Research Article

Diego Fernando Díaz Padilla and Jesús Alonso Ochoa Arango*

On an uncertainty principle for small index subgroups of finite fields

https://doi.org/10.1515/math-2025-0178
received September 25, 2024; accepted June 11, 2025

Abstract: In this article, we continue the study of the *nonvanishing minors property* initiated by Garcia, Karaali, and Katz, for the compressed Fourier matrix attached to a subgroup H of the multiplicative group of a finite field $\mathbb{F}_q$ and a character χ defined over H. Here, we provide a characterization of this aforementioned property for *symmetries* arising from an index-3 subgroup H and a nontrivial character χ.

Keywords: Fourier transform, DFT matrix, compressed Fourier transform, nonvanishing minors, uncertainty principle, Gauss sum, finite field, group character

MSC 2020: 43A32, 42A99, 43A25, 42A38, 15A15

1 Introduction

In discrete Fourier analysis, *uncertainty principles* have played an essential role due to their profound implications in signal processing. The study of these relations began in 1989 with the well-known theorem of Donoho and Stark [1]. Before stating this result, let us remind that if G is a finite group, the group algebra of G over $\mathbb{C}$, denoted by $\mathbb{C}[G]$, is the $\mathbb{C}$-vector space spanned by G,

$$\mathbb{C}[G] = \left\{\sum_{g\in G} f_g g : f_g \in \mathbb{C}\right\},$$

endowed with the convolution product. In what follows, G will denote an arbitrary finite abelian group. Recall that given $f \in \mathbb{C}[G]$, the *Fourier transform* of f is the function $\hat{f} : \hat{G} \to \mathbb{C}$ given by

$$\hat{f}(\chi) := \sum_{g\in G} f_g \chi(g),$$

where $\hat{G}$ denotes the group of characters of G. The Donoho-Stark uncertainty principle for finite abelian groups states that if $f \in \mathbb{C}[G]$ is nonzero, then

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

where $\operatorname{supp}(f) := \{g \in G : f_g \neq 0\}$ and $|X|$ denotes the cardinality of a set X. Various generalizations and results emerged from this principle, for instance [2,3], but perhaps the most important of all these is due to Tao, who in [4] proved that by considering G to be the cyclic group $\mathbb{Z}/p\mathbb{Z}$ of prime order p, a substantial improvement can be obtained: if $f \in \mathbb{C}[G]$ is nonzero, then

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1. \tag{1.1}$$

*** Corresponding author: Jesús Alonso Ochoa Arango,** Department of Mathematics, Faculty of Science, Pontificia Universidad Javeriana, Bogotá, Colombia, e-mail: jesus.ochoa@javeriana.edu.co

Diego Fernando Díaz Padilla: Department of Mathematics, University of Southern California, Los Angeles, California, United States, e-mail: dfdiaz@usc.edu

This remarkable result, also discovered independently by Biró [5] and Meshulam [6], led to the developments in [7] that gave rise to the field of *compressed sensing* and several new uncertainty relations. For more about this, see [8], where the uncertainty result was generalized to arbitrary finite cyclic groups, or [9–11] for relations to the performance of cyclic codes and group codes; other studies can be found in [12–14].

At the core of these improvements is *Chebotarëv's theorem* on roots of unity, originally proposed by Ostrowski and proved by Chebotarëv in 1926 [15]. In Tao's article [4], it is proved that, indeed, Chebotarëv's theorem is equivalent to (1.1). The theorem establishes that every minor of the *discrete Fourier transform matrix* (DFT matrix) is nonzero if the matrix has prime order. To be accurate,

Theorem 1.1. (Chebotarëv) *Let p be a prime and ζ a primitive pth root of unity. For every pair of subsets $I, J \subseteq \mathbb{F}_p$ with the same cardinality, the matrix $(\zeta^{ij})_{i\in I, j\in J}$ is nonsingular, i.e., it has nonvanishing determinant.*

The property that every minor of a given matrix is nonzero is of particular interest in this article, so we introduce the following definition:

Definition 1.2. (Nonvanishing minors [NVM] property) A matrix $A = (a_{i,j})_{1\leq i,j\leq n}$ with complex entries is said to have the NVM property if for every $I, J \subseteq \{1, \ldots, n\}$ with $|I| = |J|$, the determinant of $(a_{i,j})_{i\in I, j\in J}$ is nonzero.

