish the proof, we should still check that the constructed  $\mathbf{g}_l^p$  form indeed a set of generators of  $G_l$  over  $G_{l-1}$ . Thus we must have that  $G_l = \text{grp}_p(G_{l-1}, \mathbf{g}_l^p)$ , or by passing to the orthogonal complement,

$$\begin{aligned} H_l &= H_{l-1} \cap \bigcap_p (\mathbf{g}_l^p)^\perp \\ &= H_{l-1} \cap \bigcap_p \text{grp}_{q \neq p}\{H_l, \mathbf{h}_l^q\}. \end{aligned}$$

By construction of the  $\mathbf{h}_l^p$ , the latter is indeed satisfied.  $\square$

Lemma 6 provides us with a non-cyclic analogue of (26). To obtain an analogue of (27) as well, one should now replace the indices  $a_l, b_l$  by multi-indices  $(a_l^1, \dots, a_l^P), (b_l^1, \dots, b_l^P)$ , respectively. It follows then from the biorthogonality relations of Lemma 6 that

$$\begin{aligned} & \frac{1}{\sqrt{m_l}} \left[ \omega^{(a_l^1 \mathbf{g}_l^1 + \dots + a_l^P \mathbf{g}_l^P) \cdot (b_l^1 \mathbf{h}_l^1 + \dots + b_l^P \mathbf{h}_l^P)} \right]_{a_1, \dots, a_P; b_1, \dots, b_P} \\ &= \frac{1}{\sqrt{m_l}} \left[ \omega_{m_l^1}^{a_l^1 b_l^1} \dots \omega_{m_l^P}^{a_l^P b_l^P} \right]_{a_1, \dots, a_P; b_1, \dots, b_P} \\ &= F_{m_l^1} \otimes \dots \otimes F_{m_l^P}, \end{aligned} \tag{37}$$

where  $m_l := m_l^1 \dots m_l^P$ . This provides us with the desired analogue of (27).

Observe now that the matrix (37) can be expressed as

$$F_{\mathbb{Z}_{m_l^1} \times \dots \times \mathbb{Z}_{m_l^P}} =: F_{G_l/G_{l-1}},$$

where we used (31). It is then straightforward to adapt the proof of Theorem 3 to the present case. Indeed, one can use exactly the same proof as in the cyclic case ( $P = 1$ ), but now substituting each occurrence of the indices  $a_l, b_l$  by the multi-indices  $(a_l^1, \dots, a_l^P), (b_l^1, \dots, b_l^P)$ , respectively; the details are straightforward.

Summarizing, we have now completely finished the proof of Theorem 3, for the case of arbitrary quotient groups  $G_l/G_{l-1} \cong H_{l-1}/H_l$ .

**Remark 7** *As an illustration of Lemma 6 and the subsequent derivation of (37), let us reconsider the automorphism of  $F_3 \otimes F_3$  that was provided in (15). We have here that  $\omega^{\mathbf{g} \cdot \mathbf{h}} := \omega_3^{g_1 h_1} \omega_3^{g_2 h_2}$ . Eq. (15) follows then from the following set of biorthogonality relations:*

$$\begin{array}{c|cc} \omega^{\mathbf{g} \cdot \mathbf{h}} & (0, 1) & (1, 1) \\ \hline (2, 1) & \omega_3 & 1 \\ (1, 0) & 1 & \omega_3 \end{array}. \tag{38}$$

## 4 FFT and rank-one submatrices

In this section we show the relation between the FFT-like factorizations of the matrix  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$  discussed in Section 3, and the partitions of  $F$  in nested grids of rank-one submatrices. This section is organized as follows. In Subsection 4.1 we discuss some preliminaries about the graphical interpretation of the FFT-like factorizations of the matrix  $F$ . In Subsection 4.2 we consider the relation with grids of rank-one submatrices.

### 4.1 Preliminaries: graphical interpretation of the FFT-like factorizations

In this subsection we discuss some preliminaries about the graphical interpretation of the FFT-like factorizations of Section 3. This material serves as a preparation for some of the material discussed in the next subsection.

