



ANNALES

DE

L'INSTITUT FOURIER

John GILBERT & Ziemowit RZESZOTNIK

The norm of the Fourier transform on finite abelian groups

Tome 60, n° 4 (2010), p. 1317-1346.

http://aif.cedram.org/item?id=AIF_2010__60_4_1317_0

© Association des Annales de l'institut Fourier, 2010, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

THE NORM OF THE FOURIER TRANSFORM ON FINITE ABELIAN GROUPS

by John GILBERT & Ziemowit RZESZOTNIK (*)

ABSTRACT. — For $1 \leq p, q \leq \infty$ we calculate the norm of the Fourier transform from the L^p space on a finite abelian group to the L^q space on the dual group.

RÉSUMÉ. — Pour les valeurs de p et q comprises entre 1 et l'infini, nous déterminons la norme de la transformée de Fourier de l'espace L^p d'un groupe abélien fini vers l'espace L^q du groupe dual.

Introduction

Let G be a locally compact abelian group and \mathcal{F} be the Fourier transform on G . Hausdorff-Young inequality states, that for $1 < p < 2$, $\frac{1}{p} + \frac{1}{q} = 1$ and $f \in L^p(G)$, we have that

$$(0.1) \quad \|\mathcal{F}f\|_q \leq \|f\|_p,$$

with the norms on the appropriate Lebesgue spaces constructed relative to Haar measures. The problem of finding the sharp constants in the above inequality was resolved within the last century. In their joint paper [21] from 1927, Hardy and Littlewood showed that on \mathbb{T} the equality in (0.1) holds only for characters. The general case was treated by Hewitt and Hirschman in 1954 (see [23] or Theorem (43.13) in [24]). They found out, that the equality holds only for characters restricted to co-sets of compact open subgroups of G . It was still unknown, however, what happens if G has no compact open subgroups. The well known structure theorem states

Keywords: Fourier transform, finite abelian groups, wave packets, biunimodular functions.

Math. classification: 42C40, 43A15, 43A25.

(*) The second author was supported under the EU-project MEXT-CT-2004-517154 and MTKD-CT-2004-013389.

that every locally compact abelian group is topologically isomorphic to $\mathbb{R}^n \times G_0$, where G_0 is a locally compact abelian group that contains a compact open subgroup. Therefore, it was rather clear, that understanding the case $G = \mathbb{R}^n$ is the only missing piece of information needed to describe the extremals of (0.1). In 1961, Babenko shed some light on this topic. He showed in [4], that on \mathbb{R} , the inequality (0.1) can be improved if q is an even integer. He calculated the sharp constants in this case and showed that the equality holds only for modulations and translations of Gaussians, that is, functions given by $g(x) = e^{-ax^2}$, $a > 0$. Basing on Babenko's result, Hewitt and Ross conjectured in [24] the form of the extremal functions that maximize $\frac{\|\mathcal{F}f\|_q}{\|f\|_p}$ on locally compact abelian groups. The case $G = \mathbb{R}^n$ was solved in 1975 by Beckner, who proved in [5], that for all $1 < p < 2$ and $f \in L^p(\mathbb{R}^n)$ one has

$$(0.2) \quad \|\mathcal{F}f\|_q \leq \left(\frac{p^{\frac{1}{p}}}{q^{\frac{1}{q}}} \right)^{\frac{n}{2}} \|f\|_p$$

and equality holds for Gaussians. Finally, in 1990, Lieb showed that the equality in (0.2) holds only for Gaussians (see [30]). This ended the process of finding the norm of \mathcal{F} on locally compact abelian groups and characterizing its extremals.

Our paper is devoted to finding the norm of \mathcal{F} on finite abelian groups and characterizing the extremals for arbitrary values $1 \leq p, q \leq \infty$. That is, we no longer assume that p and q are conjugated. We show that the square $[0, 1]^2 \ni (\frac{1}{p}, \frac{1}{q})$ splits into three regions. In one of them the norm is attained on the delta functions (time basis). In the other, the characters (frequency basis) pinpoint the norm. The extremals of the third region are the most interesting. These are *biunimodular* functions, that were recently introduced in [8] by Björk and Saffari. The notion is easy to explain. Recall, that f is unimodular if $|f|$ is identically equal to 1. We say that f is biunimodular, if both f and $\mathcal{F}f$ are unimodular. Although Björk and Saffari were concentrating on cyclic groups, biunimodular functions were also considered on $G = (\mathbb{Z}_2)^N$ under the name of *bent functions*. They appear in cryptography and error-correcting codes. Investigating biunimodular functions on cyclic groups, however, can be dated back to Gauss. The general problem of finding all biunimodular functions is very complex. We provide the evidence for this in the final section.

We also characterize all the other extremals for the norm of \mathcal{F} , that occur at the boundaries of the three mentioned regions. In particular, we give an elementary proof of the result of Hewitt and Hirschman in the case of

finite abelian groups. We argue that these classical extremals together with biunimodular functions are in the hard core of modern Fourier analysis.

1. Preliminaries

Let G be a finite abelian group and $\hat{G} = \{\gamma : G \rightarrow \mathbb{T}\}$ its dual group. For $1 \leq p, q \leq \infty$ we consider the spaces $L^p(G)$ and $L^q(\hat{G})$ with the counting measure, so that the corresponding norms are given by $\|v\|_p = (\sum_{g \in G} |v(g)|^p)^{\frac{1}{p}}$, $\|w\|_q = (\sum_{\gamma \in \hat{G}} |w(\gamma)|^q)^{\frac{1}{q}}$ for $v \in L^p(G)$, $w \in L^q(\hat{G})$ if $p, q \neq \infty$ and $\|v\|_\infty = \sup_{g \in G} |v(g)|$, $\|w\|_\infty = \sup_{\gamma \in \hat{G}} |w(\gamma)|$. All these spaces have a common underlying vector space V isomorphic to $\mathbb{C}^{|G|}$, where $|G|$ denotes the cardinality of G . The characters $\gamma \in \hat{G}$ allow us to define the Fourier transform $\mathcal{F} : L^p(G) \rightarrow L^q(\hat{G})$ by

$$\mathcal{F}v(\gamma) = |G|^{-\frac{1}{2}} \langle v, \gamma \rangle,$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on V . Thus, the Fourier transform is a $|G| \times |G|$ matrix whose rows take the form $|G|^{-\frac{1}{2}} \bar{\gamma}$. Consequently, any function $f \in L^2(G)$ can be treated as a vector.

The normalized characters $\{|G|^{-\frac{1}{2}} \gamma : \gamma \in \hat{G}\}$ form an orthonormal basis of $L^2(G)$, so \mathcal{F} is unitary and $\|\mathcal{F}v\|_2 = \|v\|_2$. A standard result is that $\mathcal{F}(\chi_H) = |H| |G|^{-\frac{1}{2}} \chi_{H^\perp}$, where H is a subgroup of G and $H^\perp = \{\gamma \in \hat{G} : \ker \gamma \supset H\}$. Moreover, $|H| |H^\perp| = |G|$, for any subgroup $H \subseteq G$.

For $1 \leq p, q \leq \infty$ the norm $C_{p,q}$ of the Fourier transform is given by

$$C_{p,q} = \sup_{\|v\|_p=1} \|\mathcal{F}v\|_q.$$

Since \mathcal{F} is unitary, we have $C_{2,2} = 1$. The goal of this paper is to calculate the values of $C_{p,q}$ for arbitrary $1 \leq p, q \leq \infty$. It will be achieved by bounding $C_{p,q}$ for particular values of p and q , using Riesz-Thorin interpolation to extend these bounds to the whole Riesz square $[0, 1]^2 \ni (\frac{1}{p}, \frac{1}{q})$ and finding the functions where the upper bound is attained. We shall also characterize all extremal functions that pinpoint the norm. As we mentioned in the previous section, an important class of extremals consists of biunimodular functions. Let us close these preliminaries by making the following formal

DEFINITION 1.1. — *Let G be a finite abelian group. We say that $u \in L^2(G)$ is biunimodular if*

$$(1.1) \quad |u(g)| = 1 \quad \text{and} \quad |\mathcal{F}u(\gamma)| = 1$$

for all $g \in G$, $\gamma \in \hat{G}$.

2. Norm of the Fourier transform

To give the values of $C_{p,q}$ we need to consider three regions

$$(2.1) \quad R_F = \left\{ \left(\frac{1}{p}, \frac{1}{q} \right) \in [0, 1]^2 : \frac{1}{p} + \frac{1}{q} \leq 1, \frac{1}{q} \leq \frac{1}{2} \right\},$$

$$(2.2) \quad R_T = \left\{ \left(\frac{1}{p}, \frac{1}{q} \right) \in [0, 1]^2 : \frac{1}{p} + \frac{1}{q} \geq 1, \frac{1}{p} \geq \frac{1}{2} \right\},$$

and

$$(2.3) \quad R_{TF} = \left\{ \left(\frac{1}{p}, \frac{1}{q} \right) \in [0, 1]^2 : \frac{1}{p} \leq \frac{1}{2}, \frac{1}{q} \geq \frac{1}{2} \right\}.$$

The main result of the paper is the following (see Fig. 2.1)

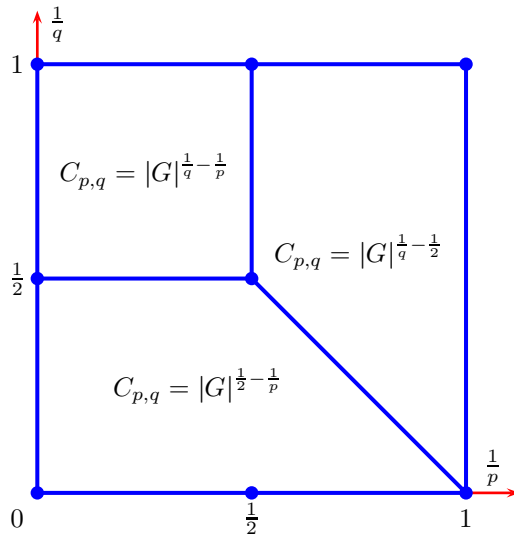


Figure 2.1. Norm of the Fourier transform.

