Small-Support Uncertainty Principles on $\mathbb{Z}/p$ over Finite Fields

Saad Quader∗  Alexander Russell†  Ravi Sundaram‡

June 27, 2019

1 Introduction

Uncertainty principles are a striking manifestation of local-global phenomena in Fourier analysis, with wide-ranging applications from quantum mechanics [1] to computational complexity theory [2]. Over a finite abelian group $G$, the classical uncertainty principle asserts that any nonzero function $f : G \to \mathbb{C}$ satisfies

$$|\text{supp } f| \cdot |\text{supp } \hat{f}| \geq |G|,$$

where $\hat{f} : \mathbb{Z}/p \to \mathbb{C}$ denotes the Fourier transform of $f$, and $\text{supp } g$ denotes the support of the function $g$. It is easy to check that inequality (1) is tight for any characteristic function $1_H$ of a subgroup $H$ of $G$. More specifically, (1) is tight precisely when the function $f$ is the scaled characteristic function of a coset of a subgroup.

This suggests that the simple groups $\mathbb{Z}/p$—having no nontrivial subgroups—may play a special role in the theory and, in particular, may enjoy a stronger uncertainty principle. Indeed, a recent article of Tao [3] establishes a remarkable strengthening over these groups: any nonzero $f : \mathbb{Z}/p \to \mathbb{C}$ satisfies

$$|\text{supp } f| + |\text{supp } \hat{f}| \geq p.$$

A subsequent article of Meshulam [4] establishes an analogous statement for the groups $\mathbb{Z}/p^n$ under the (necessary) condition that the function $f$ is suitably “distant” from any subgroup coset characteristic function. These results indicate the possibility of a refined theory that establishes stronger inequalities so long as the function under consideration avoids certain “defects” described by the subgroup structure.

The analogous questions over finite fields are not as well understood. For a prime power $q$ congruent to 1 modulo $p$, the Fourier transform can be realized over the finite field $\mathbb{F}_q$, as there is a principal $p$th root of unity $\omega$ in $\mathbb{F}_p$. In particular, the $\mathbb{F}_q$-vector space of functions $\{f : \mathbb{Z}/p \to \mathbb{F}_q\}$ is spanned by the $\mathbb{F}_q$-characters

$$\chi_t : z \mapsto \omega^{tz}, \quad t \in \mathbb{Z}/p,$$

and the associated change of basis is carried out by the familiar Fourier transform matrix

$$\mathcal{F} = p^{-1} \begin{bmatrix} \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdot & \cdot & \cdots & \cdot & \cdot \end{bmatrix}.$$ 

While the uncertainty principle (1) is preserved in this setting, the extent to which it can be strengthened along the lines of (2) remains unclear. Motivated by a direct connection to the long-standing open question

∗University of Connecticut.
†University of Connecticut. This research partially supported by the NSF under grant 1717432.
‡Northeastern University. This research partially supported by NSF grants 1535929 and 1718286.
of the existence of asymptotically good cyclic codes, Evra, Kowalski, and Lubotzky have carried out a comprehensive study of this question. They point out some particular settings where \( \mathcal{P} \) fails, but conjecture that intermediate variants—that is, inequalities stronger than \( \mathcal{P} \) but not as strong as \( \mathcal{P} \)—hold in generality.

In this note, we establish a strengthened uncertainty principle for functions \( f : \mathbb{Z}/p \to \mathbb{F}_q \) with a constant support (where \( p \mid q - 1 \)). In particular we show that for any constant \( S > 0 \), functions \( f : \mathbb{Z}/p \to \mathbb{F}_q \) for which \( |\text{supp} f| = S \) must satisfy \(|\text{supp} \hat{f}| = (1 - o(1))p\). (Here the \( o(1) \) notation denotes a function which limits to zero in \( p \).) The proof relies on an application of Szemeredi’s theorem and, in fact, the celebrated improvements by Gowers translate into slightly stronger statements in our setting (permitting conclusions for functions possessing slowly growing support as a function of \( p \)).

**Theorem 1.** Let \( p \) be a prime and \( q \) be a prime power for which \( p \mid q - 1 \). Then any nonzero function \( f : \mathbb{Z}/p \to \mathbb{F}_q \) with \(|\text{supp} f| = m \) satisfies

\[
|\text{supp} \hat{f}| \geq p - r_m(p),
\]

where \( r_m(p) \) is the size of the largest subset of \( \mathbb{Z}/p \) avoiding arithmetic progressions of length \( m \).

In preparation for the remaining discussion, we record a few facts about arithmetic progressions modulo a prime \( p \). An arithmetic progression of length \( m \) in \( \mathbb{Z}/p \) is a subset of the form \( \{a + kb \mid 0 \leq k < m\} \) with cardinality \( m \). For a prime \( p \) and a natural number \( m \) we define \( r_m(p) \) to be the cardinality of the largest subset of \( \mathbb{Z}/p \) containing no arithmetic progression of length \( m \). A historic—and highly influential—result of Szemerédi established that \( r_m(p) = o(p) \) for any constant \( m \) as \( p \to \infty \). (See the book by Tao and Vu. Theorem 10.5.) In 2001, Gowers [6, Theorem 18.6] established concrete upper bounds on \( r_m \):

\[
r_m(p) \leq \frac{p}{(\log \log p)^{2-\frac{2}{\log^2 p}}}.
\]

