Available online at www.sciencedirect.com

ScienceDirect

Linear Algebra and its Applications 429 (2008) 1587–1605

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Rank-deficient submatrices of Fourier matrices☆

Steven Delvaux, Marc Van Barel *

Department of Mathematics, Katholieke Universiteit Leuven, Celestijnenlaan 200A, B-3001 Leuven (Heverlee), Belgium

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

Received 28 September 2006; accepted 17 April 2008

Available online 13 June 2008

Submitted by V. Mehrmann

Abstract

We consider the maximal rank-deficient submatrices of Fourier matrices with order a power of a prime number. We do this by considering a hierarchical subdivision of these matrices into low rank blocks. We also explore some connections with the fast Fourier transform (FFT), and with an uncertainty principle for Fourier transforms over finite Abelian groups.

AMS classification: 42A99; 15A03; 15A23

Keywords: Fourier matrix; Rank-deficient submatrix; FFT; Uncertainty principle

1. Introduction

In Fourier analysis, several so-called uncertainty principles are known. These principles say that a continuous-time signal cannot be concentrated in both time and frequency domain. Expressing

☆ 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 and Modelling). The scientific responsibility rests with the authors.

* Corresponding author.

E-mail addresses: Steven.Delvaux@wis.kuleuven.be (S. Delvaux), Marc.VanBarel@cs.kuleuven.be (M. Van Barel).

0024-3795/$ - see front matter
doi:10.1016/j.laa.2008.04.043

this in a more exact, quantitative form, one is led to the celebrated Heisenberg–Weyl uncertainty relations, or alternatively to uncertainty principles which are based on the concept of entropy [11,10].

Instead of continuous-time signals, one can also consider discrete-time signals, which are represented as a discrete vector $\mathbf{v} \in \mathbb{C}^n$. The Fourier transform is then defined by multiplication with a suitable Fourier matrix, or more generally with a Kronecker product of Fourier matrices.

For a more detailed discussion, let us introduce some 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 $\frac{1}{\sqrt{n}}$. We will sometimes simplify notation by just writing F instead of F_n.

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 theorem was first proved by Matolcsi and Szucs [7] in a group theoretical context. For the situation at hand, we will be able to state it in matrix language.

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

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

where each F_{n_i} is the Fourier matrix of size n_i, and where $\otimes$ denotes the Kronecker product (as defined in Eq. (28)). Define $n := n_1 \cdots n_k$. Then we have

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

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), for which the matrix–vector product is concentrated on a small set as well.

In addition to the origin of Theorem 1 in Matolcsi and Szucs [7], we refer also to Refs. [3,13,12] for some interesting generalizations and analogues. In particular, it was shown by Smith [13, Section 5] that equality in the uncertainty principle (2) can be reached with $H(\mathbf{v})$ equal to an arbitrary divisor d of n.

For a proof of Theorem 1, we recall two elementary properties of Fourier matrices:

(i) The Fourier matrix is *unitary*, i.e., $\|F\mathbf{v}\|_2 = \|\mathbf{v}\|_2$ for all column vectors $\mathbf{v} \in \mathbb{C}^n$ (Here we use $\|\cdot\|_2$ to denote the Euclidean 2-norm of a vector),
(ii) The entries of F have all the same absolute value $\frac{1}{\sqrt{n}}$.

Moreover, these properties are known to be inherited when taking Kronecker products, provided that one updates $n := n_1 \cdots n_k$ in property (ii).

The proof of Theorem 1 will now reduce to the following lemma, which is basically a matrix formulation of the standard proof appearing in the literature. We include it here to keep the paper self-contained.

Lemma 2. *Given a matrix* $A \in \mathbb{C}^{m\times n}$ *which is* (i) *a dilation in the sense that* $\|A\mathbf{v}\|_2 \geqslant \|\mathbf{v}\|_2$ *for each column vector* $\mathbf{v} \in \mathbb{C}^n$, *and* (ii) *bounded entry-wise in the sense that* $|a_{i,j}| \leqslant M$ *for all indices* i, j. *Then for any nonzero vector* $\mathbf{v} \in \mathbb{C}^n$, *we have the uncertainty principle*

$$H(A\mathbf{v})H(\mathbf{v}) \geqslant \frac{1}{M^2}. \tag{3}$$

Proof. We invoke the bound

$$|\mathbf{w}\cdot\mathbf{v}|^2 \leqslant \|\mathbf{w}\|_\infty^2 H(\mathbf{v})\|\mathbf{v}\|_2^2, \tag{4}$$

where $\mathbf{v}$, $\mathbf{w} \in \mathbb{C}^n$ are arbitrary vectors, where $\mathbf{w}\cdot\mathbf{v}$ denotes the Euclidean inner product of these vectors, and where $\|\mathbf{w}\|_\infty := \max_i |\mathbf{w}_i|$. Indeed

$$\begin{aligned} |\mathbf{w}\cdot\mathbf{v}|^2 &= \left|\sum_{k=0}^{n-1} \mathbf{w}_k\mathbf{v}_k\right|^2 \\ &= \left|\sum_{k=0}^{n-1} \mathbf{w}_k 1_{\mathbf{v},k}\mathbf{v}_k\right|^2 \leqslant \sum_{k=0}^{n-1} |\mathbf{w}_k 1_{\mathbf{v},k}|^2 \sum_{k=0}^{n-1} |\mathbf{v}_k|^2 \leqslant \|\mathbf{w}\|_\infty^2 H(\mathbf{v})\|\mathbf{v}\|_2^2, \end{aligned} \tag{5}$$

where we denoted with $1_{\mathbf{v}}$ the vector which takes the value 1 on all nonzero indices of $\mathbf{v}$, and zero elsewhere, and where the third transition follows from the Cauchy–Schwarz inequality.

Applying (4) with $\mathbf{w}$ equal to the ith row of A reveals that the ith component of the vector $A\mathbf{v}$ can be bounded in modulus by

$$|(A\mathbf{v})_i|^2 \leqslant M^2 H(\mathbf{v})\|\mathbf{v}\|_2^2 \leqslant M^2 H(\mathbf{v})\|A\mathbf{v}\|_2^2,$$

where we used the assumptions in the statement of the lemma. Summing this inequality over all nonzero indices i of $A\mathbf{v}$, and subsequently dropping the factor $\|A\mathbf{v}\|_2^2$ from both sides, leads to the desired result (3). □

In what follows, we will approach the uncertainty principle from a purely linear algebra point of view. Using the notations of Lemma 2, and assuming from now on that A is square of size n, let us denote with I the set of indices where $A\mathbf{v}$ 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 $H(A\mathbf{v})$ and $H(\mathbf{v})$, respectively.) Obviously, we should have

$$A(N\setminus I, J)\mathbf{v}|_J = 0, \tag{6}$$

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 (6) states that the submatrix $A(N\setminus I, J)$ of A is *rank-deficient* in the sense that its null space is non-empty.

The uncertainty principle tells then that such a rank-deficient submatrix $A(N\setminus I, J)$ cannot have an arbitrarily large number of rows, assuming that its number of columns is fixed, since we must have the restriction $|I|\cdot|J| \geqslant \frac{1}{M^2}$. This result is *negative* since it restricts the size of the rank-deficient submatrices, and hence the structure of A.