THEOREM 2.1. —

$$C_{p,q} = \begin{cases} |G|^{\frac{1}{2} - \frac{1}{p}} & \text{for } \left(\frac{1}{p}, \frac{1}{q} \right) \in R_F \\ |G|^{\frac{1}{q} - \frac{1}{2}} & \text{for } \left(\frac{1}{p}, \frac{1}{q} \right) \in R_T \\ |G|^{\frac{1}{q} - \frac{1}{p}} & \text{for } \left(\frac{1}{p}, \frac{1}{q} \right) \in R_{TF} \end{cases}$$

The proof of the theorem will be split in two parts. In the next section we shall prove that $C_{p,q}$ is bounded by the above values. Later we will exhibit extremal functions for which the norm is attained. The difficult problem of finding all extremals will be treated at the end of the paper.

In order to proceed with the proof of the above theorem let us consider the function $K : [0, 1]^2 \rightarrow \mathbb{R}$ given by

$$K(x, y) = \begin{cases} |G|^{\frac{1}{2}-x} & \text{for } (x, y) \in R_F \\ |G|^{y-\frac{1}{2}} & \text{for } (x, y) \in R_T \\ |G|^{y-x} & \text{for } (x, y) \in R_{TF} \end{cases}$$

Clearly, we want to show that $C_{p,q} = K(\frac{1}{p}, \frac{1}{q})$. The inequality $C_{p,q} \leq K(\frac{1}{p}, \frac{1}{q})$ will follow from Riesz-Thorin convexity theorem. The remainder of this section is dedicated to the reader who is not familiar with this tool.

Although the convexity theorem can be stated in a much greater generality we shall stick to our simple setting. Let $T : \mathbb{C}^n \rightarrow \mathbb{C}^m$ be a linear operator. We define its norm $N_T(p, q)$ for $1 \leq p, q \leq \infty$ by

$$N_T(p, q) = \sup_{\|v\|_p=1} \|Tv\|_q$$

and consider the function $K_T : [0, 1]^2 \rightarrow \mathbb{R}$ given by $K_T(x, y) = N_T(x^{-1}, y^{-1})$ (with the convention $\frac{1}{0} = \infty$ and $\frac{1}{\infty} = 0$).

THEOREM (Riesz-Thorin Convexity Theorem). — *The function $\log K_T$ is convex.*

This simply means that if $P = \{p_1, p_2, \dots, p_l\}$ is a collection of points in $[0, 1]^2$ then $\log K_T(\sum_{i=1}^l \lambda_i p_i) \leq \sum_{i=1}^l \lambda_i \log K_T(p_i)$ for arbitrary $\lambda_i \geq 0$ such that $\sum_{i=1}^l \lambda_i = 1$. The functions for which the above inequality becomes an equality are affine functions, that are simply given by $f(x, y) = ax + by + c$ for some $a, b, c \in \mathbb{R}$. The set

$$\text{hull}(P) = \left\{ \sum_{i=1}^l \lambda_i p_i : \lambda_i \geq 0 \text{ for all } i \text{ and } \sum_{i=1}^l \lambda_i = 1 \right\}$$

is called the *convex hull* of P . These notions allow us to formulate an immediate consequence of the convexity theorem

COROLLARY 2.2. — *If f is an affine function and $\log K_T(p) \leq f(p)$ for all p in a finite set $P \subset [0, 1]^2$ then $\log K_T(p) \leq f(p)$ for all $p \in \text{hull}(P)$.*

Proof. — For $p \in \text{hull}(P)$ we have

$$\log K_T(p) = \log K_T \left(\sum_{i=1}^l \lambda_i p_i \right) \leq \sum_{i=1}^l \lambda_i \log K_T(p_i) \leq \sum_{i=1}^l \lambda_i f(p_i) = f(p).$$

□

In the next section we shall use the above corollary to show the upper bound for the norm of the Fourier transform.

3. The upper bound $C_{p,q} \leq K(\frac{1}{p}, \frac{1}{q})$

We have the following

PROPOSITION 3.1. — $C_{p,q} \leq K(\frac{1}{p}, \frac{1}{q})$.

Proof. — Since the regions R_F, R_T and R_{TF} are convex and the function $\log K$ restricted to any of these regions is affine, it is enough to check that the inequality $C_{p,q} \leq K(\frac{1}{p}, \frac{1}{q})$ holds at the vertices of these regions and apply Corollary 2.2 to extend this upper bound to the whole Riesz square.

Since \mathcal{F} is unitary we see that at the point $(\frac{1}{2}, \frac{1}{2})$ we have

$$C_{2,2} = 1 = K\left(\frac{1}{2}, \frac{1}{2}\right).$$

At the point $(0, 0)$ we have

$$(3.1) \quad |\mathcal{F}v(\gamma)| = |G|^{-\frac{1}{2}} |\langle v, \gamma \rangle| \leq |G|^{-\frac{1}{2}} \|v\|_\infty \|\gamma\|_1 = |G|^{\frac{1}{2}} \|v\|_\infty,$$

so $C_{\infty,\infty} \leq K(0, 0)$.

At the point $(1, 0)$ we have

$$(3.2) \quad |\mathcal{F}v(\gamma)| = |G|^{-\frac{1}{2}} |\langle v, \gamma \rangle| \leq |G|^{-\frac{1}{2}} \|v\|_1 \|\gamma\|_\infty = |G|^{-\frac{1}{2}} \|v\|_1,$$

so $C_{1,\infty} \leq K(1, 0)$.

At the point $(1, 1)$ we have

$$(3.3) \quad \|\mathcal{F}v\|_1 = \left\| \sum_{g \in G} v(g) \mathcal{F}\delta_g \right\|_1 \leq \sum_{g \in G} |v(g)| \|\mathcal{F}\delta_g\|_1 = |G|^{\frac{1}{2}} \|v\|_1,$$

where δ_g is the delta function at g . Therefore, $C_{1,1} \leq K(1, 1)$.

At the point $(\frac{1}{2}, 1)$ we have

$$(3.4) \quad \|\mathcal{F}v\|_1 = \langle |\mathcal{F}v|, \chi_G \rangle \leq \|\mathcal{F}v\|_2 \|\chi_G\|_2 = |G|^{\frac{1}{2}} \|v\|_2,$$

where χ_G is the characteristic function of G . Therefore, $C_{2,1} \leq K(\frac{1}{2}, 1)$.

At the point $(0, 1)$ we use the above estimate to get

$$(3.5) \quad \|\mathcal{F}v\|_1 \leq |G|^{\frac{1}{2}} \|v\|_2 \leq |G|^{\frac{1}{2}} \|v\|_\infty \|\chi_G\|_2 = |G| \|v\|_\infty,$$

so $C_{\infty,1} \leq K(0, 1)$.

And finally at the point $(0, \frac{1}{2})$ we have

$$(3.6) \quad \|\mathcal{F}v\|_2 = \|v\|_2 \leq |G|^{\frac{1}{2}} \|v\|_{\infty},$$

so $C_{\infty,2} \leq K(0, \frac{1}{2})$, what ends the proof. □

We close this section with a remark that Proposition 3.1 still holds if we replace the matrix of characters by any complex valued Hadamard matrix.

4. The lower bound $C_{p,q} \geq K(\frac{1}{p}, \frac{1}{q})$

We shall prove

PROPOSITION 4.1. — $C_{p,q} \geq K(\frac{1}{p}, \frac{1}{q})$.

Proof. — We will exhibit functions v such that $\|\mathcal{F}v\|_q = K(\frac{1}{p}, \frac{1}{q})\|v\|_p$. This can be easily done for regions R_F and R_T that are given in (2.1) and (2.2). Indeed, for R_F the characters $\gamma \in \hat{G}$ maximize the norm since

$$\|\mathcal{F}\gamma\|_q = |G|^{\frac{1}{2} - \frac{1}{p}} \|\gamma\|_p = K\left(\frac{1}{p}, \frac{1}{q}\right) \|\gamma\|_p.$$

In a similar fashion, the delta functions $\delta_g, g \in G$ are extremals for the norm in R_T because

$$\|\mathcal{F}\delta_g\|_q = |G|^{\frac{1}{q} - \frac{1}{2}} \|\delta_g\|_p = K\left(\frac{1}{p}, \frac{1}{q}\right) \|\delta_g\|_p.$$

The most interesting region is R_{TF} where for any biunimodular function u defined in (1.1) we have

$$\|\mathcal{F}u\|_q = |G|^{\frac{1}{q} - \frac{1}{p}} \|u\|_p = K\left(\frac{1}{p}, \frac{1}{q}\right) \|u\|_p.$$

This allows us to end the proof of Proposition 3.1 as long as we accept the existence of biunimodular functions for any finite abelian group (see Theorem 4.7 below). □

There is a natural way to find at least some of the biunimodular functions. To see it, let us make few trivial observations about the extremals exhibited in the proof of Proposition 4.1. The characters clearly give rise to the frequency basis $\{|G|^{-\frac{1}{2}}\gamma : \gamma \in \hat{G}\}$. This orthonormal basis can be also written as $\{M_\gamma(|G|^{-\frac{1}{2}}\chi_G) : \gamma \in \hat{G}\}$, where M_γ is a modulation given by $M_\gamma f = \gamma f$. Similarly, the collection of delta functions forms the time basis $\{\delta_g : g \in G\}$ that can be also viewed as $\{T_g(\delta_e) : g \in G\}$ with T_g being the translation given by $T_g f = f(\cdot - g)$. Since in the region R_F the norm

is attained on the frequency basis and in R_T on the time basis, we can ask if the norm in the region R_{TF} is attained on some sort of time-frequency basis. This motivates the following.

DEFINITION 4.2. — We say that a function $u \in L^2(G)$ gives rise to a time-frequency basis if $\{T_g(|G|^{-\frac{1}{2}}u) : g \in G\}$ is an orthonormal basis that is equal to $\{c_\gamma M_\gamma(|G|^{-\frac{1}{2}}u) : \gamma \in \hat{G}\}$ with some constants $c_\gamma \in \mathbb{T}$.

In other words, we require that the translates of $|G|^{-\frac{1}{2}}u$ form an orthonormal basis and this basis is the same (up to some constants), as the one obtained by taking the modulations of $|G|^{-\frac{1}{2}}u$.

It is not hard to see that if u generates a time-frequency basis then it must be biunimodular. Indeed, it is enough to observe that the Fourier transform of a translation is a modulation of the Fourier transform, namely

$$(4.1) \quad \mathcal{F}T_{-g} = M_g\mathcal{F},$$

where the modulation M_g on the dual group is a multiplication by the character $g \in \hat{G} = G$ that is simply given by $g(\gamma) = \gamma(g)$. Then, the claim follows immediately from the basic lemma that we give below.

LEMMA 4.3. — A function $u \in L^2(G)$ is unimodular if and only if $\{M_\gamma(|G|^{-\frac{1}{2}}u) : \gamma \in \hat{G}\}$ is an orthonormal basis.

