# UNCERTAINTY PRINCIPLES AND COMPRESSED SENSING

JORDAN BELL

In this paper I am careful to distinguish between the space of signals and the space of their Fourier transforms.

Folland and Sitaram [4] give a survey of uncertainty principles in analysis.

First we will go through the talk by Emmanuel Candès and Terence Tao, "The uniform uncertainty principle and compressed sensing", Harmonic Analysis and Related Topics, Seville, December 5, 2008.

Let $G = \mathbb{Z}/n\mathbb{Z}$. Let $L(G)$ denote the set of functions from $G$ to $\mathbb{C}$. For $T \subseteq G$, let $L(T)$ be the set of functions from $G$ to $\mathbb{C}$ whose support is contained in $T$.

For $x \in G$, define the Dirac delta function $\delta_x : G \to \mathbb{C}$ centered at $x$ by

$$\delta_x(y) = \begin{cases} 1, & y = x \\ 0, & y \neq x. \end{cases}$$

The set $\{\delta_x\}_{x \in G}$ is a basis for the vector space $L(G)$. For $f \in L(G)$,

$$f(y) = \sum_{x \in G} f(x)\delta_x(y), \qquad y \in G.$$

We define an inner product on $L(G)$ by

$$\langle f, g \rangle_G = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}, \qquad f, g \in L(G).$$

The $L^2$ norm on $L(G)$ is given by $\|f\|_{L^2(G)} = \langle f, f \rangle_G^{1/2}$. That is,

$$\|f\|_{L^2(G)} = \frac{1}{\sqrt{|G|}} \left( \sum_{x \in G} |f(x)|^2 \right)^{1/2}, \qquad f \in L(G).$$

We also define the $L^1$ norm on $L(G)$ by

$$\|f\|_{L^1(G)} = \frac{1}{|G|} \sum_{x \in G} |f(x)|,$$

and define the $L^\infty$ norm on $L(G)$ by

$$\|f\|_{L^\infty(G)} = \sup_{x \in G} |f(x)|.$$

Let $S^1$ be the unit circle in $\mathbb{C}$. Let $\widehat{G}$ be the dual group of characters $\xi : G \to S^1$; see Rudin [10, Chapter 1] on the Pontryagin dual. $\widehat{G}$ is (noncanonically) isomorphic to $G = \mathbb{Z}/N\mathbb{Z}$. In particular, $|\widehat{G}| = |G| = N$.

For $f \in L(G)$, we define its Fourier transform $\hat{f} : \widehat{G} \to \mathbb{C}$ by

$$\hat{f}(\xi) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\xi(x)}, \qquad \xi \in \widehat{G}.$$

---

*Date*: April 29, 2010.

**Lemma 1** (Fourier inversion formula)**.**

$$f(x) = \sum_{\xi \in \widehat{G}} \hat{f}(\xi)\xi(x), \qquad x \in G.$$

*Proof.* Let $x \in G$, $x \neq 0$. Let $\eta \in \widehat{G}$ such that $\eta(x) \neq 1$. Then

$$\begin{aligned} \sum_{\xi \in \widehat{G}} \xi(x) &= \sum_{\xi \in \widehat{G}} \xi(x)\eta(x)\eta(-x) \\ &= \eta(-x) \sum_{\xi \in \widehat{G}} \xi(x)\eta(x) \\ &= \eta(-x) \sum_{\xi \in \widehat{G}} \xi(x). \end{aligned}$$

But $\eta(-x) \neq 0$, so it must be that $\sum_{\xi \in \widehat{G}} \xi(x) = 0$ if $x \neq 0$.

On the other hand, $\sum_{\xi \in \widehat{G}} \xi(0) = |\widehat{G}| = |G|$. Therefore, for any $x \in G$ (zero or not),

$$\begin{aligned} \sum_{\xi \in \widehat{G}} \hat{f}(\xi)\xi(x) &= \sum_{\xi \in \widehat{G}} \frac{1}{|G|} \sum_{y \in G} f(y)\overline{\xi(y)}\xi(x) \\ &= \sum_{y \in G} \frac{f(y)}{|G|} \sum_{\xi \in \widehat{G}} \overline{\xi(y)}\xi(x) \\ &= \sum_{y \in G} \frac{f(y)}{|G|} \sum_{\xi \in \widehat{G}} \xi(x - y) \\ &= f(x). \end{aligned}$$

□

For $x \in G$, define $\chi_x : \widehat{G} \to \mathbb{C}$ by $\chi_x(\xi) = \frac{\overline{\xi(x)}}{|G|}$ for all $\xi \in \widehat{G}$. The set $\{\chi_x\}_{x \in G}$ is a basis for $L(\widehat{G})$. For $\hat{f} \in L(\widehat{G})$,

$$\hat{f}(\xi) = \sum_{x \in G} f(x)\chi_x(\xi), \qquad \xi \in \widehat{G}.$$

Another basis for $L(\widehat{G})$ is $\{\delta_\xi\}_{\xi \in \widehat{G}}$.

We define an inner product on $L(\widehat{G})$ by

$$\langle \hat{f}, \hat{g} \rangle_{\widehat{G}} = \sum_{\xi \in \widehat{G}} \hat{f}(\xi)\overline{\hat{g}(\xi)}.$$

The $L^1$, $L^2$, and $L^\infty$ norms on $L(\widehat{G})$ are defined respectively by

$$\|\hat{f}\|_{L^1(\widehat{G})} = \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|,$$

$$\|\hat{f}\|_{L^2(\widehat{G})} = \langle \hat{f}, \hat{f} \rangle_{\widehat{G}} = \left( \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^2 \right)^{1/2},$$

and

$$\|\hat{f}\|_{L^\infty(\widehat{G})} = \sup_{\xi \in \widehat{G}} |\hat{f}(\xi)|,$$

for $\hat{f} \in L(\widehat{G})$.

With these definitions of $\|\cdot\|_{L^2(G)}$ and $\|\cdot\|_{L^2(\widehat{G})}$, the Fourier transform $\mathscr{F} : L(G) \to L(\widehat{G})$ is an isometry.