We will deal here with Eq. (13), which we restate for convenience:

$$P_1^T F P_2 = \prod_{l=1}^L (I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|}) D_l. \quad (39)$$

We recall the definition of a *Givens transformation*  $G_{i,j}$  acting on rows and columns  $i, j$ , with  $i < j$ . This is defined as a matrix

$$G_{i,j} = \begin{bmatrix} I & & & & \\ & c & & s & \\ & & I & & \\ & -\bar{s} & & \bar{c} & \\ & & & & I \end{bmatrix},$$

where the  $I$  denote identity matrices of suitable sizes, where  $c$  and  $s$  are suitable complex numbers such that  $|c|^2 + |s|^2 = 1$ , and where the nontrivial entries are positioned in rows and columns  $i$  and  $j$ . When such a Givens transformation  $G_{i,j}$  acts on the columns of a matrix  $A \in \mathbb{C}^{n \times n}$ , then all the elements of  $A$  will be preserved, except for the elements in columns  $i$  and  $j$ , which are acted upon according to the 2 by 2 core of the Givens transformation

$$\begin{bmatrix} c & s \\ -\bar{s} & \bar{c} \end{bmatrix}. \quad (40)$$

More generally, one can allow the second row of (40) to be multiplied by a *complex sign*, i.e., by a complex number  $e^{i\theta}$  for some  $\theta \in \mathbb{R}$ .

To allow a graphical representation, we will often denote a Givens transformation acting on the columns of a given matrix  $A$  by means of a *wedge*, where the two legs of the wedge are placed on the position of the columns  $i, j$  of  $A$  on which the Givens transformation acts (see further).

More generally, one can define an *elementary unitary operation*  $G_{i_1, \dots, i_k}$ : this is defined as a unitary operation which equals the identity matrix, except for

the elements in rows and columns  $i_1, \dots, i_k$ . Similarly as above, we will denote an elementary unitary transformation acting on the columns of a given matrix  $A \in \mathbb{C}^{n \times n}$  by means of a wedge, where the  $k$  legs of the wedge are placed on the position of the columns  $i_1, \dots, i_k$  of  $A$  on which the transformation acts (see further).

Now we come to the graphical interpretation of (39). Let us assume for simplicity that each quotient group  $G_{l+1}/G_l$  in (39) is isomorphic to  $\mathbb{Z}_2$ , and that  $L = 3$ ; the general case is completely similar.

We start with the graphical interpretation of the rightmost factor of (39):  $I_4 \otimes F_{\mathbb{Z}_2} = I_4 \otimes F_2 = \text{diag}(F_2, F_2, F_2, F_2)$ . This matrix can clearly be factorized as  $G_{0,1}G_{2,3}G_{4,5}G_{6,7}$ , where each  $G_{2k,2k+1}$  is a Givens transformation acting on rows and columns  $2k, 2k+1$ , where it acts like  $F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ . (The order in which the Givens transformations  $G_{2k,2k+1}$  are multiplied with each other does not matter, since Givens transformations acting on strictly disjoint row and column indices commute with each other.)

Suppose now that we represent each  $G_{2k,2k+1}$  by a wedge, with legs pointing to the columns of an (invisible) matrix  $A \in \mathbb{C}^{8 \times 8}$  on which this operation acts. We can then represent the global factor  $I_4 \otimes F_2 = G_{0,1}G_{2,3}G_{4,5}G_{6,7}$  in a graphical way as

$$\wedge \quad \wedge \quad \wedge \quad \wedge$$

Second, consider now the middle factor  $I_2 \otimes F_{\mathbb{Z}_2} \otimes I_2 = I_2 \otimes F_2 \otimes I_2 = \text{diag}(F_2 \otimes I_2, F_2 \otimes I_2)$ . Obviously, the shape of  $F_2 \otimes I_2$  is given by  $\begin{bmatrix} \times & 0 & \times & 0 \\ 0 & \times & 0 & \times \\ \times & 0 & \times & 0 \\ 0 & \times & 0 & \times \end{bmatrix}$ . We