The equivalence of (1.1) with Chebotarëv's theorem raises the question of whether other transformations related to the discrete Fourier transform exhibit the NVM property in their matrix representations, and if this leads to improved uncertainty principles. For example, if $n \geq 1$ is an odd integer, then it can be proved that the $\frac{n+1}{2} \times \frac{n+1}{2}$ matrix attached to the *discrete cosine transform* (DCT) satisfies the NVM property if and only if n is prime or $n = 1$; similarly, if we let $n \geq 3$ be an odd integer, in the case of the *discrete sine transform* (DST), it can be proved that the $\frac{n-1}{2} \times \frac{n-1}{2}$ matrix attached to this transform satisfies the NVM property if and only if n is a prime (see [16] for more details).

Let $\mathbb{F}_q$ denote the finite field with q elements. Garcia et al. [16] made significant improvements on (1.1) by introducing a general notion of symmetry on elements of $\mathbb{C}[\mathbb{F}_q]$ that encompasses the aforementioned DCT and DST cases. Given a subgroup $H \leq \mathbb{F}_q^\times$ and a complex character $\chi : H \to \mathbb{C}^\times$, an element $f = \sum f_a a \in \mathbb{C}[\mathbb{F}_q]$ is said to be *χ-symmetric* if $f_{ha} = \chi(h) f_a$ for all $h \in H$ and $a \in \mathbb{F}_q$. When considering the Fourier transform on $\mathbb{C}[\mathbb{F}_q]$ restricted to the subspace of χ-symmetric elements, we arrive at the *compressed Fourier transform* (CFT) attached to the pair (H, χ) (see Definition 2.2). For instance, if p is an odd prime, $H = \{-1, 1\}$ and the character χ is such that $\chi(-1) = -1$, then χ-symmetric elements correspond precisely to elements f such that $f_{-a} = -f_a$ and the CFT corresponds to the DST. The introduction of the CFT led to the study of the NVM property for its associated matrix. For non-prime finite fields, general conditions for the NVM property to be satisfied for the CFT matrix were not obtained; however, for certain subgroups H of a non-prime field $\mathbb{F}_q$, they arrive, for example, to the following results:

- If $H = \{1\}$, then the CFT matrix does not satisfy the NVM property; refer to [16, Corollary 6.2].
- If $H = \mathbb{F}_q^\times$ or, in the case q is odd, if H an index-2 subgroup, and χ is the trivial character, then the CFT matrix exhibits the NVM property; for more details, see [16, Proposition 6.5 and Theorem 6.6].
- If q is odd, H an index-2 subgroup, and χ nontrivial, a characterization was found in terms of Gaussian sums of character extensions [16, Theorem 6.7].
- Again, if q is odd, $3|(q-1)$, H is an index-3 subgroup, and χ is the trivial character, the NVM property holds if and only if $p \equiv 1 \pmod 3$, where p is the characteristic of $\mathbb{F}_q$ (see [16, Theorem 6.12]).

In this article, we pursue this approach by providing concise necessary and sufficient conditions for the NVM property to hold in the case of index-3 subgroups H and nontrivial characters χ.

1.1 Structure of this article

In Section 2, we will review some basic notions of character theory and discrete Fourier analysis and then introduce the necessary ideas from [16], such as χ-symmetry and the CFT. In Section 3, we present our main result, Theorem 3.2, which characterizes the NVM property of the CFT matrix for index-3 subgroups and nontrivial characters.

2 Preliminaries

2.1 Characters and the Fourier transform

We begin by recalling the basic concepts of character theory on finite fields. For a more detailed explanation, we refer the reader to [17].

