Acta Math. Univ. Comenianae
Vol. LXXIII, 2(2004), pp. 155–160

THE DONOHO – STARK UNCERTAINTY PRINCIPLE FOR A FINITE ABELIAN GROUP

EWA MATUSIAK, MURAD ÖZAYDIN and TOMASZ PRZEBINDA

Abstract. Let A be a finite cyclic group and let f be a non-zero complex valued function defined on A. Donoho and Stark gave an elementary proof that the product of the cardinality of the support of f and the cardinality of the support of the Fourier transform of f is greater than or equal to the order of A. They also described the set of functions for which the equality holds. We provide an elementary proof of a generalization these results to the case when A is an arbitrary finite abelian group.

0. Introduction

The main purpose of this note is to provide an elementary proof for an uncertainty principle on a finite abelian group. By an uncertainty principle we mean an inequality involving (the concentration of) a function and its Fourier transform, along with its minimizers, that is, all functions achieving equality. Such minimizers are of interest in signal representation, see e.g. [**5**] and its references.

The uncertainty principle we consider states that the product of the cardinalities of the supports of a (non-zero complex valued) function and its Fourier transform, defined on a finite abelian group, is at least the order of the group. Moreover, the minimizers are indicator functions of subgroups up to translations, modulations and scalar multiples. When the group is cyclic an elementary proof of the inequality and the determination of its minimizers was given by Donoho and Stark, [**2**], hence the title of this note.

However, (for any finite abelian group) the inequality immediately follows from the earlier work of Matolcsi and Szücs [**3**], and the determination of minimizers from that of K. T. Smith [**6**][1]. Another proof is a consequence of an entropy based uncertainty principle, [**4**], and will be explained in Section 1. These proofs are short but not elementary and are consequences of other uncertainty principles (involving L^p norms or entropy) in the more general context of a locally compact abelian group. Our elementary proof, in Section 2, uses no more than basic concepts from

Received August 14, 2003.
2000 *Mathematics Subject Classification.* Primary 43A70; Secondary 11T99, 22B99, 42C99.
Research partially supported by NSF grant DMS 0200724.
The work was partially done while the third author was visiting the Institute for Mathematical Sciences, National University of Singapore in 2002.
[1]We would like to thank David Donoho for this reference.

finite dimensional linear algebra over complex numbers and the structure of finite abelian groups.

We would like to thank the referee for a careful review of this work.

1. The Uncertainty Principle

Let A be a finite abelian group and let $\hat{A}$ be the dual group (consisting of all characters, i.e. group homomorphisms $\alpha : A \to \mathbb{C}^\times$). For a function $f : A \to \mathbb{C}$ define the Fourier transform

$$\hat{f}(\alpha) = \sum_{a \in A} f(a)\, \alpha(-a), \qquad (\alpha \in \hat{A}),$$

a modulation

$$M_\beta f(a) = \beta(a) f(a) \qquad (\beta \in \hat{A},\ a \in A),$$

and a translation

$$T_c f(a) = f(a + c) \qquad (a, c \in A).$$

Let G be the group generated by all the modulations, all the translations and by multiplications by complex numbers of absolute value 1. Explicitly

$$G = \{z M_\beta T_c;\ z \in \mathbb{C},\ |z| = 1,\ \beta \in \hat{A},\ c \in A\}.$$

For a set S, let $|S|$ denote the cardinality of S.

Theorem 1.1. *For any non-zero function $f : A \to \mathbb{C}$,*

$$(a) \qquad |\operatorname{supp} f| \cdot |\operatorname{supp} \hat{f}| \geq |A|.$$

The set of minimizers for the inequality (a), i.e. the set of functions for which the equality occurs in (a), coincides with the union of orbits

$$(b) \qquad G \cdot f$$

where $f = const\, \mathbb{I}_B$ is a constant multiple of the indicator function $\mathbb{I}_B$ of a subgroup $B \subseteq A$.

The main goal of this article is to present an elementary proof of Theorem 1.1. This will be done in Section 2. Here we shall provide a proof based on a characterization of the minimizers for the corresponding entropy inequality, [**4**, Theorem 1.5],

Let μ denote the counting measure on A, so that

$$\int_A f(a)\, d\mu(a) = \sum_{a \in A} f(a).$$

Then the measure μ is invariant under the translations T_c, $c \in A$. Thus μ is a Haar measure on A. Let $\hat{\mu}$ be the dual Haar measure on $\hat{A}$, so that the inverse Fourier transform is given by

$$f(a) = \int_{\hat{A}} \hat{f}(\alpha)\, \alpha(a)\, d\hat{\mu}(\alpha), \qquad (a \in A).$$

Then, as is well known, $\hat{\mu}$ coincides with the counting measure on $\hat{A}$ multiplied by $\frac{1}{|A|}$.