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 $F := A$ is a Kronecker product of Fourier matrices as in the statement of Theorem 1. Let us illustrate this for $n = 4$ and $H(\mathbf{v}) = 2$. Then there are two possibilities for F:

$$F_4 = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & -1 & -\mathbf{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i} & -1 & \mathbf{i} \end{bmatrix}, \quad \text{or} \quad F_2 \otimes F_2 = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

with $\mathbf{i} := \sqrt{-1}$. Now in both cases it is easy to obtain a non-trivial rank-deficient submatrix $F(N \setminus I, J)$ with $|I| \cdot |J| = n$. This can be achieved e.g. by taking submatrices of the form $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. Note, however, that the number and the positions of these submatrices are different for F_4 and $F_2 \otimes F_2$. The underlying reason for this is that the Abelian groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ have a different pattern of subgroups.

In this paper, we treat the uncertainty principle from a linear algebra point of view. To this end, we are going to search the rank-deficient submatrices containing a maximal number of rows, assuming that the number of columns is fixed, of our matrices of interest. For the present paper we will restrict ourselves to the case where $F = F_{p^m}$ is a Fourier matrix with order a power of a prime number; the case of a general Kronecker product of Fourier matrices is handled in [1].

Using this approach, we can obtain more precise connections between $H(\mathbf{v})$ and $H(F\mathbf{v})$ than the one in (2). It turns out that the size and position of the maximal rank-deficient submatrices of $F = F_n$ depends directly on the prime number factorization of n. For example, for a prime number it turns out that the relation (2) can be made more precise, based on the fact that the Fourier matrix F_p does not have any singular submatrix (see [5] for a historical overview about this statement, and see also [16]). A generalization of this fact will be established in Theorem 9, which is the main theorem of this paper.

The paper is organized as follows. Section 2 collects some results in the literature concerning the rank-deficient submatrices of F_p with p prime. Section 3 considers the case of a Fourier matrix with order a power of a prime number. Section 4 shows some connections with the FFT. Section 5 considers a connection with the block diagonalization of Fourier matrices. Finally, some conclusions are provided in Section 6.

2. Fourier matrices with prime order

We start with the case of a Fourier matrix with prime order. We need some auxiliary definitions. We define the *generalized Vandermonde matrix* induced by two vectors $\mathbf{x} \in \mathbb{C}^n$, $\mathbf{m} \in \mathbb{N}^n$ as the matrix

$$V = [x_i^{m_j}]_{i,j=0}^{n-1}.$$

Here $\mathbf{x}$ is called the vector of data points and $\mathbf{m}$ is called the vector of exponents.

Note that for exponents $m_j = j$, the generalized Vandermonde matrix reduces to a classical Vandermonde matrix $V = [x_i^{j-1}]_{i,j}$. As it is commonly known, the determinant of such a matrix is given by

$$\det V = \prod_{i>j} (x_i - x_j).$$

A generalization of this result was already proved in the 19th century by Mitchell [9], and is stated now. Recall that a polynomial in several variables is called *symmetric* if it is invariant under the interchange of any two of its variables. The following result is nowadays well-known in the literature (see the footnote below for more information).

Theorem 3. *Let $V = [x_i^{m_j}]_{i,j}$ be a generalized Vandermonde matrix of size n by n. Then its determinant can be factorized as*

$$\det V = \left(\prod_{i>j} (x_i - x_j) \right) S(\mathbf{x}), \tag{7}$$

where $S(\mathbf{x}) = \sum_k c_k x_0^{p_{k,0}} \cdots x_{n-1}^{p_{k,n-1}}$ is a symmetric polynomial in $x_0, \ldots, x_{n-1}$. Moreover, the sum of coefficients of $S(\mathbf{x})$ is given by [1]

$$\sum_k c_k = \frac{\prod_{n>i>j\geqslant 0}(m_i - m_j)}{\prod_{n>i>j\geqslant 0}(i-j)}. \tag{8}$$

Proof. For completeness of this paper, let us provide here the main steps of the proof of Theorem 3, as suggested in [9]. We compute the determinant of V by the following series of row operations: for each $i \geqslant 1$, we subtract from the ith row the zeroth row and then divide each element of the ith row by the factor $x_i - x_0$. Next, for each $i \geqslant 2$, we subtract from the ith row the 1st row and then divide each element of the ith row by the factor $x_i - x_1$, and so on.

Let us illustrate this process for $\mathbf{m} = (1, 2, 3)$. Then the generalized Vandermonde matrix

$$V = \begin{bmatrix} x_0 & x_0^2 & x_0^3 \\ x_1 & x_1^2 & x_1^3 \\ x_2 & x_2^2 & x_2^3 \end{bmatrix} \tag{9}$$

reduces under the influence of the above described series of row operations to

$$\begin{bmatrix} x_0 & x_0^2 & x_0^3 \\ 1 & x_0 + x_1 & x_0^2 + x_0 x_1 + x_1^2 \\ 0 & 1 & x_0 + x_1 + x_2 \end{bmatrix}. \tag{10}$$

The entries of this matrix can now be recognized to be the so-called *complete symmetric polynomials* of fixed homogeneous degree. Indeed, also in general, we claim that V transforms into the new matrix

$$\begin{bmatrix} S^{m_0}(x_0) & \cdots & S^{m_{n-1}}(x_0) \\ S^{m_0-1}(x_0, x_1) & \cdots & S^{m_{n-1}-1}(x_0, x_1) \\ \vdots & & \vdots \\ S^{m_0-n+1}(x_0, \ldots, x_{n-1}) & \cdots & S^{m_{n-1}-n+1}(x_0, \ldots, x_{n-1}) \end{bmatrix}, \tag{11}$$

where

$$S^m(x_0, x_1, \ldots, x_i) := \sum_{\mathbf{p}\in\mathbb{N}^{i+1}, \sum p_k = m} \left(\prod_k x_k^{p_k} \right).$$

The proof follows by an induction argument, using the easily verified identity:

$$S^m(x_0, \ldots, x_i; x_k) - S^m(x_0, \ldots, x_i; x_{i+1}) = (x_k - x_{i+1}) S^{m-1}(x_0, \ldots, x_i, x_{i+1}; x_k)$$

as suggested in [9, p. 344].

[1] The symmetric polynomial $S(\mathbf{x})$ in (7) is nowadays often called the *Schur function* or *S-function*: see e.g. [6,15,2], among many others. According to [6, Section 1.3], the introduction of the Schur function can be traced back to the work of Jacobi. The property referred to in (8) can be interpreted as giving the value of the Schur functions at $(1, 1, \ldots, 1)$, see e.g. [14, Theorems 1.2 and 5.4].

We are now interested in the *determinant* of (11), and more precisely in the *sum of coefficients* of this determinant. Still following [9, p. 344], this means that we have to evaluate this determinant for $\mathbf{x} = (1, \ldots, 1)$. Note that for the above example (10), this yields

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 3 \end{vmatrix}. \tag{12}$$

The entries in the determinant (12) can now be recognized as a series of subsequent binomial numbers. Indeed, also in the general case, it is straighforward that the sum of coefficients in the determinant of (11) equals

$$\begin{vmatrix} \binom{m_0}{0} & \cdots & \binom{m_{n-1}}{0} \\ \binom{m_0}{1} & \cdots & \binom{m_{n-1}}{1} \\ \vdots & & \vdots \\ \binom{m_0}{n-1} & \cdots & \binom{m_{n-1}}{n-1} \end{vmatrix}. \tag{13}$$

Now the ith row of this determinant (13) contains the entries $\binom{m_j}{i} := \frac{m_j \cdots (m_j - i + 1)}{i!}$, i.e., $\frac{m_j^i}{i!}$ plus some powers of lower degree of m_j. But these lower degree powers can be eliminated by subtracting multiples of previous rows in (13). The above determinant reduces then to

$$\begin{vmatrix} m_0^0 & \cdots & m_{n-1}^0 \\ \frac{1}{1!} m_0^1 & \cdots & \frac{1}{1!} m_{n-1}^1 \\ \vdots & & \vdots \\ \frac{1}{(n-1)!} m_0^{n-1} & \cdots & \frac{1}{(n-1)!} m_{n-1}^{n-1} \end{vmatrix},$$

which is up to the scaling factor $1!2! \cdots (n-1)!$ in the denominator just a classical Vandermonde determinant in the vector of exponents. This leads to the desired formula (8), hereby finishing the proof of Theorem 3. □

According to [5], the following result was first proved by Chebotarev in 1926 using p-adic number theory.

Theorem 4. *Let p be a prime number. Then the Fourier matrix F_p does not contain any singular square submatrix.*

Proof. We use the proof suggested in [4]. By definition of $F_p = [\omega^{ij}]_{i,j}$ (where we neglected the irrelevant scaling factor $\frac{1}{\sqrt{p}}$), any $k \times k$ submatrix of F_p can be written as a generalized Vandermonde matrix $V = [x_i^{m_j}]_{i,j}$, with data points themselves of the form $x_i = \omega^{\tilde{m}_i}$ for suitable choice of exponents $\tilde{m}_i, m_j \in \{0, 1, \ldots, p-1\}$. We consider then the determinant of this generalized Vandermonde matrix, and more precisely the polynomial $S(\mathbf{x}) = \sum_k c_k x_0^{p_{k,0}} \cdots x_{n-1}^{p_{k,n-1}}$ in the statement of Theorem 3. Clearly, this polynomial can be rearranged into the form $\sum_{k=0}^{p-1} \tilde{c}_k \omega^k$ with $\tilde{c}_k \in \mathbb{Z}$ (this follows by using that $\omega^{ap+b} = \omega^b$ for all a, b). Now this polynomial can only vanish if it is divisible by $1 + \omega + \cdots + \omega^{p-1}$, the minimal polynomial of ω over $\mathbb{Z}$. (See Lemma

8 for a more general version of this result.) In particular, this polynomial can only vanish if the sum of coefficients of $S(\mathbf{x})$ is divisible by p. But from (8), it follows that the sum of coefficients of $S(\mathbf{x})$ can only be divisible by p if there are two exponents with $m_i \equiv m_j \bmod p$, $i \neq j$. The latter is impossible since $0 \leqslant \{m_i, m_j\} < p$ for all i, j, hence yielding a contradiction. □

Remark 5. Let us call a matrix $A \in \mathbb{C}^{m\times n}$ *rank-deficient* if Rank $A < n$, or equivalently, if there exists a nonzero vector $\mathbf{v} \in \mathbb{C}^n$ such that $A\mathbf{v} = \mathbf{0}$. It follows then from Theorem 4 that the Fourier matrix F_p with p prime 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.

3. Fourier matrices with non-prime order

We move now to the case of a Fourier matrix with non-prime order. To this end, note first that Theorem 4 is of a *negative* type, since it excludes the existence of any non-trivial rank-deficient submatrix of F_p with p prime.

Interestingly, it turns out that one can obtain *positive* results in case of a Fourier matrix of the form F_{mn}, with $m, n \in \mathbb{N}$.

We start with some generalities. Given a permutation P defined on the set $\{0, \ldots, mn-1\}$, the *associated matrix* of this permutation is defined as the matrix whose jth column contains an entry 1 on its $P(j)$th position, and zeros elsewhere. The action of P on a vector $\mathbf{x} \in \mathbb{C}^{mn}$ is defined as the matrix–vector product $P\mathbf{x}$. We will use the same symbol P to denote both the permutation and its associated matrix.

Note that multiplying a permutation matrix with a vector on the *left*, allows an interpretation in terms of the *inverse* permutation, since

$$\mathbf{x}^{\mathrm{T}} P = (P^{\mathrm{T}}\mathbf{x})^{\mathrm{T}} = (P^{-1}\mathbf{x})^{\mathrm{T}} \tag{14}$$

for any column vector $\mathbf{x} \in \mathbb{C}^n$, where the second transition expresses that permutation matrices are unitary.

Now we specify to a particular instance of a permutation. The *sort-modulo-m permutation* induced by $m, n \in \mathbb{N}$ is defined as the permutation map $P_{m,mn}$ on $\{0, \ldots, mn-1\}$ such that

$$P_{m,mn}: an + b \mapsto bm + a.$$

Here the involved numbers are in Euclidean division form, i.e., we assume $a \in \{0, \ldots, m-1\}$ and $b \in \{0, \ldots, n-1\}$.

For example, $P_{3,6}$ transforms the sequence $0, 1, 2, 3, 4, 5$ into the sequence $0, 3, 1, 4, 2, 5$, sorting these integers according to the subsequent residue classes modulo 3.

A way of visualizing the permutation $P_{m,mn}$ is by arranging the given numbers $0, \ldots, mn-1$ in an m by n table, e.g.

$$\begin{bmatrix} 0 & 3 \\ 1 & 4 \\ 2 & 5 \end{bmatrix}.$$

Now we claim that $P_{m,mn} F_{mn} P_{m,mn}$ can be partitioned in a natural way in an n by m grid consisting of blocks of rank one, e.g.

$$P_{3,6} F_6 P_{3,6} = \begin{bmatrix} \text{Rk 1} & \text{Rk 1} & \text{Rk 1} \\ \text{Rk 1} & \text{Rk 1} & \text{Rk 1} \end{bmatrix},$$

where each Rk 1 is a block of rank one. (For notational simplicity, we represent here each block by the same notation Rk 1, but these different blocks do not have to be equal to each other!)

To show the validity of this claim, note that the multiplication with $P_{m,mn}$ causes the columns in $P_{m,mn}F_{mn}P_{m,mn}$ to be sorted modulo m, while the rows are sorted modulo n; the latter follows from (14) with $\mathbf{x} = \mathbf{e}_i$, the ith standard basis vector, combined with the fact that $P_{m,mn}^{-1} = P_{n,mn}$.

