Rank-deficient submatrices of Kronecker products of Fourier matrices

Steven Delvaux　　*Marc Van Barel*

Report TW477, November 2006

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

Rank-deficient submatrices of Kronecker products of Fourier matrices

Steven Delvaux   *Marc Van Barel*

Report TW477, November 2006

Department of Computer Science, K.U.Leuven

Abstract

We provide a set of maximal rank-deficient submatrices of a Kronecker product of two matrices $A \otimes B$, and in particular the Kronecker product of Fourier matrices $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$. We show how in the latter case, maximal rank-deficient submatrices can be constructedas tilings of rank-one blocks. Such tilings exist for any subgroup of a suitable Abelian group associated to the matrix F. These maximal rank-deficient submatrices are also related to an uncertainty principle for Fourier transforms over finite Abelian groups, for which we can then obtain stronger versions.

Keywords : Kronecker product, Fourier matrix, rank-deficient submatrix, uncertainty principle.
AMS(MOS) Classification : Primary : 42A99, Secondary : 15A03, 15A69.

Rank-deficient submatrices of Kronecker products of Fourier matrices

Steven Delvaux *, Marc Van Barel *

15th November 2006

Abstract

We provide a set of maximal rank-deficient submatrices of a Kronecker product of two matrices $A \otimes B$, and in particular the Kronecker product of Fourier matrices $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$. We show how in the latter case, maximal rank-deficient submatrices can be constructed as tilings of rank-one blocks. Such tilings exist for any subgroup of a suitable Abelian group associated to the matrix F. These maximal rank-deficient submatrices are also related to an uncertainty principle for Fourier transforms over finite Abelian groups, for which we can then obtain stronger versions.

Keywords: Kronecker product, Fourier matrix, rank-deficient submatrix, uncertainty principle.

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

1 Introduction

In this paper we search the maximal rank-deficient submatrices of a Kronecker product of matrices, and in particular the Kronecker product of Fourier matrices. This paper can be considered as a follow-up of [1], where the case of a single Fourier matrix with order a power of a prime number was considered.

Let us start with some basic definitions. For $n \in \mathbb{N} \setminus \{0\}$, the *Fourier matrix* of size n is defined as $F_n = \frac{1}{\sqrt{n}}[\omega^{ij}]_{i,j=0}^{n-1}$, where $\omega = \exp(2\pi\mathbf{i}/n)$ with $\mathbf{i} := \sqrt{-1}$. Note that this is a special case of a *Vandermonde matrix*, at least if we neglect the scaling factor $\frac{1}{\sqrt{n}}$.

*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 column vector $\mathbf{v} \in \mathbb{C}^n$, the *Hamming weight* of $\mathbf{v}$ is defined as the number of nonzero entries of $\mathbf{v}$, and denoted by $H(\mathbf{v})$.

The following result was first proved by Matolcsi and Szucs [6] in a group theoretical context.

Theorem 1 *(Uncertainty principle:) Given a matrix*

$$F = F_{n_1} \otimes \ldots \otimes F_{n_k}, \tag{1}$$

where each F_{n_i} is the Fourier matrix of size n_i, where $\otimes$ denotes the Kronecker product (as defined in Eq. (11)*), and with $n := n_1 \ldots n_k$. Then we have*

$$H(F\mathbf{v})H(\mathbf{v}) \geq n \tag{2}$$

where $\mathbf{v} \in \mathbb{C}^n$ denotes an arbitrary nonzero vector.

The reason why we did not use brackets in (1) is that the Kronecker product is known to be associative.

Note that the above result is of a *negative* type, since it shows that for a Fourier-like matrix F as in the statement of the theorem, it is impossible to find a nonzero vector concentrated on a small set (having small Hamming weight $H(\mathbf{v})$), for which the matrix-vector product is concentrated on a small set as well, i.e., $H(F\mathbf{v})$ is small as well. This interpretation reveals why Theorem 1 goes under the name 'uncertainty principle', in analogy with the classical result in quantum physics.

We refer to the references [2, 11, 9] for some interesting generalizations and analogues of Theorem 1.

In what follows, we will approach the uncertainty principle from a linear algebra point of view. Let us denote with I the set of indices where $F\mathbf{v}$ is nonzero, and with J the set of indices where $\mathbf{v}$ is nonzero. (Note that by definition, the cardinalities of these sets are equal to the Hamming weights $H(F\mathbf{v})$ and $H(\mathbf{v})$, respectively). Obviously, we should have

$$F(N \setminus I, J)\mathbf{v}|_J = 0, \tag{3}$$

where $N := \{1, \ldots, n\}$, and where $\mathbf{v}|_J$ denotes the vector obtained by restricting $\mathbf{v}$ to the set of its nonzero indices J. In other words, (3) states that the submatrix $F(N \setminus I, J)$ of F is *rank-deficient* in the sense that its null space is non-empty.

The uncertainty principle tells then that such a rank-deficient submatrix $F(N \setminus I, J)$ can not have an arbitrarily large number of rows, assuming that its number of columns is fixed, since we must have the restriction $|I| \cdot |J| \geq n$. This result is *negative* since it restricts the size of the rank-deficient submatrices, and hence the structure of F.

Interestingly, this negative result turns out to be complemented by a *positive* result, in which the existence of rank-deficient submatrices containing many rows in comparison to their number of columns is answered *affirmatively* when F is a Kronecker product of Fourier matrices. More precisely, we will show how a set of maximal rank-deficient submatrices of F can be constructed via tilings of rank-one blocks.

This paper is organized as follows. Section 2 recalls some facts about rank-deficient submatrices of Fourier matrices from [1]. Section 3 considers low rank submatrices of a Kronecker product. Section 4 characterizes a set of maximal rank-deficient submatrices of a Kronecker product. Conclusions are given in Section 5.

2 Rank-deficient submatrices of Fourier matrices

In this section we recall some basic definitions and results concerning rank-deficient submatrices of Fourier matrices from [1], and we provide some additional results as well.

In what follows, we call a matrix $A \in \mathbb{C}^{m\times n}$ *rank-deficient* if Rank $A < n$, or equivalently, if there exists a non-zero vector $\mathbf{v} \in \mathbb{C}^n$ such that $A\mathbf{v} = \mathbf{0}$. The aim of this paper is to search the size of the maximal rank-deficient submatrices of a Fourier-like matrix of the form (1).

To make the concept of 'maximal' rank-deficient submatrix more precise, we introduce the following definition.

Definition 2 *For a matrix $A \in \mathbb{C}^{n\times n}$ and an integer $d \in \{1,\ldots,n\}$, we define the* Hamming number $H_A(d)$ *as the minimal cardinality of all index sets I for which $A(N \setminus I, J)$ is rank-deficient, under the restriction that $|J| \leq d$. Here we denote $N := \{1,\ldots,n\}$.*

It may seem odd that the above definition works with the number of row indices in the *complement* of a maximal rank-deficient submatrix, rather than the number of row indices of the rank-deficient submatrix *itself*. However, we do this to stay close to the formulation of the uncertainty principle. Indeed, it can be noted that Definition 2 allows the following reformulation of Theorem 1:

$$d \cdot H_F(d) \geq n, \tag{4}$$

where F is any matrix of the form (1).