Proof. — If u is unimodular and $\gamma \neq \gamma'$ then

$$\langle M_\gamma u, M_{\gamma'} u \rangle = \langle \gamma, \gamma' \rangle = 0$$

and $\| |G|^{-\frac{1}{2}}u \|_2 = 1$, so the assertion follows.

On the other hand if modulations of u are orthonormal then for all $\gamma \in \hat{G} \setminus \{e\}$ we have

$$0 = \langle u, M_\gamma u \rangle = \langle |u|^2, \gamma \rangle$$

and, therefore, $|u|^2 = c\chi_G$ for some $c \in \mathbb{C}$. Since the orthonormality also implies that $c = 1$, we obtain that $|u| = \chi_G$. □

The above lemma and (4.1) give us also the following.

COROLLARY 4.4. — A function $u \in L^2(G)$ is biunimodular if and only if it is unimodular and $\langle u, T_g u \rangle = 0$ for all $g \in G \setminus \{e\}$.

This corollary provides the easiest way to check if a given function is biunimodular. For example, we can use it to see that the vector $[1, 1, 1, -1]$ is biunimodular on the cyclic group \mathbb{Z}_4 . This shows that, in general, a biunimodular function does not have to generate a time-frequency basis but rather two orthonormal bases (one given by translations and the other

by modulations). However, by restricting our attention to functions that generate a time-frequency basis we get a clean result for finite cyclic groups.

THEOREM 4.5. — *A function $u \in L^2(\mathbb{Z}_N)$ generates a time-frequency basis for the cyclic group \mathbb{Z}_N , $N \in \mathbb{N}$, if and only if for some constant $c \in \mathbb{T}$ we have that*

$$(4.2) \quad u(n) = ce^{\frac{2\pi i}{N}(\lambda n^2 + \mu n)} \quad n \in \mathbb{Z}_N, \quad N \text{ odd},$$

$$(4.3) \quad u(n) = ce^{\frac{2\pi i}{N}(\frac{\lambda}{2}n^2 + \mu n)} \quad n \in \mathbb{Z}_N, \quad N \text{ even},$$

where $\lambda, \mu \in \mathbb{Z}_N$ with λ relatively prime to N .

Proof. — Let us assume that u generates a time-frequency basis. Since u is unimodular we can write

$$u(n) = e^{2\pi i f(n)},$$

where f is a real-valued function and without the loss of generality we can assume that $f(0) = 0$. We know that $T_{-1}u = c' M_{\lambda'} u$ for some constant $c' \in \mathbb{T}$, where $\lambda' \in \mathbb{Z}_N \setminus \{0\}$ and $M_{\lambda'} u(n) = e^{\frac{2\pi i}{N} \lambda' n} u(n)$. This implies that for $n = 0, 1, \dots, N - 2$ we have

$$f(n + 1) - f(n) = \frac{\lambda' n}{N} + \nu \pmod{1},$$

where $\nu \in \mathbb{R}$. Therefore, for $n = 1, \dots, N - 1$ we obtain

$$f(n) = \sum_{k=0}^{n-1} \left(\frac{\lambda' k}{N} + \nu \right) = \frac{\lambda'}{N} \frac{n(n-1)}{2} + \nu n = \frac{\lambda'}{2N} n^2 + \frac{\mu' n}{N},$$

for some $\mu' \in \mathbb{R}$. Thus, we have that

$$u(n) = e^{\frac{2\pi i}{N}(\frac{\lambda'}{2}n^2 + \mu' n)},$$

for $n \in \mathbb{Z}_N$.

To restrict further the values of λ' and μ' we observe that

$$\begin{aligned} 0 = \langle T_{-1}u, u \rangle &= u(0)\overline{u(N-1)} + \sum_{n=0}^{N-2} u(n+1)\overline{u(n)} \\ &= \overline{u(N-1)} + \sum_{n=0}^{N-2} e^{\frac{2\pi i}{N}(\lambda' n + \frac{\lambda'}{2} + \mu')}. \end{aligned}$$

Since $\sum_{n=0}^{N-1} e^{\frac{2\pi i}{N} \lambda' n} = 0$, the above equality can be transformed into

$$(4.4) \quad e^{-\frac{2\pi i}{N} \mu' N} = e^{\frac{2\pi i}{N} \frac{\lambda'}{2} N^2}.$$

This forces us to consider few cases.

If N is even, then $e^{\frac{2\pi i}{N} \frac{\lambda'}{2} N^2} = 1$ and we conclude that $\mu' \in \mathbb{Z}_N$. Therefore, our function u is of the form (4.3) with $\lambda = \lambda'$ and $\mu = \mu'$.

If N is odd and λ' is even, then (4.4) yields the same conclusion, so u is of the form (4.2) with $\lambda = \frac{\lambda'}{2}$ and $\mu = \mu'$. In the case when N and λ' are odd we obtain that $e^{-\frac{2\pi i}{N} \mu' N} = -1$. This means that $\mu' = k + \frac{1}{2}$ for some integer k . In effect, a simple calculation shows that in this case u is of the form (4.2) with $\lambda = \frac{\lambda'+N}{2}$ and $\mu = k + \frac{N+1}{2}$.

It remains to check that λ and N must be relatively prime. Since formula (4.2) is N -periodic, for any $k \in \mathbb{Z}_N \setminus \{0\}$ we have that for N odd

$$\langle u, T_k u \rangle = e^{\frac{2\pi i}{N}(-\lambda k^2 + \mu k)} \sum_{n=0}^{N-1} e^{\frac{2\pi i}{N} 2\lambda k n}.$$

Therefore, using the geometric sum argument we see that $\langle u, T_k u \rangle = 0$ for all such k if and only if $e^{\frac{2\pi i}{N} 2\lambda k} \neq 1$, that is, λ is relatively prime to N .

If N is even, we use the N -periodicity of (4.3) to get

$$\langle u, T_k u \rangle = e^{\frac{2\pi i}{N}(-\frac{\lambda}{2} k^2 + \mu k)} \sum_{n=0}^{N-1} e^{\frac{2\pi i}{N} \lambda k n}.$$

Thus, $\langle u, T_k u \rangle = 0$ if and only if $e^{\frac{2\pi i}{N} \lambda k} \neq 1$, so again λ must be relatively prime to N .

To finish the proof we observe that u given by (4.2) or (4.3) generates a time-frequency basis. Indeed, since we proved already via geometric sum argument that the translates of such u form an orthogonal basis, it is enough to notice that for $k \in \mathbb{Z}_N$ we have

$$\begin{aligned} T_k u &= e^{\frac{2\pi i}{N}(\lambda k^2 - \mu k)} M_{-2\lambda k} u, & N\text{- odd;} \\ T_k u &= e^{\frac{2\pi i}{N}(\frac{\lambda}{2} k^2 - \mu k)} M_{-\lambda k} u, & N\text{- even.} \end{aligned}$$

□

In this way we arrive to the classical example of biunimodular functions. The first to stumble upon them was Gauss. His proof of constructibility of some regular polygons (for example, the 17-sided polygon) was based on calculating certain sums of roots of unity. More precisely, the roots that are given by (4.2) with $c, \lambda = 1$ and $\mu = 0$. That is why a function of the form given in (4.2) or (4.3) is called a *Gauss sequence*. We warn the reader not to misinterpret formula (4.3). Although we consider $\lambda \in \mathbb{Z}_N$, clearly, λ and $\lambda + N$ do not yield the same u via (4.3). This, however, does not pose a problem, since $e^{\frac{2\pi i}{N} \frac{\lambda+N}{2} n^2} = e^{\frac{2\pi i}{N} (\frac{\lambda}{2} n^2 + \frac{N}{2} n)}$ for even N .

Gauss sequences can be used to generate a time-frequency basis on any finite abelian group. It turns out that the most natural idea, that is, construction via tensor products, works without any difficulties. In fact, we have the following

LEMMA 4.6. — *If a function w is biunimodular on a group G and v is biunimodular on a group H , then the function u given for $g \in G$ and $h \in H$ by $u(g, h) = w(g)v(h)$ is biunimodular on the product group $G \times H$. Moreover, if both w and v generate a time-frequency basis, then so does u .*

Proof. — The proof relies completely on the fact that $\widehat{G \times H} = \hat{G} \times \hat{H}$. Let \mathcal{F} be the Fourier transform on $G \times H$. Since for $(\gamma, \eta) \in \hat{G} \times \hat{H}$ we have that

$$\mathcal{F}u(\gamma, \eta) = \sum_{g, h \in G \times H} u(g, h) \overline{\gamma(g)\eta(h)} = \langle w, \gamma \rangle \langle v, \eta \rangle,$$

we see immediately that if w and v are biunimodular, then so is u .

Moreover, if both w and v generate a time-frequency basis, then for $(g, h) \in G \times H$ we have that $T_g w = c_\gamma M_\gamma w$ and $T_h v = c_\eta M_\eta v$ for some characters $(\gamma, \eta) \in \hat{G} \times \hat{H}$ and some constants $c_\gamma, c_\eta \in \mathbb{C}$. This implies that

$$T_{(g', h')} u = c_\gamma c_\eta M_{(\gamma, \eta)} u$$

and since we know already that u is biunimodular, the above suffices to conclude that u generates a time-frequency basis. □

Using the fact that any finite abelian group is a product of cyclic groups, Lemma 4.6 allows us to obtain the following.

THEOREM 4.7. — *For any finite abelian group there exists a biunimodular function. Moreover, this function can be chosen in such a way that it generates a time-frequency basis.*

This ends the proof of Theorem 2.1 and allows us for a coherent presentation of the extremals of the Fourier transform that we used in the proof (see Fig. 4.1).

By duality, we can restate Theorem 2.1 to include the lower bound for $\|\mathcal{F}v\|_q$ as well.

THEOREM 4.8. — *For arbitrary $1 \leq p, q \leq \infty$ and any $v \in L^p(G)$ we have*

$$(4.5) \quad C_{q,p}^{-1} \|v\|_p \leq \|\mathcal{F}v\|_q \leq C_{p,q} \|v\|_p,$$

with sharp constants $C_{p,q}$ that are given in Theorem 2.1.

