Available online at www.sciencedirect.com
ScienceDirect
Linear Algebra and its Applications 418 (2006) 719–736
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

Permutation equivalence classes of kronecker products of unitary Fourier matrices

Wojciech Tadej

Cardinal Stefan Wyszyński University, Faculty of Mathematics and Natural Sciences, College of Sciences, ul. Dewajtis 5, 01-815 Warszawa, Poland

Received 7 March 2005; accepted 5 March 2006
Available online 27 April 2006
Submitted by H. Schneider

Abstract

Kronecker products of unitary Fourier matrices play an important role in solving multilevel circulant systems by a multidimensional fast Fourier transform. They are also special cases of complex Hadamard (Zeilinger) matrices arising in many problems of mathematics and theoretical physics. The main result of the paper is splitting the set of all kronecker products of unitary Fourier matrices into permutation equivalence classes. The choice of the permutation equivalence to relate the products is motivated by the quantum information theory problem of constructing maximally entangled bases of finite dimensional quantum systems. Permutation inequivalent products can be used to construct inequivalent, in a certain sense, maximally entangled bases.

AMS classification: 65T50; 05B20; 15A69; 15A90

Keywords: Fourier matrix; Kronecker product; Permutation equivalence

1. Introduction

Kronecker products of unitary Fourier matrices, that is of matrices of the form:

$$[F_n]_{i,j} = \frac{1}{\sqrt{n}} e^{i\frac{2\pi}{n}(i-1)(j-1)}, \quad i, j \in \{1, 2, \ldots, n\}, \tag{1}$$

play an important role in solving multilevel circulant systems, that is linear systems with matrices being linear combinations of kronecker products of circulant matrices with the same structure.

E-mail address: wtadej@wp.pl

0024-3795/$ - see front matter
doi:10.1016/j.laa.2006.03.004

As Fourier matrices diagonalize circulant matrices, their kronecker products diagonalize such linear combinations, so repeated application of a multidimensional fast Fourier transform enables one to solve effectively multilevel circulant systems. Systems of this sort occur in problems of solving partial differential equations with periodic (or partially periodic) boundary conditions, image restoration problems (two-level circulants), problems of approximating multilevel Toeplitz matrices by multilevel circulants, which in turn arise in any context where one encounters a 'shift invariant property'. Some applications of multilevel circulant and Toeplitz matrices are considered in [2], while [3] exposes computational schemes for a multidimensional FFT.

This work, however, originates from an other research area, namely that of finding and classifying all real and complex Hadamard (Zeilinger) matrices, that is unitary matrices with equal moduli of their entries. Hadamard matrices find numerous applications in various mathematical problems (see e.g. [7,5,6]) and theoretical physics (see e.g. [10,11,13,9]). The question of finding all real and complex Hadamard matrices is still open, see [14,17,15,8,16] for recent developments.

This article resolves the question when a kronecker product of Fourier matrices can be transformed into another such product by left and right multiplying it by permutation matrices. It appears that the answer to this question does not change if, apart from permutations, we allow multiplication by unitary diagonal matrices. The particular problem, which motivated the author to discriminate between various kronecker products of Fourier matrices using the above criterion, presented in [18], arises in the quantum information theory and can be described, in terms of linear algebra, as follows.

Consider two d dimensional quantum systems $\mathscr{A}$ and $\mathscr{B}$, with $\mathbf{C}^d$ being the state space for each of them, and $\mathbf{C}^d \otimes \mathbf{C}^d = \mathbf{C}^{d^2}$ the state space of the composite system $\mathscr{A}\mathscr{B}$. Let $[a_j] = [a_0, a_1, \ldots, a_{d-1}]$ and $[b_k] = [b_0, b_1, \ldots, b_{d-1}]$ be orthonormal bases of $\mathbf{C}^d$, chosen for $\mathscr{A}$ and $\mathscr{B}$ respectively. Then $[a_j \otimes b_k]$, $j, k \in \{0, 1, \ldots, (d-1)\}$ is an orthonormal basis for the state space $\mathbf{C}^{d^2}$ of $\mathscr{A}\mathscr{B}$, $\otimes$ denoting the kronecker product here and onwards.

A new basis $[f^H_{j,k}]$ for $\mathscr{A}\mathscr{B}$ is generated from $[a_j \otimes b_k]$ by sending a state vector $a_j \otimes b_k$ through the 'local operation' unitary quantum gate G_1 defined on the basis vectors by

$$G_1(a_j \otimes b_k) = \left(\sum_{i=0}^{d-1} H_{i,j} a_j\right) \otimes b_k, \tag{2}$$

where H is a unitary $d \times d$ matrix, and then sending the result through the 'nonlocal operation' unitary gate G_2 defined by

$$G_2(a_j \otimes b_k) = a_j \otimes b_{(j-k) \bmod d}. \tag{3}$$

That is, $\left[f^H_{j,k}\right]$ is defined by

$$f^H_{j,k} = G_2 G_1 (a_j \otimes b_k). \tag{4}$$

The basis $\left[f^H_{j,k}\right]$ is said to be maximally entangled iff for any $j, k \in \{0, 1, \ldots, (d-1)\}$ the sum of the d disjoint $d \times d$ diagonal blocks of the $d^2 \times d^2$ projection matrix $(f^H_{j,k}) \cdot (f^H_{j,k})^{\star}$ (so called partial trace of this matrix) is equal to $\frac{1}{d} I$. A unitary matrix H must have equal moduli of its entries for $[f^H_{j,k}]$ to be maximally entangled, i.e. H must be a complex Hadamard matrix.

Next a bases equivalence relation is introduced. Two bases $\left[f^{H_1}_{j,k}\right]$ and $\left[f^{H_2}_{j,k}\right]$ are $\equiv$ equivalent iff one can transform one of these bases into the other by a 'local' unitary operation, that

is there exist unitary $d \times d$ matrices U_1 and U_2, permutations $\pi_1, \pi_2 : \{0, 1, \ldots, (d-1)\} \to \{0, 1, \ldots, (d-1)\}$ and phases $\phi_{j,k}$, $j, k \in \{0, 1, \ldots, (d-1)\}$ such that

$$f^{H_2}_{j,k} = \mathrm{e}^{\mathrm{i}\phi_{j,k}} \cdot (U_1 \otimes U_2) \cdot f^{H_1}_{\pi_1(j),\pi_2(k)}. \tag{5}$$

The phase factor $\mathrm{e}^{\mathrm{i}\phi_{j,k}}$ is allowed since multiplying a state vector of a quantum system by such a factor (or any complex number) produces a vector representing the same state.

It is shown in [18] that if H_1, H_2 are kronecker products of unitary Fourier matrices then $\left[f^{H_1}_{j,k}\right] \equiv \left[f^{H_2}_{j,k}\right]$ is equivalent to the existence of permutation matrices P_r, P_c such that $H_2 = P_r \cdot H_1 \cdot P_c$.

Section 2 of this article provides the reader with definitions of particular forms of kronecker products of Fourier matrices, as well as with some basic facts concerning permutation equivalence of these.

Section 3 features the main result, namely splitting all the kronecker products of Fourier matrices into permutation equivalence classes.

In Section 4 possible applications of this result in the operator theory and quantum information theory are presented.

2. Kronecker products of Fourier matrices and permutation equivalence

2.1. Kronecker products of Fourier matrices

By abuse of notation, we will write a Fourier matrix instead of a unitary Fourier matrix. This is defined by

Definition 2.1. A *Fourier matrix* of size n is an $n \times n$ matrix defined by

$$[F_n]_{i,j} = \frac{1}{\sqrt{n}} \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}(i-1)(j-1)}, \quad i, j \in \{1, 2, \ldots, n\}. \tag{6}$$

Definition 2.2. A *Fourier kronecker product* (FKP, FKP product, FKP subproduct) is a matrix F such that

$$F = F_{N_1} \otimes F_{N_2} \otimes \cdots \otimes F_{N_r}, \tag{7}$$

where $r, N_1, N_2, \ldots, N_r$ are some natural numbers and F_k is the Fourier matrix of size k.