As an example, consider the Fourier matrix F_5. It is known that Fourier matrices of prime order do not have any square singular submatrix (see [5] for a historical overview about this statement). Therefore, the matrix F_5 can have only rank-deficient submatrices of a *trivial* type, i.e., for which the number of rows is strictly smaller than the number of columns. We have then $H_{F_5}(d) = 5-(d-1) = 6-d$ for any $d \in \{1,\ldots,5\}$, resulting in the following table for the Hamming numbers of F_5:

d	1	2	3	4	5
$H_{F_5}(d)$	5	4	3	2	1

(5)

It can be noted that the above table satisfies a certain symmetry, in the sense that the topmost row of (5) equals the bottommost row in the reverse order. In fact, this is a special case of a more general duality principle which we state now.

Lemma 3 *1. Let $A \in \mathbb{C}^{n\times n}$ be an arbitrary nonsingular matrix, and let $d, k \in \{1,\ldots,n\}$. If $H_A(d) = k$, then $H_{A^{-1}}(k) \leq d$.*

2. Let $F \in \mathbb{C}^{n\times n}$ be any Fourier-like matrix of the form (1), and let $d, k \in \{1,\ldots,n\}$. If $H_F(d) = k$, then $H_F(k) \leq d$.

PROOF.

1. From the fact that $H_A(d) = k$, there follows the existence of a rank-deficient submatrix $A(N \setminus I, J)$ with $|I| = k$ and $|J| \leq d$. From a result in [4], this rank-deficient submatrix of A implies also a rank-deficient submatrix of the *inverse* matrix A^{-1}: $A^{-1}(N \setminus J, I)$ must be rank-deficient. It follows immediately that $H_{A^{-1}}(k) \leq d$.

2. Since the given matrix F is both unitary and symmetric, we have $F^{-1} = F^H = \bar{F}$, where the bar denotes complex conjugation. Since this complex conjugation does not affect the ranks of the submatrices of F, we can now invoke the first part of the lemma to obtain the desired result.

□

Remark 4 *It might be tempting to conjecture that in the statement of Lemma 3, the inequality $H_{A^{-1}}(k) \leq d$ can be replaced by the equality $H_{A^{-1}}(k) = d$. However, this would be incorrect. The underlying reason is that in our definition of Hamming numbers, Definition 2, we worked with the inequality $|J| \leq d$ rather than the equality $|J| = d$. We do this to guarantee that the Hamming numbers $H_A(d)$ are monotonically decreasing with respect to d.*

We recall that (5) is basically a *negative* result, since it states that the Fourier matrix of prime order can not have any non-trivial rank-deficient submatrix.

The situation turns out to be quite different in case of a Fourier matrix of non-prime order. For example, here are the Hamming numbers for F_{25}:

d	1	2	3	4	5	10	15	20	25
$H_{F_{25}}(d)$	25	20	15	10	5	4	3	2	1

(6)

We note that (6) lists only the relevant values of d, i.e., only those values of d where the Hamming number makes a jump w.r.t. the one for $d-1$. Moreover, note that the table (6) is compatible with the duality principle of Lemma 3.2.

Note that (6) is also compatible with the uncertainty principle (4), i.e., $d \cdot H_{F_{25}}(d) \geq 25$. Moreover, it can be seen that *equality* in the uncertainty principle is reached whenever d is a divisor of n, in the present case when $d \in \{1, 5, 25\}$.

We will not recall here the mechanism leading to the values in (6). The reader who wishes to find out more about this is referred to [1].

Generalizing from (5) and (6), the following result was proved in [1].

Theorem 5 *Let p^m be a power of a prime number. Let $d \in \{1, 2, \ldots, p^m\}$ be such that*

$$cp^k \leq d < (c+1)p^k, \tag{7}$$

for certain $c \in \{1, \ldots, p-1\}$, $k \in \{0, \ldots, m-1\}$. Then we have that

$$H_{F_{p^m}}(d) = (p - c + 1)p^{m-k-1}. \tag{8}$$

Note that Theorem 5 deals with the case of a single Fourier matrix whose order is a power of a prime number. For the remainder of this paper, we will generalize this by considering the Hamming numbers of a general Kronecker product of Fourier matrices. These matters are taken up in the next sections.

We conclude this section with some elementary, alternative interpretations of the Hamming numbers $H_{F_n}(d)$.

Lemma 6

1. *(Evaluating a sparse polynomial at roots of unity:) Let $v(z) = \sum_{i=0}^{n-1} v_i z^i$ be a nonzero polynomial containing d nonzero coefficients v_i. Then there must be* at least *$H_{F_n}(d)$ roots of unity $\omega^i \in \{1, \omega, \ldots, \omega^{n-1}\}$ such that $v(\omega^i) \neq 0$.*

2. *(Rank of a sparse circulant matrix:) Let C be a nonzero circulant matrix of size n by n, i.e., a matrix with (i,j)th entry depending only on $j - i$* mod *n:*

$$C = \begin{bmatrix} v_0 & v_1 & \cdots & \cdots & v_{n-1} \\ v_{n-1} & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & v_1 \\ v_1 & \cdots & \cdots & v_{n-1} & v_0 \end{bmatrix}. \tag{9}$$

   Let $\mathbf{v}^T$ denote the first row of C, containing d nonzero coefficients v_i. Then the rank of C must be at least equal to $H_{F_n}(d)$.

PROOF.

1. (See e.g. [3]). Let us consider a general matrix-vector product $F_n \mathbf{v}$: this yields a vector for which the ith component is given by $\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega^{ij} v_j$. Hence this ith component is precisely the evaluation of the polynomial $v(z) := \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} v_j z^j$ in the root of unity $z = \omega^i$. The result follows then immediately from the definition of Hamming numbers.

2. We use the well-known decomposition $C = F_n^{-1} D F_n$ where D is the diagonal matrix

$$D = \text{diag}\{v(1), v(\omega), \ldots, v(\omega^{n-1})\}, \tag{10}$$

and with $v(z) := \sum_{j=0}^{n-1} v_j z^j$ the polynomial associated to the first row of C (see [13, page 206]). Now by the first part of this lemma, at least $H_{F_n}(d)$ of the diagonal entries of D in (10) have to be different from zero. Since Rank C = Rank D, this finishes the proof.

□

3 Kronecker products and ranks

In this section we explore some connections between Kronecker products and low rank submatrices. This section is organized as follows. After reviewing some preliminaries (Subsection 3.1), we consider both the low rank submatrices of a general Kronecker product $A \otimes B$ (Subsection 3.2) and of a Kronecker product of Fourier matrices $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$ (Subsection 3.3).

3.1 Definitions

In this first subsection, we recall some basic definitions concerning Kronecker products. For $A \in \mathbb{C}^{m \times p}$ and $B \in \mathbb{C}^{n \times q}$, the *Kronecker product* of A and B is defined as the block matrix

$$A \otimes B = \begin{bmatrix} a_{0,0}B & \ldots & a_{0,p-1}B \\ \vdots & & \vdots \\ a_{m-1,0}B & \ldots & a_{m-1,p-1}B \end{bmatrix}. \tag{11}$$

For notational simplicity, we will often use the definition of Kronecker product for the case where A and B are *square* matrices, i.e., when $m = p$ and $n = q$. Nevertheless, it is straighforward that many facts extend to the case where A and B are rectangular matrices as well.