**Lemma 2** (Plancherel identity)**.** *For $f \in L(G)$,*

$$\|f\|_{L^2(G)} = \|\hat{f}\|_{L^2(\widehat{G})}.$$

*Proof.*

$$\begin{aligned}
\|\hat{f}\|^2_{L^2(G)} &= \langle \hat{f}, \hat{f} \rangle_{\widehat{G}} \\
&= \sum_{\xi \in \widehat{G}} \hat{f}(\xi)\overline{\hat{f}(\xi)} \\
&= \frac{1}{|G|^2} \sum_{\xi \in \widehat{G}} \Big( \sum_{x \in G} f(x)\overline{\xi(x)} \Big) \Big( \sum_{y \in G} \overline{f(y)}\xi(y) \Big) \\
&= \frac{1}{|G|^2} \sum_{x \in G} \sum_{y \in G} f(x)\overline{f(y)} \sum_{\xi \in \widehat{G}} \overline{\xi(x)}\xi(y) \\
&= \frac{1}{|G|} \sum_{x \in G} |f(x)|^2 \\
&= \|f\|^2_{L^2(G)};
\end{aligned}$$

the second last equality is because $\sum_{\xi \in \widehat{G}} \overline{\xi(x)}\xi(y)$ is equal to 0 if $x \neq y$ and $|G|$ if $x = y$. □

For $H$ a subgroup of $G$, define the orthogonal complement $H^\perp$ in $\widehat{G}$ as

$$H^\perp = \{\xi \in \widehat{G} : \xi(x) = 1 \quad \text{for all } x \in H\}.$$

Let $1_H$ be the indicator function for $H$, that is, $1_H(x)$ is equal to 1 if $x \in H$ and 0 if $x \notin H$.

**Lemma 3.** *If $H$ is a subgroup of $G$ then*

$$\widehat{1_H} = \frac{|H|}{|G|} 1_{H^\perp}.$$

*Proof.* If $\xi \notin H^\perp$ then there is some $x \in H$ such that $\xi(x) \neq 1$. Then

$$\begin{aligned}
\sum_{y \in H} \overline{\xi(y)} &= \xi(x) \sum_{y \in H} \overline{\xi(y)\xi(x)} \\
&= \xi(x) \sum_{y \in H} \overline{\xi(yx)} \\
&= \xi(x) \sum_{y \in H} \overline{\xi(y)},
\end{aligned}$$

for as $x \in H$ and $H$ is a subgroup of $G$, $y \mapsto yx$ is a bijection from $H$ to $H$. But $\xi(x) \neq 1$, so $\sum_{y \in H} \overline{\xi(y)} = 0$ for $\xi \notin H^\perp$. On the other hand, if $\xi \in H^\perp$ then $\sum_{y \in H} \overline{\xi(y)} = |H|$. Hence

$$\widehat{1_H}(\xi) = \frac{1}{|G|} \sum_{y \in G} 1_H(y)\overline{\xi(y)} = \frac{1}{|G|} \sum_{y \in H} \overline{\xi(y)} = \frac{|H|}{|G|} 1_{H^\perp}(\xi).$$

□

The following proof of the Poisson summation formula is from Terras [13, p. 199].

**Lemma 4** (Poisson summation formula)**.** *Let $H$ be a subgroup of $G$ and let $f \in L(G)$. Then*

$$\frac{1}{|H|}\sum_{h\in H} f(g+h) = \frac{1}{|G|}\sum_{\xi\in H^\perp}\hat{f}(\xi)\xi(g)$$

*for any $g \in G$.*

*Proof.* Define $f^\perp : G/H \to \mathbb{C}$ by

$$f^\perp(x+H) = \sum_{h\in H} f(x+h), \qquad x+H \in G/H.$$

For $\eta \in \widehat{G/H}$, let $\xi \in H^\perp$ such that $\eta(x+H) = \xi(x)$ for all $x \in G$ (indeed, there is certainly a one-to-one correspondence between the characters of $G/H$ and the characters of $G$ that are equal to 1 on $H$). Then,

$$\begin{aligned}
\langle f^\perp, \eta\rangle_{G/H} &= \sum_{x+H\in G/H} f^\perp(x+H)\overline{\eta(x+H)} \\
&= \sum_{x+H\in G/H}\sum_{h\in H} f(x+h)\overline{\xi(x+h)} \\
&= \sum_{x\in G} f(x)\overline{\xi(x)} \\
&= |G|\hat{f}(\xi);
\end{aligned}$$

the second last equality is because $G$ is a disjoint union of the cosets of $H$.

Using the Fourier inversion formula for $G/H$,

$$\begin{aligned}
f^\perp(g+H) &= \frac{1}{|G/H|}\sum_{\eta\in\widehat{G/H}} \langle f^\perp, \eta\rangle_{G/H}\eta(g+H) \\
&= \frac{|H|}{|G|}\sum_{\xi\in H^\perp} |G|\hat{f}(\xi)\xi(g),
\end{aligned}$$

i.e.,

$$\frac{1}{|H|}f^\perp(g+H) = \frac{1}{|G|}\sum_{\xi\in H^\perp}\hat{f}(\xi)\xi(g).$$

□

**Theorem 5** (Discrete uncertainty principle)**.** *For any non-trivial $f \in L(G)$,*

$$|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| \geq |G|.$$

*Proof.* First,

$$\begin{aligned}\|\hat{f}\|_{L^2(\widehat{G})} &= \Big(\sum_{\xi\in\mathrm{supp}(\hat{f})}|\hat{f}(\xi)|^2\Big)^{1/2}\\ &\le \Big(\sum_{\xi\in\mathrm{supp}(\hat{f})}\|\hat{f}\|^2_{L^\infty(\widehat{G})}\Big)^{1/2}\\ &= |\mathrm{supp}(\hat{f})|^{1/2}\|\hat{f}\|_{L^\infty(\widehat{G})}.\end{aligned}$$

It follows from the definition of the Fourier transform that $\|\hat{f}\|_{L^\infty(\widehat{G})}\le\|f\|_{L^1(G)}$, so

$$\|\hat{f}\|_{L^2(\widehat{G})}\le|\mathrm{supp}(\hat{f})|^{1/2}\|f\|_{L^1(G)}.$$

