Equality cases for the uncertainty principle in finite Abelian groups

Aline Bonami, Saifallah Ghobber

EQUALITY CASES FOR THE UNCERTAINTY PRINCIPLE IN FINITE ABELIAN GROUPS

ALINE BONAMI & SAIFALLAH GHOBBER

Abstract. We consider the families of finite Abelian groups $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$, for p, q prime numbers. We give a simple characterization of all functions f for which the size of the support is at most k and the size of the spectrum is minimal among such functions. Such equality cases were previously known when k divides the cardinal of the group, or for groups $\mathbb{Z}/p\mathbb{Z}$.

1. Introduction

In this work we consider a finite Abelian group G, which can always be described as

$$G = \mathbb{Z}/{p_1}^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_r}^{n_r}\mathbb{Z}, \tag{1}$$

where $p_i's$ are prime numbers with possible repetition.

We will write

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$

to simplify notation.

Uncertainty principles show how small the support and the spectrum of a nonzero function f may be simultaneously. The Fourier transform of f is defined, for $\chi \in \widehat{G}$, as

$$\widehat{f}(\chi) := \sum_{x \in G} f(x)\chi(-x).$$

Here $\widehat{G}$ is the group of characters of G, which identifies to G. More precisely, for G given by (1), some element x, which may be written as $x = (x_1, \cdots, x_r)$, and some character χ that identifies with $y = (y_1, \cdots, y_r)$, then

$$\chi(x) = \exp\left(2\pi i \sum_{j=1}^{r} \frac{x_j y_j}{p_j^{n_j}}\right).$$

The spectrum of f is the support of its Fourier transform $\widehat{f}$. We refer to [8] for background on finite Abelian groups.

The first well-known estimate has been stated by Matolcsi and Szücs in [6]. It is usually referred to as Stark-Donoho Uncertainty Principle and deals

1991 *Mathematics Subject Classification.* 42A99.

Key words and phrases. Uncertainty Principle, Finite Abelian Groups, Fourier Matrices.

The authors have been partially supported by the project ANR AHPI number ANR-07-BLAN-0247-01 and CMCU program 07G 1501.

simultaneously with cardinals of the supports of f and $\widehat{f}$ (see [4] or [8]):

$$|\operatorname{supp}(f)| \times |\operatorname{supp}(\widehat{f})| \geq |G|. \tag{2}$$

Here $|A|$ stands for the cardinal of the finite set A.

Equality cases for this inequality have been entirely described (see [4]), that is, nonzero functions f for which $|\operatorname{supp}(f)| \times |\operatorname{supp}(\widehat{f})| = |G|$. Up to translation, modulation and multiplication by a constant, they are given by characteristic functions of subgroups of G.

Then, it has been observed by Tao in [9] that Inequality (2) can be considerably improved for $\mathbb{Z}_p$ when p is a prime number. Namely, he proved the following theorem.

Theorem 1 (Tao)**.** *When f is a non zero function on $\mathbb{Z}_p$ with p prime, then*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\widehat{f})| \geq |G| + 1. \tag{3}$$

Moreover, for any $A \subset G$ and $B \subset \widehat{G}$ such that $|A|+|B| = |G|+s$, the space of functions with support in A and spectrum in B is exactly of dimension s.

In Tao's paper, the second part of the theorem is not exactly stated in this way, but this is seen by an easy modification of the proof.

Tao's Theorem contains a complete (but non explicit) description of equality cases, that is, of all nonzero functions f for which $|\operatorname{supp}(f)|+|\operatorname{supp}(\widehat{f})| = |G|+1$. Namely, given A and B such that $|A|+|B| = |G|+1$, there is a unique (up to a constant) function f such that $\operatorname{supp}(f) = A$ and $\operatorname{supp}(\widehat{f}) = B$.

In order to describe the situation for any finite Abelian group, let us give some definitions. Firstly, for any nonempty set A we call $L(A)$ the space of complex functions on A. Then we will use the following notations.

Definition 2. *For k, l two positive integers, we set*

$$E(k,l) := \Big\{ f \in L(G); |\operatorname{supp}(f)| \leq k, |\operatorname{supp}(\widehat{f})| = l \Big\}.$$

$$E_0(k,l) := \Big\{ f \in L(G); |\operatorname{supp}(f)| = k, |\operatorname{supp}(\widehat{f})| = l \Big\}.$$

Next, for $1 \leq k \leq |G|$, let us define *Meshulam's Function*, which we note $\theta(\cdot, G)$. It has been introduced by Meshulam in [7] as

$$\theta(k,G) := \min\{l; \quad E(k,l) \neq \{0\}\}. \tag{4}$$

For $|G|$ prime, by Tao's Theorem we have $\theta(k,G) = |G| - k + 1$ while, in general, we have only the inequality $\theta(k,G) \leq |G| - k + 1$. Donoho Stark's Uncertainty Principle asserts that in general $\theta(k,G) \geq |G|/k$, with possible equality when k is a divisor of $|G|$.

Meshulam has given a better lower bound for $\theta(\cdot, G)$ in [7], see also [5] for comments and extensions to the windowed Fourier transform. More precisely, let $u(\cdot, G)$ be the largest convex function on $[1, |G|]$ that coincides with $|G|/d$ at each divisor d of $|G|$. Equivalently, $u(\cdot, G)$ is continuous and linear between two consecutive divisors of p. Then Meshulam has shown that $\theta(\cdot, G) \geq u(\cdot, G)$.

The same problem has been considered recently by Delvaux and Van Barel [2, 3] with a different vocabulary. These authors give a large number

of examples and revisit proofs with elementary methods of linear algebra. They give the precise value of Meshulam's Function as a minimum (while Meshulam stated only an inequality). They also have partial results in the direction that we consider here.

We are interested in the values k for which there exists equality cases according to the following definition.

