ARTICLE IN PRESS

Linear Algebra and its Applications xxx (2012) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

The uncertainty principle and a generalization of a theorem of Tao

M. Ram Murty [*,1], Junho Peter Whang [2]

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

ARTICLE INFO

Article history:
Received 4 October 2011
Accepted 11 February 2012
Available online xxxx

Submitted by R. Brualdi

AMS classification:
42A99

Keywords:
Uncertainty principle
Finite cyclic groups
The Weyl character formula

ABSTRACT

Let G be a finite abelian group. If $f : G \to \mathbb{C}$ is a nonzero function with Fourier transform $\hat{f}$, the classical uncertainty principle states that $|\mathrm{supp}(f)||\mathrm{supp}(\hat{f})| \geqslant |G|$. Recently, Tao showed that, if G is cyclic of prime order p, then in fact a stronger inequality $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant p + 1$ holds. In this paper, we use representation theory of the unitary group and Weyl's character formula to derive a generalization of Tao's result for arbitrary finite cyclic groups.

1. Introduction

Let G be a finite abelian group, and let $\widehat{G}$ denote the set of irreducible characters of G. Given a function $f : G \to \mathbb{C}$, its Fourier transform $\hat{f} : \widehat{G} \to \mathbb{C}$ is given by

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

The classical uncertainty principle for finite abelian groups states that, if f is nonzero, then $|\mathrm{supp}(f)||\mathrm{supp}(\hat{f})| \geqslant |G|$.

Recently, Tao [6] proved a substantial strengthening of the uncertainty principle for cyclic groups of prime order. He showed that, for any prime number p and a nonzero function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$, we have

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant p + 1.$$

* Corresponding author. Tel.: +1 613 533 2413; fax: +1 613 533 2964.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), 8jpw1@queensu.ca (J.P. Whang).

[1] The first author was supported in part by an NSERC Discovery grant.
[2] The second author was supported by an NSERC Undergraduate Student Research Award.

0024-3795/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2012.02.009

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

Central to Tao's argument is a classical theorem of Chebotarev: given a primitive pth root of unity ω, every minor of the matrix $(\omega^{ij})_{1\leqslant i,j\leqslant p}$ is nonzero. Many papers have been written on providing new proofs of this result; see Section 5 for a particularly short proof.

In this paper, we describe an approach to Chebotarev's theorem relying on the representation theory of the unitary group $\mathbf{U}(n)$, which allows us to generalize Tao's theorem in the following way. Let $m > 1$ be an integer with prime factorization $m = p_1^{a_1}\cdots p_r^{a_r}$. For $X \subseteq \mathbb{Z}/m\mathbb{Z}$, let $P(X)$ denote the property: X is represented by integers $\kappa_1, \ldots, \kappa_n$ satisfying

$$\frac{\prod_{1\leqslant i<j\leqslant n}|\kappa_i - \kappa_j|}{\prod_{1\leqslant i<j\leqslant n}(j-i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r.$$

Our main theorem is the following.

Theorem. *Let $m > 1$ be an integer, and let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ be a nonzero function. If $P(\mathrm{supp}(f))$ or $P(\mathrm{supp}(\hat{f}))$ holds, then*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant m + 1.$$

Conversely, suppose A and B are subsets of $\mathbb{Z}/m\mathbb{Z}$ satisfying $|A| + |B| \geqslant m + 1$. If $P(A)$ holds, then there is a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that $\mathrm{supp}(f) \subseteq A$ and $\mathrm{supp}(\hat{f}) = B$. If furthermore $P(B)$ holds, then f can be made so that $\mathrm{supp}(f) = A$.

(Here, we identify $\widehat{\mathbb{Z}/m\mathbb{Z}}$ with $\mathbb{Z}/m\mathbb{Z}$ by fixing a primitive mth root of unity; see Section 4 for details.)

For the convenience of the reader, we review the basic representation theory of $\mathbf{U}(n)$ necessary for the proof. While the machinery involved is more complicated than the methods used in Tao [6], it presents a different perspective on the non-vanishing phenomenon in Chebotarev's theorem.

One of the referees has pointed out to us that this representation-theoretic approach had also been found independently by Stanley [5, p. 505], who used it to give a short proof of Chebotarev's theorem.