Let $1_{\mathrm{supp}(f)}$ be the indicator function for $\mathrm{supp}(f)$. By the Cauchy-Schwarz inequality,

$$\|f\|_{L^1(G)}=\langle|f|,1_{\mathrm{supp}(f)}\rangle_G\le\|f\|_{L^2(G)}\cdot\|1_{\mathrm{supp}(f)}\|_{L^2(G)}=\|f\|_{L^2(G)}\frac{|\mathrm{supp}(f)|^{1/2}}{\sqrt{|G|}}.$$

Thus

$$\|\hat{f}\|_{L^2(\widehat{G})} \le \frac{|\mathrm{supp}(\hat{f})|^{1/2}|\mathrm{supp}(f)|^{1/2}}{\sqrt{|G|}}\|f\|_{L^2(G)}.$$

By the Plancherel identity this gives us

$$\|\hat{f}\|_{L^2(\widehat{G})}\le\frac{|\mathrm{supp}(\hat{f})|^{1/2}|\mathrm{supp}(f)|^{1/2}}{\sqrt{|G|}}\|\hat{f}\|_{L^2(\widehat{G})}.$$

If $f$ is non-trivial then $\|\hat{f}\|_{L^2(\widehat{G})}\neq 0$ and we can divide both sides of the above inequality by it. □

There are two other versions of the discrete uncertainty principle given by Terras [13, Chapter 14].

Let $H$ be a subgroup of $G$ and let $1_H$ be the indicator function of $H$. By Lemma 3, $\mathrm{supp}(\widehat{1_H})=\mathrm{supp}(1_{H^\perp})$. But $|H^\perp|=|G/H|$, so $|\mathrm{supp}(1_H)||\mathrm{supp}(\widehat{1_H})|=G$.

Define the modulation operator $M_\beta : L(G)\to L(G)$ by

$$M_\beta f(x)=\beta(x)f(x),\qquad \beta\in\widehat{G},\quad x\in G$$

for all $f\in L(G)$. Define the translation operator $T_c : L(G)\to L(G)$ by

$$T_c f(a)=f(a+c),\qquad x,c\in G$$

for all $f\in L(G)$.

$$\begin{aligned}\widehat{M_\beta f}(\xi) &= \frac{1}{|G|}\sum_{x\in G}M_\beta f(x)\overline{\xi(x)}\\ &= \frac{1}{|G|}\sum_{x\in G}\beta(x)f(x)\overline{\xi(x)}\\ &= \hat{f}(\beta^{-1}\xi).\end{aligned}$$

$$\begin{aligned}\widehat{T_c f}(\xi) &= \frac{1}{|G|}\sum_{x\in G} T_c f(x)\overline{\xi(x)} \\ &= \frac{1}{|G|}\sum_{x\in G} f(x+c)\overline{\xi(x)} \\ &= \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\xi(x-c)} \\ &= \frac{\xi(c)}{|G|}\sum_{x\in G} f(x)\overline{\xi(x)} \\ &= \xi(c)\hat{f}(\xi).\end{aligned}$$

Note that $\operatorname{supp}(M_\beta f) = \operatorname{supp}(f)$ and that $\operatorname{supp}(\widehat{T_c f}) = \operatorname{supp}(\hat{f})$.

If $f \in L(G)$ is non-trivial, then for some $x_0 \in G$, $f(x_0) \neq 0$ and for some $\beta_0 \in \widehat{G}$, $\hat{f}(\beta_0) \neq 0$. Then $0 + (N) \in \operatorname{supp}(T_{x_0} M_{\beta_0^{-1}} f)$ and $1_G \in \operatorname{supp}(\mathscr{F}(T_{x_0} M_{\beta_0^{-1}} f))$.

The analogue of Gaussians for $G$ are the indicator functions of subgroups of $G$. This is because of the theorem proved by Donoho and Stark [3, Theorem 13] that equality in the discrete uncertainty principle is attained precisely for translations, modulations and multiplication by a constant of the indicators of subgroups. Our proof of the theorem follows [3] and [9].

**Theorem 6.** *If $f \in L(G)$ satisfies $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| = |G|$, with $0 + (N) \in \operatorname{supp}(f)$ and $1_G \in \operatorname{supp}(\hat{f})$, then $\operatorname{supp}(f)$ is a subgroup of $G$ and $\operatorname{supp}(\hat{f})$ is a subgroup of $\widehat{G}$.*

*Proof.* Let $M = |\operatorname{supp}(f)|$, and take $\operatorname{supp}(f) = \{r_1 + (N), \ldots, r_M + (N)\}$. Define $\phi : G \to \widehat{G}$ by $\phi(k+(N))(r+(N)) = e^{2\pi i k r/N}$ for all $k+(N), r+(N) \in G = \mathbb{Z}/N\mathbb{Z}$. For $0 \leq p \leq N - M$, define $w^{(p)} \in \mathbb{C}^M$ by

$$\begin{aligned}w_k^{(p)} = \hat{f}(\phi(p+k+(N))) &= \frac{1}{N}\sum_{r+(N)\in G} f(r+(N))\overline{\phi(p+k+(N))(r+(N))} \\ &= \frac{1}{N}\sum_{j=1}^{M} f(r_j+(N))e^{-2\pi i(p+k)r_j/N}\end{aligned}$$

for $k = 1, \ldots, M$. Define the $M \times M$ matrix $Z$ by $Z_{k,j} = z_j^{p+k}$, $1 \leq j, k \leq M$, where $z_j = e^{-2\pi i r_j/N}$. Let $u = (f(r_1+(N)), \ldots, f(r_M+(N))) \in \mathbb{C}^M$. Then $w^{(p)} = \frac{1}{N} Z u$. Thus $w^{(p)} = 0$ if and only if $u$ is in the kernel of $Z$. Certainly $u \neq 0$ in $\mathbb{C}^M$, since $r_1 + (N), \ldots, r_M + (N) \in \operatorname{supp}(f)$. Therefore to show that $w^{(p)} \neq 0$ it suffices to show that $\det Z \neq 0$.