Definition 3. *We say that there are equality cases for (k, G) if the set $E_0(k, \theta(k, G))$ is not empty. In this case, we call equality case for (k, G) any nonzero function $f \in L(G)$ that belongs to the set $E_0(k, \theta(k, G))$. We say that f is an equality case for G when it is an equality case for some (k, G).*

Delvaux and Van Barel implicitly pose the problem of finding all equality cases, that is, having a complete description of the set $E_0(k, \theta(k, G))$ for all (k, G).

We will answer this question in three particular cases. More precisely, we will consider groups $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_q$, for p, q distinct prime numbers. In these three cases, we are able to give a simple description of all equality cases, in the same spirit as the already known one for k a divisor of $|G|$. It is particularly simple to describe the equality cases in the third case.

Theorem 4. *Let p, q be two distinct prime numbers. Then, when a function f is an equality case for $\mathbb{Z}_p \times \mathbb{Z}_q$, it may be written as a tensor product $g \otimes h$, where g is an equality case for $\mathbb{Z}_p$, h is an equality case for $\mathbb{Z}_q$ and, moreover, one of the two functions g or h is a character or a Dirac mass.*

Our description of equality cases allows us to answer positively to a conjecture of Delvaux and Van Barel for the three families of groups. Let us give some notations. For $M = (a_{ij})_{i \in I, j \in J}$ and N two matrices, we say that N is said to be extracted from the matrix M if I' and J' are subsets of I and J, and if $N = (a_{ij})_{i \in I', j \in J'}$. We say that M can be decomposed into matrices N_ℓ that are extracted from M if $I \times J$ is the disjoint union of $I_\ell \times J_\ell$, with each N_ℓ having coefficients indexed by $I_\ell \times J_\ell$. We have the following theorem.

Theorem 5. *Let G be a group of one of the three families under consideration. Let A and B respectively in G and $\widehat{G}$, with $|A| = k$ and $|B| = \theta(k, G)$. Consider the matrix $M := M_{A,B} := (\chi_i(j))_{i \notin B, j \in A}$, which is obtained by extraction from the Fourier matrix. Then, if M does not have full rank, it has rank $k - 1$ and may be decomposed into $k - 1$ matrices, extracted from the matrix M, which have rank one.*

Our results can be summarized as the fact that there are no other equality cases than trivial ones, except for one family of equality cases in $\mathbb{Z}_{p^2}$. Unfortunately, even if solutions are simple, proofs are technical and it seems difficult to generalize them to all finite Abelian groups, especially when an arbitrary number of primes p_j are involved.

This paper is a first attempt to show that, even if Meshulam's Function is in general smaller than $k \mapsto |G| - k + 1$, there is only a "small" number of functions such that $|\operatorname{supp}(f)| + |\operatorname{supp}(\widehat{f})| \leq |G|$, a phenomenon that is observed in [1] in a random setting.

2. Some preliminary results

Let us first recall that the function θ is non increasing. If $\theta(k,G) < \theta(k-1,G)$, then there are equality cases for (k,G). We will see in Section 4 that the converse is not true.

Next we have the following lemma.

Lemma 6. *The set $E_0(k,\theta(k,G))$ is either reduced to 0, or is a finite union of vector spaces of dimension 1.*

Proof. It is sufficient to prove that $E(k,\theta(k,G))$ is contained in a finite union of vector spaces of dimension 1. The set $E(k,\theta(k,G))$ is the union of $E(A,B)$, where A and B are respectively subsets of G and $\widehat{G}$, verify $|A| = k$, $|B| = \theta(k,G)$, and

$$E(A,B) := \Big\{ f \in L(G) \ : \ \mathrm{supp}(f) \subset A \ , \ \mathrm{supp}(\widehat{f}) \subset B \Big\}. \tag{5}$$

Assume $E(A,B)$ is of dimension ≥ 2, with $|A| = k$ and $|B| = l$. Then we can find f and g two linearly independent functions in $E(A,B)$ and there exists a non zero linear combination of f and g whose Fourier transform vanishes at some $b \in B$. This implies that $\theta(k,G) \leq l-1$. □

As a corollary, all equality cases are known as soon as we know all subsets A and B for which the space of functions with support in A and spectrum in B is not reduced to 0.

Lemma 7. *For $|A| = k$ and $|B| = |G| - k + 1$, the space $E(A,B)$ is not reduced to 0. As a consequence, $\theta(k,G) \leq |G| - k + 1$.*

Proof. The function $f = \sum_{x\in A} a(x)\delta_x$ belongs to $E(A,B)$ if the k coefficients $a(x)$ satisfy the $k-1$ linear equations given by $\widehat{f}(y) = 0$ for $y \notin B$. There is at least one nonzero solution to this system. □

The next lemma allows to exchange the role of f and $\widehat{f}$.

Lemma 8. *Assume that $\theta(k,G)) < \theta(k-1,G)$. Then*

$$\theta(\theta(k,G),\widehat{G}) = k.$$

The proof is elementary and we leave it to the reader.

We next give all equality cases for a product with a supplementary assumption.

Proposition 9. *Let $G = G_1 \times G_2$ and $1 \leq k \leq |G|$. Then*

$$\theta(k,G) = \min\{\theta(k_1,G_1)\theta(k_2,G_2) \ ; k_1k_2 \leq k, \quad 1 \leq k_i \leq |G_i|, i = 1,2\}.$$

Assume that (k_1,k_2) is the only couple for which $k_1k_2 \leq k$ and

$$\theta(k,G) = \theta(k_1,G_1)\theta(k_2,G_2). \tag{6}$$

Then there are equality cases for (k,G) if and only if $k = k_1k_2$ and there are equality cases for (k_i,G_i), $i = 1,2$. Moreover, all equality cases for (k,G) may be written as $f_1(x_1)f_2(x_2)$, with f_i an equality case for (k_i,G_i), $i = 1,2$.