An *additive character* of $\mathbb{F}_q$ is a group homomorphism from the additive group of $\mathbb{F}_q$ into the group $\mathbb{C}^\times$. Similarly, a *multiplicative character* of $\mathbb{F}_q$ is a group homomorphism now defined on the multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$. It is well known that one way to obtain a complete description of additive characters is by introducing the *canonical additive character*: let p be the characteristic of $\mathbb{F}_q$, so that $q = p^m$ for some $m \in \mathbb{N}$, and consider the additive character $\varepsilon : \mathbb{F}_q \to \mathbb{C}^\times$ defined by $\varepsilon(x) := e^{2\pi i \operatorname{Tr}(x)/p}$ for all $x \in \mathbb{F}_q$, where

$$\operatorname{Tr}(x) := x + x^p + \ldots + x^{p^{m-1}}$$

is the *absolute trace* map from $\mathbb{F}_q$ to $\mathbb{F}_p$. It can be shown that for every additive character ψ, there exists $a \in \mathbb{F}_q$ such that $\psi(x) = \varepsilon(ax)$ for all $x \in \mathbb{F}_q$, which allows us to define the character $\varepsilon_a : \mathbb{F}_q \to \mathbb{C}^\times$ given by $\varepsilon_a(x) = \varepsilon(ax)$ for all $x \in \mathbb{F}_q$. Denote by $\hat{\mathbb{F}}_q$ the group of additive characters of $\mathbb{F}_q$, and if $S \subseteq \mathbb{F}_q$ define $\varepsilon_S := \{\varepsilon_s : s \in S\} \subseteq \hat{\mathbb{F}}_q$, as in [16], so that $\varepsilon_{\mathbb{F}_q} = \hat{\mathbb{F}}_q$.

There is a relevant connection between multiplicative and additive characters in a finite field in terms of certain exponential sums called Gaussian sums. Let χ be a multiplicative and ψ an additive character of $\mathbb{F}_q$. The *Gaussian sum* $G(\chi, \psi)$ is defined as

$$G(\chi, \psi) := \sum_{c \in \mathbb{F}_q^\times} \chi(c)\psi(c),$$

and we will use the notation $G(\chi)$ when $\psi = \varepsilon$. Perhaps one of the most important facts about Gaussian sums, and one that we will use later, is that if ψ and χ are both nontrivial, then we have $|G(\chi, \psi)| = \sqrt{q}$ (see [17, Theorem 5.11] for more details). The sum $G(\chi, \psi)$ is closely related to the Fourier expansion of the multiplicative character χ, as we now show. Let $\mathbb{C}^{\hat{\mathbb{F}}_q}$ be the $\mathbb{C}$-vector space of functions from $\hat{\mathbb{F}}_q$ to $\mathbb{C}$ (the expression X^Y is interpreted similarly) endowed with pointwise multiplication, and define the Fourier transform of $f \in \mathbb{C}[\mathbb{F}_q]$ as the map $\hat{f} : \hat{\mathbb{F}}_q \to \mathbb{C}$ given by:

$$\hat{f}(\psi) := \sum_{a \in \mathbb{F}_q} f_a \psi(a).$$

The $\mathbb{C}$-algebra isomorphism $\mathcal{F} : \mathbb{C}[\mathbb{F}_q] \to \mathbb{C}^{\hat{\mathbb{F}}_q}$ given by $\mathcal{F}(f) := \hat{f}$ is called the *Fourier transform on* $\mathbb{C}[\mathbb{F}_q]$, and its inverse $\mathcal{F}^{-1}$ is given by $\hat{f} \mapsto \mathcal{F}^{-1}(\hat{f}) = \sum f_a a$, where

$$f_a = \frac{1}{q} \sum_{\psi \in \hat{\mathbb{F}}_q} \overline{\psi(a)} \hat{f}(\psi).$$

We can extend a multiplicative character $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ to a multiplicative map defined over the whole $\mathbb{F}_q$ by simply mapping $\chi(0) = 0$. If we use the standard identification $\mathbb{C}[\mathbb{F}_q] \cong \mathbb{C}^{\mathbb{F}_q}$ and the definition of the Fourier transform, we can prove that $\hat{\chi}(\overline{\psi}) = G(\chi, \overline{\psi})$ for every $\psi \in \hat{\mathbb{F}}_q$. Moreover, if we seek the value of χ at $c \in \mathbb{F}_q^\times$, we can use the Fourier inversion formula to obtain the remarkable expression:

$$\chi(c) = \frac{1}{q}\sum_{\psi\in\hat{\mathbb{F}}_q} G(\chi,\overline{\psi})\psi(c),$$

in which Gaussian sums are precisely the Fourier coefficients in this expansion.