We have

$$Z = \begin{bmatrix} z_1^{p+1} & z_2^{p+1} & \cdots & z_M^{p+1} \\ z_1^{p+2} & z_2^{p+2} & \cdots & z_M^{p+2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{p+M} & z_2^{p+M} & \cdots & z_M^{p+M} \end{bmatrix},$$

so

$$\det Z = z_1^p z_2^p \cdots z_M^p \begin{vmatrix} z_1 & z_2 & \cdots & z_M \\ z_1^2 & z_2^2 & \cdots & z_M^2 \\ \vdots & \vdots & \ddots & \vdots \\ z_1^M & z_2^M & \cdots & z_M^M \end{vmatrix} = z_1^p z_2^p \cdots z_M^p \det(V).$$

$\det V$ is a Vandermonde determinant and is equal to $z_1 z_2 \cdots z_M \prod_{1 \le j < k \le M} (z_j - z_k)$; see [8]. Then $\det Z = z_1^{p+1} z_2^{p+1} \cdots z_M^{p+1} \prod_{1 \le j < k \le M} (z_j - z_k)$. But all the $z_j, 1 \le j \le M$, are distinct, so $\det Z \neq 0$ and hence for all $0 \le p \le N - M$, $w^{(p)} \neq 0$.

We have just shown that $\hat{f} \circ \phi$ does not have $M$ consecutive zeros. By assumption $\phi(0 + (N)) = 1_G \in \operatorname{supp}(\hat{f})$. Because $|\operatorname{supp}(\hat{f})| = N/M$, we therefore have

$$\operatorname{supp}(\hat{f}) = \phi(\{0 + (N), M + (N), 2M + (N), \ldots, N - M + (N)\}),$$

as if there were a gap of length $< M - 1$ between elements in $\operatorname{supp}(\hat{f})$ then there would also have to be a gap of length $\ge M$ between elements in $\operatorname{supp}(\hat{f})$. This is a subgroup of $\widehat{G}$. Likewise, $\operatorname{supp}(f)$ is a subgroup of $G$. □

Now we prove another uncertainty principle which we shall see implies the discrete uncertainty principle.

**Theorem 7** (Entropy uncertainty principle)**.** *Let $f \in L(G)$ such that $\|f\|_{L^2(G)} = 1$. Then*

$$\frac{1}{2|G|} \sum_{x \in G} |f(x)|^2 \log |f(x)| + \frac{1}{2} \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^2 \log |\hat{f}(\xi)| \le 0.$$

*Proof.* The Hausdorff-Young inequality [7, Theorem 2.1, Chapter IV, p. 111] is that

$$\|\hat{f}\|_{L^{p'}(\widehat{G})} \le \|f\|_{L^p(G)}, \qquad f \in L(G),$$

for all $1 \le p \le 2$, where $p' = p/(p-1)$ is the dual exponent to $p$, namely $p'$ satisfies $\frac{1}{p} + \frac{1}{p'} = 1$. Let

$$A(p) = \|f\|_{L^p(G)} - \|\hat{f}\|_{L^{p/(p-1)}(\widehat{G})}.$$

Let's write out what $A(p)$ is equal to.

$$A(p) = \frac{1}{|G|^{1/p}} \left( \sum_{x \in G} |f(x)|^p \right)^{1/p} - \left( \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^{p/(p-1)} \right)^{(p-1)/p} = B(p) - C(p).$$

Then

$$\log B(p) = -\frac{1}{p} \log |G| + \frac{1}{p} \log \sum_{x \in G} |f(x)|^p$$

and

$$\frac{B'(p)}{B(p)} = \frac{\log |G|}{p^2} - \frac{1}{p^2} \log \sum_{x \in G} |f(x)|^p + \frac{1}{p} \frac{\sum_{x \in G} |f(x)|^p \log |f(x)|}{\sum_{x \in G} |f(x)|^p}.$$

Since $\|f\|_{L^2(G)} = 1$, we have $B(2) = 1$ and $\sum_{x \in G} |f(x)|^2 = |G|$. Thus

$$B'(2) = \frac{1}{2|G|} \sum_{x \in G} |f(x)|^2 \log |f(x)|.$$

Likewise,

$$\log C(p) = \frac{p-1}{p} \log \sum_{\xi \in \widehat{G}} |\hat{f}|^{p/(p-1)},$$

and

$$\frac{C'(p)}{C(p)} = \frac{1}{p^2} \log \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^{p/(p-1)} + \frac{-1}{p(p-1)} \frac{\sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^{p/(p-1)} \log |\hat{f}(\xi)|}{\sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^{p/(p-1)}}$$

Because $\|\hat{f}\|_{L^2(\widehat{G})} = 1$, $C(2) = 1$ and

$$C'(2) = -\frac{1}{2} \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^2 \log |\hat{f}(\xi)|.$$

Therefore

$$A'(2) = \frac{1}{2|G|} \sum_{x \in G} |f(x)|^2 \log |f(x)| + \frac{1}{2} \sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^2 \log |\hat{f}(\xi)|.$$

As $A(p) \geq 0$ for $1 \leq p \leq 2$ and $A(2) = 0$, $A'(2) \leq 0$. □

The above theorem is called the entropy uncertainty principle because it can be formulated in terms of the entropies of $|f|^2$ and $|\hat{f}|^2$. The entropy of $|f|^2$ is

$$h(|f|^2) = -\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 \log |f(x)|^2$$

and the entropy of $|\hat{f}|^2$ is

$$h(|\hat{f}|^2) = -\sum_{\xi \in \widehat{G}} |\hat{f}(\xi)|^2 \log |\hat{f}(\xi)|^2.$$

The discrete uncertainty principle follows from the entropy uncertainty principle.