Proof. It is inspired from Meshulam's paper, who has proved the first statement. Let f be a nonzero function with support of size $\leq k$ and spectrum of size $\theta(k,G)$. For $\chi(x)=\chi_1(x_1)\chi_2(x_2)$ a character, that is, an element of $\widehat{G}=\widehat{G_1}\times\widehat{G_2}$, we write

$$\begin{aligned}\widehat{f}(\chi_1,\chi_2) &= \sum_{x_1\in G_1}\sum_{x_2\in G_2} f(x_1,x_2)\chi_1(-x_1)\chi_2(-x_2)\\ &= \widehat{F}_{\chi_1}(\chi_2).\end{aligned}$$

Here

$$F_{\chi_1}(y)=\sum f(x_1,y)\chi_1(-x_1)=\widehat{f_y}(\chi_1),$$

if we pose $f_y(x_1):=f(x_1,y)$ for $y\in G_2$. Then

$$|\operatorname{supp}\widehat{f}(\chi_1,\cdot)|\geq\theta(|\operatorname{supp}F_{\chi_1}|,G_2)$$

when $F_{\chi_1}\neq 0$. Let us pose

$$\widehat{S}:=\{\xi\in\widehat{G_1};|\ F_\xi\neq 0\}=\{\xi\in\widehat{G_1};|\ \widehat{f}(\xi,\cdot)\neq 0\}.$$

Then we have

$$|\operatorname{supp}\widehat{f}(\cdot,\cdot)|\geq|\widehat{S}|\min_{\xi\in\widehat{S}}\theta(|\operatorname{supp}F_\xi|,G_2). \tag{7}$$

Now take for t the size of $T:=\{y\mid f_y\neq 0\}$. The support of F_ξ is contained in T for all $\xi\in\widehat{G_1}$, so that, for $\xi\in\widehat{S}$, we have

$$\theta(|\operatorname{supp}F_\xi|,G_2)\geq\theta(t,G_2). \tag{8}$$

We also have

$$|\widehat{S}|\geq|\cup_{y\in T}\{\xi\mid F_\xi(y)=\widehat{f_y}(\xi)\neq 0\}|\geq\theta(s,G_1) \tag{9}$$

for s the smallest size for the support of f_y. We finally remark that $st\leq k$. So we conclude from (7), (8), (9) that

$$\theta(k,G)\geq\theta(s,G_1)\theta(t,G_2). \tag{10}$$

We have proved that

$$\theta(k,G)\geq\min\{\theta(k_1,G_1)\theta(k_2,G_2)\ ;k_1k_2\leq k,\ \ 1\leq k_i\leq|G_i|,i=1,2\}.$$

Next we prove that there is equality in this inequality. Assume that the minimum is obtained for k_1,k_2. Let $f_1\in L(G_1)$ and $f_2\in L(G_2)$ such that $|\operatorname{supp}f_i|\leq k_i$ and $|\operatorname{supp}\widehat{f_i}|=\theta(k_i,G_i)$ for $i=1,2$. Then $f_1\otimes f_2$ has support of size $\leq k_1k_2\leq k$ and its spectrum has size $\theta(k_1,G_1)\theta(k_2,G_2)=\theta(k,G)$.

Next, assume that (k_1,k_2) is the only couple for which $k_1k_2\leq k$ and (6) is valid. Let us characterize the values k for which we have equality. Assume that there is some equality case f for (k,G). If we proceed as above, the inequality (10) is an equality and the minimum is obtained for (s,t), which coincides with (k_1,k_2). Inequalities (9), (8) and (7) are also equalities. Looking at the definition of T and $\widehat{S}$, it is easily seen that T is the projection of the support of f on G_2 while $\widehat{S}$ is the projection of the support of $\widehat{f}$ on $\widehat{G}_1$. So t is the size of the projection T of $\operatorname{supp}(f)$ on G_2, while $\theta(s,G_1)$ is the size of the projection $\widehat{S}$ of $\operatorname{supp}(\widehat{f})$ on $\widehat{G}_1$. Exchanging the role of G_1 and G_2, we define as well S and $\widehat{T}$, which are respectively of size s and $\theta(t,G_2)$. In particular, the size of $\operatorname{supp}(f)$, which is contained

in $S \times T$, is at most st. This proves that $k = st$ and the support of f is exactly $S \times T$. Similarly the support of $\widehat{f}$ is exactly $\widehat{S} \times \widehat{T}$. Moreover, each f_y has the same support S and the same spectrum $\widehat{S}$. It is in particular an equality case for (s, G_1). By symmetry, there are also equality cases for (t, G_2), with support T and spectrum $\widehat{T}$. More precisely, there exists some function h_1 on G_1 (resp. h_2 on G_2) with support S and spectrum $\widehat{S}$ (resp. T and $\widehat{T}$). Then $h_1 \otimes h_2$ is an equality case for (st, G), with support $S \times T$ and spectrum $\widehat{S} \times \widehat{T}$. By Lemma 7, it coincides with f, up to some constant. We have proved that f can be written as a tensor product.

This finishes the proof of the proposition. □

3. The case of groups $\mathbb{Z}_q \times \mathbb{Z}_p$, with $q < p$ prime numbers

Let us first give Meshulam's Function, which one can already find in [3]. We give the proof, nevertheless, since we need to know when there is uniqueness of the minimum.