2.2 CFT

We now introduce, with some small modifications, the main definitions from [16]. Let H be a subgroup of the multiplicative group $\mathbb{F}_q^\times$ and $\chi : H \to \mathbb{C}^\times$ a character. Let $\mathbf{GL}(V)$ denote the group of automorphisms on a $\mathbb{C}$-vector space V, and define the map $\mathcal{L}(\chi) : H \to \mathbf{GL}(\mathbb{C}[\mathbb{F}_q])$ as follows:

$$\mathcal{L}(\chi)_h\left(\sum_{a\in\mathbb{F}_q} f_a a\right) := \sum_{a\in\mathbb{F}_q}\chi(h)f_a ha.$$

The map $\mathcal{L}(\chi)$ is a group homomorphism, and $\mathcal{L}(\chi)_h$ is a linear isomorphism of $\mathbb{C}$-vector spaces for each $h \in H$. Intuitively, $\mathcal{L}(\chi)_h$ permutes each coefficient of $f \in \mathbb{C}[\mathbb{F}_q]$ and scales them by a root of unity.

We are interested in the elements of $\mathbb{C}[\mathbb{F}_q]$ that are invariant under the action of $\mathcal{L}(\chi)$, i.e., elements of the set:

$$\mathbb{C}[\mathbb{F}_q]^\chi := \{f \in \mathbb{C}[\mathbb{F}_q] : \mathcal{L}(\chi)_h(f) = f, \text{ for all } h \in H\}.$$

It can be easily shown that the set $\mathbb{C}[\mathbb{F}_q]^\chi$ is a $\mathbb{C}$-vector subspace of $\mathbb{C}[\mathbb{F}_q]$. This subspace is actually H-invariant, that is to say, $\mathcal{L}(\chi)_h(f) \in \mathbb{C}[\mathbb{F}_q]^\chi$ for all $f \in \mathbb{C}[\mathbb{F}_q]^\chi$ and $h \in H$. The dependency on both the subgroup H and the character χ leads to the following definition:

Definition 2.1. (χ-symmetry) Let H be a subgroup of $\mathbb{F}_q^\times$ and $\chi : H \to \mathbb{C}^\times$ be a character. Elements of $\mathbb{C}[\mathbb{F}_q]^\chi$ are called *χ-symmetric*, or equivalently, $f \in \mathbb{C}[\mathbb{F}_q]$ is said to be *χ-symmetric*, provided that $f_{ha} = \chi(h)f_a$ for all $h \in H$ and $a \in \mathbb{F}_q$.

Let us recall that, given H a subgroup of $\mathbb{F}_q^\times$, the H-orbits of $\mathbb{F}_q$ are of the form $Ha = \{ha : h \in H\}$ for $a \in \mathbb{F}_q$, and when $a \neq 0$, they correspond precisely to the cosets of H in the group $\mathbb{F}_q^\times$. We say that (χ, S) is an *orbit-representative pair of H* if S is a complete set of representatives of the H-orbits of $\mathbb{F}_q$ if χ is trivial, or of all of $\mathbb{F}_q^\times$ if χ is nontrivial. If additionally, we have another set R with the same property, then (χ, R, S) is called an *orbit-representative 3-tuple of H*.

Definition 2.2. (CFT) Let H be a subgroup of $\mathbb{F}_q^\times$ and $\chi : H \to \mathbb{C}^\times$ be a character. Let (χ, S) be an orbit-representative pair of H. Recall that ε_S denotes the set of additive characters of the form ε_s for $s \in S$. The $\mathbb{C}$-vector space isomorphism

$$\begin{aligned}\mathcal{F}_\chi : \mathbb{C}[\mathbb{F}_q]^\chi &\to \mathbb{C}^{\varepsilon_S}\\ f &\mapsto \hat{f}\ |_{\varepsilon_S}\end{aligned}$$

is referred to as the *(χ, S)-CFT*.

Remark 2.3. The fact that $\mathcal{F}_\chi$ is an isomorphism [16, Proposition 3.10] shows that a χ-symmetric element f can be reconstructed with exactly $[\mathbb{F}_q^\times : H]$ measurements of its Fourier transform when χ is nontrivial, and with $[\mathbb{F}_q^\times : H] + 1$ measurements when χ is trivial, i.e., one measurement on each orbit is sufficient to achieve this by the invertibility of $\mathcal{F}_\chi$.