**Corollary 8** (Entropy uncertainty principle implies discrete uncertainty principle)**.** *If $f \in L(G)$ then*

$$|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| \geq |G|.$$

*Proof.* Jensen's inequality [5, Theorem 86] is that if $\phi$ is a convex function on the interval $[a, b]$, then for $x_1, \ldots, x_n \in [a, b]$ and any $p_1, \ldots, p_n \geq 0$,

$$\phi\left(\frac{\sum_{i=1}^n p_i x_i}{\sum_{i=1}^n p_i}\right) \leq \frac{\sum_{i=1}^n p_i \phi(x_i)}{\sum_{i=1}^n p_i}.$$

Thus we have (since $\phi(x) = -\log x$ is convex)

$$\log\left(\sum_{x \in G} \frac{|f(x)|^2}{|G|} \frac{1}{|f(x)|}\right) \geq \sum_{x \in G} \frac{|f(x)|^2}{|G|} \log \frac{1}{|f(x)|} = -\sum_{x \in G} \frac{|f(x)|^2}{|G|} \log |f(x)|.$$

So

$$\begin{aligned} -\sum_{x \in G} \frac{|f(x)|^2}{|G|} \log |f(x)| &\leq \log\left(\sum_{x \in G} \frac{|f(x)|}{|G|}\right) \\ &= \log(\langle |f|, 1_{\operatorname{supp}(f)} \rangle_G) \\ &\leq \log(\|f\|_{L^2(G)} \|1_{\operatorname{supp}(f)}\|_{L^2(G)}) \\ &= \log\left(\frac{|\operatorname{supp}(f)|^{1/2}}{|G|^{1/2}}\right). \end{aligned}$$

Equivalently,

$$\frac{1}{2|G|}\sum_{x\in G}|f(x)|^2\log|f(x)| \geq -\frac{1}{2}\log\Big(\frac{|\operatorname{supp}(f)|^{1/2}}{|G|^{1/2}}\Big).$$

Also,

$$\log\Big(\sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|^2\frac{1}{|\hat{f}(\xi)|}\Big) \geq \sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|^2\log\frac{1}{|\hat{f}(\xi)|} = -\sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|^2\log|\hat{f}(\xi)|.$$

So

$$\begin{aligned}
-\sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|^2\log|\hat{f}(\xi)| &\leq \log\Big(\sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|\Big)\\
&= \log(\langle|\hat{f}|, 1_{\operatorname{supp}(\hat{f})}\rangle_{\widehat{G}})\\
&\leq \log(\|\hat{f}\|_{L^2(\widehat{G})}\|1_{\operatorname{supp}(\hat{f})}\|_{L^2(\widehat{G})})\\
&= \log|\operatorname{supp}(\hat{f})|^{1/2},
\end{aligned}$$

which is equivalent to

$$\frac{1}{2}\sum_{\xi\in\widehat{G}}|\hat{f}(\xi)|^2\log|\hat{f}(\xi)| \geq -\frac{1}{2}\log|\operatorname{supp}(\hat{f})|^{1/2}.$$

Thus by Theorem 7 we get that

$$-\frac{1}{2}\log\Big(\frac{|\operatorname{supp}(f)|^{1/2}}{|G|^{1/2}}\Big) - \frac{1}{2}\log|\operatorname{supp}(\hat{f})|^{1/2} \leq 0$$

hence

$$\log\left(\frac{|\operatorname{supp}(f)|^{1/2}|\operatorname{supp}(\hat{f})|^{1/2}}{|G|^{1/2}}\right) \geq 0,$$

which implies that

$$\frac{|\operatorname{supp}(f)|^{1/2}|\operatorname{supp}(\hat{f})|^{1/2}}{|G|^{1/2}} \geq 1.$$

□

We saw in Theorem 6 that the only $f \in L(G)$ for which $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| = |G|$ are modifications of indicator functions of subgroups of $G$. But what if the only subgroups of $G$ are the identity and $G$ itself? Then it becomes possible to get a better inequality.

The following result is due to Tao [12].

**Theorem 9** (Uncertainty principle for cyclic groups of prime order)**.** *Suppose that $|G| = p$ is prime. Then for all non-trivial $f \in L(G)$,*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1.$$

We will prove several lemmas first and then prove the above theorem.

**Lemma 10.** *Let $p$ be a prime, $n$ a positive integer, and let $P(z_1, \ldots, z_n)$ be a polynomial with integer coefficients. If $\omega_1, \ldots, \omega_n$ are $p$th roots of unity (not necessarily distinct) such that $P(\omega_1, \ldots, \omega_n) = 0$, then $P(1, \ldots, 1)$ is a multiple of $p$.*

*Proof.* Let $\omega = e^{2\pi i/p}$. Then for each $1 \leq j \leq n$, we can write $\omega_j = \omega^{k_j}$ for some $0 \leq k_j < p$. Define $Q(z) \in \mathbb{Z}[z]$ to be the remainder when $P(z^{k_1}, \ldots, z^{k_n})$ is divided by $z^p - 1$. Because $p$ is prime, the minimal polynomial of $\omega$ is the cyclotomic polynomial $\Phi_p(z) = 1 + z + \cdots + z^{p-1}$. But $Q(\omega) = 0$ and $\deg Q(z) < p$, so $Q(z)$ is an integer multiple of $\Phi_p(z)$. Therefore $Q(1) = P(1, \ldots, 1)$ is an integer multiple of $\Phi_p(1) = p$. □

The following important lemma is due to Chebotarev [11]. Our proof of the lemma is from Tao [12]. I give more details than are necessary about the differentiation of $D(z_1, \ldots, z_n)$ because this was a statement that was clearly true after a bit of thinking, yet it was not immediately clear how to write down a formal proof of it, since each time we apply $z\frac{d}{dz}$ there is a new term that we have to differentiate when we apply $z\frac{d}{dz}$ next time. Now that I've written down all of this it is more evident.