Proposition 10. *Let $G = \mathbb{Z}_q \times \mathbb{Z}_p$, with p and q are prime numbers such that $1 < q < p$. Then*

$$\theta(k, G) = \begin{cases} p(q - k + 1) \text{ for } 1 \leq k \leq q, \\ p - [\frac{k}{q}] + 1 \text{ for } q \leq k \leq q\,\frac{p+1}{q+1}, \\ q(p - k + 1) \text{ for } q\,\frac{p+1}{q+1} \leq k \leq p, \\ q - [\frac{k}{p}] + 1 \text{ for } p \leq k \leq pq. \end{cases}$$

Proof. Using Tao's Theorem and Proposition 9, we know that

$$\theta(k, G) = \min\{(p - s + 1)(q - t + 1)\ ;\ st \leq k\ ; 1 \leq s \leq p\ ; 1 \leq t \leq q\}.$$

We claim that the minimum is obtained when one of the following four conditions is satisfied: $s = 1$, or $s = p$, or $t = 1$, or $t = q$. In the formula s and t take only integer values, but we first deal with real numbers. Let R be the rectangle defined by $1 \leq s \leq p$, $1 \leq t \leq q$ and let Δ be the region in R such that $st \leq k$, where we are looking for the minimum. If (s_0, t_0) is in Δ, the line $q(s - s_0) + p(t - t_0) = 0$, which is tangent at the curve $st = s_0 t_0$, cuts R inside Δ. Moreover the function to minimize is concave on this line, so that its minimum is obtained on the boundary of the rectangle. We are only interested in integer values, so that the minimum is the integer part of the minimum on the boundary of R. Finally we have to find the minimum of the four quantities $p(q - k + 1)$, $p - [\frac{k}{q}] + 1$, $q(p - k + 1)$, $q - [\frac{k}{p}] + 1$. We conclude easily for the value of $\theta(k, G)$, and find only one couple (s, t) for which the minimum value is obtained, except when $k = \frac{p+1}{q+1}$. □

The following proposition gives the exact form of the equality cases for each value of k and implies Theorem 4. The Dirac mass at 0 on G is denoted by δ_G.

Proposition 11. *Let $G = \mathbb{Z}_q \times \mathbb{Z}_p$, with p and q are prime numbers such that $1 < q < p$. There are equality cases if and only if $\theta(k, G) < \theta(k - 1, G)$. They can be described as follows.*

1. *For all $k \leq q$, equality cases are of the form $f \otimes \delta_{\mathbb{Z}_p}(\cdot - a)$, with $a \in \mathbb{Z}_p$ and $f \in L(\mathbb{Z}_q)$ such that $|supp(f)| = k$ and $|supp(\widehat{f})| = q - k + 1$.*

(2) *For all* $q \leq k < \frac{p+1}{q+1}$, *there are equality cases if and only if* k *is divisible by* q. *For* $k = qr$, *equality cases are of the form* $\chi \otimes f$, *with* χ *a character of* $\mathbb{Z}_q$ *and* $f \in L(\mathbb{Z}_p)$ *such that* $|supp(f)| = r$ *and* $|supp(\widehat{f})| = p - r + 1$.

(3) *For all* $\frac{p+1}{q+1} < k \leq p$, *equality cases are of the form* $\delta_{\mathbb{Z}_q}(\cdot - b) \otimes f$, *with* $b \in \mathbb{Z}_q$ *and* $f \in L(\mathbb{Z}_p)$ *such that* $|supp(f)| = k$ *and* $|supp(\widehat{f})| = p - k + 1$.

(4) *For all* $p \leq k \leq qp$, *there are equality cases if and only* k *is divisible by* p. *For* $k = pr$, *equality cases are of the form* $f \otimes \chi$, *with* χ *a character of* $\mathbb{Z}_p$ *and* $f \in L(\mathbb{Z}_q)$ *such that* $|supp(f)| = r$ *and* $|supp(\widehat{f})| = q - r + 1$.

(5) *When* $\frac{p+1}{q+1} = r$ *is an integer and* $k = rq$, *equality cases are of one of the two following forms: either* $\chi \otimes f$, *with* χ *a character of* $\mathbb{Z}_q$ *and* $f \in L(\mathbb{Z}_p)$ *such that* $|supp(f)| = r$ *and* $|supp(\widehat{f})| = p - r + 1$, *or* $\delta_{\mathbb{Z}_q}(\cdot - b) \otimes f$, *with* $b \in \mathbb{Z}_q$ *and* $f \in L(\mathbb{Z}_p)$ *such that* $|supp(f)| = k$ *and* $|supp(\widehat{f})| = p - k + 1$.

Proof. We have seen that there is only one couple (s, t) for which the minimum value is obtained, except when $k = \frac{p+1}{q+1}$. So Proposition 9 allows to conclude for the description of equality cases, except for the case *(5)*, which we now consider.

Assume now that $r = \frac{p+1}{q+1}$ is an integer. Let f be an equality case for (qr, G). We want to prove that f is of one of the forms given in the statement of the theorem. We use the notations of the proof of Proposition 9 and define $S, T, \widehat{S}, \widehat{T}$ as before. The two possibilities for (s, t), which give the minimum, are $(1, qr)$ and (q, r). So s is 1 or q, and t is r or qr. If $s = 1$, it means that S is reduced to one point and f may be written as the tensor product of a Dirac mass on $\mathbb{Z}_q$ and a function on $\mathbb{Z}_p$, from which we conclude directly. If $t = r$, then $\theta(q, \mathbb{Z}_q) = 1$ and $\widehat{S}$ is reduced to one point. So $\widehat{f}$ is the tensor product of a Dirac mass on $\mathbb{Z}_q$ and a function on $\mathbb{Z}_p$. This implies that f is the tensor product of a character of $\mathbb{Z}_q$ and a function on $\mathbb{Z}_p$.

It remains to prove that there is no other case, that is, no nonzero function f such that $|S| = |\widehat{S}| = q$, while $|T| = |\widehat{T}| = qr$, with $|\operatorname{supp}(f)| = |\operatorname{supp}(\widehat{f})| = qr$. Assume that f is such a function, which may be written as

$$f(x, y) = \sum_{j \in \mathbb{Z}_q} \delta_{\mathbb{Z}_q}(x - j) f_j(y),$$

with the functions f_j having disjoint supports of cardinality r. We identify $\mathbb{Z}_q$ with $\{0, 1, \cdots q - 1\}$ and call T_j the support of f_j, for $j = 0, 1, \cdots q - 1$. By assumption, we can also write

$$\widehat{f}(\xi, \eta) = \sum_{l \in \mathbb{Z}_q} \delta_{\mathbb{Z}_q}(\xi - l) g_l(\eta).$$

The support of g_l, which we call $\widehat{T}_l$, is also of cardinality r and $\widehat{T}$ is the disjoint union of sets $\widehat{T}_l$. We note $T' = \mathbb{Z}_p \setminus T$ and $\widehat{T}' = \mathbb{Z}_p \setminus \widehat{T}$.