can therefore factorize the matrix  $I_2 \otimes F_2 \otimes I_2$  as a product of Givens transformations  $G_{0,2}G_{1,3}G_{4,6}G_{5,7}$ . (Again, the order of the Givens transformations does not matter.) Using the same wedge notation as before, we can then represent this matrix graphically as

$$\wedge \wedge \quad \wedge \wedge$$

A similar representation can be derived for the leftmost factor  $F_2 \otimes I_4$ , which is easily seen to allow a factorization as a product of Givens transformations  $G_{0,4}G_{1,5}G_{2,6}G_{3,7}$ .

Finally, note that each of the unitary diagonal matrices  $D_l$  in (39) can be simply absorbed into the corresponding factor  $I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|}$ , hereby not changing the sparsity pattern of the latter matrix. The complete right hand side of (39) can then be visualized as (for reasons to become clear further, we show here actually the action of the *Hermitian transpose* of the right hand side of (39):)

$$\begin{array}{c} \wedge \wedge \wedge \wedge \\ \wedge \wedge \wedge \wedge \\ \wedge \wedge \wedge \wedge \\ \wedge \wedge \wedge \wedge \end{array}$$

One can also consider more general cases. For example, the FFT-like factorization of  $F_6$  induced by the chain of subgroups  $\{0\} \subset \mathbb{Z}_2 \subset \mathbb{Z}_6$ , with the

inclusions defined in the obvious way, looks like (again representing the *Hermitian transpose* of the right hand side of (39))


(41)

Note that we needed here some wedges with three legs to denote the elementary unitary operations induced by the factor  $I_2 \otimes F_3 = \text{diag}(F_3, F_3) = G_{0,1,2}G_{3,4,5}$ . On the other hand, the operations induced by the factor  $F_2 \otimes I_3 = G_{0,3}G_{1,4}G_{2,5}$  were represented by wedges with two legs.

More generally, one has the following result.

**Lemma 8** *Each factor in the right hand side of (39) allows a decomposition of the form*

$$I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|} = \prod_{a \in \mathbb{Z}_{|G_{l-1}|}, c \in \mathbb{Z}_{|H_l|}} G^{(a,c)}, \quad (42)$$

where  $G^{(a,c)}$  is defined to be the elementary unitary operation which equals the identity matrix, except for the elements in rows and columns

$$a|H_{l-1}| + b|H_l| + c, \quad b \in \mathbb{Z}_{|G_l/G_{l-1}|}, \quad (43)$$

where it has a submatrix  $F_{G_l/G_{l-1}}$ .

The correctness of Lemma 8 is easily checked. Moreover, note that the order in which the elementary unitary transformations  $G^{(a,c)}$  are multiplied in (42) is irrelevant. This follows since the expression in (43) has a Euclidean division form, so that these index sets are pairwise disjoint. (See also the examples earlier in this subsection.)

## 4.2 Relation between FFT-like factorizations and rank-one submatrices of $F$

In this subsection we show how the FFT-like factorizations as in (39) are related to the rank-one submatrices of the matrix  $F$ .

We start with some definitions.

**Definition 9** *The digit-reversing permutation induced by an integer  $p^m$ , with  $p$  prime, is defined as the permutation map  $P_{p^m}$  on  $\{0, \dots, p^m - 1\}$  which maps*

$$P_{p^m} : c_{m-1}p^{m-1} + \dots + c_0p^0 \mapsto c_0p^{m-1} + \dots + c_{m-1}p^0.$$

Here the involved numbers are expressed in the  $p$ -based number system, i.e., we assume  $c_k \in \{0, \dots, p-1\}$  for all  $k$ .

For example,  $P_8$  transforms the sequence 0, 1, 2, 3, 4, 5, 6, 7 into the sequence 0, 4, 2, 6, 1, 5, 3, 7.