We denote by $\mathbb{Z}_n$ the Abelian group $\mathbb{Z}_n := \{0, \ldots, n-1\}$, with group operation defined by the addition modulo n. It can be argued that the row indices of (11) can be naturally labeled by means of the cartesian product group $\mathbb{Z}_m \times \mathbb{Z}_n$. More precisely, the row positions of $A \otimes B$ can be naturally labeled by means of a *double* index (i_1, i_2) with $i_1 \in \{0, \ldots, m-1\}$ and $i_2 \in \{0, \ldots, n-1\}$. Indeed, the index i_1 is intended to denote on which block row of (11) an entry is situated (the row of A), while the index i_2 denotes more specifically on which position of its block row it is situated (the row of B).

Similarly, the *column* indices of (11) can be naturally labeled by means of the product group $\mathbb{Z}_p \times \mathbb{Z}_q$.

The fact that one can use double indices to parametrize the rows and columns of a Kronecker product, reflects the fact that Kronecker products are a matrix realization of the so-called *tensor product* in multilinear algebra. Using this multilinear notation, the definition of Kronecker product can be reformulated as follows:

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

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 (11), respectively.

The following property is well-known:

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

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

Using Kronecker products, it is often useful to consider a vector as a matrix-like data structure, or conversely. We need the following definition.

Definition 7 *For* $m, n \in \mathbb{N}$ *and* $\mathbf{v} \in \mathbb{C}^{mn}$*, the* associated m by n matrix of $\mathbf{v}$ *is defined as the matrix* $\mathrm{Mat}_{m\times n}(\mathbf{v})$ *with* (i,j)*th entry given by* $\mathbf{v}_{i+mj}$*, for all* $i \in \{0, \dots, m-1\}$ *and* $j \in \{0, \dots, n-1\}$.

For example, for the column vector $\mathbf{v} := [0\ 1\ 2\ 3\ 4\ 5]^T$, we have

$$\mathrm{Mat}_{2\times 3}(\mathbf{v}) = \begin{bmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{bmatrix}.$$

We will sometimes abbreviate $\mathrm{Mat}_{m\times n}(\mathbf{v})$ by the shorter notation $\mathrm{Mat}(\mathbf{v})$ whenever the value of the indices m and n is clear from the context.

The main reason for introducing the Mat-operator is the following. It is well-known that any *matrix-vector product* with a Kronecker product $A \otimes B$ can be computed by means of the formula

$$\mathrm{Mat}_{n\times m}((A \otimes B)\mathbf{v}) = B\mathrm{Mat}_{q\times p}(\mathbf{v})A^T, \tag{12}$$

for any $A \in \mathbb{C}^{m\times p}$ and $B \in \mathbb{C}^{n\times q}$.

3.2 Low rank submatrices of $A \otimes B$

We are now ready to collect some results concerning low rank submatrices of Kronecker products. The following few results are elementary and well-known.

Lemma 8 *Let* $\mathrm{Rank}\ A = r$ *and* $\mathrm{Rank}\ B = s$*. Then* $\mathrm{Rank}\,(A \otimes B) = rs$*.*

Indeed: from the fact that $\mathrm{Rank}\ A = r$, there follows the existence of a rank-revealing factorization $A = U_A V_A^T$ where U_A, V_A are matrices of full column rank having r columns. Similarly, there exists a factorization $B = U_B V_B^T$ where U_B, V_B are matrices of full column rank having s columns. It follows that

$$A \otimes B = (U_A V_A^T) \otimes (U_B V_B^T) = (U_A \otimes U_B)(V_A^T \otimes V_B^T), \tag{13}$$

which provides a rank-revealing factorization of rank rs for the Kronecker product $A \otimes B$.

Concerning this last claim, note that the factors $U_A \otimes U_B$ and $V_A \otimes V_B$ in (13) consist indeed of rs columns. To show that they have full column rank, suppose by contradiction that $(U_A \otimes U_B)\mathbf{v} = 0$. From (12) it follows then that

$U_B \mathrm{Mat}(\mathbf{v}) U_A^T = 0$. From the assumption that U_A, U_B have full column rank, these two matrices must both have a square nonsingular submatrix. It follows then easily that $\mathrm{Mat}(\mathbf{v}) = 0$ and hence $\mathbf{v} = 0$, which was to be demonstrated.

By the same mechanism as in Lemma 8, one can obtain a result concerning *submatrices* of a full matrix.

Lemma 9 *Given two low rank submatrices* Rank $A(I,J) = r$ *and* Rank $B(K,L) = s$*, for certain index sets* I, J, K, L*. Then we have that*

$$\text{Rank } (A \otimes B)(I,K;J,L) = rs.$$

In other words, Lemma 9 states that each pair formed by a low rank submatrix of A and a low rank submatrix of B gives rise to a low rank submatrix of $A \otimes B$, with rank equal to the product of the original ranks*.

As an example, suppose that A and B are arbitrary matrices of size 3 by 3. We have the trivial rank-one submatrices

$$A(\{0,1,2\},\{0\}) = \text{Rk } 1, \quad B(\{0\},\{0,1,2\}) = \text{Rk } 1. \tag{14}$$

Following Lemma 9, these two trivial rank-one submatrices of A and B can then be combined to a *non-trivial* rank-one submatrix of $A \otimes B$, involving the rows labeled by $\{0,1,2\} \times \{0\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$, and the columns labeled by $\{0\} \times \{0,1,2\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$: see the left part of Figure 1.

Similarly, the right part of Figure 1 shows a rank-one submatrix of $A \otimes B$ where the role of A and B in (14) is switched. Hence, this submatrix has rows labeled by $\{0\} \times \{0,1,2\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$, and columns labeled by $\{0,1,2\} \times \{0\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$.

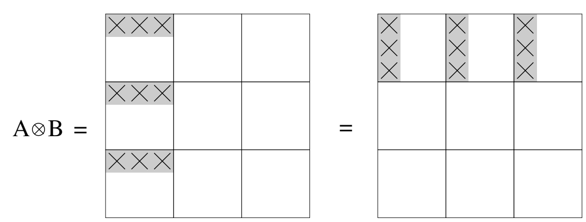

Figure 1: Given arbitrary $A, B \in \mathbb{C}^{3\times 3}$, the figure shows two types of rank-one submatrices of $A \otimes B$, indicated by highlighted entries.

Remark 10 *Another connection between Kronecker products and low rank matrices was given by Van Loan and Pitsianis [14], who showed that, provided the elements of the Kronecker product* $A \otimes B$ *are reshuffled in an appropriate way,*

*By iterating this result, one obtains the following: given a collection of low rank submatrices Rank $A_k(I_k, J_k) = r_k$, for certain index sets I_k, J_k, $k = 1, \ldots, K$. Then we have that Rank $(A_1 \otimes \ldots \otimes A_K)(I_1, \ldots, I_K; J_1, \ldots, J_K) = \prod_{k=1}^K r_k$.