Let us first prove that all $\widehat{f_j}$'s vanish on $\widehat{T'}$. Take one of the $r-1$ points in $\widehat{T'}$, say k. Then, we have

$$\widehat{f}(l,k) = \sum_j e^{-\frac{2\pi i j l}{q}} \widehat{f_j}(k) = 0$$

for $l = 0, \cdots, q-1$. This implies that each coefficient $\widehat{f_j}(k)$ is 0.

Next we consider $k \in \widehat{T_{l_0}}$. We have the $q-1$ equations, written for $l \neq l_0$

$$\widehat{f}(l,k) = \sum_j e^{-\frac{2\pi i j l}{q}} \widehat{f_j}(k) = 0,$$

which may be interpreted as the fact that the vector $(\widehat{f_j}(k))_{j=0}^{q-1}$ is orthogonal to the $q-1$ vectors $(e^{\frac{2\pi i j l}{q}})_{j=0}^{q-1}$, with $l \neq l_0$. So it is colinear to the missing vector in the Fourier basis of $\mathbb{Z}_q$. Namely,

$$\widehat{f_j}(k) = e^{\frac{2\pi i j l_0}{q}} \widehat{f_0}(k) \qquad \text{for} \quad k \in \widehat{T_{l_0}}. \tag{11}$$

So, for $k \in \widehat{T_l}$, we have that

$$g_l(k) = \widehat{f}(l,k) = q\widehat{f_0}(k).$$

In particular, because of (11), for $j = 0, 1, \cdots, q-1$ we have

$$g_0(k) = q\widehat{f_j}(k) \qquad \text{for} \quad k \in \widehat{T_0}.$$

These properties will be sufficient to find a contradiction. Let us note U_l the isomorphism from $L(T_0)$ to $L(\widehat{T_l})$ whose matrix is given by the matrix $\left(e^{-\frac{2i\pi jk}{p}}\right)_{j\in\widehat{T_l}, k\in T_0}$. Then g_l, which identifies with a function on $\widehat{T_l}$, is given by $qU_l f_0$ (identified with a function on T_0). Similarly, if V_j is the isomorphism from $L(T_j)$ to $L(\widehat{T_0})$ whose matrix is given by the matrix $\left(e^{-\frac{2i\pi kl}{p}}\right)_{k\in\widehat{T_0}, l\in T_j}$, then $g_0 = qV_j f_j$.

Because of Plancherel's Formula, we can exchange the role of G and $\widehat{G}$ and take conjugate Fourier transforms to obtain functions f_j from the functions g_k, taking into account the Plancherel constant, which is equal to pq. The role of U_0 is played by U_0^*, while the role of V_j is played by U_j^*. We get

$$pqf_0 = qU_0^* g_0 = q^2 U_0^* U_0 f_0,$$
$$pqf_0 = qU_l^* g_l = q^2 U_l^* U_l f_0.$$

Let us finally call W the operator from $L(T_0)$ to $L(\widehat{T'})$ whose matrix is given by the matrix $\left(e^{-\frac{2i\pi kl}{p}}\right)_{k\in\widehat{T'}, l\in T_0}$. Since f_0 has null coefficients on $\widehat{T'}$, we have $W^*W f_0 = 0$. As a consequence we have

$$pf_0 = q\left(\sum_{l=0}^{q-1} U_l^* U_l + W^*W\right) f_0.$$

We get a contradiction, since we assumed $q > 1$ and f_0 nonzero, by proving that $\sum_{l=0}^{q-1} U_l^* U_l + W^*W = p\,\mathrm{Id}$. But the (k,k') coefficient of the corresponding matrix is $\sum e^{-\frac{2i\pi kl}{p}} e^{\frac{2i\pi k' l}{p}}$, where the sum is taken on each $\widehat{T_l}$ separately,

then on l, then on $\widehat{T'}$. Finally the sum is taken over $0, 1, \cdots, p-1$. So it vanishes unless $k = k'$, for which it is equal to p.

This finishes the proof of *(5)*, and the proof of the proposition. □

4. The case of groups $\mathbb{Z}_p \times \mathbb{Z}_p$, with p prime

The formula for Meshulam's Function is also given in [3].

Proposition 12. *Let $G = \mathbb{Z}_p^2$, with p a prime number. Then*

$$\theta(k, G) = \begin{cases} p(p-k+1) \text{ for } 1 \leq k \leq p, \\ p - [\frac{k}{p}] + 1 \text{ for } p \leq k \leq p^2. \end{cases}$$

The proof is the same as for Proposition 10. Remark that now there is no uniqueness for the minimum. For $k < p$ it is obtained for both couples $(1, k)$ and $(k, 1)$, while, for $k > p$ and $[\frac{k}{p}] = r$, it is obtained for (p, r) and (r, p).

To describe equality cases, we will use the fact that $\mathbb{Z}_p^2$ is a vector space of dimension 2 on the field $\mathbb{Z}_p$. The main difference with the previous case is the fact that there are many subgroups of size p, namely all subgroups generated by one element $m = (m_1, m_2)$, which we write G_m. Let us define a scalar product on $\mathbb{Z}_p^2$ by $\langle x, \xi \rangle := x_1\xi_1 + x_2\xi_2$. Then the orthogonal of G_m is $G_{\widetilde{m}}$, with $\widetilde{m} = (m_1^2 + m_2^2)^{-1}(m_1, -m_2)$. So G can also be written as $G_m \times G_{\widetilde{m}}$, and there are equality cases related to each such decomposition.