**Definition 10** (See [5, p. 89]:) More generally, let there be given a sequence of numbers  $p_i \in \mathbb{N}$ ,  $p_i \geq 2$ , for  $i = 0, \dots, m-1$ . The index-reversing permutation induced by the sequence

$$\mathbf{p} := (p_{m-1}, p_{m-2}p_{m-1}, \dots, \prod_{i=0}^{m-1} p_i)$$

is defined as the permutation map  $P_{\mathbf{p}}$  on  $\{0, \dots, (\prod_{i=0}^{m-1} p_i) - 1\}$  which maps

$$P_{\mathbf{p}} : c_{m-1}p_{m-2} \dots p_0 + \dots + c_1p_0 + c_0 \mapsto c_0p_1 \dots p_{m-1} + \dots + c_{m-2}p_{m-1} + c_{m-1}.$$

Here the involved numbers are in Euclidian division form, i.e., we assume  $c_i \in \{0, \dots, p_i - 1\}$ .

For example,  $P_{3,6}$  (we have here  $m = 2$ ,  $p_0 = 2$  and  $p_1 = 3$ ) transforms the sequence 0, 1, 2, 3, 4, 5 into the sequence 0, 3, 1, 4, 2, 5. Thus the indices are sorted modulo 3.

As another example,  $P_{3,6,12}$  transforms the sequence 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 into the sequence 0, 6, 3, 9, 1, 7, 4, 10, 2, 8, 5, 11. Thus the indices are sorted simultaneously modulo 3 and modulo 6.

Definition 9 can be retrieved as a special case of Definition 10, by choosing  $p_i \equiv p$  for all  $i$ . For example, the index-reversing permutation  $P_{2,4,8}$  transforms the sequence 0, 1, 2, 3, 4, 5, 6, 7 into the sequence 0, 4, 2, 6, 1, 5, 3, 7 and can therefore be identified with the digit-reversing permutation  $P_8$  of Definition 9.

Suppose now that we have given a chain of nested subgroups  $G_l$  as in (11), and denote with  $H_l$  the annihilator of  $G_l$ . Then the definition of the index-reversing permutation  $P_{|G_1|, \dots, |G_L|}$  specifies to

$$c_{L-1}|H_1| + \dots + c_1|H_{L-1}| + c_0 \mapsto c_0|G_{L-1}| + \dots + c_{L-2}|G_1| + c_{L-1},$$

where  $c_{L-l} \in \{0, \dots, |G_l/G_{l-1}| - 1\} = \{0, \dots, |H_{l-1}/H_l| - 1\}$ , for all  $l$ . In particular, the *inverse* permutation is given then by

$$P_{|G_1|, \dots, |G_L|}^T = P_{|H_{L-1}|, \dots, |H_0|}.$$

Let us now relate the FFT-like factorizations of Theorem 3 to the rank-one submatrices of the matrix  $F$ . Consider first a chain of subgroups (11) containing only a single nontrivial subgroup:  $\{0\} \subset G_1 \subset G_2 = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . Recall that the elements in the multilevel decomposition of  $P_1^T F P_2$  can be expressed by means of the formula (22), which becomes here

$$\frac{1}{\sqrt{n}} \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \omega^{(a_2 \mathbf{g}_2) \cdot (b_1 \mathbf{h}_1)} \omega^{(a_2 \mathbf{g}_2) \cdot (b_2 \mathbf{h}_2)}.$$

Now suppose that we fix the indices  $a_2$  and  $b_1$ . The corresponding submatrix

of  $F$  becomes then

$$\begin{aligned}
& \frac{1}{\sqrt{n}} \left[ \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \omega^{(a_2 \mathbf{g}_2) \cdot (b_1 \mathbf{h}_1)} \omega^{(a_2 \mathbf{g}_2) \cdot (b_2 \mathbf{h}_2)} \right]_{a_1, b_2} \\
&= \frac{1}{\sqrt{n}} \omega^{(a_2 \mathbf{g}_2) \cdot (b_1 \mathbf{h}_1)} \left[ \omega^{(a_1 \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \omega^{(a_2 \mathbf{g}_2) \cdot b_2 \mathbf{h}_2} \right]_{a_1, b_2} \\
&= \frac{1}{\sqrt{n}} \omega^{(a_2 \mathbf{g}_2) \cdot (b_1 \mathbf{h}_1)} \begin{bmatrix} \omega^{(a_{1,1} \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \\ \vdots \\ \omega^{(a_{1,|G_1|} \mathbf{g}_1) \cdot (b_1 \mathbf{h}_1)} \end{bmatrix} \\
& \quad \left[ \omega^{(a_2 \mathbf{g}_2) \cdot (b_{2,1} \mathbf{h}_2)} \quad \dots \quad \omega^{(a_2 \mathbf{g}_2) \cdot (b_{2,|H_1|} \mathbf{h}_2)} \right] \\
&=: \text{Rk } 1,
\end{aligned}$$