**Proof.** With \( p \) and \( q \) as indicated in the statement of the theorem, consider a nonzero function \( f : \mathbb{Z}/p \to \mathbb{F}_q \). The Fourier expansion of \( f \) is determined by the equality

\[
\begin{bmatrix}
\hat{f}(0) \\
\vdots \\
\hat{f}(p-1)
\end{bmatrix} = p^{-1} F^{-1} \begin{bmatrix}
\ldots & \cdots & \cdots \\
\ldots & \omega^{kt} & \ldots \\
\ldots & \cdots & \ldots 
\end{bmatrix} \begin{bmatrix}
f(0) \\
\vdots \\
f(p-1)
\end{bmatrix},
\]

where \( F \) is the Fourier transform matrix discussed above. Writing

\[
S = \text{supp} f, \quad m = |S|, \quad \text{and} \quad Z = \text{supp} \hat{f},
\]

we first note that every minor of \( F \) given by the columns indexed by \( S \) and the rows indexed by a subset \( Z' \subset Z \) of size \( m \) must be degenerate. Otherwise, considering that \( f \) is nonzero precisely in the coordinates indexed by \( S \), a non-degenerate minor would necessarily induce a non-zero coordinate (of \( \hat{f} \)) in the set \( Z' \subset Z \) (of zeros of \( \hat{f} \)).

To complete the proof, we will see that any \( m \times m \) minor of \( F \) indexed, say, by sets \( K = \{k_1, \ldots, k_m\} \) of columns and \( L \) of rows, must necessarily have full rank if \( L \) is an arithmetic progression. This will complete the proof, as we conclude that \( Z \) can contain no arithmetic progression and hence must have cardinality no more than \( r_m(p) \), as desired. It remains to check that a minor indexed by the sets \( K \) and \( L \), as described above, is non-degenerate. If the rows \( L \) form the arithmetic progression \( a, a + b, \ldots, a + (m - 1)b \) the
determinant of the resulting matrix can be computed exactly:

\[
\begin{pmatrix}
\omega^{a k_1} & \ldots & \omega^{a k_m} \\
\omega^{(a+b)k_1} & \ldots & \omega^{(a+b)k_m} \\
\vdots & \ddots & \vdots \\
\omega^{(a+(m-1)b)k_1} & \ldots & \omega^{(a+(m-1)b)k_m}
\end{pmatrix}
\]

\[
= \det
\begin{pmatrix}
(\omega^{b k_1})^0 & \ldots & (\omega^{b k_m})^0 \\
(\omega^{b k_1})^1 & \ldots & (\omega^{b k_m})^1 \\
\vdots & \ddots & \vdots \\
(\omega^{b k_1})^{m-1} & \ldots & (\omega^{b k_m})^{m-1}
\end{pmatrix}
\cdot \prod_i \omega^{a k_i}
\]

where we recognize (†) as a Vandermonde matrix. This is nonzero, considering that \( b \neq 0 \) and the \( k_i \) are distinct.

**Remark.** Over the field \( \mathbb{C} \), every minor of the \( \mathbb{Z}/p \) Fourier transform matrix has full rank. This fact—originally discovered by Chebotarev in the 1930s (cf. Stevenhagen and Lenstra [9])—has been given attention by many authors (cf. Dieudonné [10], Frenkel [11], Evans and Isaacs [12], Reshetnyak [13], Newman [14]), and—along with the same relationship applied above between degenerate minors and the uncertainty principle—is the basic algebraic fact supporting the proof of the strong uncertainty principle over \( \mathbb{C} \) by Tao [3]. On the other hand, Evra et al. [5] provide examples of minors that are degenerate in the finite field setting. The development above provides an upper estimate for how many rows can be selected while avoiding full rank.

**Acknowledgements.** We thank Shai Evra for explaining the history of the problem and for pointing out that the proof can be realized over alternate coefficient rings.

**References**

[1] David Griffiths. *Introduction to Quantum Mechanics*. Pearson Prentice Hall, 2nd edition edition, 1995.

[2] David A Mix Barrington, Howard Straubing, and Denis Thérien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, 1990.

[3] Terence Tao. An uncertainty principle for cyclic groups of prime order. *arXiv preprint math/0308286*, 2003.

[4] Roy Meshulam. An uncertainty inequality for finite abelian groups. *European Journal of Combinatorics*, 27(1):63–67, 2006.

[5] Shai Evra, Emmanuel Kowalski, and Alexander Lubotzky. Good cyclic codes and the uncertainty principle. *arXiv preprint arXiv:1703.01080* 2017.

[6] William T Gowers. A new proof of Szemerédi’s theorem. *Geometric & Functional Analysis GAFA*, 11(3):465–588, 2001.

[7] Endre Szemerédi. On sets of integers containing \( k \) elements in arithmetic progression. *Acta Arithmetica*, 27(1):199–245, 1975.

[8] Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

[9] Peter Stevenhagen and Hendrik Willem Lenstra. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.
[10] Jean Dieudonné. Une propriété des racines de lunité. In Collection of articles dedicated to Alberto González Domínguez on his sixty-fifth birthday, volume 25, pages 1–3. Unión Matemática Argentina, 1970/71.

[11] PE Frenkel. Simple proof of Chebotarev’s theorem on roots of unity. arXiv preprint math/0312398, 2003.

[12] RJ Evans and IM Isaacs. Generalized Vandermonde determinants and roots of unity of prime order. Proceedings of the American Mathematical Society, 58(1):51–54, 1976.

[13] Yuri Grigorievich Reshetnyak. New proof of a theorem of NG Chebotarev. Uspekhi Matematicheskikh Nauk, 10(3):155–157, 1955.

[14] Morris Newman. On a theorem of Čebotarev. Linear and Multilinear Algebra, 3(4):259–262, 1976.