**Lemma 11.** *Let $p$ be a prime and let $1 \leq n \leq p$. Let $0 \leq x_1, \ldots, x_n \leq p-1$ be distinct and let $0 \leq \xi_1, \ldots, \xi_n \leq p-1$ be distinct. Then the matrix $(e^{2\pi i x_j \xi_k/p})_{1 \leq j,k \leq n}$ has nonzero determinant.*

*Proof.* Let $\omega_j = e^{2\pi i x_j/p}$. We have to show that $\det(\omega_j^{\xi_k})_{1 \leq j,k \leq n}$. First, define $D(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$ by

$$D(z_1, \ldots, z_n) = \det(z_j^{\xi_k})_{1 \leq j,k \leq n}. \tag{1}$$

Certainly $D(z_1, \ldots, z_n) = 0$ when $z_i = z_j$ for any $1 \leq i < j \leq n$. Therefore we can write

$$D(z_1, \ldots, z_n) = P(z_1, \ldots, z_n) \prod_{1 \leq i < j \leq n} (z_j - z_i).$$

Observe that

$$\Big(\frac{d}{dz_n}\Big)^{n-1} \prod_{1 \leq i < j \leq n} (z_j - z_i) = (n-1)! \prod_{1 \leq i < j \leq n} (z_j - z_i),$$

and thus

$$\Big(\frac{d}{dz_2}\Big) \cdots \Big(\frac{d}{dz_{n-1}}\Big)^{n-2} \Big(\frac{d}{dz_n}\Big)^{n-1} \prod_{1 \leq i < j \leq n} (z_j - z_i) = (n-1)!(n-2)! \cdots 1.$$

For $T_x = xD_x$, where $D_x f$ is the derivative of the function $f$ with respect to $x$,

$$(T_x)^n = \sum_{k=1}^{n} S(n,k) x^k (D_x)^k, \tag{2}$$

where $S(n,k)$ are the Stirling numbers of the second kind. $S(n,k)$ is the number of ways to partition a set of $n$ objects into $k$ groups. Equivalently, they may be defined using the recurrence $S(n,k) = kS(n-1,k) + S(n-1,k-1)$, $1 \leq k \leq n$, with the initial conditions $S(n,n) = S(n,1) = 1$. Using this definition it is straightfoward to prove (2) using induction. Then

$$\Big(z_2 \frac{d}{dz_2}\Big) \cdots \Big(z_{n-1} \frac{d}{dz_{n-1}}\Big)^{n-2} \Big(z_n \frac{d}{dz_n}\Big)^{n-1} = T_{z_2} \cdots T_{z_{n-1}}^{n-2} T_{z_n}^{n-1},$$

and

$$T_{z_2}\cdots T_{z_{n-1}}^{n-2}T_{z_n}^{n-1} = S(1,1)z_2D_{z_2}\cdots\sum_{k_{n-1}=1}^{n-2}S(n-2,k_{n-1})z_{n-1}^{k_{n-1}}D_{z_{n-1}}^{k_{n-1}} \cdot\sum_{k_n=1}^{n-1}S(n-1,k_n)z_n^{k_n}D_{z_n}^{k_n}.$$

At the point $z_1=\cdots=z_n=1$,

$$S(1,1)D_{z_2}\cdots\sum_{k_{n-1}=1}^{n-2}S(n-2,k_{n-1})D_{z_{n-1}}^{k_{n-1}}\cdot\sum_{k_n=1}^{n-1}S(n-1,k_n)D_{z_n}^{k_n}$$
$$=1\cdots\sum_{k_{n-1}=1}^{n-2}\sum_{k_n=1}^{n-1}S(1,1)\cdots S(n-2,k_{n-1})S(n-1,k_n)D_{z_2}\cdots D_{z_{n-1}}^{k_{n-1}}D_{z_n}^{k_n}.$$

When the above is applied to $D(z_1,\dots,z_n)=P(z_1,\dots,z_n)\prod_{1\le i<j\le n}(z_j-z_i)$ at the point $z_1=\cdots=z_n=1$, only the term in which all the differentiation operators are applied to $\prod_{1\le i<j\le n}(z_j-z_i)$ is nonzero, as otherwise there are factors $z_j-z_i$ that are equal to 0 at $z_1=\cdots=z_n=0$. Therefore the above applied to $D(z_1,\dots,z_n)$ at the point $z_1=\cdots=z_n=1$ is equal to $P(1,\dots,1)(n-1)!(n-2)!\cdots1$.

By the definition (1) of $D(z_1,\dots,z_n)$,

$$\Big(\frac{d}{dz_2}\Big)\cdots\Big(\frac{d}{dz_{n-1}}\Big)^{n-2}\Big(\frac{d}{dz_n}\Big)^{n-1}D(z_1,\dots,z_n)$$
$$=\Big(\frac{d}{dz_2}\Big)\cdots\Big(\frac{d}{dz_{n-1}}\Big)^{n-2}\Big(\frac{d}{dz_n}\Big)^{n-1}\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{j=1}^{n}z_j^{\xi_{\sigma(j)}}$$
$$=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\xi_{\sigma(n)}^{n-1}\xi_{\sigma(n-1)}^{n-2}\cdots\xi_{\sigma(2)}\cdot1\cdot\prod_{j=1}^{n}z_j^{\sigma(j)}.$$

Evaluated at the point $z_1=\cdots=z_n=1$ this is equal to

$$\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{j=1}^{n}\xi_{\sigma(j)}^{j-1}=\begin{vmatrix}1&\xi_1&\xi_1^2&\cdots&\xi_1^{n-1}\\1&\xi_2&\xi_2^2&\cdots&\xi_2^{n-1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&\xi_n&\xi_n^2&\cdots&\xi_n^{n-1}\end{vmatrix}=\prod_{1\le i<j\le n}(\xi_j-\xi_i).$$

Since $0\le\xi_1,\dots,\xi_n\le p-1$ are distinct, this product is not divisible by $p$. This product is equal to $P(1,\dots,1)(n-1)!(n-2)!\cdots1$; therefore $P(1,\dots,1)$ is not divisible by $p$. Thus by Lemma 10, $P(\omega_1,\dots,\omega_n)\neq0$. But

$$D(\omega_1,\dots,\omega_n)=P(\omega_1,\dots,\omega_n)\prod_{1\le j<k\le n}(\omega_k-\omega_j)$$

and the $\omega_j$ are all distinct, so $D(\omega_1,\dots,\omega_n)\neq0$. □

Let $p$ be prime and take $A\subseteq G=\mathbb{Z}/p\mathbb{Z}$ and $\tilde{A}\subseteq\widehat{G}$ with $|A|=|\tilde{A}|$, and define $\pi:L(\widehat{G})\to L(\tilde{A})$ by $\pi(\hat{f})=\pi\Big(\sum_{\xi\in\widehat{G}}\hat{f}(\xi)\delta_\xi\Big)=\sum_{\xi\in\tilde{A}}\hat{f}(\xi)\delta_\xi$. For $\mathscr{F}:L(G)\to L(\widehat{G})$

the Fourier transform and $\iota : L(A) \to L(G)$ the inclusion map, let $\mathscr{G} = \pi \circ \mathscr{F} \circ \iota$.