which is a submatrix of rank one.

Since the above argument holds for *any* fixed choice of  $a_2, b_1$ , it follows that the matrix (the provenance of the factor  $P_{|H_1|, |H_0|}^T$  will be explained further)

$$P_{|H_1|, |H_0|}^T P_1^T F P_2 \quad (44)$$

can be subdivided in a grid of rank-one submatrices, i.e.,

$$P_{|H_1|, |H_0|}^T P_1^T F P_2 = \begin{bmatrix} \text{Rk } 1 & \dots & \text{Rk } 1 \\ \vdots & & \vdots \\ \text{Rk } 1 & \dots & \text{Rk } 1 \end{bmatrix}, \quad (45)$$

where each Rk 1 denotes a matrix of rank 1, having size  $|G_1|$  by  $|H_1|$ . (For notational simplicity, we represent here each rank-one block by the same notation Rk 1, but these different blocks do not have to be equal to each other.)

Indeed, the presence of the index-reversing permutation  $P_{|H_1|, |H_0|}^T$  in (44) can be explained as follows: it was shown above that in order to obtain the grid of rank-one submatrices, the indices  $a_2, b_1$  should be fixed. Hence the indices  $a_1, a_2$  parametrizing the rows in the multilevel decomposition of  $P_1^T F P_2$  must be ordered in the *reverse* order, since we need  $a_2$  (and not  $a_1$ ) to be the fixed coordinate describing the block rows of (45). It is easy to see that the permutation achieving this reversal of coordinates  $a_1, a_2$  is precisely the index-reversing permutation  $P_{|H_1|, |H_0|}^T$  (appearing with a transpose sign, since it is applied to the *rows* and not to the columns.)

Concerning this last claim, note that the permutation  $P_1$  has image  $0, \mathbf{g}_2, \dots, (m_2 - 1)\mathbf{g}_2, \mathbf{g}_1, \dots$ , cf. (21). To select from this image the indices  $0, \mathbf{g}_1, \dots, (m_1 - 1)\mathbf{g}_1$ , it suffices then to sort these indices modulo  $m_2 = |H_1|$ , which was to be demonstrated.

Also for a general chain of subgroups (11), one can apply these ideas. One should then fix the indices  $a_{l+1}, \dots, a_L$  and  $b_1, \dots, b_l$ , for a certain value of  $l$ . By the absence of all the factors  $\omega^{(a_i \mathbf{g}_i) \cdot (b_j \mathbf{h}_j)}$  with  $i < j$  in (22), it is then easy to see that the obtained submatrix of  $F$  is of rank one. Since this must hold for

any value of  $l$ , we obtain in this way a family of partitions of the matrix  $F$  into nested grids of rank-one blocks.

We can summarize this as follows.

**Theorem 11** *Let  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$  be a matrix of the form (2), assume a chain of subgroups  $G_l$  of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  as in (11), and denote with  $H_l$  the annihilator of  $G_l$ . Denote with  $P_1, P_2$  the permutations such that  $P_1^T F P_2$  allows an FFT-like decomposition as provided by Theorem 3. Then the matrix*

$$A = P_{|H_{L-1}|, \dots, |H_0|}^T P_1^T F P_2 \quad (46)$$

*can be subdivided in a grid of rank-one blocks of size  $|G_l|$  by  $|H_l|$ , and this simultaneously for all  $l = 1, \dots, L$ . Here we used  $P_{|H_{L-1}|, \dots, |H_0|}$  to denote the index-reversing permutation defined in Definition 10.*