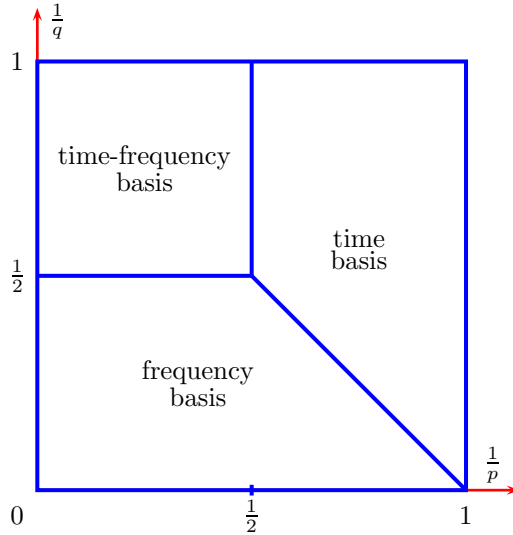


Figure 4.1. Basic extremal functions.

Proof. — The right hand side inequality of (4.5) was proved in Theorem 2.1, thus we only have to show the other inequality.

Let \mathcal{F}^* be the dual operator and $C_{p,q}^*$ be its norm. The standard duality argument gives us that $C_{p,q} = C_{q',p'}^*$ for $1 \leq p, q \leq \infty$ and $\frac{1}{p} + \frac{1}{p'} = 1$, $\frac{1}{q} + \frac{1}{q'} = 1$. Moreover, it is easy to check that $C_{p,q}$ from Theorem 2.1 satisfies $C_{p,q}^* = C_{q',p'}$. Therefore, we can conclude that $C_{p,q}^* = C_{p,q}$. This implies that for any $v \in L^p(G)$ we have

$$\|v\|_p = \|\mathcal{F}^* \mathcal{F}v\|_p \leq C_{q,p} \|\mathcal{F}v\|_q,$$

what shows that the left hand side inequality of (4.5) holds and is sharp. \square

In the following section we shall give a full characterization of the functions where the norm of the Fourier transform is attained.

5. Characterization of the extremals of the Fourier transform

For arbitrary $1 \leq p, q \leq \infty$ we define the set of extremals for the Fourier transform \mathcal{F} at the point (p, q) by

$$(5.1) \quad E_{p,q} = \{v \in L^p(G) : \|\mathcal{F}v\|_q = C_{p,q} \|v\|_p\},$$

where $C_{p,q}$ is the norm of \mathcal{F} that is given in Theorem 2.1.

Most of the extremals can be easily characterized by studying the inequalities from Proposition 3.1. The only difficulty is posed by the classical values of p, q that correspond to the Hausdorff-Young inequality. Of course, if we multiply an element of $E_{p,q}$ by a constant we obtain another element of $E_{p,q}$. Therefore, we shall characterize $E_{p,q}$ up to a constant.

THEOREM 5.1. — For $(\frac{1}{p}, \frac{1}{q}) \in [0, 1]^2$ we have that up to a constant

$$E_{p,q} = \left\{ \begin{array}{ll} \text{frequency basis} & \text{for } \frac{1}{p} + \frac{1}{q} < 1, \frac{1}{q} < \frac{1}{2} \quad (5.2) \\ \text{time basis} & \text{for } \frac{1}{p} + \frac{1}{q} > 1, \frac{1}{p} > \frac{1}{2} \quad (5.3) \\ \text{biunimodular functions} & \text{for } \frac{1}{p} < \frac{1}{2}, \frac{1}{q} > \frac{1}{2} \quad (5.4) \\ \{v \in L^p(G) : |v| = 1\} & \text{for } \frac{1}{p} < \frac{1}{2}, \frac{1}{q} = \frac{1}{2} \quad (5.5) \\ \{v \in L^p(G) : |\mathcal{F}v| = 1\} & \text{for } \frac{1}{p} = \frac{1}{2}, \frac{1}{q} > \frac{1}{2} \quad (5.6) \\ \{v \in L^p(G) : v = \gamma|v|, \gamma \in \hat{G}\} & \text{for } \frac{1}{p} = 1, \frac{1}{q} = 0 \quad (5.7) \\ L^2(G) & \text{for } \frac{1}{p} = \frac{1}{2}, \frac{1}{q} = \frac{1}{2} \quad (5.8) \\ \{M_\gamma T_g \chi_H : g \in G, \gamma \in \hat{G} \text{ and } H \subseteq G\} & \text{for } \frac{1}{p} + \frac{1}{q} = 1, \frac{1}{2} < \frac{1}{p} < 1 \quad (5.9) \end{array} \right.$$

Proof. — To show (5.2) we observe that (3.1) becomes equality if and only if $|\langle v, \gamma \rangle| = \|v\|_\infty \|\gamma\|_1$, that is, when v is a constant multiple of γ . Therefore, if v is not of this form, we can use Riesz-Thorin convexity theorem for the one-dimensional space V generated by v to see that such function can not belong to $E_{p,q}$ for the values of p, q listed in (5.2). Since we showed already in Proposition 4.1 that the characters are extremal for the region R_F given in (2.1), we see that (5.2) holds.

In a similar fashion we can use (3.3) to get (5.3). Indeed, (3.3) is based on the triangle inequality for the norm $\|\cdot\|_1$. Since for $g \in G$ the functions $\mathcal{F}\delta_g$ are linearly independent, the equality in (3.3) holds if and only if v is a delta function. Therefore, the convexity theorem and Proposition 4.1 give us (5.3).

By inspecting (3.5), that is based on (3.4), we see that the former becomes an equality if and only if $|\mathcal{F}v|$ and $|v|$ are constant. Thus, (5.4) follows as before from the convexity theorem and a calculation included in the proof of Proposition 4.1.

It is easy to check that the functions given in (5.5) and (5.6) are extremal for the indicated values of p and q . We can use (3.4) to get (5.6) and (3.6) to get (5.5) by inspecting these inequalities in a similar way we inspected (3.5) and using the convexity theorem.

Similarly, (5.7) follows from (3.2) and since (5.8) is obvious, we are only left with (5.9). The simple interpolation argument, that we were using so far, breaks down in this case. It allows us only to conclude that the extremals for $1 < p < 2$ and $q = p'$ must be of the form given in (5.7). It turns out, however, that not all functions given in (5.7) will pinpoint the norm for $1 < p < 2$ and $q = p'$. These particular values of p and q are exactly the case of the original Hausdorff-Young inequality and we shall use Young's ideas to show (5.9).

We can still apply the convexity theorem, as soon as we show that the functions given in (5.9) are the only extremals for $p = \frac{4}{3}$ and $q = 4$. We have

$$(5.10) \quad \|\mathcal{F}v\|_4 = \|\mathcal{F}v\mathcal{F}v\|_2^{\frac{1}{2}} = \|\mathcal{F}^*(\mathcal{F}v\mathcal{F}v)\|_2^{\frac{1}{2}} = |G|^{-\frac{1}{4}}\|v * v\|_2^{\frac{1}{2}},$$

where “ $*$ ” denotes the convolution and we have used that $\mathcal{F}^*(vw) = |G|^{-\frac{1}{2}}(\mathcal{F}^*v) * (\mathcal{F}^*w)$. Young's inequality (see (5.12) below) allows us to conclude that

$$(5.11) \quad \|v * v\|_2 \leq \|v\|_{\frac{4}{3}}^2.$$

Therefore, (5.10) yields a familiar estimate

$$\|\mathcal{F}v\|_4 \leq |G|^{-\frac{1}{4}}\|v\|_{\frac{4}{3}},$$

that is simply a special case of Theorem 2.1. The theorem assures that the norm of \mathcal{F} is equal to $|G|^{-\frac{1}{4}}$ for $p = \frac{4}{3}$ and $q = 4$. Thus, if we want to find the extremals corresponding to these values of p and q , it is enough to check when (5.11) becomes an equality. To keep our discussion simple, we shall use our previous remark and assume that the extremal v is of the form given in (5.7). This allows us to concentrate on a non-negative v whose support contains the neutral element of the group G , since the set of extremals at any point (p, q) is invariant under modulations and translations. It turns out that for such v , (5.11) becomes an equality if and only if v is a characteristic function of a subgroup H of G . We shall prove

this fact in Lemma 5.2 below. For now, let us finish the proof of the theorem by checking that the norm of \mathcal{F} is attained on functions given in (5.9).

Recall that for any subgroup $H \subseteq G$ we have that $\mathcal{F}(\chi_H) = |H||G|^{-\frac{1}{2}}\chi_{H^\perp}$ and $|H||H^\perp| = |G|$. Therefore, for p and q as in (5.9), we have

$$\begin{aligned} \|\mathcal{F}(\chi_H)\|_q &= |H||G|^{-\frac{1}{2}}\|\chi_{H^\perp}\|_q = |H||G|^{-\frac{1}{2}}|H^\perp|^{\frac{1}{q}} \\ &= |G|^{\frac{1}{q}-\frac{1}{2}}|H|^{\frac{1}{p}} = C_{p,q}\|\chi_H\|_p, \end{aligned}$$

where $C_{p,q}$ is the norm calculated in Theorem 2.1. Since the set of extremals at any point (p, q) is invariant under modulations and translations, we easily conclude that the functions given in (5.9) indeed yield the norm of \mathcal{F} in the specified range of p and q . \square

Although our setting is discrete, the relationship between the extremals for Young’s inequality and those for the Fourier transform with $1 < p < 2$ and $q = p'$ is pretty much the same as in the case of the real line. We shall not pursue this relationship to its full generality. Instead, we will concentrate on facts that are needed to close the proof of the above theorem.

The convolution operator “ $*$ ” on our group G is given by

$$u * v(x) = \sum_{y \in G} u(x - y)v(y),$$

where u and v are complex-valued functions on G . The basic interplay between the convolution and the Fourier transform is given by

$$\mathcal{F}(u * v) = |G|^{\frac{1}{2}}\mathcal{F}u\mathcal{F}v \quad \text{and} \quad \mathcal{F}(uv) = |G|^{-\frac{1}{2}}\mathcal{F}u * \mathcal{F}v.$$

Young’s inequality

$$(5.12) \quad \|u * v\|_r \leq \|u\|_p\|v\|_q$$

holds for $1 \leq p, q, r \leq \infty$ whenever $\frac{1}{p} + \frac{1}{q} = \frac{1}{r} + 1$. Since we want to see when the above inequality becomes an equality, we need to go over the proof of this estimate. One of the ways to show (5.12) is based on Hölder inequality (for three functions)

$$(5.13) \quad \|fgh\|_1 \leq \|f\|_a\|g\|_b\|h\|_c,$$

where $1 \leq a, b, c \leq \infty$ and $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$. Here, the equality holds if and only if there is a function ψ and constants c_1, c_2, c_3 such that $|f|^a = c_1\psi$, $|g|^b = c_2\psi$ and $|h|^c = c_3\psi$. In order to prove (5.12) we write

$$|u(x - y)v(y)| = f(y)g(y)h(y),$$

where $f(y) = |u(x - y)|^{1-\frac{p}{r}}$, $g(y) = |u(x - y)|^{\frac{p}{r}}|v(y)|^{\frac{q}{r}}$ and $h(y) = |v(y)|^{1-\frac{q}{r}}$. Then we apply (5.13) with $\frac{1}{a} = \frac{1}{p} - \frac{1}{r}$, $\frac{1}{b} = \frac{1}{r}$ and $\frac{1}{c} = \frac{1}{q} - \frac{1}{r}$. In this way we obtain an estimate on $|u * v(x)|$. Raising this estimate to the power r

and summing over G yields Young's inequality. Therefore, we can not have an equality in (5.12) unless we have an equality in (5.13). That is, for each $x \in G$, the following proportionality condition must be satisfied

$$(5.14) \quad |u(x-y)|^p = c_1\psi(y), \quad |u(x-y)|^p|v(y)|^q = c_2\psi(y) \quad \text{and} \quad |v(y)|^q = c_3\psi(y),$$

with constants c_1 , c_2 and c_3 that depend on x and some function ψ that depends on x as well.

This observation allows us to prove the following

LEMMA 5.2. — *Let v be a non-negative function on a finite abelian group G , whose support contains the neutral element e . Then*

$$\|v * v\|_2 = \|v\|_{\frac{4}{3}}^2,$$

if and only if $v = \beta\chi_H$ for some subgroup $H \subseteq G$ and a positive constant β .

Proof. — If $v = \chi_H$, then $v * v = |H|\chi_H$ and the assertion follows. Of course, we are really interested in the other implication. Clearly, what we assume is that we have an equality in (5.12) with $r = 2$, $p = q = \frac{4}{3}$ and $u = v$. As we already observed, this implies that the proportionality condition (5.14) must be satisfied. Since in our case $p = q$ and v is non-negative, we may assume that

$$(5.15) \quad v(x-y) = c_1\psi(y), \quad v(x-y)v(y) = c_2\psi(y) \quad \text{and} \quad v(y) = c_3\psi(y).$$

The whole difficulty lies in the fact that the constants c_1 , c_2 and c_3 depend on x and can be equal to zero. That is why we shall consider the following set

$$A = \{x \in G : v(x-y)v(y) = 0 \text{ for all } y \in G\}$$

and its complement $B = G \setminus A$. Since we can take $x = y = e$, we see that B is non-empty. Let us fix an $x \in B$. By definition, $v(x-\cdot)v(\cdot) \not\equiv 0$. This implies that $v(x-\cdot) \not\equiv 0$ and we already assumed that $v \not\equiv 0$. Therefore, none of the constants c_1 , c_2 and c_3 in (5.15) is equal to zero. This allows us to transform (5.15) into

$$(5.16) \quad v(x-y)v(y) = \alpha v(y),$$

$$(5.17) \quad v(x-y)v(y) = \beta v(x-y)$$

and

$$(5.18) \quad v(x-y) = \gamma v(y),$$

where α , β and γ are non-zero constants that depend on x .

Let H be the support of v . To show that $v = \beta\chi_H$, we observe that (5.16) implies that $v(x - y) \neq 0$ for all $y \in H$ (we still keep x fixed in B). This, however, together with (5.17) allows us to conclude that $v(y) = \beta$ for all $y \in H$. Thus, up to a constant, v is a characteristic function of H .

The last step is to show that H is a subgroup of G . First, we shall see that $H = B$. Let us consider an arbitrary $x \in B$. By (5.18) we get that $y \in H$ if and only if $x - y \in H$. Thus, $H = -H + x$. Since H contains the neutral element e , we see that $e = -h + x$ for some $h \in H$. Therefore, $x \in H$ and we get that $B \subset H$. On the other hand, if x is an arbitrary element of H , then $v(x - y)v(y) \neq 0$ for $y = e$. Thus, $x \in B$ and we get the other inclusion $H \subset B$.

We observed already that $H = -H + x$ whenever $x \in B$. Since $B = H$, we can take $x = e$ in order to get that $H = -H$. All of this tells us also that $H = H + x$ for all $x \in H$. Therefore, H is a subgroup of G . \square

The extremals exhibited in Theorem 5.1 should be placed on the Riesz square to visualize their dependence on the values of p and q (see Fig. 5.1).

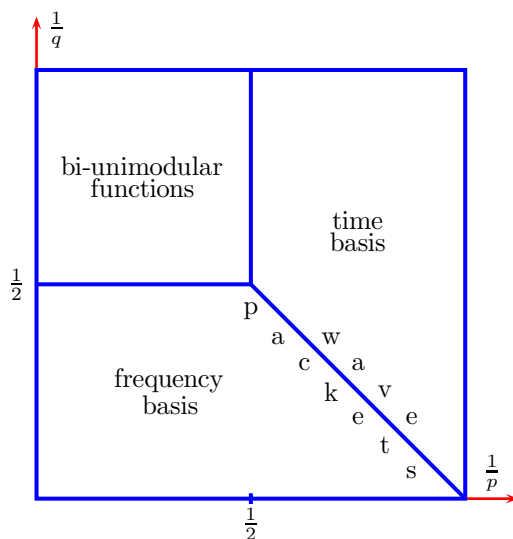


Figure 5.1. Characterization of extremal functions.

The most interesting extremals are biunimodular functions and those given in (5.9), that we call *wave packets*. With a little dose of good will, we can think that both of these occur in the range of p and q where “time meets frequency”. In fact, in light of (5.2) and (5.3) we can treat region R_F

given in (2.1) as the “frequency region” and the region R_T from (2.2) as the “time region”. In the following sections we present the further study of these extremals, that shall reveal the role they play in the time-frequency analysis.

6. Wave Packets

The extremals given in (5.9) are simply the characters restricted to the cosets of subgroups of G . Let us normalize them in the $\|\cdot\|_2$ -norm and make the following formal

DEFINITION 6.1. — *If G is a finite abelian group, then the elements of the set*

$$\{|H|^{-\frac{1}{2}} M_\gamma T_g \chi_H : g \in G, \gamma \in \hat{G} \text{ and } H \subseteq G\}$$

are called wave packets.

Remark. — To get the uniqueness (up to a constant) one should think that $g \in G/H$ and $\gamma \in \hat{G}/H^\perp$.

The importance of wave packets comes from the fact that they minimize Heisenberg Uncertainty Principle. In our setting, the principle takes the following form

THEOREM 6.2. — *Let v be a function on a finite abelian group G with the support K . If L is the support of the Fourier transform of v , then*

$$(6.1) \quad |G| \leq |K||L|.$$

Proof. — In order to show (6.1) we shall apply two inequalities that relate the norm of v to the norm of its average over the support, namely $v_a := \|v\|_2 |K|^{-\frac{1}{2}} \chi_K$ (as we see, the average is supported on K and has the same $\|\cdot\|_2$ -norm as v). It turns out that for $1 \leq p \leq 2$ we have

$$(6.2) \quad \|v\|_p \leq \|v_a\|_p,$$

while for $2 \leq q \leq \infty$ we have the opposite

$$(6.3) \quad \|v\|_q \geq \|v_a\|_q.$$

Clearly, (6.2) is nothing else than

$$(6.4) \quad \|v\|_p \leq |K|^{\frac{1}{p} - \frac{1}{2}} \|v\|_2$$

and (6.3) is simply

$$(6.5) \quad \|v\|_q \geq |K|^{\frac{1}{q} - \frac{1}{2}} \|v\|_2,$$

where $1 \leq p \leq 2 \leq q \leq \infty$. To see why these estimates hold it is enough to apply Hölder’s inequality. Indeed, we have

$$\|v\|_p^p = \|\chi_K |v|^p\|_1 \leq \|\chi_K\|_{\frac{2}{2-p}} \| |v|^p \|_{\frac{2}{p}} = |K|^{1-\frac{p}{2}} \|v\|_2^p,$$

what shows (6.4). Similarly,

$$\|v\|_2^2 = \|\chi_K |v|^2\|_1 \leq \|\chi_K\|_{\frac{q}{q-2}} \| |v|^2 \|_{\frac{q}{2}} = |K|^{1-\frac{2}{q}} \|v\|_q^2,$$

thus (6.5) follows as well.

To show (6.1) we apply (6.5) to the Fourier transform of v , (6.4) to v and Theorem 2.1 with $1 < p < 2$ and $q = p'$

$$(6.6) \quad |L|^{\frac{1}{q}-\frac{1}{2}} \|\mathcal{F}v\|_2 \leq \|\mathcal{F}v\|_q \leq |G|^{\frac{1}{q}-\frac{1}{2}} \|v\|_p \leq |G|^{\frac{1}{q}-\frac{1}{2}} |K|^{\frac{1}{p}-\frac{1}{2}} \|v\|_2.$$

Since $\frac{1}{p} - \frac{1}{2} = \frac{1}{2} - \frac{1}{q} > 0$ and $\|\mathcal{F}v\|_2 = \|v\|_2$, the above inequality yields (6.1) immediately. \square

As we observed, the discrete Heisenberg Uncertainty Principle can be treated as a quick consequence of our main result. However, it has to be mentioned that considering $p = \frac{4}{3}$ in (6.6) is sufficient to conclude (6.1) simply by using the familiar estimate $\|\mathcal{F}v\|_4 \leq |G|^{-\frac{1}{4}} \|v\|_{\frac{4}{3}}$ that has already appeared in the proof of Theorem 5.1.

Clearly, the equality in (6.1) can hold only if we have equalities in (6.6). From (5.9) it follows, that this can happen only if v is a wave packet (up to a constant). On the other hand, an easy calculation shows that if $v = M_\gamma T_g \chi_H$ for a subgroup H , then

$$(6.7) \quad \text{supp } v = H + g \quad \text{and} \quad \text{supp } \mathcal{F}v = \gamma H^\perp$$

Indeed, we can use (4.1) and the relationship $\mathcal{F}M_\gamma = T_\gamma \mathcal{F}$ to establish (6.7). Thus, for such v we get $|\text{supp } v| |\text{supp } \mathcal{F}v| = |H| |H^\perp| = |G|$. In this way we obtain the following

COROLLARY 6.3. — *The only functions that minimize Heisenberg Uncertainty Principle given in (6.1) are wave packets (up to a constant).*

Theorem 6.2 and the above corollary generalize findings of Donoho and Stark.⁽¹⁾ In [17] the case of the cyclic group \mathbb{Z}_N was treated and wave packets were called “picket fence” sequences. The nomenclature we use comes from physics, where the name “wave packets” is reserved for functions that are well localized in time and frequency. In the continuous case (on the real line) wave packets are defined by modulations, translations and dilations of

⁽¹⁾ An interested reader can see [33] for other proofs of Theorem 6.2 and Corollary 6.3. Also, if $G = \mathbb{Z}_p$, where p is prime, then one has $|G| + 1 \leq |K| + |L|$ (with notation as in Theorem 6.2) as proved recently by Tao in [42].

a Gaussian. The latter can be replaced by a smooth, compactly supported function to obtain a better time localization. These wave packets attracted attention in harmonic analysis after they were used by Fefferman in his proof of the a.e. convergence of Fourier series (see [18]). It turned out, that the attention was well deserved, because the wave packets appeared also in Lacey and Thiele’s proof of the boundedness of the bilinear Hilbert transform (see [26] and [27]). Wave packets on finite abelian groups were briefly treated by Thiele and Villemoes in [43]. The discrete scenario is not only a good training ground, where the intuitions needed for the more difficult continuous case can develop, it is also an interesting topic by itself. The underlying idea that makes wave packets useful is that we can assign to them “tiles”, that is, rectangles in the time-frequency plane. If v is a wave packet as in Definition 6.1, then the corresponding tile is

$$P_v := \text{supp } v \times \text{supp } \mathcal{F}v \subset G \times \hat{G}.$$

Conversely, if H is a subgroup of G and $P = (H + g) \times (\gamma H^\perp)$ for $g \in G$, $\gamma \in \hat{G}$, then the associated wave packet is

$$v_P := |H|^{-\frac{1}{2}} M_\gamma T_g \chi_H.$$

Moreover, by (6.7) and Corollary 6.3, v_P is the only function (up to a constant) such that $\text{supp } v_P \times \text{supp } \mathcal{F}(v_P) = P$. In this way, wave packets can be viewed as tiles, where the collection of tiles is given by

$$(6.8) \quad \mathbb{P} := \{P = (H + g) \times (\gamma H^\perp) : H \subseteq G, g \in G, \gamma \in \hat{G}\}.$$

The whole advantage of this approach is that we can start using geometric properties of these tiles for various arguments and constructions. This geometric connection can be seen in the following

PROPOSITION 6.4. — *If P and Q are tiles and v_P, v_Q are the corresponding wave packets on a finite abelian group G then*

$$(6.9) \quad |\langle v_P, v_Q \rangle| = |P \cap Q|^{\frac{1}{2}} |G|^{-\frac{1}{2}},$$

where $|P \cap Q|$ is the counting measure of the intersection of P and Q .

Proof. — Let $P = (H + g) \times (\gamma H^\perp)$ and $Q = (K + g') \times (\gamma' K^\perp)$ as in (6.8). Since $\langle v_P, v_Q \rangle = \langle \mathcal{F}v_P, \mathcal{F}v_Q \rangle$, from (6.7) it follows that if $P \cap Q = \emptyset$ then $\langle v_P, v_Q \rangle = 0$. Therefore, we can assume that $P \cap Q \neq \emptyset$.

To simplify our argument, we observe that $|(H + g) \cap (K + g')| = |H \cap (K + g' - g)|$, $|(\gamma H^\perp) \cap (\gamma' K^\perp)| = |H^\perp \cap (\gamma^{-1} \gamma' K^\perp)|$ and $|\langle v_P, v_Q \rangle| = | \langle |H|^{-\frac{1}{2}} \chi_H, |K|^{-\frac{1}{2}} \gamma^{-1} \gamma' \chi_{K+g'-g} \rangle |$. Thus, it is enough to show (6.9) for $P = H \times H^\perp$ and $Q = (K + g) \times (\gamma K^\perp)$.

From $P \cap Q \neq \emptyset$ it follows that $H \cap (K + g) \neq \emptyset$ and $H^\perp \cap (\gamma K^\perp) \neq \emptyset$. Therefore, we see that $K + g = K + h$ for some $h \in H$ and $\gamma K^\perp = \eta K^\perp$ for some $\eta \in H^\perp$. This allows us to make another reduction. Since

$$\begin{aligned} |H \cap (K + h)| &= |(H \cap K) + h| = |H \cap K|, \\ |H^\perp \cap (\eta K^\perp)| &= |(H^\perp \cap K^\perp)\eta| = |H^\perp \cap K^\perp|, \end{aligned}$$

and

$$\begin{aligned} |\langle v_P, v_Q \rangle| &= |(|H|^{-\frac{1}{2}} \chi_H, |K|^{-\frac{1}{2}} \eta \chi_{K+h})| \\ &= |(|H|^{-\frac{1}{2}} \eta^{-1} \chi_{H-h}, |K|^{-\frac{1}{2}} \chi_K)| = |(|H|^{-\frac{1}{2}} \chi_H, |K|^{-\frac{1}{2}} \chi_K)|, \end{aligned}$$

it suffices to prove (6.9) for $Q = K \times K^\perp$ (and $P = H \times H^\perp$).

The remaining calculation is straightforward

$$(6.10) \quad \langle v_P, v_Q \rangle = |H|^{-\frac{1}{2}} |K|^{-\frac{1}{2}} |H \cap K|$$

and

$$|P \cap Q| = |H \cap K| |H^\perp \cap K^\perp| = |H \cap K| |(H + K)^\perp| = |H \cap K| |H + K|^{-1} |G|,$$

so

$$(6.11) \quad |P \cap Q|^{\frac{1}{2}} |G|^{-\frac{1}{2}} = |H \cap K|^{\frac{1}{2}} |H + K|^{-\frac{1}{2}}.$$

Combining (6.10) and (6.11) with the familiar formula $|H \cap K| |H + K| = |H| |K|$ yields (6.9). \square

The above proposition implies immediately that $\langle v_P, v_Q \rangle = 0$ if and only if $P \cap Q = \emptyset$. Therefore, a simple dimension counting argument allows us to conclude the following basic result concerning tiles and wave packets.

THEOREM 6.5. — *Let G be a finite abelian group and \mathbb{P} be the corresponding set of tiles given in (6.8). A collection of wave packets $\{v_P : P \in \mathcal{P} \subset \mathbb{P}\}$ is an orthonormal basis of $L^2(G)$ if and only if \mathcal{P} tiles the time-frequency plane, that is,*

$$\bigcup_{P \in \mathcal{P}} P = G \times \hat{G}$$

and the union is disjoint.

This fundamental observation allows for treating the collection of all wave packets as a library of orthonormal bases. It also rises a serious issue in signal analysis: “Is the commonly applied discrete Fourier analysis only a glimpse of the more powerful wave packet analysis?”. Of course, the popular DFT (Discrete Fourier Transform) is a part of the wave packet analysis. Moreover, in [43] we find an argument that FFT (Fast Fourier Transform) follows easily from observing simple relations between wave packets. The

mentioned paper contains also a fast algorithm that allows for finding the “best basis” suited for a given signal. The idea of such an algorithm comes from the work of Coifman, Meyer and Wickerhauser (see [13] and [14]). For a given function in $L^2(G)$ one wants to find an orthonormal basis consisting of wave packets, as in Theorem 6.5, so that the cost of the expansion of the function in this basis is the lowest. The cost may be imposed in many ways. For example, it can be defined as the $\| \cdot \|_1$ -norm of the sequence of the coefficients in the expansion. In this way, bases yielding few large coefficients are favored. An interested reader can see [22] or [25] to find out how these ideas work in practice.

We would like to close this section by discussing briefly an application of wave packets for constructing biunimodular functions.

THEOREM 6.6. — *Let G be a finite abelian group of order N^2 with a subgroup H of order N . If $\{g_n\}_{n=1}^N$ are the representants of the distinct cosets of G/H and $\{\gamma_n\}_{n=1}^N$ are the representants of the distinct cosets of \hat{G}/H^\perp , then the function*

$$(6.12) \quad \sum_{n=1}^N c_n \gamma_n \chi_{H+g_n}$$

is biunimodular for any choice of a unimodular sequence $\{c_n\}_{n=1}^N$.

Proof. — Let us denote the function given in (6.12) by u . Since $\bigcup_{n=1}^N (H+g_n) = G$ and the union is disjoint, we get that u is unimodular. To see that so is $\mathcal{F}u$, we notice that $|H| = |H^\perp|$, since $|G| = N^2$. Thus, using (4.1) and $\mathcal{F}M_\gamma = T_\gamma \mathcal{F}$, we obtain that

$$\mathcal{F}M_\gamma T_g \chi_H = T_\gamma M_{-g} \mathcal{F} \chi_H = \gamma(g) M_{-g} T_\gamma \chi_{H^\perp}$$

for any $g \in G$ and $\gamma \in \hat{G}$ (in general, the Fourier transform of a wave packet is, up to a constant, a wave packet on the dual group). Therefore,

$$\mathcal{F}u = \sum_{n=1}^N c_n \gamma_n(g_n) M_{-g} \chi_{\gamma_n H^\perp}$$

and since we assume that the disjoint union $\bigcup_{n=1}^N \gamma_n H^\perp$ covers \hat{G} , we see that $\mathcal{F}u$ is unimodular as well. □

The above theorem, in the cyclic case, yields the same construction of biunimodular functions as in [8]. The paper presents also a more general procedure, that works for a cyclic group whose order is divisible by N^2 . We are aware of a more sophisticated way of constructing biunimodular functions via wave packets as well. However, its relationship to the result of [8] has to be still investigated.

As we have shown, biunimodular functions are characterized as the extremals of the Fourier transform in the “time-frequency” region of the Riesz square, namely R_{TF} . Therefore, they can be treated as discrete Gaussians. In the final section we shall see that a comprehensive understanding of these fundamental functions is, for now, impossible.

7. Biunimodular functions

The arguments we presented so far have revealed a simple structure. The norm of the Fourier transform on a finite abelian group can be calculated by using Riesz-Thorin convexity theorem and finding natural functions that pinpoint the norm. Characterizing such extremals is a little difficult only in the classical range of p and q that corresponds to the Hausdorff-Young inequality on the real line. Overcoming this obstacle yields wave packets that are a useful tool in time-frequency analysis. The theory of wave packets that is based on their connection to tiles can be further developed. Can we, however, hope for a similar good understanding of the other time-frequency extremals, that is, biunimodular functions? Unfortunately, although up to now everything was falling right in place, the situation complicates tremendously when we touch this final topic.

Of course, the basic question is: “How do they look like?” As we saw in Theorem 4.7, it is not hard to show that such functions exist for any finite abelian group. Since every such group is a product of cyclic groups, let us discuss what is known in the important cyclic case.

To see the complexity of the problem, let us consider the “easy” scenario of a biunimodular function u with real coefficients on a cyclic group \mathbb{Z}_N . Here, the situation is nice because at least there is a conjecture about the appearance of such u . As soon as we realize that the coefficients of u must be either 1 or -1 and use Corollary 4.4, we discover that the form all such functions u can take is described in the circulant Hadamard matrix conjecture. Indeed, a Hadamard matrix is a square matrix with entries 1 or -1 , that becomes unitary after normalization. The matrix is called circulant if its rows are consecutive translations of a given vector. Therefore, by the mentioned corollary, there is no difference between discussing circulant Hadamard matrices or real biunimodular vectors⁽²⁾ on cyclic groups. The conjecture is that, excluding the trivial case $N = 1$, there is only one such

⁽²⁾ We remind the reader that, depending on a context, we either use the name “biunimodular function” or “biunimodular vector”.

matrix (up to an obvious equivalence). In our language this statement can be formulated as follows.

CONJECTURE 7.1. — *If u is a real biunimodular vector on \mathbb{Z}_N , for $N \geq 2$, then $N = 4$ and u is a translation of the vector $\pm[1, 1, 1 - 1]$.*

The hypothesis was published by Ryser in 1963 (see [37]). Its simplicity is deceiving. The problem is one of the most intriguing in the difficult theory of difference sets. It has a couple of generalizations within the theory, namely Ryser's conjecture and Lander's conjecture (see [28]). Recently, a substantial progress towards confirming this conjecture was made by Schmidt. Let us list some basic facts first. If u is a real biunimodular vector on \mathbb{Z}_N and $N \geq 2$, then N must be even. Otherwise, there is no chance that u can be orthogonal to its translation (the product of u and Tu must have equal amount of 1's and -1 's). Moreover, $\mathcal{F}u$ is unimodular, so the inner product of u and the trivial character must have modulus equal to \sqrt{N} . Since the inner product is an integer, we see that N must be a square. Therefore, we may assume that $N = 4n^2$, for some $n \in \mathbb{N}$. The first non-trivial observation was made by Turyn, who showed that n must be odd (see [44]). He also proved that if n is divisible by a prime p that is self-conjugate modulo n (that is, -1 is a power of p modulo the p -free part of n), then the conjecture is true. Few years ago Schmidt was able to confirm the conjecture for all $N \leq 10^{11}$, with three possible exceptions (see [39], [40]). This has greatly improved all previously known bounds for which the conjecture holds. In a recent paper [28] it is shown, that the conjecture is true if n is a power of a prime $p > 3$. Despite the continued effort, Conjecture 7.1 remains unsolved.

If we stay within the cyclic setting and drop the assumption that u is real, the matters are getting much worse. There is no conjecture describing the appearance of biunimodular vectors on cyclic groups. Clearly, Gauss sequences given in (4.2) and (4.3) are the classical example of such vectors. In 1983 Enflo have raised a question if Gauss sequences are the only biunimodular vectors on \mathbb{Z}_p , where p is a prime. For $p = 2$ and $p = 3$ easy calculations show that the answer is positive. An unpublished argument of Lovász shows that the same is true for $p = 5$ (see [20] for a different proof or [7] for a numerical confirmation of this fact). However, for $p = 7$ a computer search done by Björck resulted in a counterexample

$$(7.1) \quad [1, 1, 1, e^{i\theta}, 1, e^{i\theta}, e^{i\theta}],$$

where $\theta = \arccos(-\frac{3}{4})$, what gives $e^{i\theta} = -\frac{3}{4} + i\frac{\sqrt{7}}{4}$. Björck was able to generalize this and in [6] he showed an example of a biunimodular vector

on \mathbb{Z}_p , whose coefficients are either 1 or $e^{i\theta}$ with $\theta = \arccos \frac{1-p}{1+p}$ (this gives $e^{i\theta} = \frac{1-p}{1+p} + i \frac{2\sqrt{p}}{1+p}$). Although the construction is limited to prime $p \equiv -1 \pmod{4}$, the same paper contains a similar example with coefficients 1, e^{in} and e^{-in} that works for any prime $p \equiv 1 \pmod{4}$. Further research has shown that the problem of finding all biunimodular vectors for \mathbb{Z}_p with prime p is not yet accessible. The vectors found by computers did not reveal any particular structure that can be somehow generalized. The largest prime for which the vectors were found is $p = 13$ (see [29]). The numerical methods that allow for finding biunimodular vectors concentrate on solving a system of equations whose solutions are called *cyclic N -roots*. Obtaining all unimodular cyclic N -roots is equivalent to finding all biunimodular vectors on \mathbb{Z}_N . The search for cyclic N -roots became a benchmark problem for testing the performance of some computational methods. The largest N accessed so far is $N = 14$ (see [41]).

The more general problem of finding biunimodular vectors on \mathbb{Z}_N provides additional challenges. As we mentioned already, it is not hard to see that all biunimodular vectors are Gauss sequences when $N = 2$ or 3. It is also easy to check, that for $N = 4$ the vectors $[1, z, 1, -z]$ and $[1, z, -1, z]$ are biunimodular for any $z \in \mathbb{T}$ (a more complicated calculation shows that, up to a constant, these are the only ones). Therefore, we see a dramatic difference in the appearance of biunimodular vectors depending on N . Already for $N = 4$ we obtain continuum of such vectors, while some other values of N yield only finitely many biunimodular vectors. In [8] it was shown that whenever N is divisible by a square, then \mathbb{Z}_N admits infinitely many (continuum) biunimodular vectors. The authors conjectured that if N is square-free, then the set of biunimodular vectors on \mathbb{Z}_N is finite. The conjecture is still open, even for prime N .

The cases when $N = 5, 6$ and 7 are presented by Haagerup in [20]. His interest in this topic comes from the fact that finding biunimodular vectors on \mathbb{Z}_N is closely related to classifying pairs of orthogonal maximal abelian $*$ -subalgebras. To show that for $N = 5$ biunimodular vectors coincide with Gauss sequences he proves a stronger result. Namely, that the only 5×5 unitary matrix whose entries have constant modulus is the Fourier transform. This, of course, holds up to an obvious equivalence (permuting and/or multiplying columns and/or rows by constants). Then, he shows that the unitary matrix obtained from translations of a biunimodular vector on \mathbb{Z}_N is equivalent to the matrix of the Fourier transform if and only if the vector is a Gauss sequence. The equivalence relation utilized by Haagerup is

useful in classifying biunimodular vectors. We say that two such vectors are equivalent if the unitary matrices of their translations are equivalent.

For $N > 5$ numerical calculations of [7] are used to list the classes of biunimodular vectors in [20]. When $N = 6$ we have two such classes. One consists of all Gauss sequences, and the other one is represented by

$$(7.2) \quad [1, id, -d, -i, -\bar{d}, i\bar{d}],$$

where $d = \frac{1-\sqrt{3}}{2} - i\left(\frac{\sqrt{3}}{2}\right)^{\frac{1}{2}}$. This example indicates the next difficulty within the program of finding all biunimodular vectors. In Lemma 4.6 we showed that biunimodular vectors can be obtained via tensor products. However, although $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$, the vector (7.2) is not a tensor product of biunimodular vectors on \mathbb{Z}_2 and \mathbb{Z}_3 . In fact, it is not a tensor product at all (it is possible to show, that if a biunimodular u is a tensor product of w and v , then up to a constant, w and v must be biunimodular as well).

If $N = 7$, there are five classes of biunimodular vectors. The Gaussian class, two that are represented by (7.1) and its complex conjugation and two that are given by

$$(7.3) \quad [1, a, b, c, c, b, a]$$

and its conjugation. For both explicit and numerical values of a, b, c in (7.3) see [20].

The study of the cyclic case, that we presented, indicates that biunimodular functions heavily depend on the underlying group. In particular, understanding their form on the building blocks \mathbb{Z}_p is not enough to conclude their behavior on a general finite abelian group. Although the problem, in its full generality, seems to be hopeless, its particular cases are under constant investigation. One of such cases concentrates on biunimodular functions on the group $(\mathbb{Z}_2)^N$. The problem of finding real biunimodular functions on this group was addressed in 1976 by Rothaus (see [36]). He called them *bent functions* and was able to explain how they look like for first values of N . Even earlier the same problem was studied by Dillon from the perspective of difference sets (see [15]). As we noticed before, the assumption that a biunimodular function is real forces the order of the group to be a square. Therefore, we see that N must be even. Rothaus have characterized all bent functions for $N = 2, 4$ and 6 . Despite many efforts, no characterization was found for $N = 8$. It is easy to see that when $N = 2$, then the bent functions are exactly the same that we listed in Conjecture 7.1. Therefore, we have 8 different bent functions in this case. For $N = 4$ the number of bent functions is 896 and all of them can be characterized in simple terms. The situation when $N = 6$ is more challenging.

It is known that there are 5425430528 bent functions in this case (see [34] or [12]). They were also characterized in [36] and [10]. For $N = 8$ the number of bent functions is not known. In general, there are many methods of producing bent functions. Most of them are listed in [46]. Newer ones have appeared in [34], [10], [3] and [16]. It is hard, however, to see when they yield different functions. It is not clear if the constructions allow to obtain all functions. Counting them is also a problem. The amount of research done on bent functions is extensive. This is due to the fact, that they are used in cryptography and error-correcting codes. For example, bent functions were implemented by Adams and Tavares in their CAST encryption algorithm (see [1] and [2]). For the relevance of bent functions in coding theory we refer the reader to [32].

The classical biunimodular functions, that is, Gauss sequences, appear in applications as well. In electrical engineering they are known as discrete or finite *chirps* and are used for signal processing (see [45], [35] and [11]). Also, as shown in [19], these chirps allow for finding the metaplectic representation in the case of finite cyclic groups.

The final topic that we would like to mention goes back to Littlewood work [31]. For any biunimodular function u on a finite abelian group G of order N we can consider the associated trigonometric polynomial $p_u(z) = \sum_{n=0}^{N-1} u(n)z^n$, where $z \in \mathbb{T}$. Although it looks like it would be more natural to define these polynomials only for $G = \mathbb{Z}_N$, it turns out, that one of the first examples of such polynomials was considered with G being a power of \mathbb{Z}_2 . The famous example that we are referring to are Rudin-Shapiro polynomials. The coefficients of these polynomials are bent functions (in the case when the power is even). The crucial property that they possess is that

$$(7.4) \quad \|p_u\|_\infty \leq C\sqrt{N},$$

where C is a numerical constant. This result was extended by Byrnes to a wider class of biunimodular functions (see [9]). Littlewood was interested in proving (7.4) for Gauss sequences. He was able to do it only for the sequences in the odd case (4.2) with $\lambda = \frac{N \pm 1}{2}$. The more general problem remains unsolved. On the other hand, recently Saffari has communicated that the ultimate generalization of (7.4) to all biunimodular functions fails. Even if we restrict ourselves only to the cyclic case (see [38]).

BIBLIOGRAPHY

- [1] C. M. ADAMS, "Constructing symmetric ciphers using the CAST design procedure", *Des. Codes Cryptography* **12** (1997), no. 3, p. 283-316.
- [2] C. M. ADAMS & S. E. TAVARES, "Generating bent sequences", *Discrete Appl. Math.* **39** (1992), no. 2, p. 155-159.
- [3] S. AGIEVICH, "On the representation of bent functions by bent rectangles", in *Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference* (Utrecht, Boston: VSP), 2002, p. 121-135.
- [4] K. I. BABENKO, "An inequality in the theory of Fourier integrals", *Izv. Akad. Nauk SSSR Ser. Mat.* **25** (1961), p. 531-542.
- [5] W. BECKNER, "Inequalities in Fourier analysis", *Ann. Math. (2)* **102** (1975), p. 159-182.
- [6] G. BJÖRCK, "Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and "cyclic n -roots"", Recent advances in Fourier analysis and its applications, Proc. NATO/ASI, Il Ciocco/Italy 1989, NATO ASI Ser., Ser. C 315, 1990, 131-140 pages.
- [7] G. BJÖRCK & R. FRÖBERG, "A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n -roots", *J. Symb. Comput.* **12** (1991), no. 3, p. 329-336.
- [8] G. BJÖRCK & B. SAFFARI, "New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries", *C. R. Acad. Sci., Paris, Sér. I* **320** (1995), no. 3, p. 319-324.
- [9] J. S. BYRNES, "On polynomials with coefficients of modulus one", *Bull. Lond. Math. Soc.* **9** (1997), p. 171-176.
- [10] C. CARLET, "Two new classes of bent functions", Helleseth, Tor (ed.), *Advances in cryptology - EUROCRYPT '93. Lect. Notes Comput. Sci. 765*, Springer, Berlin, 1994, 77-101 pages.
- [11] P. G. CASAZZA & M. FICKUS, "Chirps on finite cyclic groups", *Proc. SPIE* **5914** (2005), p. 175-180.
- [12] D. K. CHANG, "Binary bent sequences of order 64", *Util. Math.* **52** (1997), p. 141-151.
- [13] R. R. COIFMAN, Y. MEYER & M. V. WICKERHAUSER, "Wavelet analysis and signal processing", in *Wavelets and their applications* (M. B. Ruskai & al., eds.), Jones and Bartlett Publishers, Boston, MA, 1992, p. 153-178.
- [14] R. R. COIFMAN & M. V. WICKERHAUSER, "Entropy-based algorithms for best basis selection", *IEEE Trans. Inf. Theory* **38** (1992), no. 2, Pt. 2, p. 713-718.
- [15] J. F. DILLON, "Elementary Hadamard difference sets", Proc. 6th Southeast. Conf. Comb., Graph Theor., and Comput.; Boca Raton, Fl, 1975, 237-249 pages.
- [16] H. DOBBERTIN & G. LEANDER, "Cryptographer's Toolkit for Construction of 8-Bit Bent Functions", Cryptology ePrint Archive, Report 2005/089, 2005.
- [17] D. L. DONOHO & P. B. STARK, "Uncertainty principles and signal recovery", *SIAM J. Appl. Math.* **49** (1989), no. 3, p. 906-931.
- [18] C. FEFFERMAN, "Pointwise convergence of Fourier series", *Ann. Math. (2)* **98** (1973), p. 551-571.
- [19] H. G. FEICHTINGER, M. HAZEWINKEL, N. KAIBLINGER, E. MATUSIAK & M. NEUHAUSER, "Metaplectic operators on C^n ", preprint.
- [20] U. HAAGERUP, "Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n -roots.", Doplicher, S. (ed.) et al., *Operator algebras and quantum field theory. Accademia Nazionale dei Lincei, Roma, Italy. Cambridge, MA: International Press, 1997, 296-322 pages.*

- [21] G. H. HARDY & J. E. LITTLEWOOD, “Some new properties of Fourier constants”, *Math. Ann.* **97** (1927), p. 159-209.
- [22] C. HERLEY, Z. XIONG, K. RAMCHANDRAN & M. T. ORCHARD, “Joint space-frequency segmentation using balanced wavelet packet trees for least-cost image representation”, *IEEE Trans. on Image Proc.* **6** (1997), no. 9, p. 1213-1230.
- [23] E. HEWITT & I. HIRSCHMAN, “A maximum problem in harmonic analysis”, *Am. J. Math.* **76** (1954), p. 839-852.
- [24] E. HEWITT & K. A. ROSS, *Abstract harmonic analysis.*, vol. 2, Berlin-Heidelberg-New York: Springer-Verlag VIII, 1970.
- [25] Y. HUANG, I. POLLAK & C. A. BOUMAN, “Image Compression with Multitree Tilings”, Proc. ICASSP-2005, Philadelphia, PA., March 2005.
- [26] M. LACEY & C. THIELE, “ L^p estimates on the bilinear Hilbert transform for $2 < p < \infty$ ”, *Ann. Math. (2)* **146** (1997), no. 3, p. 693-724.
- [27] ———, “On Calderón’s conjecture”, *Ann. Math. (2)* **149** (1999), no. 2, p. 475-496.
- [28] K. H. LEUNG, S. L. MA & B. SCHMIDT, “Nonexistence of abelian difference sets: Lander’s conjecture for prime power orders”, *Trans. Am. Math. Soc.* **356** (2004), no. 11, p. 4343-4358.
- [29] T. Y. LI & X. LI, “Finding mixed cells in the mixed volume computation”, *Found. Comput. Math.* **1** (2001), no. 2, p. 161-181.
- [30] E. H. LIEB, “Gaussian kernels have only Gaussian maximizers”, *Invent. Math.* **102** (1990), no. 1, p. 179-208.
- [31] J. E. LITTLEWOOD, “On the mean values of certain trigonometrical polynomials. II”, *Ill. J. Math.* **6** (1962), p. 1-39.
- [32] F. J. MACWILLIAMS & N. J. A. SLOANE, *The theory of error-correcting codes*, vol. 16, North-Holland Mathematical Library, Amsterdam - New York - Oxford, 1977.
- [33] E. MATUSIAK, M. ÖZAYDIN & T. PRZEBINDA, “The Donoho–Stark uncertainty principle for a finite abelian group”, *Acta Math. Univ. Comen. New Ser.* **73** (2004), no. 2, p. 155-160.
- [34] B. PRENEEL, W. VAN LEEKWIJCK, L. VAN LINDEN, R. GOVAERTS & J. VANDEWALLE, “Propagation characteristics of Boolean functions”, *Advances in Cryptology, Proc. Workshop, EUROCRYPT ’90, Lect. Notes Comput. Sci.* **473**, 1991, 161-173 pages.
- [35] M. S. RICHMAN, T. W. PARKS & R. G. SHENOY, “Discrete-time, discrete-frequency, time-frequency analysis”, *IEEE Trans. Signal Process.* **46** (1998), no. 6, p. 1517-1527.
- [36] O. S. ROTHSAUS, “On “bent” functions.”, *J. Comb. Theory, Ser. A* **20** (1976), p. 300-305.
- [37] H. J. RYSER, *Combinatorial mathematics*, John Wiley and Sons, New York, 1963.
- [38] B. SAFFARI, “Some polynomial extremal problems which emerged in the twentieth century”, Byrnes, James S. (ed.), *Twentieth century harmonic analysis—a celebration. Proceedings of the NATO Advanced Study Institute, Il Ciocco, Italy, July 2-15, 2000.* Dordrecht: Kluwer Academic Publishers. NATO Sci. Ser. II, Math. Phys. Chem. **33**, 2001, 201-223 pages.
- [39] B. SCHMIDT, “Cyclotomic integers and finite geometry”, *J. Am. Math. Soc.* **12** (1999), no. 4, p. 929-952.
- [40] ———, “Towards Ryser’s conjecture”, Casacuberta, Carles (ed.) et al., *3rd European congress of mathematics (ECM), Barcelona, Spain, July 10-14, 2000. Volume I.* Basel: Birkhäuser. Prog. Math. **201**, 2001, 533-541 pages.
- [41] A. TAKEDA, M. KOJIMA & K. FUJISAWA, “Enumeration of all solutions of a combinatorial linear inequality system arising from the polyhedral homotopy continuation method”, *J. Oper. Res. Soc. Japan* **45** (2002), no. 1, p. 64-82.

- [42] T. TAO, “An uncertainty principle for cyclic groups of prime order”, *Math. Res. Lett.* **12** (2005), no. 1, p. 121-127.
- [43] C. THIELE & L. F. VILLEMOS, “A fast algorithm for adapted time-frequency tilings”, *Appl. Comput. Harmon. Anal.* **3** (1996), no. 2, p. 91-99.
- [44] R. J. TURYN, “Character sums and difference sets”, *Pac. J. Math.* **15** (1965), p. 319-346.
- [45] X. G. XIA, “Discrete chirp-Fourier transform and its application in chirp rate estimation”, *IEEE Trans. on Signal Processing* **48(11)** (2000), p. 3122-3133.
- [46] R. YARLAGADDA & J. E. HERSHEY, “Analysis and synthesis of bent sequences”, *Proc. IEE* **136, Pt. E.** (1989), p. 112-123.

Manuscrit reçu le 28 juillet 2006,
accepté le 30 janvier 2009.

John GILBERT
University of Texas
Department of Mathematics
Austin, TX 78712-1082 (USA)
gilbert@math.utexas.edu
Ziemowit RZESZOTNIK
Wrocław University
Mathematical Institute
Pl. Grunwaldzki 2/4
50-384 Wrocław (Poland)
zioma@math.uni.wroc.pl