2. Background

For an integer $n \geqslant 1$, let $\mathbf{U}(n)$ be the group of complex unitary matrices. Then $\mathbf{U}(n)$ forms a compact, connected, real Lie group. It contains, as a maximal torus (i.e. a compact, connected, abelian Lie subgroup maximal with respect to inclusion), the group T consisting of diagonal matrices

$$t = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n) := \begin{bmatrix} \varepsilon_1 & & \\ & \ddots & \\ & & \varepsilon_n \end{bmatrix}, \quad \varepsilon_i = e^{2\pi\sqrt{-1}\theta_i}.$$

Where no confusion arises, we shall write $f(\varepsilon_1, \ldots, \varepsilon_n) := f(\mathrm{diag}(\varepsilon, \ldots, \varepsilon))$ and $f(1) := f(1, \ldots, 1)$ for any function f defined on T.

In this paper, we shall mean by a *weight* a sequence $\kappa = (\kappa_1, \ldots, \kappa_n) \in \mathbb{Z}^n$. A weight κ is *dominant* if $\kappa_1 \geqslant \cdots \geqslant \kappa_n$, and *strictly dominant* if all of these inequalities are strict. Given a weight κ, define the function $e^\kappa : T \to \mathbb{C}$ by setting $e^\kappa(t) = e^\kappa(\varepsilon_1, \ldots, \varepsilon_n) = \varepsilon_1^{\kappa_1}\cdots\varepsilon_n^{\kappa_n}$ for each $t \in T$. An element $s \in S_n$ of the symmetric group acts on the weight κ by $s \cdot \kappa = (\kappa_{s^{-1}(1)}, \ldots, \kappa_{s^{-1}(n)})$.

It turns out that any element of a compact, connected Lie group is conjugate to an element of its maximal torus. In our case, each element of $\mathbf{U}(n)$ is conjugate to some $t \in T$, so any character of $\mathbf{U}(n)$, being a class function, is determined by its behavior on T. By the Weyl character formula, each dominant weight λ corresponds to a unique irreducible character χ_λ of $\mathbf{U}(n)$, given by

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

$$\chi_\lambda(t) = \frac{\sum_{s\in S_n} \operatorname{sgn}(s) e^{s\cdot(\lambda+\rho)}(t)}{\sum_{s\in S_n} \operatorname{sgn}(s) e^{s\cdot\rho}(t)} = \frac{\det(\varepsilon_i^{\lambda_j+\rho_j})}{\det(\varepsilon_i^{\rho_j})}, \quad \forall t \in T,$$

where we define $\rho = (n-1, n-2, \ldots, 1, 0)$. By the dimension formula, the degree of χ_λ, defined as $\deg \chi_\lambda := \chi_\lambda(1)$, is given by the expression,

$$\chi_\lambda(1) = \frac{\prod_{1\leqslant i<j\leqslant n}(\kappa_i - \kappa_j)}{\prod_{1\leqslant i<j\leqslant n}(j-i)}, \quad (\kappa = \lambda + \rho). \tag{$*$}$$

Note that the degree of χ_λ is equal to the dimension of the vector space V_λ underlying the representation (π_λ, V_λ) of $\mathbf{U}(n)$ associated to χ_λ.[3]

We remark that the assignment $\lambda \mapsto \chi_\lambda$ in fact sets up a bijection between the dominant weights and all irreducible characters of $\mathbf{U}(n)$. For more about the representation theory of compact Lie groups, see [1,4,9].

Finally, we recall the following result by Lam and Leung [2] on vanishing sums of roots of unity, which we will use in order to generalize Chebotarev's theorem in the next Section.

Lemma 1 (Lam and Leung [2]). *Let $p_1, \ldots, p_r$ be the prime factors of m. The set $W(m)$ of integers $n \geqslant 0$ for which there exists a vanishing sum $\omega_1 + \cdots + \omega_n = 0$, where each ω_i is an mth root of unity, is precisely*

$$W(m) = \mathbb{N}p_1 + \cdots + \mathbb{N}p_r.$$

3. Minors of Vandermonde matrices

Let $m > 1$ be an integer, and let ω be a primitive mth root of unity. The connection between an $n \times n$ minor of the Vandermonde matrix $V(m) = (\omega^{ij})_{1\leqslant i,j\leqslant m}$ and the irreducible representations of $\mathbf{U}(n)$ is given by the following.

First, an $n \times n$ submatrix of $V(m)$ is of the form $(\omega^{\iota_i\kappa_j})_{1\leqslant i,j\leqslant n}$, where we can choose $(\iota_1, \ldots, \iota_n)$ and $(\kappa_1, \ldots, \kappa_n)$ to be strictly dominant weights, each having pairwise distinct entries modulo m. In the arguments which follow, we will focus on the weight $(\kappa_1, \ldots, \kappa_n)$, and suppress $(\iota_1, \ldots, \iota_n)$ by denoting $\omega_i = \omega^{\iota_i}$ for each $1 \leqslant i \leqslant n$.