If follows that for any $a \in \{0, \ldots, n-1\}$ and $b \in \{0, \ldots, m-1\}$, the (a, b)th block element of $P_{m,mn}F_{mn}P_{m,mn}$ is given by

$$\frac{1}{\sqrt{mn}}[\omega^{(a+in)(b+jm)}]_{i,j}$$

with i running through $\{0, \ldots, m-1\}$, and j running through $\{0, \ldots, n-1\}$. We can rewrite this as $\frac{1}{\sqrt{mn}}[\omega^{ab+bin+ajm}]_{i,j}$ and thus $\frac{1}{\sqrt{mn}}\omega^{ab}[\omega^{bin}\omega^{ajm}]_{i,j}$, so that we obtain a factorization

$$\frac{1}{\sqrt{mn}}\omega^{ab}\begin{bmatrix} 1 \\ \vdots \\ \omega^{bin} \\ \vdots \\ \omega^{b(m-1)n} \end{bmatrix}\begin{bmatrix} 1 & \cdots & \omega^{ajm} & \cdots & \omega^{a(n-1)m} \end{bmatrix} =: \text{Rk } 1, \tag{15}$$

which is indeed a matrix of rank one.

For example, since $\omega_4 = \exp(\pi\mathbf{i}/2) = \mathbf{i}$, the imaginary unit, the Fourier matrix F_4 can be written as

$$F_4 = \frac{1}{\sqrt{4}}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & -1 & -\mathbf{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i} & -1 & \mathbf{i} \end{bmatrix} \tag{16}$$

and after permutation this becomes

$$P_{2,4}F_4P_{2,4} = \frac{1}{\sqrt{4}}\left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ \hline 1 & -1 & \mathbf{i} & -\mathbf{i} \\ 1 & -1 & -\mathbf{i} & \mathbf{i} \end{array}\right], \tag{17}$$

which can indeed be subdivided in 2×2 blocks of rank equal to 1.

As a final example, the partition in rank-one blocks of $P_{5,25}F_{25}P_{5,25}$ is shown in Fig. 1.

Recall that a matrix $A \in \mathbb{C}^{m\times n}$ is called *rank-deficient* if Rank $A < n$, or equivalently, if there exists a nonzero vector $\mathbf{v} \in \mathbb{C}^n$ such that $A\mathbf{v} = \mathbf{0}$.

The above discussion (cf. Fig. 1) indicates that a Fourier matrix F_{mn} should have a lot of non-trivial rank-deficient submatrices. To make this more concrete, we introduce the following definition.

Definition 6. 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 $|J| \leqslant d$. 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 uncer-

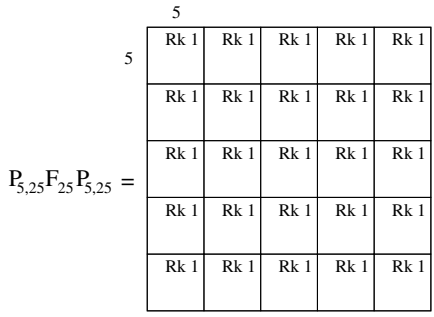


Fig. 1. The figure shows a partition of $P_{5,25}F_{25}P_{5,25}$ in a 5 by 5 grid of rank-one submatrices.

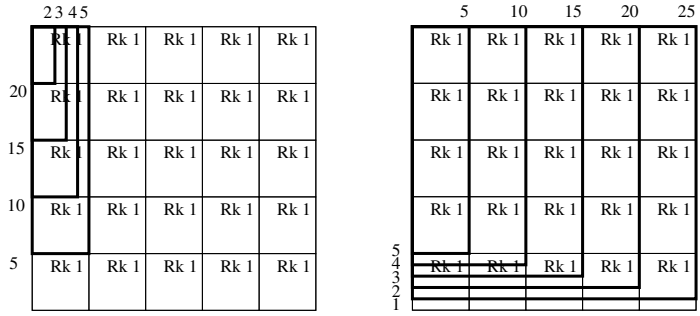


Fig. 2. The left part of the figure shows some rank-deficient submatrices of $P_{5,25}F_{25}P_{5,25}$ with 2, 3, 4 and 5 columns. The complementary sets contain 20, 15, 10 and 5 rows, respectively. Similarly, the right part of the figure shows some rank-deficient submatrices of $P_{5,25}F_{25}P_{5,25}$ with 5, 10, 15, 20 and 25 columns, and with complementary sets containing 5, 4, 3, 2 and 1 rows, respectively.

tainty principle. Indeed, it can be noted that Definition 6 allows the following reformulation of Theorem 1:

$$d \cdot H_F(d) \geqslant n, \tag{18}$$

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

We already observed in Section 1 that (18) is a result of a negative type, since it restricts the size of the rank-deficient submatrices of any Fourier-like matrix F. The idea is now to complement this by a result of a constructive type, where we actually construct rank-deficient submatrices of a Fourier matrix of non-prime order F_{mn} by suitably collecting the rank-one building blocks of $P_{m,mn}F_{mn}P_{m,mn}$. The idea is shown in the case of $P_{5,25}F_{25}P_{5,25}$ in Fig. 2.

Let us comment in Fig. 2. To this end, let us start with the submatrix of size 5 by 2, which is highlighted on the extreme left of Fig. 2. (It is the smallest of all the highlighted submatrices.) Since this submatrix has been chosen to be part of a rank-one block, it must itself have rank at most 1. But since $1 < 2$, the rank of this submatrix is smaller than its number of columns, and hence this submatrix is indeed rank-deficient.

We conclude that for $d = 2$, one can obtain a rank-deficient submatrix having 5 rows, and thus with cardinality of the *complementary* set consisting of $25 - 5 = 20$ rows. Hence, $H_{F_{25}}(d) \leqslant 20$.

One can then repeat this argument to construct rank-deficient submatrices having at most d columns, for any d. To this end, it suffices to choose each time a maximal submatrix whose entries

can be divided in at most $d-1$ rank-one blocks, for each d. Indeed, since such a submatrix must obviously have rank at most $d-1$, and since $d-1<d$, it must be rank-deficient.

The idea how to do this in practice is shown in Fig. 2. Note that for each of the highlighted rank-deficient submatrices in this figure, the number of rows in the complementary subset is indicated in the bottom leftmost corner of the submatrix. This number is greater than or equal to $H_{F_{25}}(d)$.

Collecting all the relevant information from Fig. 2 leads to the following upper bounds for 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

(19)

We note that (19) 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 $d-1$.

It can be shown that the bounds in (19) are indeed correct, in the sense that it is impossible to obtain smaller Hamming numbers (or equivalently, larger rank-deficient submatrices) than the ones obtained in Fig. 2. This will be shown in Theorem 9.

Note that (19) is compatible with the uncertainty principle (18), i.e., $d \cdot H_{F_{25}}(d) \geqslant 25$. 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 $d \in \{1, 5, 25\}$ (see also [13]).

In case of a matrix F_n with dimension n containing at least three prime divisors, we want to apply the above ideas in an iterative way. We will do this under the assumption that n is a power of a prime number $n = p^m$.

We need an auxiliary definition. The *digit-reversing permutation* induced by a power of a prime number p^m is defined as the permutation map P_{p^m} on $\{0, \ldots, p^m - 1\}$ which maps

$$P_{p^m}: c_{m-1}p^{m-1} + \cdots + c_0 p^0 \mapsto c_0 p^{m-1} + \cdots + c_{m-1}p^0.$$

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

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

Note that in the above example of P_8, the digit-reversing permutation sorts *both* modulo 4 and modulo 2, at least up to some ordering of the residue classes. Also in general, the digit-reversing permutation P_{p^m} has a close affinity with each of the sort-modulo-p^k permutations P_{p^k,p^m}, $k = 1, \ldots, m-1$, which we introduced earlier, with the only difference that the order in which the residue classes modulo p^k are sorted may differ. We can then use the same argument leading to (15) to show the following result.

Lemma 7. *If p^m denotes a power of a prime number, and if P_{p^m} denotes the digit-reversing permutation introduced above, then the permuted Fourier matrix $P_{p^m} F_{p^m} P_{p^m}$ allows a subdivision in a p^{m-k} by p^k grid of rank-one blocks, for any $k = 1, \ldots, m-1$.*

As an example we consider the Fourier matrix of size $n = 3^3 = 27$, see Fig. 3.

These rank-one partitions can again be used as building blocks for constructing greater rank-deficient submatrices. For the example in Fig. 3, this leads to the table (only the relevant values of d are shown):

d	1	2	3	6	9	18	27
$H_{F_{27}}(d)$	27	18	9	6	3	2	1

(20)

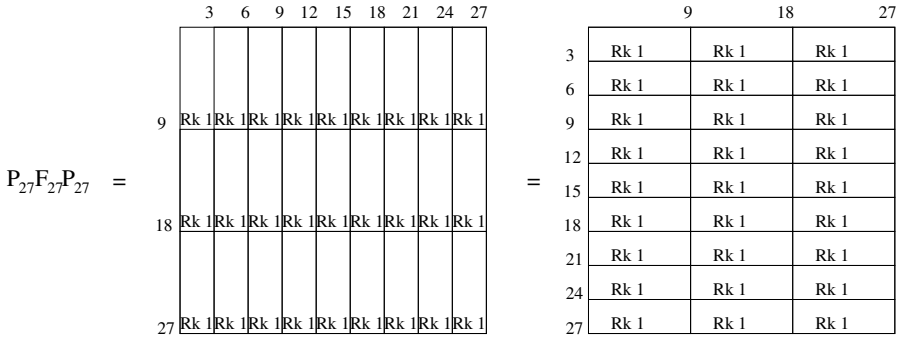


Fig. 3. The figure shows a partition of $P_{27}F_{27}P_{27}$ in a 3 by 9 grid of rank-one submatrices on the left, and a partition in a 9 by 3 grid of rank-one submatrices on the right.

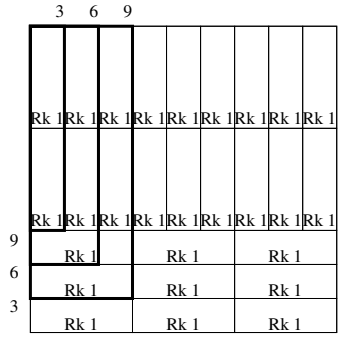


Fig. 4. The figure shows some rank-deficient submatrices of $P_{27}F_{27}P_{27}$ with 3, 6 and 9 columns. The complementary sets contain 9, 6 and 3 rows, respectively. Note that rank-deficient submatrices are built from rank-one blocks of *both* of the types of Fig. 3, i.e., from both blocks of size 3 by 9 and of size 9 by 3.

For example, the way how to obtain the Hamming numbers $H_{F_{27}}(d)$ for the cases $d = 3$, 6 and 9 is illustrated in Fig. 4.

Note that the above table (20) is again compatible with the uncertainty principle, and that it shows that equality in the uncertainty principle can be reached for each divisor of n.

We want now to formalize the above results, in particular showing that the depicted bounds for the Hamming numbers in tables (19) and (20) are indeed the best possible.

The theorem requires the following well-known lemma.

Lemma 8. *For a power of a prime number p^m, the minimal polynomial over $\mathbb{Z}$ of the corresponding root of unity ω equals*[2]

$$1 + \omega^{p^{m-1}} + \cdots + \omega^{(p-1)p^{m-1}}. \tag{21}$$

Proof. We include the proof of this well-known lemma for completeness of this paper. The factorization

$$1 - \omega^{p^m} = (1 - \omega^{p^{m-1}})(1 + \omega^{p^{m-1}} + \cdots + \omega^{(p-1)p^{m-1}})$$

[2] The minimal polynomial of the nth root of unity ω_n over $\mathbb{Z}$ is often called the *cyclotomic polynomial* of degree n.

shows that (21) is an annihilating polynomial for ω. The fact that it is precisely the *minimal* polynomial follows then since its degree equals *Euler's phi-function* of p^m, i.e., the number of roots of unity ω^k whose exponent $k \in \{0, \ldots, p^m - 1\}$ is relatively prime to p^m. (The fact that the minimal polynomial of ω over $\mathbb{Z}$ must have degree precisely equal to Euler's phi-function is well-known and usually attributed to Gauss.) □

The following is the main theorem of this paper.

Theorem 9. *Let p^m be a power of a prime number. Let $d \in \{1, 2, \ldots, p^m\}$ be such that*

$$cp^k \leqslant d < (c+1)p^k \tag{22}$$

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

$$H_{F_{p^m}}(d) = (p - c + 1)p^{m-k-1}. \tag{23}$$

Proof. First we will show that the bound in (23) cannot be sharpened. Suppose by contradiction that we can find subsets I, J for which the submatrix $F_{p^m}(N \setminus I, J)$ is rank-deficient, such that $|J| \leqslant d$, and $|I|$ is strictly less than the number in (23). We will prove a contradiction by showing that $F_{p^m}(N \setminus I, J)$ must have a square *nonsingular* submatrix.

To construct this submatrix, we are going to choose d row indices $m_i \in N \setminus I$ that are simultaneously *uniformly distributed* modulo each power p^r of p, $r \in \{1, \ldots, k+1\}$. This means that each residue class modulo p^r, $r \in \{1, \ldots, k+1\}$, should contain either $\lfloor d/p^r \rfloor$ or $\lceil d/p^r \rceil$ of the elements m_i. Assuming that we can do this, then all factors p in the numerator of (8) are cancelled by those in the denominator, and hence the sum of coefficients of the determinant of the constructed submatrix cannot be divisible by p. If follows then from Lemma 8 that this determinant cannot vanish, yielding the desired contradiction.

Thus we should show that it is possible to assign the row indices m_i, $i = 1, \ldots, d$ to be uniformly distributed modulo each power p^r of p, $r \in \{1, \ldots, k+1\}$. Consider first the values $r = k+1$ and $r = k$. The uniform distribution property requires us to choose in each residue class modulo p^{k+1} at most $\lceil d/p^{k+1} \rceil = 1$ representative m_i, and to choose in each residue class modulo p^k (obtained by stacking p of the residue classes modulo p^{k+1} together) either $\lfloor d/p^k \rfloor = c$ or $\lceil d/p^k \rceil \leqslant c+1$ representatives m_i.