We shall view the function $f : A \to \mathbb{C}$ as a member of the Hilbert space $L^2(A, \mu)$. Suppose $\| f \|_2 = 1$. Then, by the Plancherel formula, $\| \hat{f} \|_2 = 1$. Hence we have the entropies

$$H(|f|^2) = -\int_A |f(a)|^2 \log(|f(a)|^2)\, d\mu(a),$$
$$H(|\hat{f}|^2) = -\int_{\hat{A}} |\hat{f}(\alpha)|^2 \log(|\hat{f}(\alpha)|^2)\, d\hat{\mu}(\alpha),$$

where the log stands for the natural logarithm. Notice that

$$\| \mu(\operatorname{supp} f)^{-1/2} \mathbb{I}_{\operatorname{supp} f} \|_2 = 1.$$

Since the entropy of a uniform probability distribution is maximal, we have

$$H(|f|^2) \le H(|\mu(\operatorname{supp} f)^{-1/2} \mathbb{I}_{\operatorname{supp} f}|^2) = \log(\mu(\operatorname{supp} f)).$$

Similarly

$$H(|\hat{f}|^2) \le H(|\hat{\mu}(\operatorname{supp} \hat{f})^{-1/2} \mathbb{I}_{\operatorname{supp} \hat{f}}|^2) = \log(\hat{\mu}(\operatorname{supp} \hat{f})).$$

Hence, by the entropy inequality, [**4**, Theorem 1.5 (a)] or [**1**],

$$\log(\mu(\operatorname{supp} f) \cdot \hat{\mu}(\operatorname{supp} \hat{f})) \ge H(|f|^2) + H(|\hat{f}|^2) \ge 0. \tag{1.2}$$

This verifies the inequality (a) of Theorem 1.1.

The equality in part (a) of Theorem 1.1, together with (1.2), imply the following equality

$$H(|f|^2) + H(|\hat{f}|^2) = 0. \tag{1.3}$$

Hence, Theorem 1.5 (b) in [**4**] shows that the function f is of the desired form.

2. An elementary proof of Theorem 1.1

For a subset $S \subseteq A$ let $S^\perp = \{\alpha \in \hat{A},\ \alpha|_S = 1\}$. Then, as is well known, for any subgroup $B \subseteq A$,

$$|B| \cdot |B^\perp| = |A|. \tag{2.1}$$

Consider a non-zero function $f : A \to \mathbb{C}$, as in Theorem 1.1. We may, and shall, assume that $0 \in \operatorname{supp} f$ and that $1 \in \operatorname{supp} \hat{f}$ (translating and modulating f if necessary). Here $1 \in \hat{A}$ is the identity element. Notice first that, in order to prove the theorem, it would suffice to show that $\operatorname{supp} f$ is a subgroup of A. Indeed, since the Fourier transform $\hat{f}$ is invariant under the translations by $(-\operatorname{supp} f)^\perp$, ($\hat{f}(\alpha\beta) = \hat{f}(\alpha)$ for all $\alpha \in \hat{A}$ and all $\beta \in (-\operatorname{supp} f)^\perp$), the equation (2.1) implies the inequality (a) of the theorem. Furthermore, the equality in part (a) of Theorem 1.1, implies that $\hat{f}$ is supported on $B^\perp$, where $B = \operatorname{supp} f$. Since $\hat{f}$ is $B^\perp$-invariant, $\hat{f}$ is a constant on $B^\perp$. Then f is a constant multiple of $\mathbb{I}_B$. Thus we shall be done as soon as we verify the following Proposition.

Proposition 2.2. *For a finite abelian group A and a function $f : A \to \mathbb{C}$ we have*

(a) *if $f \neq 0$, then $|\operatorname{supp} f| \cdot |\operatorname{supp} \hat{f}| \geq |A|$;*

(b) *if $|\operatorname{supp} f| \cdot |\operatorname{supp} \hat{f}| = |A|$ and $0 \in \operatorname{supp} f$, then $\operatorname{supp} f$ is a subgroup of A.*

Proof. When the group A is cyclic the Proposition follows from [**2**]. Thus we may assume that there are nontrivial subgroups $B, C \subseteq A$ such that $A = B \oplus C$. Then

$$\hat{A} = \hat{B} \times \hat{C}.$$

For a function $f : A \to \mathbb{C}$ let

$$f_c(b) = f(b + c) \qquad (b \in B,\ c \in C),$$

and let

$$g_\beta(c) = \hat{f}_c(\beta) \qquad (\beta \in \hat{B},\ c \in C).$$

Then, in particular,

$$\hat{f}(\beta\gamma) = \hat{g}_\beta(\gamma) \qquad (\beta \in \hat{B},\ \gamma \in \hat{C}). \tag{2.3}$$