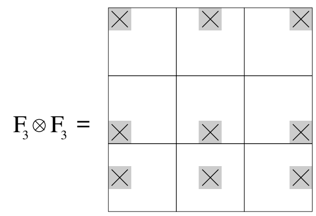

Figure 2: The figure shows a rank-one submatrix of the matrix $F_3 \otimes F_3$ whose existence can not be predicted by Lemma 9.

they can be recombined to form a rank-one matrix. This property is very important since it reduces the problem of approximation with a sum of Kronecker products, to a low rank approximation of the reshuffled data, see also [12, 8]. However, note that this result is of a different type than the results considered above, since the reshuffling of [14] can not *be expressed as* $P_1(A \otimes B)P_2$ *for any permutation matrices* P_1 *and* P_2*.*

3.3 Low rank submatrices of $F_{n_1} \otimes \ldots \otimes F_{n_k}$

We recall that the intention of this paper is to consider the low rank blocks of a Kronecker product of Fourier matrices F as in (1). Unfortunately, it turns out that not all rank-one submatrices of such a matrix F can be traced by means of Lemma 9. For example, observing that

$$F_3 \otimes F_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} F_3 & F_3 & F_3 \\ F_3 & \omega F_3 & \omega^2 F_3 \\ F_3 & \omega^2 F_3 & \omega F_3 \end{bmatrix}, \quad F_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \quad \omega^3 = 1,$$

it is easy to check that 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 $(0,0)$, $(1,1)$, $(2,2) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, must be of the form

$$\frac{1}{\sqrt{9}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \tag{15}$$

and hence of rank one: see Figure 2.

It should be stressed that this rank-one submatrix is specific for $F_3 \otimes F_3$, but that it is not present for arbitrary $A \otimes B$.

Considering the example of Figure 2 in more detail, note that the row indices $(0,0), (1,2), (2,1)$ of this submatrix form a *subgroup* $G \subset \mathbb{Z}_3 \times \mathbb{Z}_3$. Similarly, the column indices $(0,0), (1,1), (2,2)$ form a subgroup $H \subset \mathbb{Z}_3 \times \mathbb{Z}_3$. Moreover, the subgroups G and H are *annihilating* in the sense that the submatrix $(F_3 \otimes F_3)(G, H)$ has all its entries equal to 1, at least if we neglect the scaling factor $\frac{1}{\sqrt{9}}$, cf. (15).

More generally, let us consider a matrix F of the form (1), i.e.,

$$F = F_{n_1} \otimes \ldots \otimes F_{n_k}, \tag{16}$$

and denote $n := n_1 \ldots n_k$. Similarly as in the case of a single Kronecker product, one can naturally label the rows and columns of (16) by means of *multi-indices*, belonging to the cartesian product group $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$[†].

Let G be any subgroup of $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. It is known from a theory called *Pontryagin duality* [10] that there exists a corresponding *annihilator subgroup* $H \subset \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, of size $|H| = n/|G|$, defined by the property

$$\omega^{\mathbf{g}\cdot\mathbf{h}} = 1, \quad \text{for all } \mathbf{g} \in G, \mathbf{h} \in H.$$

Here we used the vectorial notation $\omega := (\omega_{n_1}, \ldots, \omega_{n_k})$, where $\omega_k = \exp(2\pi\mathbf{i}/k)$ denotes the kth root of unity, $\mathbf{i} = \sqrt{-1}$. We also denoted the multi-indices $\mathbf{g} := (g_1, \ldots, g_k)$, $\mathbf{h} := (h_1, \ldots, h_k) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, and we used the short notation $\omega^{\mathbf{g}\cdot\mathbf{h}} := \omega_{n_1}^{g_1 h_1} \cdot \ldots \cdot \omega_{n_k}^{g_k h_k}$. We will use these vectorial notations also in what follows.

Given a permutation P of $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, 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.

Given a subgroup $G \subseteq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, a permutation P of $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ (assuming lexicographical ordering) is said to *sort the indices modulo G* if the image set under P can be naturally partitioned into a collection of cosets[‡] of G. For example, for the subgroup $G = \{0, 3\} \subset \mathbb{Z}_6$, the permutation $P_1 : 0, 1, 2, 3, 4, 5 \mapsto 0, 3, 1, 4, 2, 5$ sorts the indices modulo G.

The observation of Figure 2 allows then the following generalization.

Lemma 11 *Let F be a matrix of the form (16). Let $G, H \subseteq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ be a pair of annihilating subgroups. Let P_1, P_2 be permutations on the group $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ that sort the indices modulo G and H, respectively, for some order of the cosets. Then the matrix $P_1^T F P_2$ can be subdivided in a grid of rank-one submatrices, i.e.,*

$$P_1^T F P_2 = \begin{bmatrix} \text{Rk } 1 & \ldots & \text{Rk } 1 \\ \vdots & & \vdots \\ \text{Rk } 1 & \ldots & \text{Rk } 1 \end{bmatrix},$$

where each Rk 1 *denotes a matrix of rank* 1*, having size $|G|$ by $|H|$. (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.)*

[†]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 $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$. It is in this terminology that virtually all the results about the matrix F encountered in the literature are stated, e.g. [6, 2, 11, 9, 7].

[‡]Recall that for a subgroup $G \subseteq G_0$, a *coset* of G is defined as a set of the form $g_0 + G := \{g_0 + g | \, g \in G\}$. The collection of all cosets of G forms a partition of G_0. In case G is a cyclic group of order n, the cosets of G reduce to the *residue classes* modulo n.

PROOF. Using the fact that G and H are annihilating subgroups, it follows that the $(\mathbf{i},\mathbf{j})$th block element of the matrix $P_1^T F P_2$ equals

$$\begin{aligned}
\left[\omega^{(\mathbf{i}+\mathbf{g})(\mathbf{j}+\mathbf{h})}\right]_{\mathbf{g}\in G,\mathbf{h}\in H} &= \left[\omega^{\mathbf{ij}+\mathbf{ih}+\mathbf{gj}}\right]_{\mathbf{g}\in G,\mathbf{h}\in H} \\
&= \omega^{\mathbf{ij}}\left[\omega^{\mathbf{ih}}\omega^{\mathbf{gj}}\right]_{\mathbf{g}\in G,\mathbf{h}\in H} \\
&= \omega^{\mathbf{ij}}\begin{bmatrix} \omega^{\mathbf{g}_1\mathbf{j}} \\ \vdots \\ \omega^{\mathbf{g}_{|G|}\mathbf{j}} \end{bmatrix}\begin{bmatrix} \omega^{\mathbf{ih}_1} & \dots & \omega^{\mathbf{ih}_{|H|}} \end{bmatrix} =: \mathrm{Rk}\ 1,
\end{aligned}$$

which is indeed a submatrix of rank one. □

In case of a matrix F with order a power of a prime number, one can apply the above idea recursively.

Lemma 12 *Let F be a matrix of the form (16) with order equal to a power of a prime number p^m. Then there exist permutations P_1, P_2 such that $P_1^T F P_2$ can be subdivided in a $p^l \times p^{m-l}$ grid of rank-one submatrices, and this* simultaneously *for all $l \in \{0, \dots, m\}$.*

PROOF. It suffices to take a chain of nested subgroups

$$\{0\} = G_0 \subset G_1 \subset \dots \subset G_m, \tag{17}$$

where $|\frac{G_l}{G_{l-1}}| = p$ for all l. Obviously, one can then find a permutation P_1 that sorts *simultaneously* modulo all of the G_l, for some order of the cosets. Similarly, one can consider the corresponding chain of annihilator subgroups

$$H_0 \supset H_1 \supset \dots \supset H_m = \{0\},$$

and find a permutation P_2 that sorts simultaneously modulo all of the H_l, for some order of the cosets. The result follows then by Lemma 11. □

Remark 13 *Lemmas 11 and 12 are closely related to the exposition in [1]. Indeed, in case of a single Fourier matrix $F = F_{p^m}$ with p prime, the associated Abelian group equals $\mathbb{Z}_{p^m}$. But since $\mathbb{Z}_{p^m}$ has a* unique *subgroup of order p^l for each l, the chain of subgroups (17) is then uniquely determined. The corresponding permutation that sorts simultaneously along the cosets of each of the subgroups of (17) can be chosen to be the so-called* digit-reversing permutation*, as we did in [1].*

The partition in rank-one blocks of the matrix F suggests that this matrix should have a lot of *rank-deficient* submatrices. Indeed: the idea is to construct a submatrix $F(N \setminus I, J)$ which can be covered by a collection of at most $|J| - 1$ rank-one blocks of F. Since $|J| - 1 < |J|$, the rank of such a submatrix is then smaller than its number of columns, so that it is indeed rank-deficient; see also [1].