To obtain a matrix representation for the CFT, it is necessary to determine some basis for $\mathbb{C}[\mathbb{F}_q]^{\chi}$. To this end, in [16, Lemma 3.9], the authors attach a suitable basis $\{u_{\chi,r}\}_{r\in R}$ to each orbit-representative pair (χ, R) of H. Thus, if we fix an orbit-representative 3-tuple (χ, R, S) of H, where R and S are endowed with some orderings, the representation matrix in this basis of the CFT is referred to as the (χ, R, S)-*CFT matrix*. For our purpose, it will not be necessary to introduce this basis since, as will be seen in the next section, an explicit expression for the entries of the (χ, R, S)-CFT matrix is already known [16]. Note also that the order of this matrix is $[\mathbb{F}_q^{\times} : H]$ when χ is nontrivial, and $[\mathbb{F}_q^{\times} : H] + 1$ if χ is trivial. If $S = R$ and we impose the same ordering, then the (χ, R, S)-CFT matrix is symmetric.

Since the NVM property for CFT matrices is independent of the choice of sets of representatives and orderings then, for simplicity, it is said that the pair $(\mathbb{F}_q, \chi)$ has or does not have the *NVM property*. The next proposition, proved in [16], provides a criteria, in terms of χ-symmetric functions, for a pair $(\mathbb{F}_q, \chi)$ to have the NVM property:

Proposition 2.1. [16, Proposition 4.8] *Let $H \le \mathbb{F}_q^{\times}$ and $\chi : H \to \mathbb{C}^{\times}$ be a character. Then, $(\mathbb{F}_q, \chi)$ has the NVM property if and only if for every nonzero χ-symmetric element $f \in \mathbb{C}[\mathbb{F}_q]^{\chi}$, we have*

(1) *if χ is nontrivial,*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \ge q + |H| - 1,$$

(2) *if χ is trivial,*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \ge \begin{cases} q + 2|H| - 1, & \textit{if } f_0 = 0 \textit{ and } \hat{f}(\varepsilon_0) = 0, \\ q + |H|, & \textit{if } f_0 = 0 \textit{ or } \hat{f}(\varepsilon_0) = 0, \\ q + 1, & \textit{otherwise}. \end{cases}$$

The aforementioned proposition gives us an alternative version of the NVM property directly related to the uncertainty principle of Biró-Meshulam-Tao.

3 Index-3 subgroups and nontrivial characters

The NVM property of $(\mathbb{F}_q, \chi)$ when H is an index-3 subgroup and χ is the trivial character is satisfied if and only if $p \equiv 1 \pmod 3$, where p is the characteristic of $\mathbb{F}_q$ [16, Theorem 6.12]. Our result completes the characterization for nontrivial characters by giving concise necessary and sufficient conditions for the NVM property to hold.

We shall comment on character extensions. Suppose H is a subgroup of a finite abelian group G, and let $\chi : H \to \mathbb{C}^{\times}$ be a character. If we denote the set of extensions of χ to G by $\mathrm{Ext}(\chi)$, it can be proved that its cardinality is the index $[G : H]$. To describe this set of extensions, consider first the *annihilator* of H in $\hat{G}$:

$$\mathrm{Ann}(H) \coloneqq \{\chi \in \hat{G} : \chi(h) = 1, \text{ for all } h \in H\}.$$

It can be shown that the annihilator of H in $\hat{G}$ is a subgroup of $\hat{G}$ of order $[G : H]$. If we write $s = [G : H]$ and $\mathrm{Ann}(H) = \{\vartheta_0, \vartheta_1, \ldots, \vartheta_{s-1}\}$ then, given an extension φ_0 of χ, it is clear that for every $\vartheta_i \in \mathrm{Ann}(H)$ the product $\varphi_0\vartheta_i$ is an extension of χ, and there are precisely s extensions, hence

$$\mathrm{Ext}(\chi) = \varphi_0 \mathrm{Ann}(H) = \{\varphi_0\vartheta_i : i = 0, \ldots, s-1\}.$$

