REPORTS @SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Maximal values for the simultaneous number of null components of a vector and its Fourier transform

*Alberto Debernardi Pinos
Centre de Recerca Matemàtica
(CRM), Bellaterra (Barcelona)
adebernardi@crm.cat

∗Corresponding author

Resum *(CAT)*

Motivat pel principi d'incertesa, el propòsit d'aquest treball és el de trobar el valor dels nombres $L(N) = \max_{x\in\mathbb{C}^N\setminus\{0\}} \min\left\{Z(x), Z(\hat{x})\right\}$, on $\hat{x}$ i $Z(x)$ denoten la transformada de Fourier discreta i el nombre de components nul·les de x, respectivament. Dit d'una altra manera, ja que el principi d'incertesa ens assegura que $Z(x)$ és inversament proporcional a $Z(\hat{x})$, estudiem el millor balanç que hi pot haver entre aquests dos nombres.

Abstract *(ENG)*

Motivated by the uncertainty principle, the purpose of this work is to find the value of the numbers $L(N) = \max_{x\in\mathbb{C}^N\setminus\{0\}} \min\left\{Z(x), Z(\hat{x})\right\}$, where $\hat{x}$ and $Z(x)$ denote the discrete Fourier transform and the number of null components of x, respectively. In other words, since the uncertainty principle ensures that $Z(x)$ is inversely proportional to $Z(\hat{x})$, we study the best possible balance between these two numbers.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

Keywords: *Uncertainty principle, Fourier matrix, Fourier submatrix, DFT.*
MSC (2010): *42A99, 15A03.*
Received: *January 30th, 2015.*
Accepted: *June 12th, 2015.*

Acknowledgement

The author acknowledges the support of prof. J. Soria de Diego (Universitat de Barcelona), who advised the Master thesis in which this research was carried out. The research was partially supported by an AGAUR master's grant (course 2013–14) and the grant MTM2014–59174–P.

1. Introduction

In quantum mechanics, the uncertainty principle (due to Heisenberg, 1927) is a very basic result, asserting that we cannot determine the position and the momentum of a particle at the same time; in particular, the more precisely the position of a particle is determined, the less accurate its momentum can be known (and vice versa).

In mathematics there are many versions of this result, but the most remarkable one is the following: suppose that we have a function $f \in L^2(\mathbb{R})$. Then, we cannot arbitrarily concentrate both f and its Fourier transform, namely $\hat{f}$. Concretely, one of its many generalizations states that if f is practically zero outside a measurable set T, and $\hat{f}$ is practically zero outside a measurable set S, then $|T| \cdot |S| \geq 1 - \delta$, where δ is a small number which depends on the meaning of the phrase "practically zero" (for an accurate statement, see [4, Thm. 2]).

The version of this principle that we are going to deal with is the discrete one, i.e., for finite-dimensional vectors $x \in \mathbb{C}^N$. The discrete Fourier transform (DFT) of $x = (x_0, x_1, \dots, x_{N-1})$ is defined term-wise as

$$\hat{x}_j = \sum_{k=0}^{N-1} x_k e^{-2\pi ijk/N}, \quad j = 0, 1, \dots, N-1,$$

or it can also be defined as the linear map

$$\hat{x} = \Omega_N x, \tag{1}$$

where Ω_N is the so-called *N-dimensional Fourier matrix*, defined as $\Omega_N = (\omega_{j,k})$, $\omega_{j,k} = e^{-2\pi ijk/N}$, for $0 \leq j, k \leq N-1$. If we set $H(x) := \left|\{0 \leq n \leq N-1 : x_n \neq 0\}\right|$, then the discrete uncertainty principle states the following:

Theorem 1.1 (Donoho–Stark, [4]). *$H(x) \cdot H(\hat{x}) \geq N$.*

Once we know that we cannot concentrate arbitrarily the nonzero elements of a vector and its discrete Fourier transform (DFT) on very few components, we may be interested on the greatest number of null components that we can find on x and $\hat{x}$.

The goal of this paper is to determine the value of

$$L(N) := \max_{x \in \mathbb{C}^N \setminus \{0\}} \min \left\{Z(x), Z(\hat{x})\right\},$$

where $Z(x)$ is the number of null components of x or, equivalently, $Z(x) = N - H(x)$. The numbers $L(N)$ obviously depend on N but, furthermore, we will see that they strongly depend on the decomposition of N as a product of two numbers (see Theorem 2.4 below). For certain values of N, such as $N = n^2$ or $N = 2^n$, we will be able to give a formula for $L(N)$. However, finding a closed expression for all N is still an open problem. Despite of this fact, we are going to find an algorithm that will allow us to determine $L(N)$ for every N.