Note that the permutations acting on the rows and columns of  $F$  in (46) sort simultaneously *modulo* each of the  $G_l, H_l$ , respectively. This follows since the need to reverse the order of the coordinates  $a_l$ , i.e., the presence of the factor  $P_{|H_{L-1}|, \dots, |H_0|}^T$  in (46), turns the *anti-modulo* sorting permutation  $P_1$  of Theorem 3 into a *modulo* sorting permutation. In this way, the conclusion of Theorem 11 is consistent with an observation in [3].

Conversely, and maybe surprisingly, the presence of the rank-one submatrices in Theorem 11 is in fact sufficient to guarantee the existence of an underlying FFT-like factorization. This correspondence is not *total* in the sense that the factors in (39) will now not need to be of Kronecker type ( $I_{|G_{l-1}|} \otimes F_{G_l/G_{l-1}} \otimes I_{|H_l|}$ )  $D_l$  anymore; but they will at least have the same *sparsity pattern*.

The way how to see this was essentially presented in [2]. We will now adapt these arguments to the present case.

We will illustrate the idea for a *unitary* matrix  $A \in \mathbb{C}^{6 \times 6}$ , under the assumption that this matrix can be simultaneously subdivided in a grid of rank-one blocks of size 2 by 3, and a (trivial) grid of rank-one blocks of size 1 by 6. We want then to obtain an FFT-like factorization for this matrix: see Figure 2.

Let us comment on this figure. The general idea is to compress the elements in the low rank blocks of the matrix  $A$  by means of elementary unitary transformations. In the first step of the compression process, we consider the partition of the matrix  $A$  in a 3 by 2 grid of rank-one blocks: see Figure 2(a). Since the three columns of such a rank-one block are obviously linear multiples of each other, it is possible to find elementary unitary transformations  $G_{0,1,2}, G_{3,4,5}$ , chosen to annihilate the elements in columns 1, 2, 4, 5 of the topmost collection of rank-one blocks, and in columns 2, 5 of the middle collection of rank-one blocks.

From the assumed unitarity of the matrix  $A$ , it follows then that simultaneously the elements in columns 0, 3 of the middle rank-one blocks, and columns 0, 1, 3, 4 of the *bottommost* collection of rank-one blocks must be annihilated under this process, hereby leading to the sparsity pattern in Figure 2(c).

Indeed: note that after applying an elementary unitary transformation  $G_{3k, 3k+1, 3k+2}$  to a triple of columns, by construction, the submatrix formed