To show that this is possible, we recall our assumption on the size of $N \setminus I$. More precisely, we recall that we are assuming (by contradiction) that $|I|$ is strictly less than the number in (23). This implies that there can be at most $p - c$ residue classes modulo p^{k+1} which have no representative in $N \setminus I$. It follows that we have at least $c+1$ representatives to choose from in each of the residue classes modulo p^k, except for at most one "exceptional" residue class modulo p^k (in the worst case), for which c representatives is the best possible. Without loss of generality, we can assume that this exceptional residue class (if it exists) corresponds to the last residue class, i.e., the numbers which equal $p^k - 1$ modulo p^k.

Define now $\tilde{d} := d \bmod p^k$. In each of the first $\tilde{d}$ residue classes modulo p^k, choose exactly $c+1$ representatives m_i, and in each of the last $p^k - \tilde{d}$ residue classes modulo p^k, choose exactly c representatives m_i. It is easy to check that with this construction, we have a total number of

$$\tilde{d}(c+1) + (p^k - \tilde{d})c = \tilde{d} + p^k c = d$$

representatives m_i, and moreover, that for all choices of $r \in \{1, \ldots, k+1\}$, the row indices m_i are uniformly distributed modulo p^r. (Indeed: the values $r = k+1$ and $r = k$ have been discussed

above. The uniform distribution property for the other values $r \in \{1, \ldots, k-1\}$ follows since modulo p^k, we have assigned the indices m_i according to an exact Vandermonde distribution.) This finishes the proof that the bound in (23) cannot be sharpened, i.e., we established now the inequality $\geqslant$ in (23).

Conversely, the fact that the bounds in (23) can indeed be realized (i.e., the inequality $\leqslant$ in (23)) follows easily from the discussion in the paragraphs before the statement of this theorem; cf. Lemma 7. See also [1, Corollary 16] for a more formal and more general argument establishing the inequality $\leqslant$ in (23). $\square$

Remark 10. The proof of Theorem 9 shows in fact a slightly stronger statement: a rank-deficient submatrix $F_{p^m}(N \setminus I, J)$ such that $|J| \leqslant d$ and $|I|$ equals the number $H_{F_{p^m}}(d)$ in (23) is only possible if I equals precisely the union of $p - c + 1$ residue classes modulo p^{k+1}, all of them contained in the same residue class modulo p^k.

Remark 11. By choosing $m = 1$, the statement of Theorem 9 reduces to

$$H_{F_p}(d) = (p - d + 1)$$

for any prime number p and $d \in \{1, \ldots, p\}$. It follows that for a Fourier matrix of prime order F_p, a rank-deficient submatrix of F_p with d columns can contain at most $d - 1$ rows. We retrieve in this way Theorem 4; see also Remark 5.

Remark 12. Given a matrix F as in (1), 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 $d \cdot H_F(d) = n$. Following a suggestion in [16], a stronger version of this result was shown in [8], where it was essentially proved that these grid points must be situated above the polyline formed by the grid points $(d, H_F(d))$ where d ranges over the subsequent *divisors* of n. Note that Theorem 9 shows that this bound is rather tight in case of F_n where $n = p^m$ is a power of a prime number.

Remark 13. Theorem 9 characterizes the Hamming numbers for the case of a Fourier matrix F_n with $n = p^m$ a power of a prime number. The generalization to the case of an arbitrary $n = p_1^{m_1} \cdots p_i^{m_i}$ is the subject of [1]. In the latter paper we also show how to obtain an alternative proof of Theorem 9 using ideas from multilinear algebra. However, we were *not* able to retrieve the result of Remark 10 using that multilinear approach.

4. Fast Fourier transform

In this section, we pay some attention to the connection with Fast Fourier transform (FFT) factorizations of Fourier matrices.

The reader should first recall the partition in rank-one blocks of $P_{p^m} F_{p^m} P_{p^m}$, as in Lemma 7. The presence of these rank-one blocks allows then the entries of this matrix to be gradually annihilated by means of *Givens transformations* $G_{i,j}$, i.e., elementary unitary matrices which equal the identity matrix, except for the submatrix formed by rows and columns i, j. (We assume here the case of a *radix-2* Fourier matrix, i.e., F_{p^m} with $p = 2$.)

More precisely, a Givens transformation acting on rows and columns i, j is defined as a matrix

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

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

$$\begin{bmatrix} c & s \\ -\bar{s} & \bar{c} \end{bmatrix}. \tag{24}$$

More generally, one can allow the second row of (24) to be multiplied by a *complex sign*, i.e., by a complex number $e^{\mathbf{i}\theta}$ for some $\theta \in \mathbb{R}$.

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

The idea of compressing the (permuted) Fourier matrix by means of Givens transformations is depicted for the matrix $P_8 F_8 P_8$ in Fig. 5.

Let us comment on this figure. In the first step of the compression process, we consider the partition of the matrix $P_8 F_8 P_8$ in a 2 by 4 grid of rank-one blocks: see Fig. 5a. Since the two columns of such a rank-one block are obviously linearly dependent, it is possible to find Givens transformations $G_{0,1}$, $G_{2,3}$, $G_{4,5}$, $G_{6,7}$, chosen to annihilate the elements in columns 1, 3, 5, 7 of the topmost collection of rank-one blocks.

From the unitarity of the Fourier matrix, it follows then that simultaneously the elements in columns 0, 2, 4, 6 of the *bottom*most collection of rank-one blocks must be annihilated under this process: see Fig. 5c.

Indeed: note that after applying a Givens transformation to a couple of columns, the submatrix formed by these two columns takes the form

$$\begin{bmatrix} \mathbf{u} & \mathbf{0} \\ a\mathbf{v} & b\mathbf{v} \end{bmatrix} \tag{25}$$

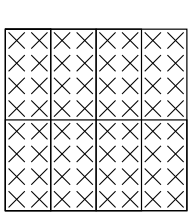
for suitable vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^4$ and scalars $a, b \in \mathbb{C}$. (We expressed here that the bottom block must still be of rank one, and hence must have row space spanned by a single vector $\mathbf{v}$.) Now since both the Fourier matrix and the applied Givens transformation are *unitary*, the columns of (25) should be orthonormal to each other. It follows that $a\bar{b}\|\mathbf{v}\|^2 = 0$. But since both $b = 0$ and $\|\mathbf{v}\| = 0$ are impossible since they would imply the matrix to be singular, it follows that necessarily $a = 0$, which was to be demonstrated.

We can summarize the resulting sparsity pattern of Fig. 5c by

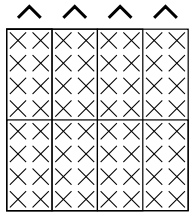
$$(0, 1, 2, 3, 4, 5, 6, 7) \mapsto (0, 1, 0, 1, 0, 1, 0, 1),$$

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

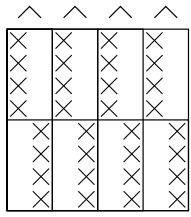
We consider now the partition in a 4 by 2 grid of rank-one blocks: see Fig. 5d. Note that the row grid is refined by this operation. Now for each of the rank-one blocks positioned on an



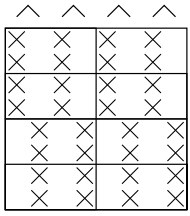
(a) Starting matrix $P_8F_8P_8$, divided in a 2 by 4 grid of rank-one blocks.