2. First approach: bounds for L(N)

We are going to determine upper and lower bounds for $L(N)$; in some very special cases those will coincide, yielding an equality. We start with a trivial upper bound being a direct consequence of Theorem 1.1.

Proposition 2.1. *For all N, we have $L(N) \leq N - \sqrt{N}$.*

Proof. Suppose that there exists $x \in \mathbb{C}^N$ such that $\min \left\{ Z(x), Z(\hat{x}) \right\} > N - \sqrt{N}$. Then,

$$H(x) = N - Z(x) < \sqrt{N}, \qquad H(\hat{x}) = N - Z(\hat{x}) < \sqrt{N},$$

and we conclude that $H(x)H(\hat{x}) < N$, which contradicts Theorem 1.1. □

Our next task is to start finding lower bounds for $L(N)$. The next result will provide a lower bound that will be sharp in general. However, there are special cases in which it will coincide with the bound given in Proposition 2.1.

Theorem 2.2. *(i) Let $N > 3$ be non-prime and suppose that $N = m \cdot n$, with $m \geq n$. Then,*

$$L(N) \geq \max \left\{ K \,:\, m|K,\ K \leq N - \sqrt{N} \right\} = m(n-1). \tag{2}$$

(ii) Among all the possible decompositions $N = m \cdot n$, with $m \geq n$, the greatest lower bound of $L(N)$ that can be obtained from equation (2) is given when $m - n$ is minimized.

Proof. Consider the sequence

$$x_j = x_j^n = \left\{ \begin{array}{ll} 1, & \text{if } j = k \cdot n, \text{ for } k = 0, \dots, m-1, \\ 0, & \text{otherwise.} \end{array} \right.$$

We observe that $Z(x) = N - m = m(n-1)$. Now let us compute $\hat{x}$. Suppose that $k \in \{0, \dots, N-1\}$ is such that $k = m \cdot l$, i.e., m divides k. Then,

$$\hat{x}_k = \sum_{j=0}^{N-1} x_j e^{-2\pi ijk/N} = \sum_{s=0}^{m-1} x_{s \cdot n} e^{-2\pi isnk/(mn)} = \sum_{s=0}^{m-1} e^{-2\pi isml/m} = \sum_{s=0}^{m-1} 1 = m.$$

On the other hand, if m does not divide k, then $k = m \cdot q + d$, with $d \neq 0$, and

$$\begin{aligned} \hat{x}_k &= \sum_{j=0}^{N-1} x_j e^{-2\pi ijk/N} = \sum_{s=0}^{m-1} x_{s \cdot n} e^{-2\pi isn(mq+d)/(nm)} = \sum_{s=0}^{m-1} e^{-2\pi isnmq/(nm)} e^{-2\pi isnd/(nm)} \\ &= \sum_{s=0}^{m-1} e^{-2\pi isd/m} = \frac{1 - e^{-2\pi idm/m}}{1 - e^{-2\pi id/m}} = \frac{1-1}{1 - e^{-2\pi id/m}} = 0. \end{aligned}$$

In the last expression the denominator can never vanish, since $0 < d \leq m-1$. We also note that $\hat{x} = \widehat{x^n} = m \cdot x^m$. Therefore, $Z(\hat{x}) = N - n = n(m-1)$. Since we are assuming $m \geq n$, it follows that $m(n-1) \leq n(m-1)$, so we have found a vector $x = x^n \in \mathbb{C}^N \backslash \{0\}$ such that $\min \left\{ Z(x), Z(\hat{x}) \right\} = m(n-1)$. This implies that $L(N) \geq m(n-1)$, proving (i).