We will restrict ourselves here to one result of this type.

Theorem 14 *Let F be a matrix of the form (16), and let $G_1 \subset G_2$ be subgroups of $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ such that $|\frac{G_2}{G_1}| = p$ is a prime number. Let H_1, H_2 be the annihilator subgroups of G_1, G_2, respectively. Assume that I, J are index sets such that*

$$G_1 \subseteq I \subseteq G_2, \qquad I \text{ consists of } p+1-c \text{ cosets of } G_1,$$
$$H_2 \subseteq J \subseteq H_1, \qquad J \text{ consists of } c \text{ cosets of } H_2,$$

for some $c \in \{1, \ldots, p\}$. Then the submatrix $F(N \setminus I, J)$ can be subdivided as a collection of $|J| - 1$ rank-one submatrices and hence is rank-deficient.

Remark 15 *Theorem 14 remains true if $|\frac{G_2}{G_1}| = p$ is an arbitrary whole number, which needs not to be prime. However, it turns out that for the aim of finding the* maximal *rank-deficient submatrices of F, only the case with p prime is of relevance (See Section 4).*

Proof of Theorem 14. Firstly, let us cover $F((N \setminus G_2) \times J)$ by a collection of rank-one blocks of size $|G_2| \times |H_2|$. Obviously, this requires

$$\frac{|N \setminus G_2|}{|G_2|} \frac{|J|}{|H_2|} = (|H_2| - 1)c$$

of these blocks.

Now let us cover $F((G_2 \setminus I) \times J)$ by a collection of rank-one blocks of size $|G_1| \times |H_1|$. This can be done by

$$\frac{|G_2 \setminus I|}{|G_1|} = \frac{(c-1)|G_1|}{|G_1|} = c - 1$$

of these blocks.

Summarizing, we have covered now $F(N \setminus I, J)$ with a collection of $(|H_2| - 1)c + (c - 1) = c|H_2| - 1 = |J| - 1$ rank-one blocks. Since $|J| - 1 < |J|$, this shows that the rank of $F(N \setminus I, J)$ must be strictly smaller than its number of columns, and hence that this matrix is rank-deficient. □

Corollary 16 *Let F be a matrix of the form (16), of size $n = n_1 \ldots n_k$. For any set of divisors d, pd of n, with p prime, and for any $c \in \{1, \ldots, p\}$, we have the following bound involving Hamming numbers:*

$$H_F(cd) \leq (p + 1 - c)\frac{n}{pd}. \tag{18}$$

proof. Using the notations of Theorem 14, we have shown there that a rank-deficient submatrix $F(N \setminus I, J)$ can be constructed having $|J| = c|H_2|$ and $|I| = (p+1-c)|G_1| = (p+1-c)\frac{n}{|H_1|} = (p+1-c)\frac{n}{p|H_2|}$. Identifying $d := |H_2|$, the desired bound (18) follows. □

4 Kronecker products and rank defects

In this section we characterize the size of the maximal rank-deficient submatrices (in the sense of Hamming numbers) of a Kronecker product $A \otimes B$, in terms of those of the original matrices A and B. This result will then be applied to the case of a matrix $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$, showing that the upper bound in Corollary 16 of the previous section is 'sharp', in a sense to be specified further.

4.1 Rank-deficient submatrices of $A \otimes B$

We recall the formula (12), which we can restate as follows:

$$\mathrm{Mat}((A \otimes B)\mathbf{v}) = B\mathrm{Mat}(\mathbf{v})A^T.$$

Then we have the following result.

Theorem 17 *For any matrices A, B and for any integer d we have*

$$H_{A\otimes B}(d) = \min_{ab \leq d} H_A(a)H_B(b). \tag{19}$$

PROOF. First we show the *negative* inequality $\geq$. Suppose that $\mathrm{Mat}(\mathbf{v})$ has precisely k nonzero rows and $d =: qk + r$ nonzero elements, $r \in \{0, \ldots, k-1\}$. (The variable q denotes here a Euclidean quotient and should not be confused with the variable q occurring in some earlier parts of this paper.) Thus the matrix $\mathrm{Mat}(\mathbf{v})$ must have a nonzero row vector $\mathbf{r}$ with not more than q nonzero elements. But then the number of nonzero entries of $\mathbf{r}A^T$ must be at least $H_A(q)$, and hence also the number of nonzero columns of $\mathrm{Mat}(\mathbf{v})A^T$ must be at least $H_A(q)$. On the other hand, note that each column of $\mathrm{Mat}(\mathbf{v})A^T$ contains at most k nonzero entries, by construction of k. Thus for each of the nonzero columns of $\mathrm{Mat}(\mathbf{v})A^T$ (of which we already established that there must be at least $H_A(q)$ of them), there must be at least $H_B(k)$ rows of B which are not eliminated by this column. This gives us the desired inequality

$$H_{A\otimes B}(d) \geq H_A(q)H_B(k) \geq \min_{ab \leq d} H_A(a)H_B(b),$$

where the last transition follows since $qk \leq qk + r =: d$.

Now we show the *positive* inequality $\leq$. Let there be given two integers a and b with $ab \leq d$. Let $\mathbf{s}$ be a nonzero vector with at most a nonzero entries such that $A\mathbf{s}$ has $H_A(a)$ nonzero entries, and let $\mathbf{t}$ be a nonzero vector with at most b nonzero entries such that $B\mathbf{t}$ has $H_B(b)$ nonzero entries. Then we construct the rank-one matrix $\mathrm{Mat}(\mathbf{v}) := \mathbf{t}\mathbf{s}^T$. It is clear that $\mathrm{Mat}(\mathbf{v})$ has at most ab nonzero entries, and that $B\mathrm{Mat}(\mathbf{v})A^T$ has exactly $H_A(a)H_B(b)$ nonzero entries. Since we can construct such a $\mathrm{Mat}(\mathbf{v})$ for any two integers a and b with $ab \leq d$, this establishes the inequality $\leq$. □

Remark 18 *For example, when $A, B \in \mathbb{C}^{n\times n}$ are random matrices and $d = n$, then we have (for a sufficiently generic choice of A and B) that*

$$H_{A\otimes B}(n) = H_A(1)H_B(n) = n \times 1 = n.$$

The proof of Theorem 17 shows then that a minimizer can be obtained by writing

$$B \begin{bmatrix} \times & \dots & 0 \\ \vdots & & \vdots \\ \times & \dots & 0 \end{bmatrix} A^T = \begin{bmatrix} \times & \dots & \times \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{bmatrix}, \tag{20}$$

where the entries which are not indicated, are all equal zero. Thus the matrix $\mathrm{Mat}(\mathbf{v})$ *in* (20) *is zero except for its first column, which should be chosen orthogonal to the space formed by rows $2, \dots, n$ of B. (Of course, note that such a counterexample is only unique up to a permutation of the rows and columns of* $\mathrm{Mat}(\mathbf{v})$*.)*