Definition 2.3. A *factored Fourier kronecker product* (FFKP, FFKP product, FFKP subproduct) is a matrix F such that

$$F = F_{P_1} \otimes F_{P_2} \otimes \cdots \otimes F_{P_r}, \tag{8}$$

where r is a natural number, $P_1, P_2, \ldots, P_r$ are natural powers of prime numbers, not necessarily distinct ones.

Definition 2.4. A *pure FFKP* (p.FFKP) is an FFKP (see Definition 2.3) of the form, where a is a prime number:

$$F = F_{a^{k_m}} \otimes F_{a^{k_{m-1}}} \otimes \cdots \otimes F_{a^{k_1}}. \tag{9}$$

It is called *ordered* (p.o.FFKP) if $k_m \geqslant k_{m-1} \geqslant \cdots \geqslant k_1$.

2.2. Types of rows in FKP's

Definition 2.5. A *row of type* $1/(n)$, n a natural number, of an FKP product of size N (see Definition 2.2), is a row containing the elements:

$$\frac{1}{\sqrt{N}}\exp\left(\mathrm{i}\frac{2\pi}{n}0\right), \frac{1}{\sqrt{N}}\exp\left(\mathrm{i}\frac{2\pi}{n}1\right), \ldots, \frac{1}{\sqrt{N}}\exp\left(\mathrm{i}\frac{2\pi}{n}(n-1)\right) \tag{10}$$

each of which occurs the same number of times in this row.

We omit the proofs of the following easy lemmas that will be used further. The lemmas are implied by the rules of arithmetic modulo N.

Lemma 2.6. *A Fourier matrix* F_{a^m}, *where* a *is a prime number and* m *is natural, contains only rows of types* $1, 1/(a), 1/(a^2), \ldots, 1/(a^m)$. *The number of rows of each of those types is, respectively,* $1, (a-1), (a-1)a, \ldots, (a-1)a^{m-1}$. *That is, there are* $(a-1)a^{r-1}$ *rows of type* $1/(a^r)$.

Lemma 2.7. *The kronecker product of two rows of types* $1/(a^k)$, $1/(a^l)$ *is a row of type* $1/(a^{\max(k,l)})$.

Lemma 2.8. *The kronecker product of two rows of types* $1/(p), 1/(q)$, *where* p *and* q *are relatively prime natural numbers is a row of type* $1/(pq)$.

Using the above lemmas and the fact that rows of a kronecker product are kronecker products of rows of kronecker product factors, one can easily prove the two lemmas below.

Lemma 2.9. *A pure ordered FFKP* (*see Definition* 2.4) *product of the form*

$$F = F_{a^{k_m}} \otimes F_{a^{k_{m-1}}} \otimes \cdots \otimes F_{a^{k_1}} \tag{11}$$

contains only rows of types $1, 1/(a), 1/(a^2), \ldots, 1/(a^{k_m})$.

Lemma 2.10. *An FFKP product* F *being a kronecker product of two pure ordered FFKP's* (*see Definitions* 2.3 *and* 2.4), $a \neq b$ *prime numbers*:

$$F = F' \otimes F'', \quad F' = F_{a^{k_m}} \otimes \cdots \otimes F_{a^{k_1}}, \quad F'' = F_{b^{l_n}} \otimes \cdots \otimes F_{b^{l_1}} \tag{12}$$

contains only rows of types $1/(a^k b^l)$ *where* $k \in \{0, 1, \ldots, k_m\}$, $l \in \{0, 1, \ldots, l_n\}$.

More generally, we have:

Lemma 2.11. *An FFKP product* F *being a kronecker product of* r *pure ordered FFKP's for* r *different primes* $a_1, a_2, \ldots, a_r$:

$$F = F^{(1)} \otimes F^{(2)} \otimes \cdots \otimes F^{(r)}, \tag{13}$$

where

$$F^{(k)} = F_{a_k^{p_{m^{(k)}}^{(k)}}} \otimes \cdots \otimes F_{a_k^{p_1^{(k)}}} \tag{14}$$

contains only rows of types $1/(a_1^{l_1} \cdots a_r^{l_r})$, *where* $l_k \in \left\{0, 1, \ldots, p_{m^{(k)}}^{(k)}\right\}$.

2.3. Kronecker multiindexing and reordering products

We will need the alternative way of indexing elements in a matrix having a kronecker product structure.

Definition 2.12. A *kronecker multiindex* $i_1, \ldots, i_r; j_1, \ldots, j_r$, where $i_k, j_k \in \{1, \ldots, n_k\}$, $n_k \in \mathbf{N}$ into a square matrix A of size $n = n_1 \cdot n_2 \cdots n_r$ (corresponding to the potential kronecker product structure of $A = A_1 \otimes A_2 \otimes \cdots \otimes A_r$, where A_k of size n_k) indicates the i, jth element of A, where

$$i = (i_1 - 1)\prod_{k=2}^{r} n_k + (i_2 - 1)\prod_{k=3}^{r} n_k + \cdots + (i_{r-1} - 1)n_r + i_r,$$
$$j = (j_1 - 1)\prod_{k=2}^{r} n_k + (j_2 - 1)\prod_{k=3}^{r} n_k + \cdots + (j_{r-1} - 1)n_r + j_r.$$

We write $i_1, \ldots, i_r$ or $j_1, \ldots, j_r$ to kronecker multiindex a row or column, respectively.

The newly introduced method of indexing has the following property:

Remark 2.13. Let $H = H_1 \otimes H_2 \otimes \cdots \otimes H_r$ be a kronecker product of matrices H_k of size n_k. Then the $i_1, \ldots, i_r; j_1, \ldots, j_r$th element of H is given by

$$H_{i_1,\ldots,i_r;j_1,\ldots,j_r} = [H_1]_{i_1,j_1} \cdot [H_2]_{i_2,j_2} \cdots [H_r]_{i_r,j_r} \tag{15}$$

as well as it allows us to construct left and right permutation matrices effectively changing the order of factors in a kronecker product:

Remark 2.14. Reordering factors of a kronecker product is equivalent to left and right multiplying this product by appropriate permutation matrices (thus reordering does not change the row types present in an FKP).

These permutations are defined in the following way. Suppose we reorder $H = H_1 \otimes \cdots \otimes H_r$, H_k of size n_k, into $H' = H_{\sigma(1)} \otimes \cdots \otimes H_{\sigma(r)}$, where σ is a permutation. Then the i, jth element of H, kronecker multiindexed also by $i_1, \ldots, i_r; j_1, \ldots, j_r$ (see Definition 2.12), where $i_k, j_k \in \{1, \ldots, n_k\}$, is moved by the appropriate permutation matrices into the $i_{\sigma(1)}, \ldots, i_{\sigma(r)}; j_{\sigma(1)}, \ldots, j_{\sigma(r)}$th position within H'.

For a different, more direct, construction of these permutation matrices, see Corollary 4.3.10 and the following problem 19 in [1].

2.4. Numbers of rows of a given type and introduction indices in pure ordered FFKP's

Lemma 2.15. *Let there be an m factor pure ordered FFKP given*:

$$F = F_{a^{k_m}} \otimes \cdots \otimes F_{a^{k_1}} \tag{16}$$

with $p_1^{(m)}$ *rows of type* 1, $p_{1/(a)}^{(m)}$ *rows of type* $1/(a), \ldots, p_{1/(a^{k_m})}^{(m)}$ *rows of type* $1/(a^{k_m})$.

Then a new pure ordered FFKP product:

$$F' = F_{a^{k_{m+1}}} \otimes F, \quad k_{m+1} \geqslant k_m \tag{17}$$

contains rows of types $1, 1/(a), \ldots, 1/(a^{k_{m+1}})$ *in quantities given by the formulas*:

$$p_1^{(m+1)} = 1 \cdot p_1^{(m)}, \tag{18}$$

$$p_{1/(a^k)}^{(m+1)} = a^{k-1}(a-1)\left(p_1^{(m)} + p_{1/(a)}^{(m)} + \cdots + p_{1/(a^{k-1})}^{(m)}\right) + a^k \cdot p_{1/(a^k)}^{(m)}$$

$$\text{for } 1 < k \leqslant k_m, \tag{19}$$

$$\begin{aligned} p_{1/(a^l)}^{(m+1)} &= a^{l-1}(a-1)\left(p_1^{(m)} + p_{1/(a)}^{(m)} + \cdots + p_{1/(a^{k_m})}^{(m)}\right) \\ &= a^{l-1}(a-1)a^{\sum_{i=1}^{m} k_i} \end{aligned}$$

$$\text{for } k_m < l \leqslant k_{m+1}. \tag{20}$$

Proof. From Lemma 2.9 F contains rows of types $1, 1/(a), \ldots, 1/(a^{k_m})$ and F' has rows of types $1, 1/(a), \ldots, 1/(a^{k_{m+1}})$.