To see (ii), suppose that $N = m \cdot n = m_0 \cdot n_0$, with $m \geq n$ and $m_0 \geq n_0$. Also, assume that $m - n \leq m_0 - n_0$. Under these conditions we have that $m_0 \geq m \geq n \geq n_0$. We want to prove that

$$m(n-1) \geq m_0(n_0 - 1).$$

But this happens if and only if $N - m \geq N - m_0$, which is obviously true, since $m_0 \geq m$. □

As an example to illustrate this result, we consider $N = 30 = 6 \cdot 5 = 2 \cdot 15$. Then:

$$Z\left(x^5\right) = 30 - 6 = 24, \quad Z\left(\widehat{x^5}\right) = Z\left(x^6\right) = 30 - 5 = 25,$$
$$Z\left(x^2\right) = 30 - 15 = 15, \quad Z\left(\widehat{x^2}\right) = Z\left(x^{15}\right) = 30 - 2 = 28.$$

We can observe that $\min\left\{Z\left(x^5\right), Z\left(x^6\right)\right\} = 24$ and $\min\left\{Z\left(x^2\right), Z\left(x^{15}\right)\right\} = 15$. Hence, $L(30) \geq 24$. Moreover, by Proposition 2.1, it holds that $L(30) \leq \left\lfloor 30 - \sqrt{30} \right\rfloor = 24$, where $\lfloor \cdot \rfloor$ denotes the floor function. Therefore, the conclusion is that $L(30) = 24$. As we are going to see, there are certain N for which we can determine $L(N)$ explicitly.

Corollary 2.3. *(i) If $N = n^2$ for some n, then $L(N) = N - \sqrt{N} = n^2 - n = n(n-1)$;*

(ii) if $N = n(n-1)$ for some n, then $L(N) = \left\lfloor N - \sqrt{N} \right\rfloor = n(n-2)$.

Proof. By Theorem 2.2, we have that $L(N) \geq N - \sqrt{N} = n(n-1)$. On the other hand, Proposition 2.1 tells us that $L(N) \leq N - \sqrt{N}$. This proves (i).

To see (ii), again by Theorem 2.2, $L(N) \geq n(n-2)$. Moreover, we have that

$$\begin{gathered}
\left\lfloor n(n-1) - \sqrt{n(n-1)} \right\rfloor = n(n-2) \\
\Updownarrow \\
n(n-2) \leq n(n-1) - \sqrt{n(n-1)} < n(n-2) + 1 \\
\Updownarrow \\
-n \leq -\sqrt{n(n-1)} < -n + 1 \\
\Updownarrow \\
n - 1 < \sqrt{n(n-1)} \leq n,
\end{gathered}$$

and the last expression is trivially true. Hence, using Proposition 2.1, $L(N) = \left\lfloor N - \sqrt{N} \right\rfloor = n(n-2)$. □

Before proceeding, we are going to improve the lower bound found in Theorem 2.2:

Theorem 2.4. *Let $N > 3$ be non-prime, and assume $N = m \cdot n$, with $m \geq n$. Define the set*

$$A_n = \{m_0 \cdot n \,|\, 1 \leq m_0 < m,\ m_0 < N - m_0 n \leq m\}.$$

Then, $L(N) \geq \max\left(A_n \cup \{m(n-1)\}\right)$.

Proof. We already know from Theorem 2.2 that $L(N) \geq m(n-1)$. Thus, it only remains to prove that $L(N) \geq \max A_n$ whenever such set is not empty (otherwise we are done). If A_n is not empty, then fix $m_0 < m$ satisfying $m_0 < N - nm_0 \leq m$. We are going to obtain the stated lower bound by finding $x \in \mathbb{C}^N$ with $Z(x) \geq nm_0$ and such that $Z(\hat{x}) \geq nm_0$. To this end, we choose x to be of the following form

$$x_q = \begin{cases} a_j \in \mathbb{C}, & \text{if } q = j \cdot n, \text{for } j \in \{0, 1, \dots, N - nm_0 - 1\}, \\ 0, & \text{otherwise.} \end{cases}$$

That is, the nonzero components of x can only be indexed by multiples of n. The first thing to note is that the condition $N - nm_0 \leq m$ is imposed in order to ensure that we do not exceed the number of multiples of n that are strictly less than N (there are exactly m, since $N = m \cdot n$). Second, we also notice that, by construction, $Z(x) \geq N - (N - nm_0) = nm_0$. Now let $\omega = e^{2\pi i/N}$ and, for simplicity, let us denote $k := N - nm_0$ and $c := m_0 - 1$. Then we can build the following system of equations corresponding to certain components of $\hat{x}$, according to (1):

$$\begin{pmatrix} \hat{x}_0 \\ \hat{x}_1 \\ \hat{x}_2 \\ \vdots \\ \hat{x}_c \\ \hat{x}_m \\ \hat{x}_{m+1} \\ \vdots \\ \hat{x}_{m+c} \\ \vdots \\ \vdots \\ \hat{x}_{(n-1)m+c} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{n} & \cdots & \omega^{n(k-1)} \\ 1 & \omega^{2n} & \cdots & \omega^{2n(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{nc} & \cdots & \omega^{cn(k-1)} \\ 1 & \omega^{nm} & \cdots & \omega^{nm(k-1)} \\ 1 & \omega^{n(m+1)} & \cdots & \omega^{n(m+1)(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n(m+c)} & \cdots & \omega^{n(m+c)(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n((n-1)m+c)} & \cdots & \omega^{n((n-1)m+c)(k-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_n \\ \vdots \\ x_{n(k-1)} \end{pmatrix}. \tag{3}$$