We proceed via the induction on $|A|$. Suppose the proposition holds for the groups B and C. Let $\mathcal{B} = \{\beta \in \hat{B};\ g_\beta \neq 0\}$ and $\mathcal{C} = \{c \in C;\ f_c \neq 0\}$. Pick $c \in \mathcal{C}$ with $|\operatorname{supp} f_c|$ minimal. Then

$$|\operatorname{supp} f_c| \leq \frac{|\operatorname{supp} f|}{|\mathcal{C}|}. \tag{2.4}$$

Hence, by the inductive assumption,

$$|\operatorname{supp} \hat{f}_c| \geq \frac{|B|}{|\operatorname{supp} f_c|}. \tag{2.5}$$

From (2.4) and (2.5) we deduce

$$|\operatorname{supp} \hat{f}_c| \geq \frac{|B| \cdot |\mathcal{C}|}{|\operatorname{supp} f|}. \tag{2.6}$$

Notice that $\operatorname{supp} \hat{f}_c \subseteq \mathcal{B}$, so that

$$|\operatorname{supp} \hat{f}_c| \leq |\mathcal{B}|. \tag{2.7}$$

Also,

$$\operatorname{supp} g_\beta \subseteq \mathcal{C} \qquad (\beta \in \mathcal{B}). \tag{2.8}$$

By the inductive assumption and by (2.8) we have

$$|\operatorname{supp} \hat{g}_\beta| \geq \frac{|C|}{|\operatorname{supp} g_\beta|} \geq \frac{|C|}{|\mathcal{C}|}. \tag{2.9}$$

We see from (2.3) that

$$\operatorname{supp} \hat{f} = \bigcup_{\beta \in \mathcal{B}} \operatorname{supp} \hat{g}_\beta \times \{\beta\}.$$

Therefore,

$$|\operatorname{supp}\hat{f}| = \sum_{\beta\in\mathcal{B}} |\operatorname{supp}\hat{g}_\beta| \geq \sum_{\beta\in\mathcal{B}} \frac{|C|}{|\mathcal{C}|} = |C|\cdot\frac{|\mathcal{B}|}{|\mathcal{C}|}, \tag{2.10}$$

where the inequality follows from (2.9). We see from (2.6) and (2.7) that

$$|\operatorname{supp} f| \geq |B|\cdot\frac{|\mathcal{C}|}{|\operatorname{supp}\hat{f}_c|} \geq |B|\cdot\frac{|\mathcal{C}|}{|\mathcal{B}|}. \tag{2.11}$$

By combining (2.10) and (2.11) we get

$$|\operatorname{supp} f|\cdot|\operatorname{supp}\hat{f}| \geq |B|\cdot|C| = |A|. \tag{2.12}$$

This verifies the inequality (a) in our Proposition 2.2.

Suppose from now on that we have equality in (2.12). Also, we may and shall assume that $1\in\operatorname{supp}\hat{f}$.

The equality in (2.12) forces equalities in (2.4), (2.5), (2.6), (2.7), (2.9) and (2.10). Therefore

$$|\operatorname{supp} f_c| = \frac{|\operatorname{supp} f|}{|\mathcal{C}|}, \tag{2.13}$$

$$|\operatorname{supp} f_c|\cdot|\operatorname{supp}\hat{f}_c| = |B|, \tag{2.14}$$

$$\operatorname{supp}\hat{f}_c = \mathcal{B}, \tag{2.15}$$

$$\operatorname{supp} g_\beta = \mathcal{C} \qquad (\beta\in\mathcal{B}), \tag{2.16}$$

$$|\operatorname{supp} g_\beta|\cdot|\operatorname{supp}\hat{g}_\beta| = |C| \qquad (\beta\in\mathcal{B}). \tag{2.17}$$

Also,

$$1\in\mathcal{B}, \text{ and } 0\in\mathcal{C}, \tag{2.18}$$

because

$$\hat{g}_1(1) = \hat{f}(1)\neq 0, \text{ and } f_0(0) = f(0)\neq 0. \tag{2.19}$$