Alternatively, one could use here the characterization

$$H_{A\otimes B}(n) = H_A(n)H_B(1) = 1 \times n = n,$$

which suggests that a minimizer may be chosen by switching the place of the two sparse matrices in the above equation (20)*, i.e.,* $\mathrm{Mat}(\mathbf{v})$ *is zero except for its first row.*

Surprisingly, the fact that we have here two different ways for obtaining $H_{A\otimes B}(n)$, turns out to open the door for other minimizers as well, which may be not directly related to a rank-one form for $\mathrm{Mat}(\mathbf{v})$*. For example, in case where $A = B^{-T}$, one can trivially write down the equation*

$$BIB^{-1} = I,$$

with $\mathrm{Mat}(\mathbf{v}) := I$ *a sparse matrix (the identity matrix). Hence for this very special choice of A and B, we obtain here a nontrivial way for obtaining the same Hamming number $H_{A\otimes B}(n) = n$.*

To apply Theorem 17 in an efficient way, it is useful to introduce an auxiliary rank-one matrix $M_{A\otimes B}$ with (i, j)th element defined as the product $H_A(i)H_B(j)$. For example, recalling that $H_{F_p}(d) = p+1-d$ for any prime number p, we have

$$M_{F_3\otimes F_7} = \begin{array}{c|ccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 1 & \mathbf{21} & 18 & 15 & 12 & 9 & \mathbf{6} & \mathbf{3} \\ 2 & \mathbf{14} & 12 & 10 & 8 & 6 & 4 & \mathbf{2} \\ 3 & \mathbf{7} & \mathbf{6} & 5 & 4 & 3 & 2 & \mathbf{1} \end{array}. \tag{21}$$

Note that the row and column indices of $M_{A\otimes B}$ run from one (instead of zero), and that we separated them with a horizontal and vertical line from the actual matrix $M_{A\otimes B}$. Moreover, the 'relevant' matrix entries (in the sense that they can achieve equality in the mimimum of (19)), are indicated in boldface.

Collecting the above relevant matrix entries, an application of Theorem 17 leads to the following table for the Hamming numbers $H_{F_3 \otimes F_7}$ (or by the same means, for any $H_{A \otimes B}$ with both $A \in \mathbb{C}^{3\times 3}$ and $B \in \mathbb{C}^{7\times 7}$ having no nontrivial rank-deficient submatrices)

d	1	2	3	6	7	14	21
$H_{F_3\otimes F_7}(d)$	21	14	7	6	3	2	1

.

Another example (only the relevant rows and columns are shown)

$$M_{F_3\otimes F_{49}} = \begin{array}{c|ccccccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 14 & 21 & 28 & 35 & 42 & 49 \\ \hline 1 & \mathbf{147} & 126 & 105 & 84 & 63 & \mathbf{42} & \mathbf{21} & 18 & 15 & 12 & 9 & \mathbf{6} & \mathbf{3} \\ 2 & \mathbf{98} & 84 & 70 & 56 & 42 & 28 & \mathbf{14} & 12 & 10 & 8 & 6 & 4 & \mathbf{2} \\ 3 & \mathbf{49} & \mathbf{42} & 35 & 28 & 21 & 14 & \mathbf{7} & \mathbf{6} & 5 & 4 & 3 & 2 & \mathbf{1} \end{array}, \tag{22}$$

leading to

d	1	2	3	6	7	14	21	42	49	98	147
$H_{F_3\otimes F_{49}}(d)$	147	98	49	42	21	14	7	6	3	2	1

.

A final example is

$$M_{F_5\otimes F_5} = \begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & \mathbf{25} & \mathbf{20} & \mathbf{15} & \mathbf{10} & \mathbf{5} \\ 2 & \mathbf{20} & 16 & 12 & 8 & \mathbf{4} \\ 3 & \mathbf{15} & 12 & 9 & 6 & \mathbf{3} \\ 4 & \mathbf{10} & 8 & 6 & 4 & \mathbf{2} \\ 5 & \mathbf{5} & \mathbf{4} & \mathbf{3} & \mathbf{2} & \mathbf{1} \end{array}, \tag{23}$$

leading to

d	1	2	3	4	5	10	15	20	25
$H_{F_5\otimes F_5}(d)$	25	20	15	10	5	4	3	2	1

,

which yields exactly the same behavior as we found for F_{25}. From this and other examples, the attentive reader will notice that the Hamming numbers of $\bigotimes_{l=1}^{m} F_p$, with p prime are exactly the same as the Hamming numbers which we obtained for F_{p^m}. A proof of this and some related observations will be given in the next subsection.

4.2 Rank-deficient submatrices of $F_{n_1} \otimes \ldots \otimes F_{n_k}$

We will now apply the results of the previous subsection to give an exact determination of the Hamming numbers of an arbitrary matrix F as in (16).

Given such a matrix F, let us consider the points $(d, H_F(d))$, $d \in \{1, \ldots, n\}$ as *grid points* in $\mathbb{N}^2$. The uncertainty principle tells that these grid points must be situated above the hyperbola $d \cdot H_F(d) = n$. We want now to obtain finer estimates of this result.

Let us assume by induction that we have two matrices A, B for which the grid points $(a, H_A(a))$, $(b, H_B(b))$ are completely known. Theorem 17 states then that in order to obtain the grid points $(d, H_{A\otimes B}(d))$ for the Kronecker product $A \otimes B$, we should form all the *candidate points* $(ab, H_A(a)H_B(b))$, and subsequently retain only those candidate points that can reach equality in the minimum (19).

The main point will be now to characterize these relevant candidate points $(ab, H_A(a)H_B(b))$. Observing from (21), (23) that when $A = F_p$ and $B = F_q$ with $p \leq q$ two prime numbers, only those values which are at a *border* of the auxiliary matrix $M_{A\otimes B}$ which we introduced in the previous subsection can be of relevance, we will show the following result.

Lemma 19 *Let $p \leq q$ be two prime numbers and consider the matrix $F_p \otimes F_q$. Then the indices $a \in \{1, \ldots, p\}$ and $b \in \{1, \ldots, q\}$ can only lead to equality in the minimum* (19) *if at least one of them takes its extreme value, i.e., if either $a \in \{1, p\}$ or $b \in \{1, q\}$.*

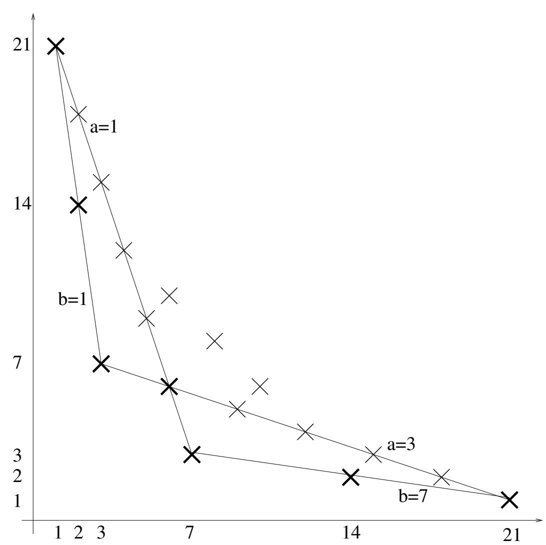

Figure 3: Two-dimensional representation of all the candidate points $(ab, H_{F_3}(a)H_{F_7}(b)) = (ab, (4-a)(8-b))$, $a \in \{1, \ldots, 3\}$, $b \in \{1, \ldots, 7\}$ for the matrix $F_3 \otimes F_7$; note that we have here $p = 3$ and $q = 7$. The candidate points which are *relevant* in the sense that they can lead to equality in the minimum (19), are precisely those for which no other candidate point exists on the lower left of it, and are indicated in boldface in the figure. Note that these relevant points all lie on the union of the 4 extremal lines $b = 1, a = 3, b = 7, a = 1$; these 4 lines correspond to the border of the table (21).