Now we are going to prove that the homogeneous system associated to (3) has solutions besides the trivial one, or in other words, that there exist nontrivial choices of x such that $Z(\hat{x}) \geq nm_0$, so that $L(N) \geq nm_0$. This will happen if the matrix of the system (3), say Ω, has rank strictly less than the number of variables $N - nm_0$. We observe that Ω is formed by n identical blocks B_q of size $(c+1) \times k$ (or equivalently, $m_0 \times (N - nm_0)$), each one of them consisting on the rows indexed by the values $qm + b$, where $q \in \{0, 1, \dots n-1\}$ is fixed, and $b \in \{0, 1, \dots, c\}$ (see (4) below). Then, the rank of Ω is less than or equal to the rank of one B_q, reaching equality if the block has maximum rank, so that rank $\Omega \leq c + 1 = m_0$. Actually, this rank is maximum, since each one of the blocks consists on the rows of a Vandermonde matrix, which is known to have maximum rank (cf. [5, Prop. 3.19]); indeed, if we denote $\beta = e^{2\pi i/m} = \omega^n$, we have, by the exponential periodicity,

$$B_q = \begin{pmatrix} 1 & \omega^{nqm} & \cdots & \omega^{nqm(k-1)} \\ 1 & \omega^{n(qm+1)} & \cdots & \omega^{n(qm+1)(k-1)} \\ 1 & \omega^{n(qm+2)} & \cdots & \omega^{n(qm+2)(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n(qm+c)} & \cdots & \omega^{n(qm+c)(k-1)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & \cdots & \beta^{(k-1)} \\ 1 & \beta^2 & \cdots & \beta^{2(k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^c & \cdots & \beta^{c(k-1)} \end{pmatrix}. \tag{4}$$

So, we conclude that rank $\Omega = c + 1 = m_0$. Thus, the system (3) is compatible and indeterminate whenever the number of columns of Ω (or the amount of indeterminates, which is the same number) is strictly greater than its rank, which we are actually assuming with the condition $m_0 < N - nm_0$. Since this procedure works for all $1 \leq m_0 < m$ satisfying $m_0 < N - nm_0 \leq m$, we conclude that $L(N) \geq \max A_n$. □

Example 2.5. In order to illustrate how Theorem 2.4 improves the result from Theorem 2.2, let us compute a lower bound for $L(39)$ using both results. Since the only nontrivial decomposition of 39 is $13 \cdot 3$, Theorem 2.2 tells us that $L(39) \geq 13 \cdot 2 = 26$. On the other hand, the corresponding set to A_n in Theorem 2.4 in this particular case is $A_3 = \{3m_0 : 1 \leq m_0 < m, m_0 < 39 - 3m_0 \leq 13\}$. It is easy to verify that the only m_0 satisfying $1 \leq m_0 < m$ and $m_0 < 39 - 3m_0 \leq 13$ is $m_0 = 9$. Therefore, we conclude that $L(39) \geq 3 \cdot 9 = 27$, which improves the lower bound obtained previously.

Notice that in the theorems we have presented so far, we have excluded the case of N being a prime number. Our next result deals with the missing case; first of all we will need the following auxiliary theorem.

Theorem 2.6 (Chebotarev)**.** *Let $\Omega_N = \left(\omega_{j,k}\right)$, as defined in (1). If N is prime, then any minor of Ω_N is nonzero.*

There are several proofs for this theorem. We can find one similar to the original made by Chebotarev in [6], and Dieudonné also gave an independent proof for this theorem, cf. [3]. So, if N is prime, whatever submatrix we select from the N-dimensional Fourier matrix will have maximum rank. Using this fact we can compute the exact value of $L(N)$.