Since κ is strictly dominant, $\lambda = \kappa - \rho$ is a dominant weight, corresponding to an irreducible character χ_λ of $\mathbf{U}(n)$. By the Weyl character formula, we obtain

$$\det(\omega_i^{\kappa_j}) = \chi_\lambda(\omega_1, \ldots, \omega_n) \det(\omega_i^{\rho_j}).$$

But we easily see that $\det(\omega_i^{\rho_j}) = \pm\prod_{1\leqslant i<j\leqslant n}(\omega_i - \omega_j)$, which is nonzero. Hence, the vanishing of the minor $\det(\omega_i^{\kappa_j})$ is equivalent to the vanishing of the character χ_λ at $\operatorname{diag}(\omega_1, \ldots, \omega_n) \in \mathbf{U}(n)$. Using this key observation, we now have the following generalization of Chebotarev's theorem to composite moduli.

Proposition 2. *Let $p_1, \ldots, p_r$ be the prime factors of m. Let $\kappa_1, \ldots, \kappa_n$ be integers distinct modulo m such that*

$$\frac{\prod_{1\leqslant i<j\leqslant n}|\kappa_i - \kappa_j|}{\prod_{1\leqslant i<j\leqslant n}(j-i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r. \tag{$**$}$$

Then $\det(\omega_i^{\kappa_j}) \neq 0$ for any distinct mth roots of unity $\omega_1, \ldots, \omega_n$.

[3] It is worth noting that the dimension formula leads to the following result: given distinct positive numbers $\kappa_1 > \kappa_2 > \cdots > \kappa_n$, then $(*)$ implies that $\prod(j-i) \mid \prod(\kappa_i - \kappa_j)$. It would be interesting to see if a proof using elementary number theory can be given for this fact.

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

Proof. By rearranging $\kappa_1, \ldots, \kappa_n$ if necessary, we may assume that $\kappa = (\kappa_1, \ldots, \kappa_n)$ is a strictly dominant weight. Hence, it suffices to show that $\chi_\lambda(\omega_1, \ldots, \omega_n) \neq 0$, where $\lambda := \kappa - \rho$.

Let π_λ be the representation of $\mathbf{U}(n)$ corresponding to χ_λ. For convenience, let us denote $\widetilde{\omega} = \operatorname{diag}(\omega_1, \ldots, \omega_n) \in \mathbf{U}(n)$. Since $\widetilde{\omega}^m = 1$, we have $\pi_\lambda(\widetilde{\omega})^m = 1$, for π_λ being a group homomorphism. In particular, every eigenvalue of $\pi_\lambda(\widetilde{\omega})$ is an mth root of unity. Hence, $\chi_\lambda(\widetilde{\omega}) = \operatorname{tr} \pi_\lambda(\widetilde{\omega})$ is a sum of mth roots of unity, and there are exactly $\deg(\chi_\lambda)$ of them, counting multiplicity. Suppose $\chi_\lambda(\widetilde{\omega}) = 0$. Then by Lemma 1, $\deg(\chi_\lambda) \in \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$. But together with the dimension formula, our hypothesis excludes this possibility; hence the result. □

Remark. In the case $m = p$ is prime, the condition $(**)$ is automatically satisfied for any set of integers $\kappa_1, \ldots, \kappa_n$ distinct modulo p. Hence, we obtain Chebotarev's theorem as an immediate corollary.

As another special case when $m = q$ is a prime power, note that $(**)$ is satisfied if $\kappa_1, \ldots, \kappa_n$ is an arithmetic progression with common difference r, with $(q, r) = 1$. In Section 5, we show that a version of Proposition 2 in this special case still holds when we replace q by any modulus.

4. Proof of the main theorem

Let $m > 1$ be an integer, and let ω be a fixed primitive mth root of unity. For each irreducible character χ of $\mathbb{Z}/m\mathbb{Z}$, there is a unique $i \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\chi(j) = \omega^{ij}, \quad \forall j \in \mathbb{Z}/m\mathbb{Z}.$$

The assignment $\chi \mapsto i$ is a bijection, and we shall identify $\widehat{\mathbb{Z}/m\mathbb{Z}}$ with $\mathbb{Z}/m\mathbb{Z}$ by this map. Let $A \subseteq \mathbb{Z}/m\mathbb{Z}$ be a subset. As in Section 1, let $P(A)$ denote the property: A is represented by integers $\kappa_1, \ldots, \kappa_n$ satisfying

$$\frac{\prod_{1 \leqslant i < j \leqslant n} |\kappa_i - \kappa_j|}{\prod_{1 \leqslant i < j \leqslant n} (j - i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r,$$

where $p_1, \ldots, p_r$ are the prime factors of m. Also, let $\ell^2(A)$ denote the set of functions $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ which are zero outside of A. We present an immediate corollary of Proposition 2, following Tao [6].