$$\begin{array}{ccc} L(G) & \xrightarrow{\mathscr{F}} & L(\widehat{G}) \\ {\scriptstyle\iota}\uparrow & & \downarrow{\scriptstyle\pi} \\ L(A) & \xrightarrow{\mathscr{G}} & L(\tilde{A}) \end{array}$$

**Theorem 12.** *For $A \subseteq G$ and $\tilde{A} \subseteq \widehat{G}$ with $|A| = |\tilde{A}|$, the map $\mathscr{G} : L(A) \to L(\tilde{A})$ defined above is an isomorphism.*

*Proof.* Let $A = \{x_1, \ldots, x_n\} \subseteq G$ and $\tilde{A} = \{\xi_1, \ldots, \xi_n\} \subseteq \widehat{G}$.

For $x \in G$ and $\eta \in \widehat{G}$, $\langle \widehat{\delta_x}, \delta_\eta \rangle_{\widehat{G}} = \frac{\overline{\eta(x)}}{|G|}$, so

$$\mathscr{G}\delta_x = \sum_{j=1}^n \frac{\overline{\xi_j(x)}}{|G|} \delta_{\xi_j}.$$

Therefore with the basis $\{\delta_{x_1}, \ldots, \delta_{x_n}\}$ for $L(G)$ and the basis $\{\delta_{\xi_1}, \ldots, \delta_{\xi_n}\}$ for $L(\widehat{G})$, the matrix for the linear map $\mathscr{G}$ is

$$\frac{1}{|G|} \begin{bmatrix} \overline{\xi_1(x_1)} & \overline{\xi_1(x_2)} & \cdots & \overline{\xi_1(x_n)} \\ \overline{\xi_2(x_1)} & \overline{\xi_2(x_2)} & \cdots & \overline{\xi_2(x_n)} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{\xi_n(x_1)} & \overline{\xi_n(x_2)} & \cdots & \overline{\xi_n(x_n)} \end{bmatrix}$$

For $0 \leq r_1, \ldots, r_n \leq p-1$ such that $x_i = r_i + (p)$ and for $0 \leq h_1, \ldots, h_n \leq p-1$ such that $\xi_j(x_i) = e^{-2\pi i h_j r_k}$ for all $1 \leq j, k \leq n$, this is equal to

$$\frac{1}{|G|} \begin{bmatrix} e^{2\pi i h_1 r_1/p} & e^{2\pi i h_1 r_2/p} & \ldots & e^{2\pi i h_1 r_n/p} \\ e^{2\pi i h_2 r_1/p} & e^{2\pi i h_2 r_2/p} & \ldots & e^{2\pi i h_2 r_n/p} \\ \vdots & \vdots & \ddots & \vdots \\ e^{2\pi i h_n r_1/p} & e^{2\pi i h_n r_2/p} & \ldots & e^{2\pi i h_n r_n/p} \end{bmatrix}$$

By Lemma 11 this matrix has nonzero determinant. Therefore $\mathscr{G} : L(A) \to L(\tilde{A})$ is an isomorphism. □

*Proof of Theorem 9.* Suppose by contradiction that there were some non-trivial $f \in L(G)$ such that $|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \leq p$. Let $A = \operatorname{supp}(f)$. Then $|\widehat{G} - \operatorname{supp}(\hat{f})| \geq |A|$, so there is a subset $\tilde{A} \subseteq \widehat{G} - \operatorname{supp}(\hat{f})$ with $|A| = |\tilde{A}|$. But $\mathscr{G}(f) = 0$ yet $f|_A \neq 0$, contradicting that $\mathscr{G} : L(A) \to L(\tilde{A})$ is an isomorphism. □

Most subsets of $G = \mathbb{Z}/N\mathbb{Z}$ are not of the form of the supports of the functions in Theorem 6. The number of subgroups of $G = \mathbb{Z}/N\mathbb{Z}$ is $d(N)$, where $N$ is the the number of positive divisors of $N$, e.g. $d(6) = 4$. If $\sigma(N)$ is the sum of the positive divisors of $N$, e.g. $\sigma(6) = 12$, then the number of cosets of subgroups of $G = \mathbb{Z}/N\mathbb{Z}$ is $d(N)\sigma(N)$. But $d(N) = O(N^\delta)$ for all $\delta > 0$ [6, Theorem 315] and $\sigma(N) = O(N^{1+\delta})$ for all $\delta > 0$ [6, Theorem 322]. So the number of cosets of subgroups of $G$ is $O(N^{1+\delta})$ for all $\delta > 0$. The number of subsets of $G$ is $2^N$. Hence the proportion of subsets of $G$ that are cosets of subgroups is $O(N^{1+\delta}2^{-N})$ for all $\delta > 0$, which is minuscule.

Now we shall go through Terence Tao's blog entry "Ostrowski lecture: The uniform uncertainty principle and compressed sensing", April 15, 2007.

If $f \in L(G)$ and $\Lambda \subseteq G$ and we can measure $\hat{f}(\xi)$ for $\xi \in \Lambda$, can we uniquely reconstruct $f$ from this information? Let us put this another way. Let $f \in L(G)$. For $\Lambda \subseteq \widehat{G}$, is there a unique $g \in L(G)$ such that $\hat{g}|_\Lambda = \hat{f}|_\Lambda$? Of course if there is such a unique $g$ then $g = f$. If $\Lambda = \widehat{G}$ then using the Fourier inversion formula there is a unique $g$ satisfying

$$\hat{g}|_\Lambda = \hat{f}|_\Lambda. \tag{3}$$

Now, the Fourier transform is an isomorphism of the vector spaces $L(G)$ and $L(\widehat{G})$, and we can define $g \in L(G)$ by defining $\hat{g} \in L(\widehat{G})$. If $\Lambda \neq G$ then there is some $\xi_0 \in \widehat{G} - \Lambda$. Take $\hat{g}(\xi)$ to be equal to $\hat{f}(\xi)$ for $\xi \neq \xi_0$ and take $\hat{g}(\xi_0) \neq \hat{f}(\xi_0)$. Then (3) is satisfied but $g \neq f$.