We calculate the number of rows of type $1/(a^k)$, where $1 < k \leqslant k_m$, in F' using Lemma 2.7. Let $p_{1/(a^n)}$ denote the number of type $1/(a^n)$ rows in $F_{a^{k_{m+1}}}$, which is given by Lemma 2.6, and let $\mathscr{P}$ denote the cartesian product $\{0, 1, \ldots, k_{m+1}\} \times \{0, 1, \ldots, k_m\}$. Then

$$\begin{aligned} p_{1/(a^k)}^{(m+1)} &= \sum_{\{(g,h)\in\mathscr{P}:\max(g,h)=k\}} p_{1/(a^g)} \cdot p_{1/(a^h)}^{(m)} \\ &= \sum_{h=0}^{k-1} p_{1/(a^k)} \cdot p_{1/(a^h)}^{(m)} + \sum_{g=0}^{k} p_{1/(a^g)} \cdot p_{1/(a^k)}^{(m)} \\ &= a^{k-1}(a-1)\left(p_1^{(m)} + p_{1/(a)}^{(m)} + \cdots + p_{1/(a^{k-1})}^{(m)}\right) \\ &\quad + (1 + (a-1) + \cdots + (a-1)a^{k-1}) \cdot p_{1/(a^k)}^{(m)} \\ &= a^{k-1}(a-1)\left(p_1^{(m)} + p_{1/(a)}^{(m)} + \cdots + p_{1/(a^{k-1})}^{(m)}\right) + a^k \cdot p_{1/(a^k)}^{(m)}. \end{aligned}$$

Rows of type 1 are obtained in F' only as kronecker products of rows of type 1, so from Lemma 2.6:

$$p_1^{(m+1)} = p_1 \cdot p_1^{(m)} = 1 \cdot p_1^{(m)}.$$

The number of rows of type $1/(a^l)$, where $k_m < l \leqslant k_{m+1}$, if there are any in F' (if $k_{m+1} > k_m$), is calculated in the following way, where $\mathscr{P}$ defined above:

$$\begin{aligned} p_{1/(a^l)}^{(m+1)} &= \sum_{\{(g,h)\in\mathscr{P}:\max(g,h)=l\}} p_{1/(a^g)} \cdot p_{1/(a^h)}^{(m)} \\ &= \sum_{h=0}^{k_m} p_{1/(a^l)} \cdot p_{1/(a^h)}^{(m)} \\ &= a^{l-1}(a-1)\left(p_1^{(m)} + p_{1/(a)}^{(m)} + \cdots + p_{1/(a^{k_m})}^{(m)}\right) \\ &= a^{l-1}(a-1)a^{(k_1+\cdots+k_m)}. \end{aligned}$$

This completes the proof. □

We will also need the definition of an *introduction index*:

Definition 2.16. An *introduction index* for type $1/(a^k)$ rows in F being an ordered pure FFKP product of F_{a^n} matrices, denoted $\tilde{n}_k^F$, is the position (number) of the factor of F, counting from right to left starting from 1 for the first factor, which first introduces rows of type $1/(a^k)$ in the process of constructing F by left kronecker multiplying by consecutive factors of nondecreasing size.

Example 2.17. Introduction indices for $F_{16} \otimes F_8 \otimes F_8 \otimes F_2$.

Take the ordered pure FFKP : $F = F_{16} \otimes F_8 \otimes F_8 \otimes F_2$. Then its introduction indices are

$$\tilde{n}_0^F = 1, \quad \tilde{n}_1^F = 1, \quad \tilde{n}_2^F = 2, \quad \tilde{n}_3^F = 2, \quad \tilde{n}_4^F = 4. \tag{21}$$

Remark 2.18. Let F and $F' = F_{a^{k_{m+1}}} \otimes F$ be ordered pure FFKP products of F_{a^n} matrices. Then introduction indices for F' are inherited from F.

Because of the remark above, in the proofs below we will usually omit the upper index F when writing introduction indices for a p.o.FFKP F, as we will often have to consider p.o.FFKP subproducts of F.

Lemma 2.19. *Let F be a pure ordered FFKP, consisting of s factors*:

$$F = F_{a^{k_s}} \otimes \cdots \otimes F_{a^{k_1}}. \tag{22}$$

Then F has $p_1^{(s)}$ rows of type 1, $p_{1/(a)}^{(s)}$ rows of type $1/(a), \ldots, p_{1/(a^m)}^{(s)}$ rows of type $1/(a^m), \ldots,$ where $0 \leqslant m \leqslant k_s$, and the numbers $p_1^{(s)}, p_{1/(a)}^{(s)}, \ldots, p_{1/(a^m)}^{(s)}, \ldots$ are given by

$$\begin{aligned}
&p_1^{(s)} = 1\\
&p_{1/(a)}^{(s)} = a^s - 1\\
&p_{1/(a^2)}^{(s)} = a^{2s-(\tilde{n}_2-1)} - a^s\\
&p_{1/(a^3)}^{(s)} = a^{3s-(\tilde{n}_3-1)-(\tilde{n}_2-1)} - a^{2s-(\tilde{n}_2-1)}\\
&p_{1/(a^4)}^{(s)} = a^{4s-(\tilde{n}_4-1)-(\tilde{n}_3-1)-(\tilde{n}_2-1)} - a^{3s-(\tilde{n}_3-1)-(\tilde{n}_2-1)}\\
&\cdots\\
&p_{1/(a^m)}^{(s)} = a^{ms-\sum_{l=0}^{m}(\tilde{n}_l-1)} - a^{(m-1)s-\sum_{l=0}^{m-1}(\tilde{n}_l-1)}\\
&\cdots
\end{aligned}$$

where $\tilde{n}_0 = 1$, $\tilde{n}_1 = 1$, $1 \leqslant \tilde{n}_2 \leqslant \cdots \leqslant \tilde{n}_m \leqslant \cdots \leqslant \tilde{n}_{k_s}$ are the introduction indices of rows of the type $1, 1/(a), 1/(a^2), \ldots, 1/(a^m), \ldots, 1/(a^{k_s})$, respectively.

Each mth formula giving $p_{1/(a^m)}^{(s)}$, where $1 \leqslant m \leqslant k_s$, is valid for $s \geqslant (\tilde{n}_m - 1)$, the threshhold argument value used when applying the formula to the right $(\tilde{n}_m - 1)$ factor subproduct of F.

Proof. The type 1 and $1/(a)$ rows are present in any F_{a^n}, that is why we put $\tilde{n}_0 = 1, \tilde{n}_1 = 1$, i.e. these row types are introduced by the first right factor of a pure ordered FFKP of F_{a^n} matrices.

Lemma 2.15 gives us the rules for changing $p_1^{(s)}$ when adding left new factors to a p.o.FFKP:

$$p_1^{(s+1)} = 1 \cdot p_1^{(s)}. \tag{23}$$

Because in the first, Fourier matrix, factor we have 1 row of type 1 (see Lemma 2.6), so we have $p_1^{(s)} = 1$ for any s and any s-factor p.o.FFKP of F_{a^n} matrices, for any a prime.

The number of type $1/(a)$ rows in the first factor is equal to $p_{1/(a)}^{(1)} = (a-1)$ (again Lemma 2.6), and using Lemma 2.15 we get the rule

$$p_{1/(a)}^{(s+1)} = (a-1)p_1^{(s)} + ap_{1/(a)}^{(s)} \tag{24}$$

which yields $p_{1/(a)}^{(s)} = a^s - 1$ for any s-factor p.o.FFKP of F_{a^n} matrices. Since $p_{1/(a)}^{(0)} = 0$ for the 0-factor subproduct, we regard $p_{1/(a)}^{(s)}$ as valid for $s \geqslant 0 = \tilde{n}_1 - 1$.