Proposition 2.7. *Let $N \geq 3$ be a prime number. Then, $L(N) = \lfloor N/2 \rfloor$.*

Proof. First, we prove that $L(N) \geq \lfloor N/2 \rfloor$. After that, using Chebotarev's theorem, it is easy to see that $L(N) < \lfloor N/2 \rfloor + 1$. Let us define $K = \lfloor N/2 \rfloor$, and let $x = (x_0, x_1, \dots, x_K, 0, \dots, 0) \in \mathbb{C}^N$, with $x_j \neq 0$ for $j = 0, \dots, K$. It is clear that $Z(x) = N - (K+1) = K$, since N is odd. Now let us consider the following homogeneous system of equations:

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & e^{-2\pi i/N} & \cdots & e^{-2\pi iK/N} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & e^{2\pi i(K-1)/N} & \dots & e^{2\pi iK(K-1)/N} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_K \end{pmatrix}.$$

It is clearly compatible and indeterminate, since the matrix of the system is a Vandermonde matrix (we note that it has rank K, while there are $K+1$ unknowns). Then, it has an infinite number of solutions, and moreover, we note that each row j of the latter system corresponds by definition to the j-th component of the vector $\hat{x}$. Therefore, there exist vectors $x \in \mathbb{C}^N$ with $Z(x) = N - K = K + 1$ and $Z(\hat{x}) = K$, and hence, $L(N) \geq K$.

Now suppose that there exists a vector $x \in \mathbb{C}^N$ with $Z(x) \geq K+1$, $Z(\hat{x}) \geq K+1$. Then, there exists a homogeneous system of equations which is again compatible and indeterminate,

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} e^{-2\pi i s_1 r_1/N} & e^{-2\pi i s_1 r_2/N} & \dots & e^{-2\pi i s_1 r_K/N} \\ e^{-2\pi i s_2 r_1/N} & e^{-2\pi i s_2 r_2/N} & \dots & e^{-2\pi i s_2 r_K/N} \\ \vdots & \vdots & \vdots & \vdots \\ e^{-2\pi i s_{K+1} r_1/N} & e^{-2\pi i s_{K+1} r_2/N} & \dots & e^{-2\pi i s_{K+1} r_K/N} \end{pmatrix} \begin{pmatrix} x_{r_1} \\ x_{r_2} \\ \vdots \\ x_{r_K} \end{pmatrix},$$

but this happens if and only if the matrix of the system has rank strictly less than K. By Theorem 2.6, we have that this rank is exactly K, which contradicts the existence of such x. This proves $L(N) < K + 1$, and therefore, we conclude that $L(N) = K$. □

3. The algorithm for finding L(N)

In this section we will carry the arguments used before one step further: we have been using homogeneous systems of equations with submatrices of a Fourier matrix in order to place zeros arbitrarily in a vector $\hat{x}$, with the only restriction that the previous submatrix should have rank less than the number of unknowns, i.e., the components of x that are different from zero (see, for example, the system (3)). Roughly speaking, those matrices have many rows (one for each zero of $\hat{x}$), and only a few columns. Therefore, the matrices we are going to treat from now on will be of size $M \times N$, with $M > N$.

Definition 3.1. For a matrix $A \in \mathbb{C}^{M\times N}$, we say that A is *rank-deficient* if $\operatorname{rank} A < N$, or equivalently, if there exists $x \in \mathbb{C}\backslash\{0\}$ such that $Ax = 0$.

Let us fix $N \in \mathbb{N}$, and let $x \in \mathbb{C}^N$. Defining I to be the set of indexes where $\hat{x}$ is nonzero, J the set of indexes where x is nonzero, and $\overline{N} := \{0, 1, \dots, N-1\}$, we would like to find submatrices of the Fourier matrix Ω_N such that $\Omega_N\big(\overline{N}\backslash I, J\big)x_{|J} = 0$ and $\Omega_N\big(\overline{N}\backslash I, J\big)$ is rank-deficient, where $x_{|J}$ is the vector x restricted to the set of indexes J and $\Omega_N\big(\overline{N}\backslash I, J\big)$ is the restriction of Ω_N to the rows and columns indexed by $\overline{N}\backslash I$ and J, respectively. If we find one of those submatrices, then automatically $L(N) \geq \min\{N - |I|, N - |J|\}$. However, computing the ranks of every $m \times n$ submatrix of Ω_N is not an option, since the number of ranks to compute in this case has order $m!$. To solve this issue we introduce the following definition, that will lead to an easier reformulation of the problem.