We consider the set of linear transformations $A(m)$, given for $m \in \mathbb{Z}_p \times \mathbb{Z}_p$ by the matrix (that we still note $A(m)$)

$$A(m) := \begin{pmatrix} m_1 & -m_2 \\ m_2 & m_1 \end{pmatrix}.$$

It is easily seen that $A(m)^{-1} = A(\widetilde{m})$, and

$$\langle A(m)x, A(m)\xi \rangle = (m_1^2 + m_2^2)\langle x, \xi \rangle.$$

It follows in particular that the function $g(x) := f(A(m)^{-1}x)$, which is the image of f under the action of $A(m)$, has Fourier transform $\widehat{g}(\xi) = f((m_1^2 + m_2^2)A(m)^{-1}\xi)$. Transformations $A(m)$ preserve the size of the support and the spectrum of a function, so that the sets $E(k, l)$ and $E_0(k, l)$ are invariant through the action of $A(m)$. We can now state the theorem.

Theorem 13. *Let $G = \mathbb{Z}_p^2$, with p a prime number. there are equality cases if and only if $\theta(k, G) < \theta(k-1, G)$. They can be described as follows.*

1. *For all $k \leq p$, equality cases are transforms under some transformation $A(m)$ of a function of the form $f \otimes \delta_{\mathbb{Z}_p}(\cdot - a)$, with $a \in \mathbb{Z}_p$ and $f \in L(\mathbb{Z}_p)$ such that $|supp(f)| = k$ and $|supp(\widehat{f})| = p - k + 1$.*
2. *For all $p \leq k \leq p^2$, there are equality cases if and only k is divisible by p. For $k = pr$, equality cases are transforms under some transformation $A(m)$ of a function of the form $f \otimes \chi$, with χ a character of $\mathbb{Z}_p$ and $f \in L(\mathbb{Z}_p)$ such that $|supp(f)| = r$ and $|supp(\widehat{f})| = p - r + 1$.*

Proof. It is clear that the functions given in the statement are equality cases. Let us prove that they are the only ones. We consider an equality case f. Without loss of generality we can assume that $f(0) \neq 0$. We define T as

before, as the projection on the second factor of the support of f. Using the same proof as in Proposition 9, we see that $|T|$ take the values 1 or k. If $|T| = 1$, we recognize directly a function of the required form. Assume that $|T| = k$. Since $|\operatorname{supp} f| = k$, it means that $\operatorname{supp} f$ has no other point than 0 in $\mathbb{Z}_p \times \{0\}$. We claim that it is not possible for all transforms of f through some $A(m)$, which are also equality cases. Indeed, consider some nonzero $m \in \operatorname{supp} f$, which can be written as $A(m)(1,0)$.We call g the image by $A(\widetilde{m})$ of f. Then $(1,0)$ belongs to the support of g. It follows that the support of g is entirely contained in $\mathbb{Z}_p \times \{0\}$. We recognize for g one of the equality cases described in the statement. The same is valid for its transform by $A(m)$, that is, f.

Let us now consider $p \leq k \leq p^2$. The value of θ is obtained as before, with the minimum obtained for $(s,t) = (p, [\frac{k}{p}])$ or $(s,t) = ([\frac{k}{p}], p)$. For $k = pr$, the equality cases are deduced from the ones of $p - r + 1$ by taking Fourier transforms, and we recognize the functions given in the statement of the theorem. It remains to prove that there are no equality cases when k cannot be divided by p. Assume that $pr < k < p(r+1)$. Let f be an equality case for k. Then, proceeding as in Proposition 9 and defining $\widehat{S}$ and $\widehat{T}$ as before, we know that $|\widehat{S}|$ and $|\widehat{T}|$ take the values 1 or $p - r + 1$, and this is also valid for the supports of transforms of $\widehat{f}$ through all transformations $A(m)$. So after one of these transforms, the projection on one of the factors of the support of $\widehat{f}$ is reduced to one point. This implies that the size of the support of its Fourier transform, that is, the size of the support of f is a multiple of p. This gives a contradiction. □

5. The case of groups $\mathbb{Z}_{p^2}$, with p prime

As remarked in [3], the functions $\theta(k, \mathbb{Z}_{p^2})$ and $\theta(k, \mathbb{Z}_p^2)$ are identical (and equal to the function $u(k,G)$). We will see that the values of f for which there are identity cases are the same except for an exceptional new one, but there are much less equality cases. Remark that this exceptional example proves that there may exist equality cases for (k,G) when $\theta(k,G) = \theta(k-1,G)$.

Let us give some notations. We note H the subgroup $\{pj; j = 0, 1, \cdots, p-1\}$, which identifies with $\mathbb{Z}_p$. For A a subset of G we note δ_A its characteristic function. When A is reduced to one point a, then we write δ_a.

We have the following theorem.

Theorem 14. *Let $G = \mathbb{Z}_{p^2}$, with p a prime number. Then*

$$\theta(k,G) = \begin{cases} p(p-k+1) \text{ for } 1 \leq k \leq p, \\ p - [\frac{k}{p}] + 1 \text{ for } p \leq k \leq p^2. \end{cases}$$

Moreover there are equality cases if and only if $\theta(k,G) < \theta(k-1,G)$ or $k = p^2 - 1$. They can be described as follows.

(1) For all $k \leq p$, equality cases are of the form

$$f(px + x') = g(x)\delta_{a+H}(x'), \quad x, x' = 0, \cdots, p-1,$$

with $g \in L(\mathbb{Z}_p)$ such that $|supp(g)| = k$ and $|supp(\widehat{g})| = p - k + 1$, and a taking one of the values $0, \cdots, p-1$.