Now assume that the formulas for $p_{1/(a^k)}^{(s)}$ are correct for $k = 0, 1, 2, \ldots, m$ and that they are valid for $s \geqslant (\tilde{n}_k - 1)$, respectively. We will show that for $s \geqslant (\tilde{n}_{m+1} - 1)$ and $m \geqslant 1$:

$$p_{1/(a^{m+1})}^{(s)} = a^{(m+1)s - \sum_{l=0}^{m+1}(\tilde{n}_l - 1)} - a^{ms - \sum_{l=0}^{m}(\tilde{n}_l - 1)}. \tag{25}$$

Note that even $p_{1/(a)}^{(s)}$ can be written using the general scheme:

$$p_{1/(a)}^{(s)} = a^s - 1 = a^{1s - (\tilde{n}_1 - 1) - (\tilde{n}_0 - 1)} - a^{0s - (\tilde{n}_0 - 1)}. \tag{26}$$

Case $s = \tilde{n}_{m+1} - 1$. We start from calculating $p_{1/(a^{m+1})}^{(s)}$ for $s = \tilde{n}_{m+1} - 1$ substituted into (25). The result is 0 as it should for there are no rows of type $1/(a^{m+1})$ before they are introduced by the $\tilde{n}_{m+1}$th factor of a p.o.FFKP. It is 0 also if $\tilde{n}_{m+1} = 1$ (we can interpret $p_{1/(a^{m+1})}^{(0)}$ as the number of type $1/(a^{m+1})$ rows in no product at all), so $p_{1/(a^{m+1})}^{(0)}$ if used in a sum (fortunately it will not be) will not cause any damage because of abuse of index s.

Case $s = \tilde{n}_{m+1}$. To check whether the formula (25) gives the correct value for $s = \tilde{n}_{m+1}$ we have to consider two subcases.

Firstly, let $s = \tilde{n}_{m+1} = \tilde{n}_m = \tilde{n}_{m-1} = \cdots = \tilde{n}_0 = 1$, which means that rows of type $1/(a^{m+1})$ are introduced by the first factor of a p.o.FFKP and from Lemma 2.6 their number is $a^m(a-1)$. Let us substitute all those 1's into (25). We will get the required value:

$$a^{(m+1)\cdot 1} - a^{m\cdot 1} = a^m(a-1). \tag{27}$$

Secondly, let $s = \tilde{n}_{m+1} > 1$. Recall that we are talking about the situation in which the so far constructed (s factors) p.o.FFKP has just had type $1/(a^{m+1})$ rows introduced by the $\tilde{n}_{m+1}$th (sth) right factor. That is why we have to use the formula (20) from Lemma 2.15 to calculate the resulting number of type $1/(a^{m+1})$ rows. Note that we do not know 'the highest' present row type, so we write (which will be shown to be correct in a moment):

$$p_{1/(a^{m+1})}^{(\tilde{n}_{m+1})} = a^m(a-1)\left(p_1^{(\tilde{n}_{m+1}-1)} + p_{1/(a)}^{(\tilde{n}_{m+1}-1)} + \cdots + p_{1/(a^m)}^{(\tilde{n}_{m+1}-1)}\right). \tag{28}$$

Note that even if for some right $p_{1/(a^k)}^{(\tilde{n}_{m+1}-1)}$ (except for the first two left) we have that $\tilde{n}_m = \cdots = \tilde{n}_{m-d}$ are all equal to $\tilde{n}_{m+1}$, that is the types $1/(a^{m+1}), 1/(a^m), \ldots, 1/(a^{m-d})$ are introduced together, the corresponding $p_{1/(a^m)}^{(\tilde{n}_{m+1}-1)}, \ldots, p_{1/(a^{m-d})}^{(\tilde{n}_{m+1}-1)}$ values are in fact the values of $p_{1/(a^m)}^{(\tilde{n}_m-1)}, \ldots, p_{1/(a^{m-d})}^{(\tilde{n}_{m-d}-1)}$. From the induction assumption on correct formulas for $p_{1/(a^k)}^{(s)}, s \geqslant \tilde{n}_k - 1, k = 0, \ldots, m$ we can apply safely these formulas to calculate $p_{1/(a^{m+1})}^{(\tilde{n}_{m+1})}$ from (28). The values $p_{1/(a^m)}^{(\tilde{n}_m-1)}, \ldots, p_{1/(a^{m-d})}^{(\tilde{n}_{m-d}-1)}$ will in this case be zeros as they should.

The long sum in (28), from the induction assumption formulas, is equal to

$$a^{m(\tilde{n}_{m+1}-1)-\sum_{l=0}^{m}(\tilde{n}_l-1)}. \tag{29}$$

Note that it is also true if $m = 1$ at the beginning of the induction process, as (26) is satisfied.

So, what on one hand we get from (28) is

$$p_{1/(a^{m+1})}^{(\tilde{n}_{m+1})} = a^m(a-1)a^{m(\tilde{n}_{m+1}-1)-\sum_{l=0}^{m}(\tilde{n}_l-1)} \tag{30}$$

and on the other, substituting $\tilde{n}_{m+1}$ into (25), we obtain the same:

$$\begin{aligned} p_{1/(a^{m+1})}^{(\tilde{n}_{m+1})} &= a^{(m+1)\tilde{n}_{m+1}-\sum_{l=0}^{m+1}(\tilde{n}_l-1)} - a^{m\tilde{n}_{m+1}-\sum_{l=0}^{m}(\tilde{n}_l-1)} \\ &= a^{m(\tilde{n}_{m+1}-1)-\sum_{l=0}^{m}(\tilde{n}_l-1)}(a^{\tilde{n}_{m+1}+m-(\tilde{n}_{m+1}-1)} - a^m) \\ &= a^{m(\tilde{n}_{m+1}-1)-\sum_{l=0}^{m}(\tilde{n}_l-1)}(a^m(a-1)). \end{aligned}$$

Case $s > \tilde{n}_{m+1}$. Consider the formula (25) for $s > \tilde{n}_{m+1}$, that is type $1/(a^{m+1})$ is introduced by a factor preceding the sth one. Since formula (25) is correct, as we have shown above, for $s = \tilde{n}_{m+1}$, we can use formula (19) from Lemma 2.15 to obtain next values of $p_{1/(a^{m+1})}^{(s)}$ for $s = \tilde{n}_{m+1}+1, \tilde{n}_{m+1}+2, \ldots$. We will show that in each step of this process we get $p_{1/(a^{m+1})}^{(s)}$ of the form (25). We start from $p_{1/(a^{m+1})}^{(s)}$ given by (25), then from (19) we get

$$p_{1/(a^{m+1})}^{(s+1)} = a^m(a-1)\left(p_1^{(s)} + p_{1/(a)}^{(s)} + \cdots + p_{1/(a^m)}^{(s)}\right) + a^{m+1}p_{1/(a^{m+1})}^{(s)}, \tag{31}$$

where the long sum in brackets can be safely replaced, even for $m = 1$, by $a^{ms-\sum_{l=0}^{m}(\tilde{n}_l-1)}$ from the main induction assumption, then $p_{1/(a^{m+1})}^{(s+1)}$ is given by

$$\begin{aligned} p_{1/(a^{m+1})}^{(s+1)} &= a^m(a-1)a^{ms-\sum_{l=0}^{m}(\tilde{n}_l-1)} + a^{m+1}\left(a^{(m+1)s-\sum_{l=0}^{m+1}(\tilde{n}_l-1)} - a^{ms-\sum_{l=0}^{m}(\tilde{n}_l-1)}\right) \\ &= a^{(m+1)(s+1)-\sum_{l=0}^{m+1}(\tilde{n}_l-1)} - a^{m(s+1)-\sum_{l=0}^{m}(\tilde{n}_l-1)} \end{aligned}$$

which is analogous to (25), with s replaced by $s+1$. This, combined with (25) working for $s = \tilde{n}_{m+1}$, means that (25) works also for $s > \tilde{n}_{m+1}$.