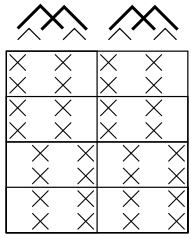
(b) Apply the first Givens transformations to the columns.



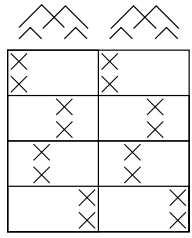
(c) Entries are annihilated as shown.



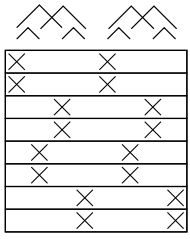
(d) Consider the partition in a 4 by 2 grid of rank-one blocks.



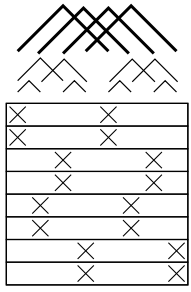
(e) Apply the next Givens transformations to the columns.



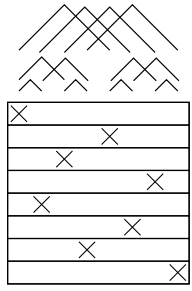
(f) Entries are annihilated as shown.



(g) Consider the partition in a 8 by 1 grid of rank-one blocks.



(h) Apply the final Givens transformations to the columns.



(i) Entries are annihilated as shown.

Fig. 5. FFT interpretation for $P_8F_8P_8$.

even block row 0, 2 of this new row grid, we choose Givens transformations $G_{0,2}$, $G_{1,3}$, $G_{4,6}$, $G_{5,7}$ to eliminate the elements in the rightmost nonzero column. Again, the unitarity of the matrix will require simultaneously the elements in the *left* most nonzero columns of the rank-one blocks positioned on an *odd* block row 1,3 of the new row grid to be annihilated: see Fig. 5f.

We can summarize the resulting sparsity pattern of Fig. 5f by

$$(0, 1, 2, 3, 4, 5, 6, 7) \mapsto (0, 2, 1, 3, 0, 2, 1, 3),$$

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

Finally, we consider the grid formed by the partition in rank-one blocks of size 1 by 8: see Fig. 5g. Note that the row grid is again refined by this operation. Proceeding in exactly the same way as before, we choose Givens transformations $G_{0,4}$, $G_{1,5}$, $G_{2,6}$, $G_{3,7}$, to eliminate the rightmost nonzero columns of each of the blocks positioned on an even block row 0, 2, 4, 6 of the new row grid: see Fig. 5i.

We can summarize the sparsity pattern of Fig. 5(i) by

$$(0, 1, 2, 3, 4, 5, 6, 7) \mapsto (0, 4, 2, 6, 1, 5, 3, 7), \tag{26}$$

where k is mapped to the index of the only remaining nonzero entry of the kth column.

From the above description of the compression process, it follows that the matrix resulting at the end of this process, will have precisely the same sparsity pattern as the *digit-reversing permutation* P_{2^m}, cf. (26).

In fact, by the unitarity of the matrix, each of the columns of the compressed matrix must still have norm equal to one, and hence by suitable choice of the complex signs of the used Givens transformations, the resulting matrix can be chosen to be precisely *equal* to the digit-reversing permutation P_{2^m}: see Fig. 6.

Summarized, we obtain

$$P_{2^m} F_{2^m} P_{2^m} G = P_{2^m},$$

where G denotes the product of all the Givens transformations used in the compression process. Hence

$$F_{2^m} P_{2^m} = G^H. \tag{27}$$

The factorization (27) allows the Fourier matrix F_n, with $n = 2^m$, to be described using only $\frac{1}{2} n \log n$ Givens transformations. In fact, it is nothing but the well-known *Cooley–Tukey FFT factorization* [17]; see Fig. 7.

Remark 14. It is possible to carry this example one step further, by deriving the exact values of the Givens transformations used in the FFT-process. But it is *not* our intention to re-derive here all the well-known formulae for the Cooley–Tukey FFT factorization [17]. Instead, our only concern was to show that the FFT factorization can be interpreted in the sense of a product of elementary

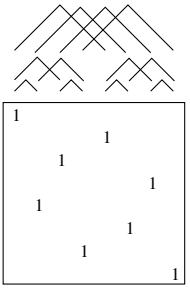


Fig. 6. The figure shows the resulting permutation matrix P_8 obtained at the end of Fig. 5.

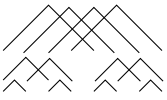


Fig. 7. The figure shows the resulting (Hermitian transposed) Cooley–Tukey FFT factorization for the matrix $F_8 P_8$.

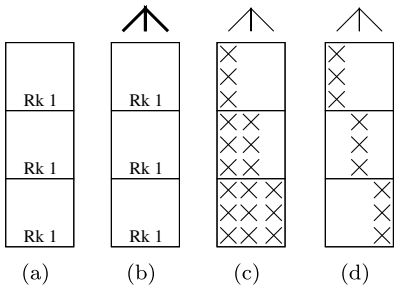


Fig. 8. Using elementary unitary operations in the FFT-factorization in the radix-3 case. Given the partition in 3 rank-one blocks as in (a), one can choose an elementary unitary operation to bring these columns to block lower triangular form: see (c). But since the columns in (c) must still be orthonormal to each other, the upper triangular shape implies the block diagonal form in (d), in a similar way as in the radix-2 case (25).

Givens transformations used to compress the subsequent rank-one blocks of the Fourier matrix. Moreover, obtaining the precise value of the Givens transformations can be more easily done using the more standard, recursive approach to the FFT [17].

Finally, we point out that similar ideas can be applied also in the general radix case, i.e., in the case F_{p^m} with p not necessarily equal to 2. For example, when $p = 3$ the role of Givens transformations should be replaced by elementary unitary operations of the form $G_{i,j,k}$, which differ from the identity matrix only in 3 different rows and columns i, j, k. If such an operation acts on the columns of a given matrix, it can again be represented as a wedge, this time having three different legs pointing to the columns on which it acts.

The main point that one should be cautious for is then how to show how these elementary unitary operations can be chosen to create zeros *simultaneously* in the several rank-one blocks of the rank-one grid of the Fourier matrix. This topic is illustrated in Fig. 8.

5. Block diagonalization of Fourier matrices

In the previous sections, it was shown that the Fourier matrix F_n might have non-trivial rank-deficient submatrices, depending on the prime factorization of n. We recall that the elementary building blocks were the matrices F_p with p prime, which do not have any non-trivial rank-deficient submatrix.

However, we want to use the present section to show that even these Fourier matrices F_p with p prime are not completely without structure, provided that the structure is defined in an appropriate way. This follows from the next result, which might be well-known, although we could not find a reference for it. It is stated here only for Fourier matrices of odd size.