(2) *For all $p \leq k \leq p^2$, there are equality cases if and only k is divisible by p or $k = p^2 - 1$. For $k = pr$, equality cases are of the form*

$$f(px + x') = \chi(x)g(x'), \quad x, x' = 0, \cdots, p-1,$$

with χ a character of $\mathbb{Z}_p$ and $g \in L(\mathbb{Z}_p)$ such that $|supp(g)| = r$ and $|supp(\widehat{g})| = p - r + 1$. For $k = p^2 - 1$, then the Fourier transforms of the equality cases are of the form $\alpha\chi(\delta_x - \delta_y)$, with α a constant, χ a character and x, y two points such that $x - y \notin H$.

Proof. Even if not stated in the same way, most of this theorem is practically proved in [2] (and even its analog for any arbitrary power of p) but using a different vocabulary, with decomposition of Fourier matrices that are not simple to follow from a group point of view. So we give the complete proof in our vocabulary.

As for products of groups, the computation of θ is given by Meshulam in [7]. We nevertheless give the whole proof, which we will use again for equality cases. For f a nonzero function such that $|\operatorname{supp}(f)| \leq k$, one defines s et t, with t the number of $m = 0, \cdots, p-1$ such that $f_m(x) = f(m + px)$ is not identically 0 on $\mathbb{Z}_p$ and s the minimum of $|\operatorname{supp}(f_m)|$, so that $st \leq k$. It is then proved that

$$|\operatorname{supp}(\widehat{f})| \geq \theta(s, \mathbb{Z}_p)\theta(t, \mathbb{Z}_p) = (p + 1 - s)(p + 1 - t),$$

so that

$$\theta(k, G) \leq \min\{(p - s + 1)(p - t + 1) \ ; \ st \leq k; 1 \leq s, t \leq p\}.$$

In the right hand side we recognize the same expression as in the product case. So the minimum is obtained for $(1, k)$ or $(k, 1)$ when $k \leq p$ (resp. (p, r) or (r, p) when $rp \leq k < (r + 1)p$, with $r = 1, \cdots, p - 1$). It is easy to see that the functions given in the statement of the theorem give the equality. This gives the value of the function θ.

It remains to prove that there are no other equality cases. Let us first assume that $k \leq p$. Let f be an equality case. By invariance by translation, we can assume that $f(0) \neq 0$ (so that a will be 0). We define s and t as before. If $t = 1$, we conclude directly that the support of f is contained in one coset $a + H$, and $a = 0$ since the coset contains 0. We claim that in this case f is of the form given in the theorem: the function g on $\mathbb{Z}_p$ is such that $f(pj) = g(j)$, so that $|\operatorname{supp}(g)| = k$. If we note also $\widehat{g}$ the Fourier transform on $\mathbb{Z}_p$, then the Fourier transform of f is given by $\widehat{f}(p\xi + \eta) = \widehat{g}(\eta)$ for all $\xi \in \{0, 1, \cdots, p-1\}$, which gives that $|\operatorname{supp}(\widehat{f})| = p(p-k+1) = p|\operatorname{supp}(\widehat{g})|$.

So it remains to prove that there is no possible equality case f for which $t = k > 1$. If it was the case, since the support of f has cardinal k, then each non zero f_m is a Dirac mass, so that

$$f = \sum_{j=1}^{k} a_j \delta_{m_j + pm'_j}.$$

We conclude directly from the following lemma.

Lemma 15. *For $k \geq 2$ let f be a nonzero function that may be written as*

$$f = \sum_{j=1}^{k} a_j \delta_{m_j + pm'_j}$$

with m_j taking k different values between 0 and $p-1$ and m'_j integers between 0 and $p-1$. Then its spectrum has size at least $p(p-k+2)$, or $k=2$ and $\widehat{f}$ vanishes exactly at one point.

Proof. From the expression

$$\widehat{f}(y) = \sum_{j=1}^{k} a_j e^{2i\pi \frac{(m_j + pm'_j)y}{p^2}},$$

we see that for each fixed $y' \notin H$, the function defined on $\mathbb{Z}_p$ by $y'' \mapsto \widehat{f}(y' + py'')$ has its support of cardinal $\geq p+1-k$ by Theorem 3. Assume that $\widehat{f}$ takes $p(p+1-k)+j$ non zero values on $\mathbb{Z}_{p^2}$, with $0 \leq j < p-1$. So at least one of the p functions $y'' \mapsto \widehat{f}(y' + py'')$ has its support of size $p+1-k$ and at least one of the other ones has support of size less than p, unless $k=2$ and $j = p-1$. From now on we assume that we are not in this particular case and want to find a contradiction. By replacing eventually f by its product with a character, which has the effect to translate its Fourier transform, we can assume that for $y'=0$ the size is p. By replacing eventually f by $f(x_0 \cdot)$ for some $x_0 \in \mathbb{Z}_p$, we can assume that for $y'=1$ the function $y'' \mapsto \widehat{f}(y' + py'')$ vanishes at least at one point. This means that the sequence $a_1, \cdots, a_k$ is a nonzero solution of a system of k equations, whose determinant vanishes. The determinant is the value at $w = e^{\frac{2i\pi}{p^2}}$ of a polynomial in one variable X with coefficients in $\mathbb{Z}$. If we expand the determinant along the last row, which comes from the equation relative to $y'=1$, it can be written as

$$P = \sum_{j=1}^{k} X^{m_j} P_j(X^p) X^{p(m_j y'' + m'_j)},$$

with P_j's cofactors obtained from the $k-1$ first rows. It is easily seen that, up to a multiplicative constant, each $P_j(w^p)$ is a $(k-1)\times(k-1)$ determinant extracted from the Fourier matrix of $\mathbb{Z}_p$, so it does not vanish by Chebotarev's Lemma (see [9]). Since $P(X)$ has coefficients in $\mathbb{Z}$ and vanishes at w, it can be factorized by the polynomial

$$Q = 1 + X^p + \cdots + X^{(p-1)p},$$

see for instance [2]. The uniqueness of the writing of P as $\sum_{j=0}^{k} X^j R_j(X^p)$ allows to see that each $P_j(X^p)$ can also be factorized by the polynomial Q. So it vanishes at w, which gives a contradiction.