We have thus shown that (25) gives correct values of the number of rows of type $1/(a^{m+1})$ for $s \geqslant \tilde{n}_{m+1} - 1$, which completes the proof by induction. □

Theorem 2.20. *Let there be two pure ordered FFKP products of F_{a^n} matrices given (a prime)*:

$$\begin{aligned} F' &= F_{a^{k_{s_1}}} \otimes F_{a^{k_{s_1-1}}} \otimes \cdots \otimes F_{a^{k_1}} \quad k_{s_1} \geqslant k_{s_1-1} \geqslant \cdots \geqslant k_1, \\ F'' &= F_{a^{l_{s_2}}} \otimes F_{a^{l_{s_2-1}}} \otimes \cdots \otimes F_{a^{l_1}} \quad l_{s_2} \geqslant l_{s_2-1} \geqslant \cdots \geqslant l_1. \end{aligned}$$

Then the following statements (a)–(c) *are equivalent*:

(a) *Both FFKP products, F' and F'', contain*:
- *equal numbers of type* 1 *rows*: $p_1^{\prime(s_1)} = p_1^{\prime\prime(s_2)}$
- *equal numbers of type* $1/(a)$ *rows*: $p_{1/(a)}^{\prime(s_1)} = p_{1/(a)}^{\prime\prime(s_2)}$
- $\ldots$
- *equal numbers of type* $1/(a^{k_{s_1}}) = 1/(a^{l_{s_2}})$ *rows*: $p_{1/(a^{k_{s_1}})}^{\prime(s_1)} = p_{1/(a^{l_{s_2}})}^{\prime\prime(s_2)}$

(b) *Introduction indices* $\tilde{n}_0, \tilde{n}_1, \ldots, \tilde{n}_{k_{s_1}=l_{s_2}}$ *are common to both* F' *and* F'', *and* $s_1 = s_2$.
(c) *The p.o. FFKP products* F' *and* F'' *are identical, that is* $s_1 = s_2$ *and* $k_1 = l_1$, $k_2 = l_2, \ldots, k_{s_1} = l_{s_2}$.

Proof. We consider the cases of implication:

Case (a) $\Longrightarrow$ (b). Introduction indices $\tilde{n}_0 = 1$ and $\tilde{n}_1 = 1$ are common to both F' and F'', for rows of types 1 and $1/(a)$ are introduced by any first right factor F_{a^n}, $n \geqslant 1$.

Assume that common to F' and F'' are the introduction indices $\tilde{n}_0, \tilde{n}_1, \ldots, \tilde{n}_k \in \{1, 2, \ldots, \min(s_1, s_2)\}$, where $k < k_{s_1} = l_{s_2}$. Note that the last equality results from the statement (a) and the last inequality must be in accordance with Lemma 2.9. We will show now that $\tilde{n}_{k+1}$ is also common to F' and F'', that is $\tilde{n}'_{k+1} = \tilde{n}''_{k+1}$.

Rows of type $1/(a^{k+1})$ are introduced into F' by the $\tilde{n}'_{k+1}$th factor of F' and into F'' by $\tilde{n}''_{k+1}$th factor of F'', where $\tilde{n}'_{k+1} \leqslant s_1$, $\tilde{n}''_{k+1} \leqslant s_2$ and $k+1 \leqslant k_{s_1} = l_{s_2}$. Lemma 2.19 provides us with the written below formulas for the number of type $1/(a^{k+1})$ rows in F' and F''. From the statement (a) these numbers are equal, which is expressed by

$$a^{(k+1)s_1-(\tilde{n}'_{k+1}-1)-\sum_{l=0}^{k}(\tilde{n}_l-1)} - a^{ks_1-\sum_{l=0}^{k}(\tilde{n}_l-1)} = a^{(k+1)s_2-(\tilde{n}''_{k+1}-1)-\sum_{l=0}^{k}(\tilde{n}_l-1)} - a^{ks_2-\sum_{l=0}^{k}(\tilde{n}_l-1)}$$

which is equivalent to

$$a^{ks_1-\sum_{l=0}^{k}(\tilde{n}_l-1)}(a^{s_1-(\tilde{n}'_{k+1}-1)} - 1) = a^{ks_2-\sum_{l=0}^{k}(\tilde{n}_l-1)}(a^{s_2-(\tilde{n}''_{k+1}-1)} - 1). \tag{32}$$

From the uniqueness of prime number factorization of a natural number and the fact that a is prime, powers of a on the left and right side of (32) are equal, so $s_1 = s_2$, which we get in each step of the induction process. As a result the factors not divided by a in (32) are also equal, what is more $s_1 = s_2$, so $\tilde{n}'_{k+1} = \tilde{n}''_{k+1} = \tilde{n}_{k+1}$.

Thus all $\tilde{n}_k$, $k \in \{0, 1, 2, \ldots, k_{s_1} = l_{s_2}\}$ are common to F' and F'', and the implication (a) $\Longrightarrow$ (b) is proved.

Case (b) $\Longrightarrow$ (c). From the statement (b) we have that $s_1 = s_2$.

Now, assume that F' and F'' are not identical. That is, for some $s \leqslant s_1 = s_2$ the 1st, 2nd, …, $(s-1)$th right factors of F' and F'' are equal and the sth factors are not. Say, they are F_{a^k} for F' and F_{a^l} for F'' such that $k > l$. Then the introduction indices $\tilde{n}'_k, \tilde{n}''_k$ for F', F'' must satisfy $\tilde{n}'_k \leqslant s < \tilde{n}''_k$. The reason is that in F'' rows of type $1/(a^k)$ have not yet been introduced by the sth factor, whereas in F' they have already been introduced by some $(s-t)$th factor, $t \geqslant 0$. So F' and F'' cannot have all their introduction indices common.

Case (c) $\Longrightarrow$ (b). Obvious.

Case (b) $\Longrightarrow$ (a). The implication is given by (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a), where (c) $\Longrightarrow$ (a) is obvious.

Cases (a) $\Longrightarrow$ (c) and (c) $\Longrightarrow$ (a). It is obvious that (c) $\Longrightarrow$ (a). Further, (a) $\Longrightarrow$ (b) and (b) $\Longrightarrow$ (c) implies (a) $\Longrightarrow$ (c). □

2.5. *Permutation equivalence of FKP's*

In this subsection we provide basic facts on permutation equivalence, denoted by $\overset{P}{\simeq}$ and defined below, of kronecker products of Fourier matrices.

Definition 2.21. Two square matrices A and B of the same size are *permutation equivalent*, i.e. $A \overset{P}{\simeq} B$, if and only if there exist permutation matrices P_r, P_c of the proper size such that

$$A = P_r \cdot B \cdot P_c$$

Theorem 2.20 leads to the corollary:

Corollary 2.22. *Pure ordered FFKP products F' and F'' are $\overset{P}{\simeq}$ equivalent if and only if they are identical ($\Longleftrightarrow$ equal).*

Proof. If F' and F'' are $\overset{P}{\simeq}$ equivalent, they satisfy the statement (a) of Theorem 2.20, which, by this theorem, is equivalent to F' anf F'' being identical ($\Leftrightarrow$ equal in the sense of Theorem 2.20 c).