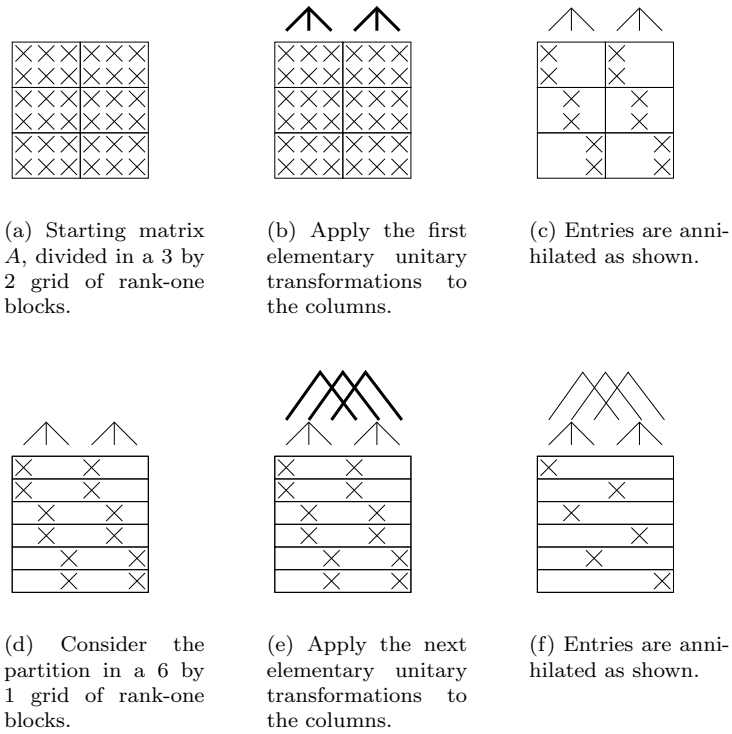


Figure 2: Obtaining an FFT-like factorization for a unitary matrix  $A \in \mathbb{C}^{6 \times 6}$ . It is assumed that this matrix can be simultaneously subdivided in a grid of rank-one blocks of size 2 by 3, and one with blocks of size 1 by 6.

by these three columns takes the form

$$\begin{bmatrix} \mathbf{u} & \mathbf{0} & \mathbf{0} \\ a\mathbf{v} & b\mathbf{v} & \mathbf{0} \\ c\mathbf{w} & d\mathbf{w} & e\mathbf{w} \end{bmatrix}, \quad (47)$$

for suitable column vectors  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^{2 \times 1}$  and scalars  $a, b, c, d, e \in \mathbb{C}$ . (We expressed here that the middle block row must still be of rank one, and hence must have column space spanned by a single vector  $\mathbf{v} \in \mathbb{C}^{2 \times 1}$ , and similarly for the bottom block row). Now since both the matrix  $A$  and the applied elementary unitary transformation are *unitary*, the columns of (47) should be orthonormal to each other. It follows that  $d\bar{e}\|\mathbf{w}\|^2 = 0$ . But since both  $e = 0$  and  $\|\mathbf{w}\| = 0$  are impossible since they would imply the matrix to be singular, it follows that necessarily  $d = 0$ . Similarly, it can be shown that  $a = 0$  and  $c = 0$ , which was to be demonstrated.

We can summarize the resulting sparsity pattern of Figure 2(c) by

$$(0, 1, 2, 3, 4, 5) \mapsto (0, 1, 2, 0, 1, 2), \quad (48)$$

where we have  $k \mapsto 0$  when the weight of the  $k$ th column is completely concentrated in its two topmost rows,  $k \mapsto 1$  when it is concentrated in the two middle rows, and  $k \mapsto 2$  when it is concentrated in the two bottommost rows.

We consider now the partition of  $A$  in a 6 by 1 grid of rank-one blocks: see Figure 2(d). Note that the row grid is refined by this operation. Now we choose elementary unitary transformations  $G_{0,3}, G_{1,4}, G_{2,5}$  to eliminate the topmost nonzero element in each of the columns 3, 4, 5. Again, the unitarity of the matrix  $A$  will then imply simultaneously the *bottommost* nonzero element of the columns 0, 1, 2 to be annihilated, resulting in the sparsity pattern of Figure 2(f).

We can summarize the resulting sparsity pattern of Figure 2(f) by

$$(0, 1, 2, 3, 4, 5) \mapsto (0, 2, 4, 1, 3, 5), \quad (49)$$

where we have  $k \mapsto 0$  when the weight of the  $k$ th column is completely concentrated in its topmost row, and similarly for the other values 1, 2, 3, 4, 5.

From the above description of the compression process, it follows that the matrix resulting at the end of this process, will have precisely the same sparsity pattern as the *index-reversing permutation*  $P_{2,6}$ : cf. (49).

To see the general mechanism behind this, note that in the first step of the compression process, we have brought the weight of the  $k$ th column completely to the 0th, the first or the second block row of  $A$ , cf. (48). It was found that this assignment depends only on the column index modulo 3, which is the *trailing* digit  $c_0$  in the Euclidean division  $k = c_1 3 + c_0$ . On the other hand, the assigned block row can be considered as assigning the *leading* digit  $c_0$  in the Euclidean division  $r = c_0 2 + c_1$ , where  $r$  denotes the row index corresponding to the column index  $k$ . Applying this argument recursively, the relation with the index-reversing permutation should now be clear.