We say that $f \in L(G)$ is $S$-sparse if $|\operatorname{supp}(f)| \leq S$. If we know that $f \in L(G)$ is an $S$-sparse function and $\Lambda \subseteq \widehat{G}$ and we can measure $\hat{f}(\xi)$ for $\xi \in \Lambda$, can we uniquely reconstruct $f$ from this information? Again, let us put this another way. Let $f \in L(G)$ be $S$-sparse. For $\Lambda \subseteq \widehat{G}$, is there a unique $S$-sparse $g \in L(G)$ such that $\hat{g}|_\Lambda = \hat{f}|_\Lambda$?

Having unique reconstruction of all $S$-sparse signals is a property of pairs of $S$ and $\Lambda$. We have unique reconstruction with $\Lambda$ and $S$ if and only if for each $2S$-sparse $f \in L(G)$, measuring $\hat{f}$ on $\Lambda$ can determine whether $f \in L(G)$ is the zero function.

**Lemma 13.** *Let $\Lambda \subseteq \widehat{G}$ and let $S$ be a positive integer. The following are equivalent:*

1. *for all $S$-sparse $f \in L(G)$ there is a unique $S$-sparse $g \in L(G)$ such that $\hat{g}|_\Lambda = \hat{f}|_\Lambda$*
2. *for all non-trivial $2S$-sparse $f \in L(G)$ there is some $\xi \in \Lambda$ such that $\hat{f}(\xi) \neq 0$*

Certainly to reconstruct all $S$-sparse signals by measuring them on $\Lambda$ we will need that $|\Lambda| \geq S$. In fact, it is necessary that $|\Lambda| \geq 2S$.

**Lemma 14.** *A necessary condition for the statements in the previous lemma to be true is that $|\Lambda| \geq 2S$.*

*Proof.* Suppose that $|\Lambda| < 2S$. Let $U = \{0+(N), S+(N), S+1+(N), \ldots, 2S+(N)\}$ and let $\mathscr{G} : L(U) \to L(\Lambda)$ be defined by $\mathscr{G} = \pi \circ \mathscr{F} \circ \iota$, where $\iota : L(U) \to L(G)$ is the inclusion map and $\pi : L(\widehat{G}) \to L(\Lambda)$ is the projection map. $L(U)$ has dimension $2S$ while $L(\Lambda)$ has dimension $|\Lambda| < 2S$, so there is a nonzero element, say $f \in L(G)$, in the kernel of $\mathscr{G}$. Write $f = f_1 - f_2$, $f_1, f_2 \in L(G)$, where $f_1$ is supported on $\{1, \ldots, S\}$ and $f_2$ is supported on $\{S+1, \ldots, 2S\}$. Then $f_1, f_2$ are $S$-sparse functions and $\hat{f}_1|_\Lambda = \hat{f}_2|_\Lambda$, contrary to the first statement in the previous lemma. □

If we can get the Fourier support of sparse signals to be big enough, then they will have to intersect $\Lambda$. This is where uncertainty principles come into compressed sensing.

The discrete uncertainty principle (Theorem 5) tells us that we have unique reconstruction for $\Lambda$ and $S$ if $|\Lambda| > N - \frac{N}{2S}$, which hardly tells us anything.

The uncertainty principle for cyclic groups of prime order (Theorem 9) tells us something much better. It gives us unique reconstruction for $\Lambda$ and $S$ if $|\Lambda| \geq 2S$, which as we saw in Lemma 14 is the best possible.

The paper [1] of Candès, Romberg and Tao shows that most choices of frequencies $\Lambda \subseteq \widehat{G}$ are good choices: The uniform uncertainty principle (usually summing $|\hat{f}(\xi)|^2$ over a big enough $\Lambda$ will pick up its fair share of the $L^2$ energy)

When there is noise, Dirac comb examples exist for $\mathbb{Z}/p\mathbb{Z}$ using adapted bump functions on arithmetic progressions. Reconstruction of non-sparse signals (when there are $S$ possibly large coefficients and then the rest of the coefficients decay according to a power law, i.e. the $n$th coefficient decays as $O(n^{-1/p})$ for some $p > 0$) is dealt with in the other paper by Candès and Tao [2].

## References


1. Emmanuel J. Candès, Justin Romberg, and Terence Tao, *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 489–509.
2. Emmanuel J. Candes and Terence Tao, *Near-optimal signal recovery from random projections: universal encoding strategies?*, IEEE Trans. Inform. Theory **52** (2006), no. 12, 5406–5425.
3. David Donoho and Philip B. Stark, *Uncertainty principles and signal recovery*, SIAM J. Appl. Math. **49** (1989), no. 3, 906–931.
4. Gerald B. Folland and Alladi Sitaram, *The uncertainty principle: a mathematical survey*, J. Fourier Anal. Appl. **3** (1997), no. 3, 207–238.
5. G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1988, Reprint of the 1952 edition.
6. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., Oxford University Press, 1980.
7. Yitzhak Katznelson, *An introduction to harmonic analysis*, third ed., Cambridge University Press, 2004.
8. Donald E. Knuth, *The art of computer programming, volume 1: Fundamental algorithms*, third ed., Addison-Wesley, 1997.
9. E. Matusiak, M. Özaydın, and T. Przebinda, *The Donoho-Stark uncertainty principle for a finite abelian group*, Acta Math. Univ. Comenian. (N.S.) **73** (2004), no. 2, 155–160.
10. Walter Rudin, *Fourier analysis on groups*, Interscience Tracts in Pure and Applied Mathematics, no. 12, Interscience Publishers, New York, 1962.
11. P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.
12. Terence Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12** (2005), no. 1, 121–127.
13. Audrey Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, 1999.