The opposite implication is obvious. □

A more general lemma states that:

Lemma 2.23. *Let there be two FFKP products F' and F'' given (see Definition 2.3) of size $N = a_1^{b_1} \cdot a_2^{b_2} \cdots a_r^{b_r}$, where $a_1 > a_2 > \cdots > a_r$ are prime factors of N.*

Then F' and F'' are $\overset{P}{\simeq}$ equivalent if and only if F' and F'' are identical up to the order of their factors ($\Longleftrightarrow$ their corresponding maximal pure ordered FFKP subproducts are identical in the sense of statement (c) *of Theorem 2.20).*

Proof. It is enough to prove Lemma 2.23 in the case of F' and F'' ordered (which by Remark 2.14 corresponds to left and right permuting) in such a way that:

$$F' = F'^{(1)} \otimes F'^{(2)} \otimes \cdots \otimes F'^{(r)},$$
$$F'' = F''^{(1)} \otimes F''^{(2)} \otimes \cdots \otimes F''^{(r)},$$

where $F'^{(k)}$ and $F''^{(k)}$ are pure ordered FFKP's such that

$$F'^{(k)} = F_{\substack{g_{s_1^{(k)}}^{(k)} \\ a_k}} \otimes F_{\substack{g_{s_1^{(k)}-1}^{(k)} \\ a_k}} \otimes \cdots \otimes F_{\substack{g_1^{(k)} \\ a_k}},$$
$$F''^{(k)} = F_{\substack{h_{s_2^{(k)}}^{(k)} \\ a_k}} \otimes F_{\substack{h_{s_2^{(k)}-1}^{(k)} \\ a_k}} \otimes \cdots \otimes F_{\substack{h_1^{(k)} \\ a_k}},$$

where

$$\sum_{s=1}^{s_1^{(k)}} g_s^{(k)} = \sum_{s=1}^{s_2^{(k)}} h_s^{(k)} = b_k. \tag{33}$$

Let us denote by $p'^{(s_1^{(k)})}_{1/(a_k{}^m)}$, $p''^{(s_2^{(k)})}_{1/(a_k{}^m)}$ the numbers of type $1/(a_k^m)$ rows in $s_1^{(k)}$ factor p.o.FFKP subproduct $F'^{(k)}$ and $s_2^{(k)}$ factor p.o.FFKP subproduct $F''^{(k)}$, respectively.

From Lemma 2.8 each row of type $1/(a_k^m)$ of F' is obtained as a kronecker product of type 1 rows from $F'^{(l)}$ where $l \in \{1, 2, \ldots, r\}\backslash\{k\}$ and a row of type $1/(a_k^m)$ from $F'^{(k)}$. Similarly for F''. So, the numbers of type $1/(a_k^m)$ rows in F' and F'' will be, by Lemma 2.19:

$$\left(\prod_{l\in\{1,2,\ldots,r\}\backslash\{k\}} p'^{(s_1^{(l)})}_{1}\right)\cdot p'^{(s_1^{(k)})}_{1/(a_k{}^m)} = p'^{(s_1^{(k)})}_{1/(a_k^m)},$$

$$\left(\prod_{l\in\{1,2,\ldots,r\}\backslash\{k\}} p''^{(s_2^{(l)})}_{1}\right)\cdot p''^{(s_2^{(k)})}_{1/(a_k{}^m)} = p''^{(s_2^{(k)})}_{1/(a_k^m)}.$$

If F' and F'' are $\overset{P}{\simeq}$ equivalent, then for each $k \in \{1, 2, \ldots, r\}$ the above numbers of type $1/\left(a_k^m\right)$ rows in F' and F'' are equal, where $m \in \left\{0, 1, \ldots, g^{(k)}_{s_1^{(k)}} = h^{(k)}_{s_2^{(k)}}\right\}$ (the last equality in the set description follows from $\overset{P}{\simeq}$ equivalence of F', F'' and Lemmas 2.8, 2.9). That is the pairs $p'^{(s_1^{(k)})}_{1/(a_k^m)}$, $p''^{(s_2^{(k)})}_{1/(a_k^m)}$ are pairs of equal numbers, k and m as above. Then, from Theorem 2.20 $F'^{(k)}$ and $F''^{(k)}$ are identical (equal) for each $k \in \{1, 2, \ldots, r\}$. This means that F' and F'', assumed ordered, are identical.

If F' and F'' are identical, they are $\overset{P}{\simeq}$ equivalent of course.

Now, taking Remark 2.14 into consideration, we can generalize the above implications to unordered FFKP's, to obtain Lemma 2.23. □

The result of the lemma below can also be found in [3]:

Lemma 2.24. *If p and q are relatively prime natural numbers, then there exist permutation matrices P_r, P_c such that*

$$P_r \cdot (F_p \otimes F_q) \cdot P_c = F_{(p\cdot q)}. \tag{34}$$

Proof. Let $\tilde{i}', \tilde{i}''; \tilde{j}', \tilde{j}''$ denote a *shifted* kronecker multiindex into a matrix with the kronecker product structure $p \times q$, such as, for example, $F_p \otimes F_q$. The term *shifted* here means that numbering starts from 0. The relation between shifted ordinary index $\tilde{i}, \tilde{j}$ and shifted kronecker multiindex is, according to Definition 2.12:

$$\tilde{i}', \tilde{i}''; \tilde{j}', \tilde{j}'' \longleftrightarrow \tilde{i}' \cdot q + \tilde{i}'', \quad \tilde{j}' \cdot q + \tilde{j}'', \tag{35}$$

where

$$\tilde{i}', \tilde{j}' \in \{0 \cdots (p-1)\}, \tag{36}$$

$$\tilde{i}'', \tilde{j}'' \in \{0 \cdots (q-1)\}. \tag{37}$$

Now let the permutation matrices P_r^{-1}, P_c^{-1} move the $\tilde{i}$th row and $\tilde{j}$th column, respectively, into the specified below the $\tilde{i}', \tilde{i}''$th row and $\tilde{j}', \tilde{j}''$th column of the result:

$$\tilde{i} \longrightarrow \tilde{i}', \tilde{i}'' = (a\tilde{i} \bmod p), \quad (b\tilde{i} \bmod q), \tag{38}$$

$$\tilde{j} \longrightarrow \tilde{j}', \tilde{j}'' = (c\tilde{j} \bmod p), \quad (d\tilde{j} \bmod q), \tag{39}$$

where a, b, c, d are natural numbers satisfying, for some integers e, f:

$$ep + (ac)q = 1, \qquad (bd)p + fq = 1. \tag{40}$$

Note that since p, q are relatively prime, there exist integers $e, x > 0, y > 0, f$ such that $ep + xq = 1$ and $yp + fq = 1$. To have $ac = x$ and $bd = y$ we can take $a = 1, c = x, b = 1, d = y$.

Note also, that (40) implies that a, c are relatively prime to p, and b, d are relatively prime to q. Otherwise 1 would have to have a divisor greater than 1.

To show that maps (38) and (39) properly define permutations, that is that they are bijective, let us take $\tilde{i}_1 \neq \tilde{i}_2$ belonging to $\{0, \ldots, (pq-1)\}$. If they are mapped by (38) into equal pairs $\tilde{i}'$, $\tilde{i}''$, then:

$$\begin{aligned} a\tilde{i}_1 \bmod p = a\tilde{i}_2 \bmod p &\Longleftrightarrow a(\tilde{i}_1 - \tilde{i}_2) \quad \text{is divided by } p, \\ b\tilde{i}_1 \bmod q = b\tilde{i}_2 \bmod q &\Longleftrightarrow b(\tilde{i}_1 - \tilde{i}_2) \quad \text{is divided by } q \end{aligned}$$

so $\tilde{i}_1 - \tilde{i}_2$ is divided by pq because pairs a, p and b, q and p, q are relatively prime. But this cannot be so for $\tilde{i}_1, \tilde{i}_2 \in \{0, \ldots, (pq-1)\}$. Thus the map (38) must be injective and similarly we show this for the second map (39). Thus both maps map the sets $\{0, \ldots, (pq-1)\}$ and $\{0, \ldots, (p-1)\} \times \{0, \ldots, (q-1)\}$ one to one, that is they are bijective.