In fact, by the unitarity of the matrix  $A$ , each of the columns of the compressed matrix must still have norm equal to one, and hence by suitable choice of the complex signs of the applied elementary unitary transformations, the resulting matrix can be chosen to be precisely *equal* to the index-reversing permutation  $P_{2,6}$ : see Figure 3.

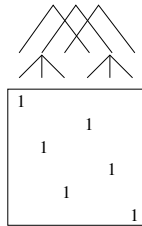


Figure 3: The figure shows the resulting permutation matrix  $P_{2,6}$  obtained at the end of the compression process of Figure 2.

Summarized, we have obtained a factorization

$$AG^H = P_{2,6},$$

where  $G^H$  denotes the product of all the elementary unitary transformations used in the compression process. It follows that

$$A = P_{2,6}G.$$

Since the matrix  $G^H$  has exactly the same sparsity pattern as we obtained in (41), this provides us then with the desired ‘FFT-like factorization’ of the matrix  $A$ .

In the general case, we have the following result.

**Theorem 12** *Assume a chain of subgroups  $G_l$  of  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$  as in (11), and let  $A \in \mathbb{C}^{n \times n}$  be a unitary matrix which can be subdivided in a grid of rank-one blocks of size  $|G_l|$  by  $|H_l|$ , and this simultaneously for all  $l = 1, \dots, L$ . Then we have the following converse of Theorem 11: there exists a factorization*

$$A = P_{|G_1|, \dots, |G_k|} G,$$

where  $P_{|G_1|, \dots, |G_k|}$  denotes the index-reversing permutation defined in Definition 10, and where  $G$  is a product of elementary unitary matrices, whose factors have exactly the same sparsity pattern as the factors in the right hand side of (39), in the sense of Lemma 8.

## 5 Conclusion

In this paper we described a class of FFT-like factorizations for a Kronecker product of Fourier matrices  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$ . We showed that there exists

such a factorization for any chain of nested subgroups of the Abelian group  $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ . The obtained class of FFT-like factorizations generalizes the classical Cooley-Tukey FFT-factorizations, the latter corresponding to the case of a *single* Fourier matrix  $F_n$ .

The mechanism behind the FFT-like factorizations of this paper is a multi-level decomposition of the matrix  $F$ , where the generators  $\mathbf{g}_l, \mathbf{h}_l$ ,  $l = 1, \dots, L$  of the different levels of the rows and columns have to satisfy certain partial biorthogonality conditions. The trivial multilevel factorization of  $F = F_{n_1} \otimes \dots \otimes F_{n_k}$  (induced by the very definition of  $F$  as a Kronecker product) follows as a special case by choosing the generators of rows and columns as the standard basis vectors  $\mathbf{e}_l$ ,  $l = 1, \dots, k$ , in which case the system of generators is completely biorthogonal.

We showed that the FFT-like factorizations lead to a partition of  $F$  into nested grids of rank-one submatrices, hereby retrieving an observation from [3]. Conversely, we showed that (a slightly larger class of) FFT-like factorizations can be obtained under the weaker assumption that the given matrix allows a subdivision into nested grids of rank-one matrices, hereby generalizing an observation from [2]. Some graphical illustrations of these factorizations, and of the corresponding construction mechanism, have been provided.

## References

- [1] J. W. Cooley and J. W. Tukey. An algorithm for the machine computation of complex Fourier series. *Mathematics of Computation*, 19:297–301, 1965.
- [2] S. Delvaux and M. Van Barel. Rank-deficient submatrices of Fourier matrices. Technical Report TW470, Department of Computer Science, Katholieke Universiteit Leuven, September 2006.
- [3] S. Delvaux and M. Van Barel. Rank-deficient submatrices of Kronecker products of Fourier matrices. Technical Report TW477, Department of Computer Science, Katholieke Universiteit Leuven, November 2006.
- [4] W. Rudin. *Fourier Analysis on Groups*. Wiley Interscience, 1962.
- [5] C. F. Van Loan. *Computational Frameworks for the Fast Fourier Transform*. Frontiers in Applied Mathematics. SIAM, 1992.