Corollary 3. *Let $A, \widetilde{A} \subseteq \mathbb{Z}/m\mathbb{Z}$ be nonempty subsets of equal cardinality. Suppose $P(A)$ or $P(\widetilde{A})$ holds. Then the linear map $T : \ell^2(A) \to \ell^2(\widetilde{A})$ given by $Tf = \hat{f}|_{\widetilde{A}}$ is an isomorphism.*

The corollary follows immediately from Proposition 2. Indeed, the coefficient matrix of T above is essentially of the form considered in Proposition 2. Below, we restate our main theorem and give its proof.

Theorem 4. *Let $m > 1$ be an integer, and let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ be a nonzero function. If $P(\operatorname{supp}(f))$ or $P(\operatorname{supp}(\hat{f}))$ holds, then*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geqslant m + 1.$$

Conversely, suppose A and B are subsets of $\mathbb{Z}/m\mathbb{Z}$ satisfying $|A| + |B| \geqslant m + 1$. If $P(A)$ holds, then there is a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that $\operatorname{supp}(f) \subseteq A$ and $\operatorname{supp}(\hat{f}) = B$. If furthermore $P(B)$ holds, then f can be made so that $\operatorname{supp}(f) = A$.

Proof. We proceed along the lines of Tao [6]. We first consider the case where $P(\operatorname{supp}(f))$ holds. Suppose $|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \leqslant m$ for a contradiction. Then there exists a subset $\widetilde{A} \subseteq \mathbb{Z}/m\mathbb{Z}$ such that $|\operatorname{supp}(f)| = |\widetilde{A}|$ and $\operatorname{supp}(\hat{f}) \cap \widetilde{A} = \emptyset$. Let T be the linear map of Corollary 3 for $A = \operatorname{supp}(f)$ and $\widetilde{A}$. By the corollary, Tf is nonzero since f is nonzero. But then we have $\operatorname{supp}(\hat{f}) \cap \widetilde{A} = \operatorname{supp}(Tf) \neq \emptyset$, contradicting our hypothesis on $\widetilde{A}$. Thus $|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geqslant m + 1$.

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

The case where $P(\mathrm{supp}(\hat{f}))$ holds follows from the first case and the Fourier inversion formula. Let $g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ be the function given by $g(x) = \hat{f}(-x)$, $\forall x \in \mathbb{Z}/m\mathbb{Z}$. Then $\mathrm{supp}(g) = \{-x : x \in \mathrm{supp}(\hat{f})\}$, so $P(\mathrm{supp}(g))$ holds, and also $|\mathrm{supp}(g)| = |\mathrm{supp}(\hat{f})|$. Then by the first case, we have

$$|\mathrm{supp}(g)| + |\mathrm{supp}(\hat{g})| \geqslant m + 1.$$

But by the Fourier inversion formula, we have

$$\mathcal{F}(\hat{g})(x) = \frac{1}{m} g(-x) = \frac{1}{m} \hat{f}(x), \quad \forall x \in \mathbb{Z}/m\mathbb{Z},$$

where $\mathcal{F}(\hat{g})$ refers to the Fourier transform of $\hat{g}$ (cf. [7, p. 36]; note that their definition of Fourier transform differs from ours by a multiplicative factor). This implies that $m\hat{g} = f$ by the uniqueness of the Fourier transform, so in particular we have $|\mathrm{supp}(\hat{g})| = |\mathrm{supp}(f)|$. Then $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant m + 1$ by the inequality above, as desired.

We now prove the converse. For the first statement, it suffices to prove the case $|A| + |B| = m + 1$, for we can apply the claim to the pair A, B' for varying $B' \subseteq B$ such that $|A| + |B'| = m + 1$, and take generic linear combinations to obtain f.

So assume $|A| + |B| = m + 1$. For each $\xi \in B$, let A_ξ be the complement of $B \setminus \{\xi\}$ in $\mathbb{Z}/m\mathbb{Z}$. Then since $P(A)$ holds and $|A| = |A_\xi|$, applying Corollary 3 there exists $f_\xi \in \ell^2(A)$ such that $\hat{f}_\xi$ is zero on $A_\xi \setminus \{\xi\}$ and nonzero at ξ. We thus have $\mathrm{supp}(\hat{f}_\xi) \subseteq B$ for each $\xi \in B$. By taking generic linear combinations of the functions f_ξ, we obtain a function $f \in \ell^2(A)$ such that $\mathrm{supp}(\hat{f}) = B$. This gives the first statement of the converse.