Given $H \le \mathbb{F}_q^{\times}$ and a character $\chi : H \to \mathbb{C}^{\times}$, the Gaussian sums (with $\psi = \varepsilon$) of the $s = [\mathbb{F}_q^{\times} : H]$ character extensions $\varphi_0, \varphi_1, \ldots, \varphi_{s-1}$ are denoted as G_i for all $i \in \{0, 1, \ldots, s-1\}$. Now we are ready to state the following technical lemma that provides the entries of the CFT matrices:

Lemma 3.1. [16, Lemma 6.4] *Let $\mathbb{F}_q$ be a finite field, let m be a positive integer such that $m|(q-1)$, and H be the unique index-m subgroup of $\mathbb{F}_q^{\times}$. Let $\chi : H \to \mathbb{C}^{\times}$ be a character and (χ, R, S) an orbit-representative 3-tuple of H.*

Then, for any $r \in R$ and $s \in S$, the (r, s)-entry of a (χ, R, S)-CFT matrix is

$$[\mathcal{F}_\chi]_{r,s} = \begin{cases} |H|, & \text{if } rs = 0, \\ \dfrac{1}{m}\displaystyle\sum_{i=0}^{m-1} \overline{\varphi_i}(rs)G_i, & \text{if } rs \neq 0. \end{cases}$$

When fixing a character $\chi : H \to \mathbb{C}^\times$ of an index-3 subgroup $H \leq \mathbb{F}_q^\times$, given the notation G_i for the Gaussian sums of its character extensions, we introduce for simplicity the notation $T_j \coloneqq \sum_{i=0}^{2} \zeta_3^{ji} G_i$ for $j \in \mathbb{Z}$, where $\zeta_3 = e^{2\pi i/3}$.

Theorem 3.2. *Let $\mathbb{F}_q$ be a finite field such that $3|(q-1)$, let H be the unique index-3 subgroup in $\mathbb{F}_q^\times$, and let $\chi : H \to \mathbb{C}^\times$ be a nontrivial character. Then, the pair $(\mathbb{F}_q, \chi)$ has the NVM property if and only if $G_i \neq G_j$ for some $i, j \in \{1, 2, 3\}$ and $T_0 \neq 0$.*

Proof. Let κ and $\overline{\kappa}$ be so that $\{\chi_0, \kappa, \overline{\kappa}\}$ is the annihilator of H, i.e., κ and $\overline{\kappa}$ are the cubic multiplicative characters of $\mathbb{F}_q^\times$. Let $\alpha \in \mathbb{F}_q$ be such that $\overline{\kappa}(\alpha) = \zeta_3$. Consider $R = S = \{1, \alpha, \alpha^2\}$; this way (χ, R, S) is an orbit-representative 3-tuple of H. Let φ_0 be a character extension of χ and φ_1, φ_2 the other two extensions $\varphi_0\kappa$ and $\varphi_0\overline{\kappa}$, respectively. The (χ, R, S)-CFT matrix is then

$$\begin{bmatrix} \dfrac{T_0}{3} & \dfrac{\overline{\varphi_0}(\alpha)T_1}{3} & \dfrac{\overline{\varphi_0}(\alpha^2)T_2}{3} \\ \dfrac{\overline{\varphi_0}(\alpha)T_1}{3} & \dfrac{\overline{\varphi_0}(\alpha^2)T_2}{3} & \dfrac{T_0}{3} \\ \dfrac{\overline{\varphi_0}(\alpha^2)T_2}{3} & \dfrac{T_0}{3} & \dfrac{\overline{\varphi_0}(\alpha)T_1}{3} \end{bmatrix}.$$

We may scale rows and columns to obtain the matrix

$$M = \begin{bmatrix} T_0 & T_1 & T_2 \\ T_1 & T_2 & T_0 \\ T_2 & T_0 & T_1 \end{bmatrix},$$

which has the NVM property if and only if the (χ, R, S)-CFT matrix does. The minors of 1×1 submatrices are precisely the entries T_0, T_1, and T_2. For the minors of 2×2 submatrices, one can check that these are, up to sign, of the form $T_{i+1}T_{i+2} - T_i^2$ for $i \in \{0, 1, 2\}$, where the index j in T_j is considered mod 3. The result of this expression can be reduced by grouping the products of Gaussian sums and using the fact that $\zeta_3^2 + \zeta_3 - 2 = -3$:

$$\begin{aligned} T_{i+1}T_{i+2} - T_i^2 &= -3(\zeta_3^{2i}G_0G_2 + \zeta_3^{i}G_0G_1 + G_1G_2) \\ &= -3G_0G_1G_2\left(\frac{\zeta_3^{2i}}{G_1} + \frac{\zeta_3^{i}}{G_2} + \frac{1}{G_0}\right) \\ &= -3G_0G_1G_2\left(\frac{\zeta_3^{2i}\overline{G_1}}{|G_1|^2} + \frac{\zeta_3^{i}\overline{G_2}}{|G_2|^2} + \frac{\overline{G_0}}{|G_0|^2}\right). \end{aligned}$$