Definition 3.2. For a matrix $A \in \mathbb{C}^{N\times N}$ and an integer $d \in \{1, \dots, N\}$, we define the Hamming number $H_A(d)$ as the minimal cardinality of all index sets I for which $A\big(\overline{N}\backslash I, J\big)$ is rank-deficient, for a suitable J with $|J| \leq d$.

In other words, $H_A(d) = k$ means that we can find $x \in \mathbb{C}^N\backslash\{0\}$ such that $A\big(\overline{N}\backslash I, J\big)x_{|J} = 0$ and $x_{|\overline{N}\backslash J} = 0$, where $|J| \leq d$ and $|I| = k$. Therefore, in terms of Fourier matrices, this would mean that we can find $x \in \mathbb{C}^N\backslash\{0\}$ such that $Z(x) \geq \big|\overline{N}\backslash J\big| \geq N - d$ and $Z(\hat{x}) \geq Z\big(\Omega_N\big(\overline{N}\backslash I, J\big)x_{|J}\big) = \big|\overline{N}\backslash I\big| = N - k$, which implies that

$$L(N) \geq \min\big\{N - d, N - k\big\} = \min\big\{N - d, N - H_{\Omega_N}(d)\big\} = N - \max\big\{d, H_{\Omega_N}(d)\big\}.$$

Remark 3.3. We have defined the Hamming numbers to depend on the complement of the set I instead of the set itself. Doing so, we stay close to the formulation of the uncertainty principle (cf. [1, p. 351]). Indeed, note that we can rewrite it as $d \cdot H_{\Omega_N}(d) \geq N$, for all $1 \leq d \leq N$.

In papers [1, 2], the numbers $H_{\Omega_N}(d)$ are investigated, concluding with an equality for any N and d; see Theorem 3.7 below. Those equalities will become crucial for us to compute the numbers $L(N)$.

Theorem 3.4. *Let $N \in \mathbb{N}$ and $1 \leq k < N$. Then, $L(N) = k$ if and only if*

$$N - H_{\Omega_N}(N - k) \geq k, \tag{5}$$

and

$$N - H_{\Omega_N}(N - (k+1)) \leq k. \tag{6}$$

We would like to make some comments about the meaning of equations (5) and (6) before proving the theorem. The first one means that we can find a vector $z \in \mathbb{C}^N$ with at least k zero components such that $\hat{x}$ also has more than k zero components. On the other hand, the second inequality tells us that we can find no vector $z \in \mathbb{C}^N$ such that both z and $\hat{z}$ have more than k zero components.

Proof of Theorem 3.4. First of all, we observe that, by definition,

$$N - H_{\Omega_N}(d) = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, H(x) \leq d\right\} = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, Z(x) \geq N - d\right\}. \tag{7}$$

($\Rightarrow$) Suppose that $L(N) = k$. Then, by (7), $N - H_{\Omega_N}(N-k) = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, Z(x) \geq k\right\} \geq k$, where the last inequality is our assumption. This proves (5). In order to prove (6), if $x \in \mathbb{C}^N$ is such that $Z(x) \geq k+1$ then, necessarily, $Z(\hat{x}) \leq k$ (otherwise, $L(N) = k$ would be false). Joining this fact along with relation (7), we get $N - H_{\Omega_N}(N-(k+1)) = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, Z(x) \geq k+1\right\} \leq k$, which proves the result.

($\Leftarrow$) We prove this implication by contradiction. Suppose that $L(N) \neq k$. Then, either (i) $L(N) < k$, or (ii) $L(N) > k$. In the case of (i), for any vector $x \in \mathbb{C}^N$ such that $Z(x) \geq k$, necessarily $Z(\hat{x}) < k$ (otherwise, $L(N) < k$ would be false). By (7), we deduce that

$$N - H_{\Omega_N}(N-k) = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, Z(x) \geq k\right\} < k,$$

i.e., inequality (5) is false. Finally, if (ii) holds true, then there exists $N > \tilde{k} > k$ such that $L(N) = \tilde{k}$. Since $H_{\Omega_N}(d)$ is decreasing on the variable d, it follows that the expression $N - H_{\Omega_N}(N-M)$ is decreasing on the variable M. Now, since $k+1 \leq \tilde{k}$,

$$N - H_{\Omega_N}(N-(k+1)) \geq N - H_{\Omega_N}\left(N-\tilde{k}\right) = \max\left\{Z(\hat{x}) : x \in \mathbb{C}^N, Z(x) \geq \tilde{k}\right\} \geq \tilde{k} > k,$$

so that inequality (6) is false. □

The following results we state are due to S. Delvaux and M. Van Barel; the proofs can be found in the corresponding citations.