By the inductive assumption, (2.14) and by (2.19), $\operatorname{supp} f_0$ is a subgroup of B. We see from (2.14) and (2.19) that $\operatorname{supp}\hat{f}_0 = (\operatorname{supp} f_0)^\perp$ is a subgroup of $\hat{B}$. Hence, (2.15) implies that $\mathcal{B}$ is a subgroup of $\hat{B}$ and $\hat{f}_0 = const\,\mathbb{I}_{\mathcal{B}}$. Similarly

$$\mathcal{C} = \operatorname{supp} g_1 \text{ is a subgroup of } C \text{ and } g_1 = const\,\mathbb{I}_{\mathcal{C}}. \tag{2.20}$$

By the inductive assumption and by (2.14), $\operatorname{supp} f_c$ is a translation of the subgroup $(\operatorname{supp}\hat{f}_c)^\perp = \mathcal{B}^\perp \subseteq B$. Thus there is a function $\phi : C\to B$ such that

$$\operatorname{supp} f_c = \mathcal{B}^\perp + \phi(c) \qquad (c\in\mathcal{C}), \tag{2.21}$$

where $\phi(0) = 0$. Again, by (2.14) and (2.21),

$$\hat{f}_c(\beta) = \overline{\beta(\phi(c))}\,\hat{f}_c(0) \qquad (\beta\in\mathcal{B},\ c\in\mathcal{C}). \tag{2.22}$$

Notice that $\hat{f}_c(0) = g_1(c) = g_1(0)$. Thus (2.22) may be rewritten as

$$\hat{f}_c(\beta) = \overline{\beta(\phi(c))}\,g_1(0), \qquad (\beta\in\mathcal{B},\ c\in\mathcal{C}). \tag{2.23}$$

Similarly, for some $\gamma_\beta \in \hat{C}$,

$$g_\beta(c) = \gamma_\beta(c)\, g_\beta(0) \qquad (c \in \mathcal{C}). \tag{2.24}$$

Since $g_\beta(c) = \hat{f}_c(\beta)$, we have

$$g_\beta(0) = \hat{f}_0(\beta) = \hat{f}_0(0) = g_1(0).$$

Thus (2.24) may be rewritten as

$$\hat{f}_c(\beta) = \gamma_\beta(c)\, g_1(0) \qquad (\beta \in \mathcal{B},\ c \in \mathcal{C},). \tag{2.25}$$

By combining (2.23) and (2.25) we deduce the following equality,

$$\beta(\phi(c)) = \gamma_\beta(c) \qquad (\beta \in \mathcal{B},\ c \in \mathcal{C}).$$

Hence for $\beta \in \mathcal{B}$, and for $c_1, c_2 \in \mathcal{C}$,

$$\begin{aligned}\beta(\phi(c_1) + \phi(c_2) - \phi(c_1 + c_2)) &= \beta(\phi(c_1))\beta(\phi(c_2))\beta(\phi(c_1 + c_2))^{-1} \\ &= \gamma_\beta(c_1)\gamma_\beta(c_2)\gamma_\beta(c_1 + c_2)^{-1} = \gamma_\beta(0) = 1.\end{aligned}$$

Therefore

$$\phi(c_1) + \phi(c_2) - \phi(c_1 + c_2) \in \mathcal{B}^\perp \qquad (c_1, c_2 \in \mathcal{C}). \tag{2.26}$$

We see from (2.21) and (2.26) that

$$\operatorname{supp} f = \bigcup_{c \in \mathcal{C}} \operatorname{supp} f_c \times \{c\} = \bigcup_{c \in \mathcal{C}} (\mathcal{B}^\perp + \phi(c)) \times \{c\}$$

is closed under addition. Therefore $\operatorname{supp} f$ is a subgroup of A. $\square$

References

1. Dembo A., Cover T. M. and Thomas J. A., *Information Theoretic Inequalities*, IEEE Transactions on Information Theory, **37** (1991), 1501–21518.

2. Donoho D. L. and Stark P. B., *Uncertainty Principles and Signal Recovery*, SIAM Journal of Applied Mathematics, **49** (1989), 906–931.

3. Matolcsi T. and Szücs J., *Intersections des mesures spectrales conjugees*, C. R. Acad. Sci. Paris **277** (1973), 841–843.

4. Özaydın M. and Przebinda T., *An Entropy-based Uncertainty Principle for a Locally Compact Abelian Group*, to appear in the Journal of Functional Analysis.

5. Przebinda T., DeBrunner V. and Özaydın M., *The Optimal Transform for the Discrete Hirschman Uncertainty Principle*, IEEE Transactions on Information Theory **47** (2001), 2086–2090.

6. Smith K. T., *The Uncertainty Principle on Groups*, SIAM Journal of Applied Mathematics **50** (1990), 876–882.

Ewa Matusiak, Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA, *e-mail*: `tprzebinda@ou.edu`

Murad Özaydın, Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA

Tomasz Przebinda, Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA