Applications of the uncertainty principle for finite abelian groups to communications engineering

Felix Krahmer[1], Götz Pfander[2], Peter Rashkov[2*]
[1] Courant Institute of Mathematical Sciences, New York University, 10009 New York NY, USA
[2] School of Engineering and Science, Jacobs University, 28759 Bremen, Germany

We obtain uncertainty principles for finite abelian groups relating the cardinality of the support of a function to the cardinality of the support of its short-time Fourier transform and discuss their applications. These uncertainty principles are based on well-established uncertainty principles for the Fourier transform. Areas of applications include the existence of a class of equal norm tight Gabor frames that are maximally robust to erasures and implications for to the theory of recovering and storing signals with sparse time-frequency representation.

1. Uncertainty principles.

Let *G* be a finite abelian group with dual group $\hat{G}$ consisting of the group homomorphisms $\xi : G \to S^1$. The space of complex-valued functions *f* with domain G (vectors) will be denoted by $\mathbf{C}^G$, and the support size of a function is $\| f \|_0 := | \{x : f(x) \neq 0\} |$. The Fourier transform is defined as $f(\xi) := \sum_{x \in G} f(x) \cdot \overline{\xi(x)}$ for $f \in \mathbf{C}^G, \xi \in \hat{G}$. The Euclidean norm on $\mathbf{C}^G$ will be denoted by $\| . \|_2$. Note that $\| . \|_0$ is not a norm.

A well-known result [4] states that $\| f \|_0 \cdot \| \hat{f} \|_0 \geq |G|$ for $f \in \mathbf{C}^G \setminus \{0\}$. This inequality can be improved for groups of prime order, namely for $G = \mathbf{Z}_p$ with *p* prime, $\| f \|_0 + \| \hat{f} \|_0 \geq p+1$ holds for all $f \in \mathbf{C}^{\mathbf{Z}_p} \setminus \{0\}$ [5, 11]. We illustrate all pairs $(\| f \|_0, \| \hat{f} \|_0)$ for $\mathbf{Z}_4, \mathbf{Z}_2^2, \mathbf{Z}_5, \mathbf{Z}_6$ (in this order) in Fig. 1. The achieved combinations $(\| f \|_0, \| \hat{f} \|_0)$ are represented by a white square, whereas the nonexistent ones by a black square.

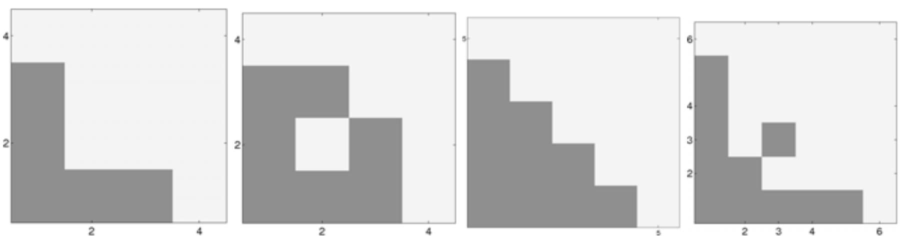

Figure 1.

---
[*] E-mail: p.rashkov@jacobs-university.de

Fig. 2 illustrates the achieved and impossible combinations $(\| f \|_0, \| \hat{f} \|_0)$ for the groups $\mathbf{Z}_8, \mathbf{Z}_2 \times \mathbf{Z}_4, \mathbf{Z}_2^3$ (in this order). Numerically verified combinations (by MatLab) are represented in a shaded square of the respective colour.

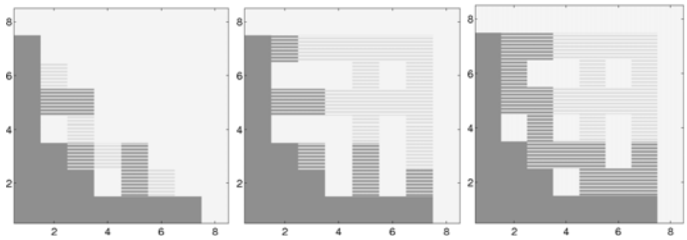

Figure 2.

Let $g \in \mathbf{C}^G \setminus \{0\}$ be a window function. The short-time Fourier transform with respect to *g* is given by

$$V_g f(x,\xi) := \sum_{y \in G} f(y) \overline{g(y-x)\xi(y)}, \quad f \in \mathbf{C}^G, (x,\xi) \in G \times \hat{G}$$

The linear mapping $V_g : \mathbf{C}^G \to \mathbf{C}^{G \times \hat{G}}$ has a matrix representation that will be denoted by $A_{G,g}$. For groups *G* of prime order the fact that for a generic *g*, all minors of $A_{G,g}$ are non-zero allows us to establish the fact that the cardinality of the support of the short-time Fourier transform must be larger than $|G|^2 - |G| + 1$ [7, 8].

Theorem 1. Let $G = \mathbf{Z}_p$, *p* prime. For almost every $g \in \mathbf{C}^G$, $\| f \|_0 + \| V_g f \|_0 \ge |G|^2 + 1$ for all $f \in \mathbf{C}^G \setminus \{0\}$. Moreover, for $1 \le k \le |G|$ and $1 \le l \le |G|^2$ with $k + l \ge |G|^2 + 1$ there exists *f* with $\| f \|_0 = k$ and $\| V_g f \|_0 = l$.

The result stated in Theorem 1 can be improved further, namely we can choose a unimodular window function $g \in \mathbf{C}^{\mathbf{Z}_p}$, that is, a vector *g* all of whose entries have absolute value 1 [7].

Similar to [9], in order to establish lower bounds on $\| V_g f \|_0$ for a general group *G*, we define for $0 < k \le |G|$,

$$\phi(G,k) := \max_{g \in \mathbf{C}^G \setminus \{0\}} \min \left\{ \| V_g f \|_0 : f \in \mathbf{C}^G \text{ and } 0 < \| f \|_0 \le k \right\}.$$

Proposition. For $0 < k \le |G|$, let d_1 be the largest divisor of |*G*| which is less than or equal to *k* and let d_2 be the smallest divisor of |*G*| which is larger than or equal to *k*. Then

$$\phi(G,k) \ge \frac{|G|^2}{d_1 d_2}(d_1 + d_2 - k).$$

For $G = \mathbf{Z}_{pq}$, (*p*, *q* prime) the bound can be improved, namely

$$\phi(G,k) \geq \begin{cases} p^2(q^2-k+1) & \text{if } \quad k<q; \\ (p^2-\frac{k}{q}+1)(q^2-q+1) & \text{else.} \end{cases}$$

We illustrate the possible pairs $\left(\| f\|_0, \|V_g f\|_0\right)$ for a generic window $g \neq 0$ for $\mathbf{Z}_4, \mathbf{Z}_2^2, \mathbf{Z}_6, \mathbf{Z}_7$ in Figure 3 (due to space limitations the figures actually show the mirror points $(\|V_g f\|_0, \|f\|_0)$. We use the colour coding from Fig. 1 and 2.

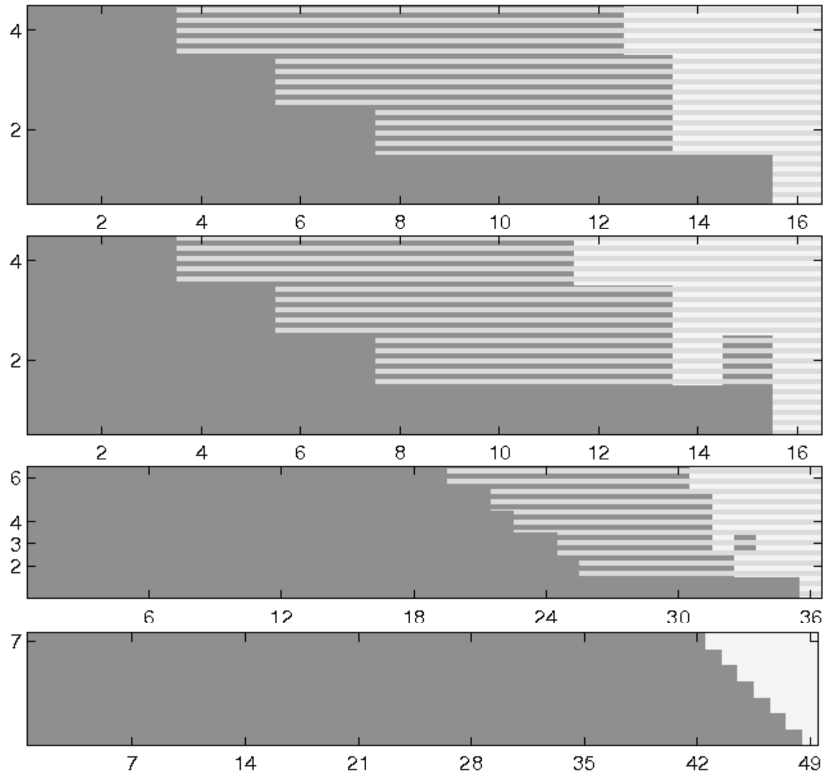

Figure 3.

We note that for the cyclic groups $\mathbf{Z}_4$ and $\mathbf{Z}_6$ and for generic *g*, $\|V_g f\|_0 \geq |G|^2 - |G| + 1$ for all $f \in \mathbf{C}^G \setminus \{0\}$. While such a statement turns out to be false in the case of arbitrary abelian groups (for instance, $\mathbf{Z}_2^2$ - see Fig. 3), we believe that for cyclic groups the inequality remains valid, namely that for *G* cyclic,

$$\left\{(\|f\|_0, \|V_g f\|_0),\ f \in \mathbf{C}^G \setminus \{0\}\right\} = \left\{(\|f\|_0, \|\hat{f}\|_0 + |G|^2 - |G|),\ f \in \mathbf{C}^G \setminus \{0\}\right\}.$$

This question is discussed further for the group $\mathbf{Z}_8$ in [7].

2. Gabor frames and erasure channels.

In generic communication systems, information (a vector $f \in \mathbf{C}^G$) is not sent directly, but must be coded in such a way that allows recovery of *f* at the receiver regardless of errors and disturbances introduced by the channel. We can choose a frame $\{\varphi_k : k \in K\}$ for $\mathbf{C}^G$ and send the coded coefficients

$\{\langle f,\varphi_k\rangle : k \in K\}$ (see for example [2] for definition and properties of frames in finite-dimensional vector spaces and [6] for definition of Gabor systems and frames in particular). If none of the transmitted coefficients are lost, a dual frame $\{\varphi'_k\}$ of $\{\varphi_k\}$ can be used by the receiver to recover *f* via the inversion formula $f = \sum_k \langle f,\varphi_k\rangle \varphi'_k$ (see [2]).

In the case of an erasure channel, some coefficients are lost during the transmission. Suppose that only the coefficients $\{\langle f,\varphi_k\rangle : k \in K'\}, K' \subset K$ are received. The original vector *f* can still be recovered if and only if the subset $\{\varphi_k : k \in K'\}$ remains a frame for $\mathbf{C}^G$. Of course this requires $|K'| \geq |G| = \dim \mathbf{C}^G$. Hence we define a frame $\Im = \{\varphi_k : k \in K\}$ in $\mathbf{C}^G$ to be *maximally robust to erasures* if the removal of any $l \leq |K| - |G|$ elements from $\Im$ still leaves a frame. Furthermore, we have shown in [7] that for any $g \in \mathbf{C}^G \setminus \{0\}$, the columns of the matrix $A_{G,g}$ form an equal norm tight Gabor frame for $\mathbf{C}^G$.

Theorem 2. For $g \in \mathbf{C}^G \setminus \{0\}$, the following are equivalent:

- For all $f \in \mathbf{C}^G \setminus \{0\}, \|V_g f\|_0 \geq |G|^2 - |G| + 1$.
- The Gabor system, consisting of the columns of the matrix $A_{G,g}$, is an equal norm tight frame which is *maximally robust to erasures*.

For |*G*| prime, Theorem 1 guarantees the validity of the first statement of Theorem 2 for a generic *g* and in particular, for some unimodular *g*. As Figure 3 shows, this statement is true also for the groups $\mathbf{Z}_4, \mathbf{Z}_6$. It remains yet an open question to verify it for general cyclic groups and show the existence of such frames in the general case.

3. Signals with sparse representations.

The classical theory of sparse representations centres around the problem of recovering a signal, which is a linear combination of a small number of frequencies, from very few of its sampled values. In a more general setting, we consider dictionaries $D = \{g_0, g_1, \ldots, g_{N-1}\}$ of *N* vectors in $\mathbf{C}^n$. For $k \leq n$ we shall examine the sets

$$\Sigma_k^D = \{f \in £^n : f = \sum_r c_r g_r, \text{ for all sequences } \mathbf{c} : \|\mathbf{c}\|_0 \leq k\}.$$

In other words Σ_k^D is the set of vectors (signals) in $\mathbf{C}^n$ that have *k*-sparse representations in the dictionary *D*. Every such vector $f = M_D \mathbf{c}$ where M_D is the matrix of the respective linear transformation associated to *D*. For example, a classical dictionary for $\mathbf{C}^G$ is the set of frequencies $D_G = \{\xi : \xi \in \hat{G}\}$. In this case $\Sigma_k^D = \{\hat{f} : f \in \mathbf{C}^G : \|f\|_0 \leq k\}$.

The main question is to find out how many values of $f \in \Sigma_k^D$ need to be known (or stored), in order for $\mathbf{c} \in \mathbf{C}^N$ with $f = \sum_r c_r g_r$ and $\|\mathbf{c}\|_0 \leq k$, and therefore *f*, to be uniquely determined by the known data? Let us recall a well-known result [1, 3, 10]:

Theorem 3. Let $\psi(D,k) := \min\left\{\| f \|_0 : f \in \Sigma_k^D\right\}$. Any $f \in \Sigma_k^D \subseteq \mathbf{C}^N$ is fully determined by any choice of $N - \psi(D,2k)+1$ values of *f*.

We can extend the results in [1] to vectors having sparse representations in the dictionary $D_{G,g}$ which consists of the columns of $A_{G,g}$. In fact, $F \in \Sigma_k^{D_{G,g}}$ if and only if $F = V_g f$ for some $f \in \mathbf{C}^G$ with $\| f \|_0 \le k$ and, therefore,

$$\psi(D_{G,g},k) = \min\left\{\| V_g f \|_0 : \| f \|_0 \le k\right\} = \phi(G,k).$$

As a second application of the uncertainty principle for the short-time Fourier transform, in [7] we state and prove the following

Theorem 4. Let $g \in \mathbf{C}^p$, *p* prime, be such that for all $f \in \mathbf{C}^p \setminus \{0\}, \| V_g f \|_0 \ge p^2 - p + 1$.

Then any $f \in \mathbf{C}^p$ is completely determined by sampling the values of $V_g f$ on any $\Lambda \subset \mathbf{Z}_p \times \mathbf{Z}_p$ with $|\Lambda| = p$. Furthermore, any $f \in \mathbf{C}^p$ with $\| f \|_0 \le \frac{1}{2} |\Lambda|, \Lambda \subset \mathbf{Z}_p \times \mathbf{Z}_p$ is uniquely determined by Λ and the sampled values $V_g f$ on Λ.

Bibliography.

[1] E. J. Candes, J. Romberg, T. Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inf. Theory*. **52** (2006) 489-509.

[2] O. Christensen. *An Introduction to Frames and Riesz Bases*. Birkhäuser, Boston, 2003.

[3] D. Donoho. Compressed sensing. *IEEE Trans. Inf. Theory*. **52** (2006) 1289-1306.

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

[5] P. E. Frenkel. Simple proof of Chebotarev's theorem on roots of unity. *preprint*, math.AC/0312389 (2004).

[6] K. H. Gröchenig. *Foundations of time-frequency analysis*. Birkhäuser, Boston, 2001.

[7] F. Krahmer, G. Pfander, P. Rashkov. Uncertainty in time-frequency representations on finite abelian groups and applications. *Appl. Comp. Harm. Anal*. **25** (2007) 209-225.

[8] J. Lawrence, G. Pfander, D. Walnut. Linear independence of Gabor systems in finite dimensional vector spaces. *J. Four. Anal. Appl*. **11** (2005) 715-726.

[9] R. Meshulam. An uncertainty inequality for finite abelian groups. *Eur. J. Comb.* **27** (2006) 227-254.

[10] H. Rauhut. Random sampling of sparse trigonometric polynomials. *Appl. Comp. Harm. Anal*. **22** (2007) 16-42.

[11] T. Tao. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett*. **12** (2005) 121-127.