Theorem 3.5. *[2, Thm. 9] Let p^m be a power of a prime number p. Let $d \in \{1, 2, \dots, p^m\}$ be such that $cp^t \leq d < (c+1)p^t$ for certain $c = 1, \dots, p-1$ and $t = 0, \dots, m-1$. Then, $H_{\Omega_{p^m}}(d) = (p-c+1)p^{m-t-1}$.*

Theorem 3.6. *[1, Cor. 23] For each divisor d of N, we have that $H_{\Omega_N}(d) = N/d$, i.e., equality in the uncertainty principle is reached.*

Theorem 3.7. *[1, Eq. (4)] Let $1 \leq t < N$. Then,*

$$H_{\Omega_N}(t) = \min\left\{(p-c+1)\frac{N}{pd} : pd \text{ divides } n,\ p \text{ prime},\ c \in \{1, \dots, p\},\ cd \leq t\right\}.$$

In fact, if we assume $t < N$, then the numbers p, c, d can be chosen to be such that $c < p$, $cd \leq t < (c+1)d$, and p is the smallest prime divisor of n/d.

Finally, the algorithm to find $L(N)$ is done in the following steps (always for N non-prime).

Algorithm 3.8. Let k be the lower bound of $L(N)$ obtained through Theorem 2.4.

1. If k equals the higher bound $\lfloor N - \sqrt{N} \rfloor$ (given by Proposition 2.1), then we trivially have $L(N) = k$, so we do not need extra computations (as it occurs in Corollary 2.3).

2. If $k < \lfloor N - \sqrt{N} \rfloor$, then we check the veracity of (5) and (6), where the candidate to be $L(N)$ is k. If both inequalities are true, then by Theorem 3.4, we have $L(N) = k$. In order to compute the hamming numbers appearing in these inequalities, we make use of Theorems 3.5, 3.6 and 3.7.

3. If either (5) or (6) does not hold for k, then $L(N) > k$, so we proceed to check the veracity of (5) and (6) with $k+1$ in place of k.

4. We repeat the previous step until we find $\tilde{k}$ for which (5) and (6) hold. Then, $L(N) = \tilde{k}$.

Example 3.9. Consider $N = 2^{2n+1}$, with $n \in \mathbb{N}$. It can be checked that $2^{2n+1} - 2^{n+1} < \left\lfloor 2^{2n+1} - \sqrt{2^{2n+1}} \right\rfloor$ for all n, so we will have to use the algorithm to compute $L(N)$. So, let $k = 2^{n+1}(2^n - 1) = 2^{2n+1} - 2^{n+1}$, which is the lower bound of $L(N)$ found in Theorem 2.4 (which, in this case, is the same given by Theorem 2.2). Note that we are only considering odd powers of 2, since any even power is covered by the case $N = m^2$. Now we check that inequality (5) holds:

$$N - H_{\Omega_N}\big(N - \big(2^{2n+1} - 2^{n+1}\big)\big) = 2^{2n+1} - H_{\Omega_N}\big(2^{n+1}\big).$$

By Theorem 3.6, we have that $H_{\Omega_N}\big(2^{n+1}\big) = 2^n$. Therefore, $2^{2n+1} - 2^n \geq 2^{2n+1} - 2^{n+1} = k$. Now we prove inequality (6). Note that $N - \big(2^{2n+1} - 2^{n+1} + 1\big) = 2^{n+1} - 1$. Using Theorem 3.5 to compute $H_{F_N}\big(2^{n+1} - 1\big)$, we observe that $t = n$ and $c = 1$. Hence,

$$H_{\Omega_N}\big(2^{n+1} - 1\big) = (2 - 1 + 1) \cdot 2^{2n+1-n-1} = 2 \cdot 2^n = 2^{n+1}.$$

Finally, since $N - H_{\Omega_N}\big(2^{n+1} - 1\big) = N - 2^{n+1} = 2^{2n+1} - 2^{n+1} = k$, we obtain that $L\big(2^{2n+1}\big) = 2^{2n+1} - 2^{n+1}$.

In this example we did not need to go further than step 1 of the algorithm, since the lower bound we started with was the precise number we were looking for. Now, we have the following example that will force us to carry the algorithm one step further, and will as well illustrate how Theorem 2.4 improves Theorem 2.2.