Since Gaussian sums all have absolute value $\sqrt{q}$, we obtain

$$T_{i+1}T_{i+2} - T_i^2 = -\frac{3G_0G_1G_2}{q}\overline{(\zeta_3^{i}G_1 + \zeta_3^{2i}G_2 + G_0)} = -\frac{3G_0G_1G_2}{q}\overline{T_i}.$$

Therefore, the 2×2 minors can be reduced to the entries T_j for $j \in \{0, 1, 2\}$, so that $T_{i+1}T_{i+2} - T_i^2 = 0$ if and only if $T_i = 0$. Finally, the determinant of M, which is the only minor of a 3×3 submatrix, is $-27G_0G_1G_2$ and is never zero. With these results at hand, the NVM property is satisfied if and only if T_0, T_1, and T_2 are all nonzero. First, suppose the NVM property holds, then we just have to show that $G_i \neq G_j$ for some $i, j \in \{0, 1, 2\}$. If $G_0 = G_1 = G_2$, then $T_1 = T_2 = 0$ arriving at a contradiction.

For the converse, suppose T_0 is nonzero and $G_i \neq G_j$ for some $i, j \in \{0, 1, 2\}$. Assume $T_1 = 0$, then since Gaussian sums have absolute value $\sqrt{q}$, it follows that $\zeta_3 G_1 = \zeta_3^{\gamma} G_0$ and $\zeta_3^2 G_2 = \zeta_3^{\beta} G_0$, for some combination $\gamma, \beta \in \{1, 2\}$ such that $\gamma + \beta = 3$. If $\gamma = 1$ and $\beta = 2$, then $G_1 = G_0 = G_2$, which is not possible, and if $\gamma = 2$ and $\beta = 1$, then $G_1 = \zeta_3 G_0$ and $G_2 = \zeta_3^2 G_0$, which leads to $T_0 = 0$, again a contradiction. Following, assume $T_2 = 0$, then again $\zeta_3^2 G_1 = \zeta_3^{\gamma} G_0$ and $\zeta_3 G_2 = \zeta_3^{\beta} G_0$ for combination $\gamma, \beta \in \{1, 2\}$ such that $\gamma + \beta = 3$. If $\gamma = 1$ and $\beta = 2$, then $G_1 = \zeta_3^2 G_0$ and $G_2 = \zeta_3 G_0$, which leads to $T_0 = 0$, and if $\gamma = 2$ and $\beta = 1$, then $G_1 = G_0 = G_2$. Thus, the result holds. □

An equivalent formulation of Theorem 3.2 in terms of an uncertainty principle can be achieved with Proposition 2.1:

Corollary 3.3. *Let $\mathbb{F}_q$ be a finite field with $3|(q-1)$, and let H be the unique index-3 subgroup of $\mathbb{F}_q^\times$. Let $\chi : H \to \mathbb{C}^\times$ be a nontrivial character. For every nonzero χ-symmetric element $f \in \mathbb{C}[\mathbb{F}_q]^{\chi}$, we have*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geq q + \frac{q-1}{3} - 1,$$

if and only if $G_i \neq G_j$ for some $i, j \in \{1, 2, 3\}$ and $T_0 \neq 0$.