Theorem 15. *Given the Fourier matrix F_n with n an odd integer. Then this matrix can be brought to block diagonal form by means of a unitary similarity operation*

$$\left(\prod_{k=1}^{\frac{n-1}{2}} G_{k,n-k}\right) F_n \left(\prod_{k=1}^{\frac{n-1}{2}} G_{k,n-k}^H\right) = \operatorname{diag}(C, S),$$

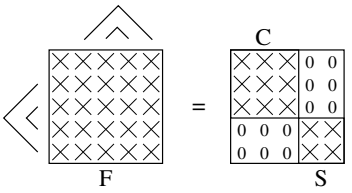


Fig. 9. The figure shows how the Fourier matrix F_n with n odd can be transformed to block diagonal form, based on a similarity operation by means of a set of Givens transformations $G_{k,n-k}, k = 1, \ldots, \frac{n-1}{2}$ (denoted by the wedges in the figure).

where C and S are matrices specified in the proof of this theorem. Here we denoted with each $G_{k,n-k}$ *the Givens transformation acting on rows and columns* $k, n-k$*, where it is defined to act as* $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, k = 1, \ldots, \frac{n-1}{2}$*. See Fig.* 9.

Proof. It is easily checked that the matrix $(\prod_{k=1}^{\frac{n-1}{2}} G_{k,n-k})\sqrt{n}F_n$ has (i, j)th entry given by

$$\omega_n^{0j} = 1, \quad i = 0,$$
$$\frac{1}{\sqrt{2}}\left(\omega_n^{ij} + \omega_n^{i(n-j)}\right) = \sqrt{2}\cos\frac{2\pi ij}{n}, \quad i \in \left\{1, \ldots, \frac{n-1}{2}\right\},$$
$$\frac{1}{\sqrt{2}}\left(\omega_n^{ij} - \omega_n^{i(n-j)}\right) = \sqrt{2}\sin\frac{2\pi ij}{n}, \quad i \in \left\{\frac{n+1}{2}, \ldots, n\right\}.$$

If we now apply the Hermitian transposes of the Givens transformations $G_{k,n-k}$ to the columns, it is easy to check that the (i, j)th entry becomes

$$1, \quad (i, j) = (0, 0),$$
$$\sqrt{2}, \quad i = 0, j \in \left\{1, \ldots, \frac{n-1}{2}\right\},$$
$$\sqrt{2}, \quad i \in \left\{1, \ldots, \frac{n-1}{2}\right\}, \quad j = 0,$$
$$2\cos\frac{2\pi ij}{n}, \quad \{i, j\} \in \left\{1, \ldots, \frac{n-1}{2}\right\},$$
$$0, \quad i \in \left\{0, \ldots, \frac{n-1}{2}\right\}, j \in \left\{\frac{n+1}{2}, \ldots, n-1\right\},$$
$$0, \quad i \in \left\{\frac{n+1}{2}, \ldots, n-1\right\}, j \in \left\{0, \ldots, \frac{n-1}{2}\right\},$$
$$2\sin\frac{2\pi ij}{n}, \quad \{i, j\} \in \left\{\frac{n+1}{2}, \ldots, n-1\right\},$$

which was to be demonstrated (see Fig. 9). □

6. Conclusions and future work

We considered the maximal rank-deficient submatrices of Fourier matrices with order a power of a prime number. 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 made use of a hierarchical subdivision of the matrix in a grid of rank-one submatrices, and it was shown how this is connected to the FFT, which can be considered as a product of elementary Givens transformations used to compress the rank-one blocks on the different levels.

In the follow-up paper [1] we consider some topics which were left open here. We recall that for $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{p\times q}$, the *Kronecker product* of A and B is defined as the block matrix

$$A \otimes B = \begin{bmatrix} a_{0,0}B & \cdots & a_{0,n-1}B \\ \vdots & & \vdots \\ a_{m-1,0}B & \cdots & a_{m-1,n-1}B \end{bmatrix}. \tag{28}$$

Using Kronecker products, we are able in [1] to cover some topics which were left open in the present paper. For example, we show in [1] how to obtain the precise Hamming numbers for a Fourier matrix F_n with arbitrary $n \in \mathbb{N}$ (which needs not be a power of a prime number), and for a general Kronecker product of Fourier matrices $F = F_{n_1} \otimes \cdots \otimes F_{n_k}$. We also show in [1] how to obtain an alternative proof of Theorem 9; cf. Remark 13 above.

References

[1] S. Delvaux, M. Van Barel, Rank-deficient submatrices of Kronecker products of Fourier matrices, Linear Algebra Appl. 426 (2007) 349–367.
[2] J.W. Demmel, P. Koev, Accurate and efficient evaluation of Schur and Jack functions,Math. Comp., 75 (2006) 223–239.
[3] D.L. Donoho, P.B. Stark, Uncertainty principles and signal recovery, SIAM J. Appl. Math. 49 (1989) 906–931.
[4] R.J. Evans, I.M. Isaacs, Generalized Vandermonde determinants and roots of unity of prime order, Proc. Amer. Math. Soc. 58 (1976) 51–54.
[5] P.E. Frenkel, Simple proof of Chebotarev's theorem on roots of unity, December 2003. <http://front.math.ucdavis.edu/math.AC/0312398>.
[6] I.G. Macdonald, Symmetric Functions and Hall Polynomials, Clarendon Press, Oxford, 1979.
[7] T. Matolcsi, J. Szucs, Intersection des mesures spectrales conjugées,C.R. Acad. Sci. Sér. I Math. 277 (1973) 841–843.
[8] R. Meshulam, An uncertainty inequality for finite Abelian groups, European J. Combin. 27 (2006) 63–67.
[9] O.H. Mitchell, Note on determinants of powers, Amer. J. Math. 4 (1881) 341–344.
[10] M. Özaydin, T. Przebinda, An entropy-based uncertainty principle for a locally compact Abelian group, J. Funct. Anal. 215 (1) (2004) 241–252.
[11] T. Przebinda, Three uncertainty principles for an Abelian locally compact group, in: E.-C. Tane, C.-B. Zhu (Eds.), Representations of Real and p-adic Groups, Lecture Notes Series, vol. 2, Institute for Mathematical Sciences, National University of Singapore, April 2004.
[12] M. Quisquater, B. Preneel, J. Vandewalle, A new inequality in discrete Fourier theory, IEEE Trans. Inform. Theory 49 (8) (2003) 2038–2040.
[13] K.T. Smith, The uncertainty principle on groups, SIAM J. Appl. Math. 50 (1990) 876–882.
[14] R. Stanley, Some combinatorial properties of Jack symmetric functions, Adv. Math. 1 (1989) 76–115.
[15] R. Stanley, Enumerative Combinatorics 2, Cambridge Stud. Adv. Math., vol. 62, Cambridge University Press, 1999.
[16] T. Tao, An uncertainty principle for cyclic groups of prime order, Math. Res. Lett. vol. 62 (12) (2005) 121–127.
[17] C.F. Van Loan, Computational Frameworks for the Fast Fourier Transform, Frontiers Appl. Math., SIAM, 1992.