PROOF. Note that the candidate point $(x, y) := (ab, H_A(a)H_B(b))$ achieves equality in the minimum (19) if and only if there exists no other candidate point $(\tilde{x},\tilde{y}) := (\tilde{a}\tilde{b}, H_A(\tilde{a})H_B(\tilde{b}))$ for which both $\tilde{x} \leq x$ and $\tilde{y} < y$. Graphically, this means that the point $(x,y) \in \mathbb{N}^2$ should be such that there is no other candidate point $(\tilde{x},\tilde{y})$ on the *lower left* of it. An illustration of this feature is shown in Figure 3, where the relevant candidate points are distinguished from the irrelevant ones by putting them in boldface.

Consider now the case of a candidate point $(x,y) = (ab, H_A(a)H_B(b))$ for which $x \leq p$. Taking into account the characterization of the previous paragraph, it is easy to see graphically that only those points for which $a \in \{1,\ldots,p\}$, $b = 1$ can be of relevance here. These correspond to the extremal line $b = 1$ in Figure 3.

Consider now the case $p \leq x \leq q$. Let us take a *fixed* grid point $(a, H_{F_p}(a)) = (a, p+1-a)$ and a *variable* grid point $(b, H_{F_q}(b)) = (b, q+1-b)$. The corresponding candidate points

$$(ab, H_A(a)H_B(b)) = (ab, (p+1-a)(q+1-b)),$$

$b \in \{1,\ldots,q\}$, must then all be situated on the line in $\mathbb{R}^2$ with equation

$$\frac{x}{a} + \frac{y}{p+1-a} = q+1.$$

Now we intersect this line with the border line for $a = 1$: $x + \frac{y}{p} = q+1$. This intersection can be easily computed to be given by the point

$$(x,y) = (\frac{q+1}{p+1}a, \frac{p}{p+1}(q+1)(p+1-a)).$$

But now it is easily checked that $\frac{p}{p+1}(q+1)(p+1-a)) > q$ provided $a < p$. Recalling our assumption that $p \leq x \leq q$, it follows that for any $a \in \{2,\ldots,p-1\}$, the line with fixed a can only contain relevant points (x,y) for which $y > q$. But then these points must all have the extreme candidate point $(\tilde{x},\tilde{y}) = (p,q)$ on the lower left of it. We conclude that if $p \leq x \leq q$, only the extreme lines $a = 1$ and $a = p$ can be of relevance: see Figure 3.

Finally, for the case where $x \geq q$ it is easy to see graphically that all the relevant candidate points must be on the extremal line $b = q$: see Figure 3. (Alternatively, this can be shown from the result for $x \leq p$ by invoking the duality principle of Lemma 3.)

□

We will now use Lemma 19 to obtain a characterization of the Hamming numbers for any Kronecker product of Fourier matrices.

Theorem 20 *Let F be a matrix of the form (16), of size $n = n_1 \ldots n_k$. We have the following converse of Corollary 16: for any integer l, there exist divisors d, pd of n, with p prime, and a value $c \in \{1,\ldots,p\}$ such that $cd \leq l$ and*

$$H_F(l) = H_F(cd) = (p+1-c)\frac{n}{pd}. \tag{24}$$

PROOF. We will prove the result by induction on the number of factors in the Kronecker product $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$. From the fact that F_{mn} equals $P_1(F_m \otimes F_n)P_2$ for certain permutations P_1 and P_2 whenever m and n are coprime ([13, page 195]), we may assume without loss of generality that all the components of F are of the form F_{p^m} where p^m is a power of a prime number.

Now by Theorem 5, (24) holds in case of a single Fourier matrix F_{p^m} where p^m is a power of a prime number. To prove the general case, let us write $F = F_1 \otimes F_2$, let l be any integer, and let $(a, b) =: (a_1, a_2)$, $a_1 a_2 \leq l$ be two indices leading to equality in the minimum (19). By the induction hypothesis, we have for each $i \in \{1, 2\}$ that there exist divisors d_i, $p_i d_i$ of $|F_i|$, with p_i prime, such that $a_i = c_i d_i$, $c_i \in \{1, \ldots, p_i\}$, and such that $H_{F_i}(a_i) = (p_i + 1 - c_i)\frac{|F_i|}{p_i d_i}$. We want now to show that either $c_1 \in \{1, p_1\}$ or $c_2 \in \{1, p_2\}$.

To show this, consider the table with (c_1, c_2)th element given by

$$H_{F_1}(c_1 d_1) H_{F_2}(c_2 d_2) = (p_1 + 1 - c_1)\frac{|F_1|}{p_1 d_1}(p_2 + 1 - c_2)\frac{|F_2|}{p_2 d_2},$$

$c_1 \in \{1, \ldots, p_1\}$, $c_2 \in \{1, \ldots, p_2\}$. Discarding the common factor $\frac{|F_1|}{p_1 d_1}\frac{|F_2|}{p_2 d_2}$, the values in the table reduce to

$$(p_1 + 1 - c_1)(p_2 + 1 - c_2),$$

and hence the proof reduces to the proof of Lemma 19. □

As an illustration of Theorem 20, the reader could reconsider each of the examples in (21), (22) and (23), as well as the resulting tables of Hamming numbers for each of these three cases.

We will now state some corollaries of Theorem 20.

Corollary 21 *We have that* $H_{F_{n_1} \otimes \ldots \otimes F_{n_k}} \equiv H_{F_n}$, *where* $n := n_1 \ldots n_k$.

Indeed: this follows since the characterization of the Hamming numbers in Theorem 20 is only dependent on the global matrix dimension n, but not on the underlying distribution of $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$ as a Kronecker product of Fourier matrices.

Remark 22 *The fact that the matrices* F_{p^m} *and* $\otimes_{k=1}^m F_p$ *have exactly the same Hamming numbers, allows also a more intuitively pleasing explanation. The reason is that the formula (12) for Kronecker products, allows an analog for* Fourier matrices. *Indeed: we have the following formula for computing a matrix-vector product with a Fourier matrix* F_{mn}*:*

$$\mathrm{Mat}(F_{mn} P_{m,mn} \mathbf{v}) = \left(C \odot (F_n \mathrm{Mat}(\mathbf{v}))\right) F_m^T, \tag{25}$$

where

$$C := F_{mn}(0 : n-1, 0 : m-1),$$

with $\odot$ denoting the Hadamard (entrywise) product of matrices, and with $P_{m,mn}$ denoting a certain permutation matrix (for a definition, see [1]). This formula (25) could be derived e.g. from [13, page 82].

Note that the transpose sign in (25) could of course be dropped since the Fourier matrix is symmetric: $F_m = F_m^T$. However, we placed this transpose sign to stress the analogy with the formula (12).