Example 3.10. Let $N = 39 = 13 \cdot 3$. We have already seen in Example 2.5 that $L(39) \geq 9 \cdot 3 = 27$. Since $\left\lfloor 39 - \sqrt{39} \right\rfloor = 32 > 27$, we have to use the algorithm in order to find $L(39)$, i.e., we check whether the inequalities (5) and (6) hold with $k = 27$. As we are going to see, (6), which in this case reads as

$$39 - H_{\Omega_{39}}(11) \geq 27$$

does not hold. In order to prove it, we use Theorem 3.7. In this case, we note that the choice of p, c, and d must be the following:

$$p = 13, \qquad c = 3, \qquad d = 3. \tag{8}$$

Then, $H_{\Omega_{39}}(11) = (13 - 3 + 1) = 11$, so that $39 - H_{\Omega_{39}}(11) = 28 \not\leq 27$. Now we have to apply the second step of the algorithm: let $k = 28$. We can use the previous computations to see that

$$39 - H_{\Omega_{39}}(39 - 28) = 39 - H_{\Omega_{39}}(11) = 28,$$

so inequality (5) holds. Further, we have to compute $H_{\Omega_{39}}(39 - 29) = H_{\Omega_{39}}(10)$. Again, we apply Theorem 3.7 with the choice of p, c, and d as in (8), which is suitable, since $3 \cdot 3 \leq 10 < 3 \cdot 4$. Since the parameters involved in Theorem 3.7 did not change, we have that $H_{\Omega_{39}}(10) = H_{\Omega_{39}}(11) = 11$, and

$$39 - H_{\Omega_{39}}(10) = 39 - 11 = 28,$$

so that inequality (6) holds. Therefore, $L(39) = 28$.

	0	1	2	3	4	5	6	7	8	9
0		0	0	1	2	2	3	3	4	6
10	6	5	8	6	8	10	12	8	12	9
20	15	15	14	11	18	20	16	21	21	14
30	24	15	24	24	22	28	30	18	24	28
40	32	20	35	21	34	36	30	23	40	42
50	40	37	40	26	45	45	48	42	38	29
60	50	30	40	54	56	53	55	33	53	51
70	60	35	63	36	48	65	60	66	66	39
80	70	72	54	41	72	70	56	64	77	44
90	80	78	72	69	62	78	84	48	84	88

Table 1: Values of $L(N)$, where at each cell, N is given by the sum of the top value of its column and the leftmost value of its row. This table can be easily obtained by coding the algorithm 3.8 in any numerical programming language.

To conclude, we present the table 1 with the values of $L(N)$ for $N = 1, \dots, 99$. Observe that we trivially have $L(1) = L(2) = 0$. We observe that for the first 10 natural numbers, $L(N)$ seems to be monotone, but $L(11) = 5 < L(10)$. This is because, as we have already mentioned, $L(N)$ depends strongly on its possible decompositions as a product of two numbers. Since 11 is prime, it cannot have such a decomposition besides the trivial one, while $10 = 5 \cdot 2$ does and, therefore, it has a "better" behavior in terms of getting $L(N)$ as close as possible to $N - \sqrt{N}$. Finally, we remark that the lower bound for the numbers $L(N)$ given in Theorem 2.4 is often optimal (when N is not prime) for the first 99 natural numbers: indeed, this lower bound fails to be equal to $L(N)$ only for the following values of N:

$$27, 39, 44, 51, 65, 68, 75, 87, 95.$$

References

[1] S. Delvaux and M. Van Barel, "Rank-deficient submatrices of Kronecker products of Fourier matrices", *Linear Algebra Appl.* **426** (2007), 349–367.

[2] S. Delvaux and M. Van Barel, "Rank-deficient submatrices of Fourier matrices", *Linear Algebra Appl.* **429** (2008), 1587–1605.

[3] J. Dieudonné, "Une propriété des racines de l'unité", *Rev. Un. Mat. Argentina* **25** (1970/71), 1–3.

[4] D.L. Donoho and P.B. Stark, "Uncertainty principles and signal recovery", *SIAM J. Appl. Math.* **49** (1989), 906–931.

[5] P.A. Fuhrmann, "A polynomial approach to linear algebra", Universitext, Springer, New York, 2012.

[6] P. Stevenhagen and H.W. Lenstra Jr., "Chebotarëv and his density theorem", *Math. Intelligencer* **18** (1996), 26–37.