To show that $(F_p \otimes F_q) = P_r^{-1} \cdot F_{pq} \cdot P_c^{-1}$ we will show that the $\tilde{i}, \tilde{j}$th element of F_{pq} is mapped (or equal to) the $\tilde{i}', \tilde{i}''; \tilde{j}', \tilde{j}''$th, as defined in (38) and (39), element of $F_p \otimes F_q$, i.e.:

$$\frac{1}{\sqrt{pq}} \exp\left(\mathrm{i}\frac{2\pi}{pq}\tilde{i}\tilde{j}\right) = \frac{1}{\sqrt{p}} \exp\left(\mathrm{i}\frac{2\pi}{p}\tilde{i}'\tilde{j}'\right) \frac{1}{\sqrt{q}} \exp\left(\mathrm{i}\frac{2\pi}{q}\tilde{i}''\tilde{j}''\right) \tag{41}$$

which is equivalent to the equality of phases:

$$\frac{2\pi}{pq}\tilde{i}\tilde{j} \overset{\bmod 2\pi}{=} \frac{2\pi}{pq}\left(q\tilde{i}'\tilde{j}' + p\tilde{i}''\tilde{j}''\right), \tag{42}$$

or to the equality for indices:

$$\tilde{i}\tilde{j} \overset{\bmod pq}{=} q\tilde{i}'\tilde{j}' + p\tilde{i}''\tilde{j}''. \tag{43}$$

Consider the difference:

$$\begin{aligned} &\tilde{i}\tilde{j} - q\tilde{i}'\tilde{j}' - p\tilde{i}''\tilde{j}'' \\ &\quad = \frac{1}{ac}(a\tilde{i})(c\tilde{j}) - q(a\tilde{i} \bmod p)(c\tilde{j} \bmod p) - p\tilde{i}''\tilde{j}'' \\ &\quad = \frac{1}{ac}(p\alpha + (a\tilde{i} \bmod p))(p\beta + (c\tilde{j} \bmod p)) - q(a\tilde{i} \bmod p)(c\tilde{j} \bmod p) - p\tilde{i}''\tilde{j}'' \\ &\quad = \frac{1}{ac}(pA + (a\tilde{i} \bmod p)(c\tilde{j} \bmod p)) - q(a\tilde{i} \bmod p)(c\tilde{j} \bmod p) - p\tilde{i}''\tilde{j}'' \\ &\quad = \frac{1}{ac}(pA + (a\tilde{i} \bmod p)(c\tilde{j} \bmod p)(1 - qac)) - p\tilde{i}''\tilde{j}'' \end{aligned}$$

which is divided by p, for $1 - qac = ep$ and a, c are relatively prime to p.

In the same way we show that it is divided by q:

$$\tilde{i}\tilde{j} - q\tilde{i}'\tilde{j}' - p\tilde{i}''\tilde{j}'' = \frac{1}{bd}(qB + (b\tilde{i} \bmod q)(d\tilde{j} \bmod q)(1 - pbd)) - q\tilde{i}'\tilde{j}',$$

where $1 - pbd = fq$ and b, d are relatively prime to q.

Thus the considered difference is divided by relatively prime numbers p and q, so it is divided by pq, which is equivalent to (43). □

Corollary 2.25. *Let F be an FKP product*:

$$F = F_{n_1} \otimes F_{n_2} \otimes \cdots \otimes F_{n_r}. \tag{44}$$

Then there exist permutation matrices P_r, P_c such that we have $\overset{P}{\simeq}$ equivalence of matrices:

$$P_r \cdot F \cdot P_c = F_{m_1} \otimes F_{m_2} \otimes \cdots \otimes F_{m_s}, \tag{45}$$

where the sequence $m_1, \ldots, m_s$ is obtained from the sequence $n_1, \ldots, n_r$ using a series of operations from the list below:

1. *permuting a sequence, for example $n_1, n_2, n_3 \to n_1, n_3, n_2$;*
2. *merging a sequence: a subsequence n_a, n_b can be replaced by $n_c = n_a n_b$ if n_a, n_b are relatively prime;*
3. *division in a sequence: a sequence element n_c can be replaced by a subsequence n_a, n_b if $n_c = n_a n_b$, and n_a, n_b are relatively prime.*

Proof. Permuting the factors of a kronecker product, corresponding to operation 1 from the list, is equivalent to left and right permuting this product (see Remark 2.14).

Operations 2 and 3 from the list correspond to left and right permuting subproducts $F_{n_a} \otimes F_{n_b}$, F_{n_c} respectively, by Lemma 2.24. Left and right permuting a subproduct means left and right permuting the whole product, for example

$$\begin{aligned} A \otimes (P_1 B P_2) \otimes C &= A \otimes (P_1 \otimes I_C)(B \otimes C)(P_2 \otimes I_C) \\ &= (I_A \otimes P_1 \otimes I_C)(A \otimes B \otimes C)(I_A \otimes P_2 \otimes I_C), \end{aligned}$$

where A, B, C square matrices, I_A, I_B, I_C the identity matrices of the same size, respectively.

Combining all the permutation matrices corresponding to the operations performed on the size sequence (factor sequence) leads to P_r, P_c. □

3. Main result on permutation equivalence of kronecker products of Fourier matrices

Let $\mathscr{F}$ denote the set of all FKP products (Definition 2.2) and let $\mathscr{F}_N$ denote the set of all FKP products of size N.

Corollary 2.25 (on operations on FKP 's preserving $\overset{P}{\simeq}$ equivalence) and Lemma 2.23 (on the criteria of two FFKP's (Definition 2.3) being $\overset{P}{\simeq}$ equivalent) imply:

Theorem 3.1. *Each $\overset{P}{\simeq}$ equivalence class in $\mathscr{F}_N$ is uniquely represented by an* ordered *FFKP with pure ordered FFKP subproducts* (*Definition* 2.4), *that is by an FFKP of the form*:

$$\left(F_{\substack{k_1^{(1)} \\ a_1 m^{(1)}}} \otimes \cdots \otimes F_{\substack{k_1^{(1)} \\ a_1}} \right) \otimes \cdots \otimes \left(F_{\substack{k_1^{(r)} \\ a_r m^{(r)}}} \otimes \cdots \otimes F_{\substack{k_1^{(r)} \\ a_r}} \right), \tag{46}$$

where $a_1, a_2, \ldots, a_r$ are prime numbers satisfying

$$a_1 > a_2 > \cdots > a_r \tag{47}$$

and $k_m^{(l)}$, $m = 1, \ldots, m^{(l)}$, $l = 1, \ldots, r$ *are respective exponents such that*

$$k_{m^{(l)}}^{(l)} \geqslant k_{m^{(l)}-1}^{(l)} \geqslant \cdots \geqslant k_1^{(l)} \quad \text{for } l = 1, \ldots, r \tag{48}$$

and

$$N = a_1^{\sum_{m=1}^{m^{(1)}} k_m^{(1)}} \cdots a_r^{\sum_{m=1}^{m^{(r)}} k_m^{(r)}} \tag{49}$$

is the prime number factorization of N.

and the extended result of Lemma 2.24:

Theorem 3.2. *Two FKP's* $F_p \otimes F_q$ *and* $F_{(p\cdot q)}$ *are* $\overset{P}{\simeq}$ *equivalent if and only if* p *and* q *are relatively prime natural numbers*.

Expressing it in a less formal way, we can say that one needs to split, merge and reorder ('division', 'merging' and 'permuting' operations of Corollary 2.25) the factors of an FKP to obtain the unique representative, in the sense of Theorem 3.1, of the class this FKP is in.

To calculate the number of $\overset{P}{\simeq}$ equivalence classes of FKP 's of a given size N, that is in $\mathscr{F}_N$, we need the definition of a partition:

Definition 3.3. A *partition* of a natural number N is any ordered sequence of positive (>0) integers $(n_1, n_2, \ldots, n_p)$ such that $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_p$ and $n_1 + n_2 + \cdots + n_p = N$.

The number of partitions of N is usually denoted by $p(N)$ and we will use this notation. A good reference on partitions is [19].

From what was said above about the representatives of $\overset{P}{\simeq}$ equivalence classes in $\mathscr{F}$ (Theorem 3.1) we immediately have:

Theorem 3.4. *The number of* $\overset{P}{\simeq}$ *equivalence classes within* $\mathscr{F}_N$, *where* N *has the prime number factorization*:

$$N = a_1^{b_1} \cdot a_2^{b_2} \cdots a_r^{b_r}, \quad a_1 > a_2 > \cdots > a_r \tag{50}$$

is equal to the product of the numbers of partitions:

$$p(b_1) \cdot p(b_2) \cdots p(b_r). \tag{51}$$

We will denote the number of $\overset{P}{\simeq}$ equivalence classes in $\mathscr{F}_N$ by P_N. Below we present a few examples of sets of all $\overset{P}{\simeq}$ equivalence classes for the values of N: 30, 48, 36. $[F]_{\underset{\simeq}{P}}$ denotes the class represented by F. For each class, all (up to the order of factors) FKP's contained in it are listed.

Example 3.5. Sets of all $\overset{P}{\simeq}$ equivalence classes within $\mathscr{F}_N$, $N = 30, 48, 36$.