Note that (25) has the same form as (12), where we had the special choice $C = 1$, i.e., the rank-one matrix containing all entries equal to one. It can be seen that the argument in the proof of Theorem 17 which we applied to establish the inequality $\geq$, can be extended to the more general form of (25), with the only requirement being that C does not contain zero entries.

Of course, this leaves the question open for the inequality $\leq$, i.e., the positive *inequality expressing that the indicated values can be attained for a sufficiently large rank-deficient submatrix. This needs not always be the case, but for Fourier matrices it holds since these can be written in many different ways as such a formula (25). Hence, these ideas could be used to give an inductive proof of Theorem 5.*

We state some other corollaries of Theorem 20.

Corollary 23 *(See [11]:) For each divisor d of n, we have that $H_{F_n}(d) = \frac{n}{d}$, i.e., equality in the uncertainty principle* (4) *is reached.*

Corollary 24 *(See [7]:) The grid points $(d, H_F(d))$ must lie above the polyline formed by connecting the grid points $(d, H_F(d))$ where d ranges over the subsequent* divisors *of n.*

Corollary 24 was also obtained in [7] using group theoretical induction. In fact, note that Theorem 20 shows that from the couples of divisors of n, only those whose quotient is a prime number (and in particular a whole number) p are relevant for determining the Hamming numbers of F. Hence, this is a refinement of Corollary 24.

We stress that Theorem 20 gives a characterization of the Hamming numbers, i.e., the *size* of the maximal rank-deficient submatrices of the matrix F, as well as a particular way to construct such maximal rank-deficient submatrices. On the other hand, this result does not characterize the *uniqueness* of these submatrices (cf. Remark 18).

Concerning this uniqueness question, note first that a *translation*, i.e., any update of the form $I := I + \mathbf{a}$, $J := J + \mathbf{b}$ for $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ transforms the submatrix $F(I, J)$ to the form $D_\mathbf{b} F(I, J) D_\mathbf{a}$ for suitable unitary diagonal matrices $D_\mathbf{a}, D_\mathbf{b}$ [§]. In particular, it follows immediately that the *rank* of $F(I, J)$ is invariant under any translation of I and J.

We can then state the following conjecture.

[§] This follows since $F(I + \mathbf{a}, J) = \frac{1}{\sqrt{n}}[\omega^{(\mathbf{i}+\mathbf{a})\cdot\mathbf{j}}]_{\mathbf{i},\mathbf{j}} = \frac{1}{\sqrt{n}}[\omega^{\mathbf{i}\cdot\mathbf{j}}\omega^{\mathbf{a}\cdot\mathbf{j}}]_{\mathbf{i},\mathbf{j}} = \frac{1}{\sqrt{n}}[\omega^{\mathbf{i}\cdot\mathbf{j}}]_{\mathbf{i},\mathbf{j}}\mathrm{diag}(\omega^{\mathbf{a}\cdot\mathbf{j}_1}, \ldots, \omega^{\mathbf{a}\cdot\mathbf{j}_{|J|}})$, where we used the vectorial notations of Section 3.3. The translation with the vector $\mathbf{b}$ can be dealt with similarly.

Conjecture 1 *We have the following converse of Theorem 14: up to a suitable translation of I and J, each rank-deficient submatrix $F(N \setminus I, J)$ for which $|J| \leq d$ and $|I| = H_F(d)$ can be constructed as a union of rank-one submatrices as specified in Theorem 14.*

Conjecture 1 is known to be true when d is a divisor of n. Indeed, in the latter case we have $H_F(d) = \frac{n}{d}$, and the corresponding maximal rank-deficient submatrices $F(N \setminus I, J)$ must then satisfy equality in the uncertainty principle of Eq. (4). But it was shown in [11] that this can only happen when both I and J are tranlated subgroups. Hence up to translation, I and J must satisfy the requirements in the statement of Theorem 14, and hence Conjecture 1 must apply in this case.

In the case of a general $d \in \mathbb{N}$ and a general Fourier-like matrix F, Conjecture 1 appears to be more difficult. Nevertheless, we are able to prove the correctness of Conjecture 1 whenever the matrix F has order a *power of prime number*, thus e.g. $F = F_5 \otimes F_{25}$. These matters will be reported elsewhere.

5 Conclusion

We characterized the size of the maximal rank-deficient submatrices of Kronecker products, and in particular of a Kronecker product of Fourier matrices $F = F_{n_1} \otimes \ldots \otimes F_{n_k}$. In doing so, it turned out to be more appropriate to characterize the number of rows in the *complement* of such a maximal rank-deficient submatrix, giving rise to what we called the Hamming numbers for the given matrix. We showed how each subgroup $G \subseteq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ gives rise to a partition in rank-one blocks of the matrix F, and how these rank-one blocks can be used as building stones to obtain larger rank-deficient submatrices, hereby generalizing the approach in [1]. To prove the maximality of the constructed rank-deficient submatrices, we derived some bounds on the size of the maximal rank-deficient submatrices of a general Kronecker product $A \otimes B$, and we showed how these arguments apply to some Kronecker-related matrices as well (cf. Remark 22).

References

[1] S. Delvaux and M. Van Barel. Rank-deficient submatrices of Fourier matrices. Technical Report TW470, Department of Computer Science, Katholieke Universiteit Leuven, September 2006.

[2] D. L. Donoho and P. B. Stark. Uncertainty principles and signal recovery. *SIAM Journal on Applied Mathematics*, 49:906–931, 1989.

[3] R. J. Evans and I. M. Isaacs. Generalized Vandermonde determinants and roots of unity of prime order. *Proceedings of the American Mathematical Society*, 58:51–54, 1976.

[4] M. Fiedler and T. L. Markham. Completing a matrix when certain entries of its inverse are specified. *Linear Algebra and its Applications*, 74:225–237, 1986.

[5] P. E. Frenkel. Simple proof of Chebotarev's theorem on roots of unity. eprint: http://front.math.ucdavis.edu/math.AC/0312398, December 2003.

[6] T. Matolcsi and J. Szucs. Intersection des mesures spectrales conjugées. *Comptes Rendus de l'Académie des Sciences. Séries I Mathématique*, 277:841–843, 1973.

[7] R. Meshulam. An uncertainty inequality for finite abelian groups. preprint. math.CO/0312407, 2003.

[8] V. Olshevsky, I. Oseledets, and E. E. Tyrtyshnikov. Tensor properties of multilevel Toeplitz and related matrices. *Linear Algebra and its Applications*, 412:1–21, 2006.

[9] M. Quisquater, B. Preneel, and J. Vandewalle. A new inequality in discrete Fourier theory. *IEEE Transactions on Information Theory*, 49(8):2038–2040, August 2003.

[10] W. Rudin. *Fourier Analysis on Groups*. Wiley Interscience, 1962.

[11] K. T. Smith. The uncertainty principle on groups. *SIAM Journal on Applied Mathematics*, 50:876–882, 1990.

[12] E. E. Tyrtyshnikov. Kronecker-product approximations for some function-related matrices. *Linear Algebra and its Applications*, 379:423–437, 2004.

[13] C. F. Van Loan. *Computational Frameworks for the Fast Fourier Transform*. Frontiers in Applied Mathematics. SIAM, 1992.

[14] C. F. Van Loan and N. P. Pitsianis. Approximation with Kronecker products. In M. S. Moonen and G. H. Golub, editors, *Linear Algebra for Large Scale and Real Time Applications*. Kluwer Academic Publishers, Dordrecht, the Netherlands, 1993.