When $k=2$ and $j=p-1$, we conclude by hand. The fact that there exists such functions f is elementary. Up to a translation we can assume that $f = a\delta_0 + b\delta_x$ with $x \notin H$. Up to multiplication by a character we can assume that its Fourier transform vanishes at 0. So $a+b=0$. It remains to see that it does not vanish at another point. This is only possible if $xy=0$ in $\mathbb{Z}_{p^2}$ for some $y \neq 0$, which is excluded by the condition that $x \notin H$. □

We have been able to conclude for the theorem when $1 \leq k \leq p$. It is easy to conclude for $k = pr$, with $1 \leq r \leq p$. Indeed, $pr = \theta(l, G)$, so that $\theta(pr, G) = l$ and equality cases are given by Fourier transforms of equality cases for l. We consider now values k such that $pr < k \leq pr + p - 1$. Assume that f is a nonzero equality case for k. We claim that we are lead to a contradiction if we can say that the number of nonzero g_y, with $g = \widehat{f}$, is 1 or l. Indeed, we have seen that if it is 1 then the support of f is a multiple of p, which is excluded. If it is l, we use Lemma 15 to conclude.

So let us prove that the number of nonzero g_y is 1 or l. Coming back to Meshulam's proof for g, if we define s and t as before, we know that $k = |\operatorname{supp}(f)| \geq (p + 1 - s)(p + 1 - t)$ and $st \leq l$. It is easy to see that the two inequalities $p(p - l + 1) + p - 1 \geq p + 1 - s)(p + 1 - t)$ and $st \leq 1$ imply that $(s, t) = (1, l)$ or $(s, t) = (l, 1)$. Recall that t is the number of nonzero g_y's.

This allows to conclude for the proof of the theorem. □

6. EXTRACTED MATRICES OF RANK ONE

Let us prove Theorem 5. Remark first that the conclusion is easily seen for $\mathbb{Z}_p$, with p prime. Indeed, the matrix under consideration has k columns and $k-1$ lines. So one decomposes it into the $k-1$ line matrices, which have rank one. In general, the number of lines is much larger than the number of columns. It has rank less than k only if there exists some equality case in $E(A, B)$. Recall that this space is at most of dimension 1 by Lemma 7. So the rank of the matrix is at least $k-1$. It remains to look at each particular case, corresponding to one of the equality cases that we have described. It is possible to use a construction of Delvaux and Van Barel (see [3] Theorem 14) to conclude from this point. We choose to give a complete proof for the reader.

We do it for $\mathbb{Z}_{p^2}$, the proof being analogous, but simpler, in the other cases. Assume first that $1 \leq k \leq p$. After translation (which gives the same multiplication on each line of the Fourier matrix, and, so, does not change ranks of extracted matrices), an equality case has support A of size k in the subgroup H, which gives k columns. Its spectrum is of the form $C + H$, with C of size $p - k + 1$. Moreover, for $x \in H$ the character $e^{\frac{2i\pi xy}{p^2}}$ is constant on each coset $c + H$. So, in the matrix M under consideration, there are only $k - 1$ different lines, each of them being repeated p times, which allows to conclude.

Let us now show the construction for $\mathbb{Z}_{p^2}$ with $k = rp$ and $\theta(k, G) = p - r + 1$. By eventually performing a translation on the Fourier side, we can assume that the character is trivial. So A can be written as $C + H$, with C of size r and the support of $\widehat{f}$, say B, is contained in H, and of size $p - r + 1$. Recall that the matrix M is defined as a matrix with coefficients in $G \setminus B \times A$. We decompose this set as follows: we first consider the $r(p-1)$ sets $(a+H) \times (c+H)$, for $a \neq 0$ and $c \in C$, then the $r-1$ sets $\{b\} \times (C+H)$. It is elementary to see that the corresponding $rp - 1$ matrices are of rank one.

The exceptional case gives directly a matrix of rank one.

The construction given for $1 \leq k \leq p$ works for the other groups under consideration when there is a Dirac mass in the expression of the equality case. For $\mathbb{Z}_p^2$, transformations $A(m)$ do not change ranks of extracted matrices, which allows also to conclude when the decomposition of f into a tensor product can only be done after having used some transformation $A(m)$. The second construction is used when there is a character in the expression of the equality case.

References

[1] E. J. Candès, J. Romberg, and T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inform. Theory 52 (2006), no. 2, 489–509.

[2] S. Delvaux and M. Van Barel, Rank-deficient submatrices of Fourier matrices. Linear Algebra Appl. 429 (2008), no. 7, 1587–1605.

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

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

[5] F. Krahmer, G. E. Pfander and P. Rashkov, Uncertainty in time-frequency representations on finite abelian groups and applications. Appl. Comput. Harmon. Anal. 25 (2008), no. 2, 209–225.

[6] T. Matolcsi and J. Szucs, Intersection des mesures spectrales conjugées, C.R. Acad. Sci. Sér. I Math. 277 (1973), 841-843.

[7] R. Meshulam, An uncertainty inequality for finite abelian groups. European J. Combin. 27 (2006), no. 1, 63–67.

[8] A. Terras, Fourier Analysis on Finite Groups and Applications, Cambridge University Press, Cambridge, 1999.

[9] T. Tao, An uncertainty principle for cyclic groups of prime order. Math. Res. Lett. 12 (2005), no. 1, 121–127.

(Aline Bonami)
Fédération Denis Poisson
MAPM-UMR 6628 CNRS
Université d'Orléans
45067 Orléans France.
E-mail address: aline.bonami@univ-orleans.fr

(SaifAllah Ghobber)
Fédération Denis Poisson
MAPM-UMR 6628 CNRS
Université d'Orléans
45067 Orléans France.
&
Département de Mathématiques
Faculté des Sciences de Tunis
Université de Tunis El Manar
1060 Tunis, Tunisie.
E-mail address: Saifallah.Ghobber@math.cnrs.fr