Proof. It is a direct consequence of Theorem 3.2 and Proposition 2.1. □

Remark 3.4. Before finishing, it is worth mentioning a few words about symmetric elements in the complex group algebra of a finite field $\mathbb{F}_q$. In the trivial character case, the symmetric elements boil down to those elements $f \in \mathbb{C}[\mathbb{F}_q]$ with constant value f_a on each H-orbit Ha, for all $a \in \mathbb{F}_q$. When χ is nontrivial, the χ-symmetric elements can be described as follows: suppose $d \mid (q-1)$ and that H is the unique subgroup of order d, so that $H = \langle \omega \rangle$ with ω a primitive dth root of unity in $\mathbb{F}_q^\times$. Let $\chi : H \to \mathbb{C}^\times$ be the character defined by $\chi(\omega) = \zeta_d$, where $\zeta_d = e^{2\pi i/d}$. All other characters are of the form $\varphi = \chi^k$ for some $k \in \{0, 1, \ldots, d-1\}$, consequently $\varphi(\omega) = \zeta_d^k$. Then, an element $f \in \mathbb{C}[\mathbb{F}_q]$ is φ-symmetric if and only if $f_{\omega^j a} = \zeta_d^{kj} f_a$ for all $j \in \{0, \ldots, d-1\}$.

With regard to the NVM property for CFT matrices, the question remains whether more characterizations can be found for subgroups of larger index in terms of concise conditions, for both trivial and nontrivial characters.

Acknowledgments: The authors would like to thank Daniel J. Katz for his suggestions and observations regarding Theorem 3.2 that helped to improve the result. Diego Fernando Díaz Padilla would like to express sincere gratitude to Jesús Alonso Ochoa Arango for guidance and support during the development of his undergraduate thesis [18], from which the results of this article are derived.

Funding information: This work was supported by Pontificia Universidad Javeriana at Bogotá, Colombia, under the research project with ID 9714.

Author contributions: Both authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all the results, and approved the final version of the manuscript. Both authors contributed equally to the manuscript.

Conflict of interest: The authors state no conflicts of interest.

Data availability statement: Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] D. L. Donoho and P. B. Stark, *Uncertainty principles and signal recovery*, SIAM J. Appl. Math. **49** (1989), no. 3, 906–931.

[2] R. Meshulam, *An uncertainty inequality for groups of order pq*, European J. Combin. **13** (1992), no. 5, 401–407.

[3] K. T. Smith, *The uncertainty principle on groups*, SIAM J. Appl. Math. **50** (1990), no. 3, 876–882.

[4] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. **12** (2005), no. 1, 121–127.

[5] A. Biró, *Schweitzer Competition, Problem 3*, 1998, https://www.math.u-szeged.hu/~mmaroti/schweitzer/schweitzer-1998.pdf.

[6] R. Meshulam, *An uncertainty inequality for finite abelian groups*, European J. Combin. **27** (2006), no. 1, 63–67.

[7] E. J. Candes, J. Romberg, and T. Tao, *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information*, IEEE Trans. Inf. Theory **52** (2006), no. 2, 489–509.

[8] M. Ram Murty and J. P. Whang, *The uncertainty principle and a generalization of a theorem of Tao*, Linear Algebra Appl. **437** (2012), no. 1, 214–220.

[9] M. Borello and P. Solé, *The uncertainty principle over finite fields*, Discrete Math. **345** (2022), no. 1, 112670.

[10] S. Evra, E. Kowalski, and A. Lubotzky, *Good cyclic codes and the uncertainty principle*, Enseign. Math. **63** (2017), no. 3–4, 305–332.

[11] M. Borello, W. Willems, and G. Zini, *On ideals in group algebras: An uncertainty principle and the Schur product*, Forum Math. **34** (2022), no. 5, 1345–1354.

[12] A. Bonami and S. Ghobber, *Equality cases for the uncertainty principle in finite Abelian groups*, Acta Sci. Math. **79** (2013), no. 3, 507–528.

[13] S. Ghobber and P. Jaming, *On uncertainty principles in the finite dimensional setting*, Linear Algebra Appl. **435** (2011), no. 4, 751–768.

[14] F. Nicola, *The uncertainty principle for the short-time Fourier transform on finite cyclic groups: Cases of equality*, J. Funct. Anal. **284** (2023), no. 12, 109924.

[15] P. Stevenhagen and H. W. Lenstra, *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), 26–37.

[16] S. R. Garcia, G. Karaali, and D. J. Katz, *An improved uncertainty principle for functions with symmetry*, J. Algebra **586** (2021), 899–934.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[18] D. F. D. Padilla, *An uncertainty principle for functions with symmetries over finite fields*, Undergraduate Thesis, Pontificia Universidad Javeriana, 2023.