$\mathscr{F}_{5\cdot3\cdot2}$:

$[F_5 \otimes F_3 \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_5 \otimes F_3 \otimes F_2, \quad F_6 \otimes F_5, \quad F_{10} \otimes F_3, \quad F_{15} \otimes F_2, \quad F_{30}.$$

$\mathscr{F}_{3\cdot 2^4}$:

$[F_3 \otimes F_{2^4}]_{\underset{\simeq}{P}}$ contains

$$F_{16} \otimes F_3, \quad F_{48}.$$

$[F_3 \otimes F_{2^3} \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_8 \otimes F_2 \otimes F_3, \quad F_{24} \otimes F_2, \quad F_8 \otimes F_6.$$

$[F_3 \otimes F_{2^2} \otimes F_{2^2}]_{\underset{\simeq}{P}}$ contains

$$F_4 \otimes F_4 \otimes F_3, \quad F_{12} \otimes F_4.$$

$[F_3 \otimes F_{2^2} \otimes F_2 \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_4 \otimes F_2 \otimes F_2 \otimes F_3, \quad F_{12} \otimes F_2 \otimes F_2, \quad F_4 \otimes F_2 \otimes F_6.$$

$[F_3 \otimes F_2 \otimes F_2 \otimes F_2 \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_3 \otimes F_2 \otimes F_2 \otimes F_2 \otimes F_2, \quad F_6 \otimes F_2 \otimes F_2 \otimes F_2.$$

$\mathscr{F}_{3^2\cdot 2^2}$:

$[F_{3^2} \otimes F_{2^2}]_{\underset{\simeq}{P}}$ contains

$$F_9 \otimes F_4, \quad F_{36}.$$

$[F_{3^2} \otimes F_2 \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_9 \otimes F_2 \otimes F_2, \quad F_{18} \otimes F_2.$$

$[F_3 \otimes F_3 \otimes F_{2^2}]_{\underset{\simeq}{P}}$ contains

$$F_4 \otimes F_3 \otimes F_3, \quad F_{12} \otimes F_3.$$

$[F_3 \otimes F_3 \otimes F_2 \otimes F_2]_{\underset{\simeq}{P}}$ contains

$$F_3 \otimes F_3 \otimes F_2 \otimes F_2, \quad F_6 \otimes F_3 \otimes F_2, \quad F_6 \otimes F_6.$$

4. Conclusions

The notion of permutation equivalence can be extended to what we will denote as $\simeq$ equivalence. Two unitary matrices U and V are $\simeq$ equivalent if and only if there exist permutation matrices P_r, P_c and unitary diagonal matrices D_r, D_c such that

$$V = P_r D_r \cdot U \cdot D_c P_c. \tag{52}$$

Since phasing a kronecker product of unitary Fourier matrices of the total size N, that is left and right multiplying it by some D_r and D_c, in such a way that still there is a row and column filled with $1/\sqrt{N}$ in the result, is equivalent to row and column permutation, it appears that permutation equivalence classes are the same as $\simeq$ equivalence classes in the set of the considered kronecker products. In other words, we have a method of checking whether two given kronecker products of Fourier matrices, F' and F'', are $\simeq$ equivalent. This is done by comparing unique representatives, in the sense of Theorem 3.1, obtained from F' and F'' by using operations of Corollary 2.25.

Distinguishing between $\simeq$ inequivalent (unitary) complex $N \times N$ Hadamard matrices (biunitaries, Zeilinger matrices), of which the considered products are special cases, plays important role in the search for nonisomorphic pairs of orthogonal maximal abelian *-subalgebras (MASA's) of the algebra of complex $N \times N$ matrices, see [4,7,8]. Isomorphic pairs are generated by $\simeq$ equivalent complex Hadamard matrices.

$\simeq$ inequivalence is also a source of inequivalence of the so called bases of $N \times N$ unitary operators:

$$\{U_k : \mathrm{tr}\,(U_i^* U_j) = N\delta_{i,j},\ U_k \text{ is unitary},\ k \in \{1 \cdots N^2\}\} \tag{53}$$

created with the use of complex Hadamard matrices, see [12,13].

The bases, in turn, allow construction of the following types of objects considered in the quantum information theory [13]:

- teleportation schemes,
- dense coding schemes,
- bases of maximally entangled vectors,
- unitary depolarizers.

For a more detailed description of possible applications of complex Hadamard matrices in the quantum information theory, accompanied by an extensive survey of literature, see [17].

The research on complex Hadamard matrices has revealed the existence of continuous families of $\simeq$ inequivalent matrices, dephased in the sense of having a row and column filled with real positive values ($1/\sqrt{N}$ for unitary Hadamard matrices of size N), see [7,8,14]. With the exception of Fourier matrices of prime dimensions, kronecker products of Fourier matrices belong to such families. There are indications, however, that all the kronecker products of a given total size N, suitably permuted, lie within a single family [17]. That is to say, $\simeq$ inequivalent kronecker products of Fourier matrices do not generate $\simeq$ inequivalent families.

Acknowledgments

This work was supported by the Polish Ministry of Scientific Research and Information Technology under the (solicited) grant no. PBZ-Min-008/P03/2003.

References

[1] R.A. Horn, C.R. Johnson, Topics in Matrix Analysis, Cambridge University Press, 1991.
[2] Xiao-Qing Jin, Developments and Applications of Block Toeplitz Iterative Solvers, Kluwer Academic Publisher, Dortrecht, Netherlands, 2002.
[3] C. Van Loan, Computational Frameworks for the Fast Fourier Transform, SIAM, Philadelphia, 1992.
[4] S. Popa, Orthogonal pairs of *-subalgebras in finite von Neumann algebras, J. Operator Theory 9 (1983) 253–268.
[5] G. Björk, R. Fröberg, A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots, J. Symbolic Comput. 12 (1991) 329–336.
[6] G. Björck, B. Saffari, New classes of finite unimodular sequences with unimodular Fourier transform. Circulant Hadamard matrices with complex entries, C. R. Acad. Sci. Paris 320 (1995) 319–324.
[7] U. Haagerup, Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots, in: Operator Algebras and Quantum Field Theory (Rome), International Press, Cambridge, MA, 1996, pp. 296–322.
[8] R. Nicoara, A finiteness result for commuting squares of matrix algebras. Available from: <www.arxiv.org/abs/math.OA/0404301>.

[9] I.D. Ivanović, Geometrical description of quantal state determination, J. Phys. A 14 (1981) 3241–3245.
[10] M. Reck, A. Zeilinger, H.J. Bernstein, P. Bertani, Experimental realization of any discrete unitary operator, Phys. Rev. Lett. 73 (1994) 58–61.
[11] I. Jex, S. Stenholm, A. Zeilinger, Hamiltonian theory of a symmetric multiport, Opt. Commun. 117 (1995) 95–1001.
[12] K.G.H. Volbrecht, R.F. Werner, Why two qubits are special, J. Math. Phys. 41 (2000) 6772–6782. Available from: <arxiv.org/abs/quant-ph/9910064>.
[13] R.F. Werner, All teleportation and dense coding schemes, J. Phys. A 34 (2001) 7081–7094. Available from: <arxiv.org/abs/quant-ph/0003070>.
[14] P. Diţă, Some results on the parameterization of complex Hadamard matrices, J. Phys. A 37 (2004) 5355–5374. Available from: <www.arxiv.org/abs/quant-ph/0212036>.
[15] M. Petrescu, Existence of Continuous Families of Complex Hadamard Matrices of Certain Prime Dimensions, Ph.D. Thesis, UCLA, 1997.
[16] N.J.A. Sloane, A library of Hadamard matrices. Available from: <http://www.research.att.com/∼njas/hadamard/>
[17] W. Tadej, K. Życzkowski, A concise guide to complex Hadamard matrices, Open Systems Infor. Dyn., in press. Available from: <www.arxiv.org/abs/quant-ph/0512154>.
[18] A. Wojcik, A. Grudka, R.W. Chhajlany, Generation of inequivalent generalized Bell bases, Quantum Inform. Process. 2 (2003) 201.
[19] Mathworld, Partition function. Available from: <http://mathworld.wolfram.com/PartitionFunctionP.html>.