For the second statement, we again use the Fourier inversion formula. So suppose furthermore that $P(B)$ holds. Then $P(-B)$ holds, and hence by the first statement of the converse there exists $g \in \ell^2(-B)$ such that $\mathrm{supp}(\hat{g}) = A$. Let $f_1 = \hat{g}$, so $\mathrm{supp}(f_1) = A$. From the Fourier inversion formula, we obtain $\mathrm{supp}(\hat{f}_1) \subseteq B$. Let $f_2 \in \ell^2(A)$ be such that $\mathrm{supp}(\hat{f}_2) = B$, as constructed in the first statement. Taking a generic linear combination of f_1 and f_2, we obtain a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that $\mathrm{supp}(f) = A$ and $\mathrm{supp}(\hat{f}) = B$, as desired. □

Motivated by the remark in Tao [6], we present the following application of our main result. Let $m > 1$ be an integer, and let $P(z) = \sum_{j=1}^{n} c_j z^{\kappa_j}$ be a polynomial with $n \geqslant 1$ nonzero complex coefficients, where the exponents $\kappa_1, \ldots, \kappa_n$ are integers distinct modulo m such that

$$\frac{\prod_{1 \leqslant i < j \leqslant n} |\kappa_i - \kappa_j|}{\prod_{1 \leqslant i < j \leqslant n} (j - i)} \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_r,$$

where $p_1, \ldots, p_r$ are the prime factors of m. Then $P(z)$ has at most $n - 1$ zeros which are mth roots of unity. For, viewing $P(\omega^j)$ as a function of $j \in \mathbb{Z}/m\mathbb{Z}$, its having n nonzero coefficients implies that the support of its Fourier transform has cardinality n. Thus its support has cardinality at least $m + 1 - n$ by Theorem 4, and hence P has at most $n - 1$ zeros on the set of mth roots of unity.

Let p be a prime number. The Cauchy–Davenport inequality states that, for any two nonempty subsets A and B of $\mathbb{Z}/p\mathbb{Z}$, we have the inequality

$$|A + B| \geqslant \min(|A| + |B| - 1, p),$$

where $A + B := \{a + b : a \in A, b \in B\}$. Theorem 4 allows us to generalize the Cauchy–Davenport inequality in the following way.

Theorem 5. *Let $m > 1$ be an integer, and let A and B be subsets of $\mathbb{Z}/m\mathbb{Z}$ such that $P(A)$ and $P(B)$ hold. Then*

$$|A + B| \geqslant \min(|A| + |B| - 1, m).$$

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

Proof. We proceed as in Tao [6]. Since A and B are nonempty, there exist $X, Y \subseteq \mathbb{Z}/m\mathbb{Z}$ such that $|A| + |X| = |Y| + |B| = m + 1$, and $|X \cap Y| = \max(|X| + |Y| - m, 1)$. Furthermore, we may choose X and Y so that $P(X \cap Y)$ holds, noting that $P(X \cap Y)$ holds if it is given by an arithmetic progression with common difference 1. Then by Theorem 4, there exist functions f and g such that

$$\operatorname{supp}(f) \subseteq A, \quad \operatorname{supp}(\hat{f}) = X, \quad \operatorname{supp}(g) \subseteq B, \quad \operatorname{supp}(\hat{g}) = Y.$$

Then $\operatorname{supp}(f * g) \subseteq A + B$ and $\operatorname{supp}(\widehat{f * g}) = X \cap Y$. Since $P(X \cap Y)$ holds and $f * g$ is nonzero, by Theorem 4 we have $|A + B| + |X \cap Y| \geqslant m + 1$, which gives $|A + B| \geqslant \min(2m + 1 - |X| - |Y|, m)$. Using the definition of X and Y, we obtain the desired result. □

5. Remarks

Below, we give a proof of Chebotarev's theorem using only the rudimentary tools of algebraic number theory. While the approach is not the one mainly explored in this paper, the proof is notable in its particular simplicity and short length.

Theorem 6. *Let p be a prime number, and let ζ_p be a primitive pth root of unity. Let $A, B \subseteq \{0, \ldots, p-1\}$ such that $|A| = |B|$. Then* $\det(\zeta_p^{ij})_{i \in A, j \in B} \neq 0$.

Proof. We use the well-known fact that $(1 - \zeta_p)$ is a prime ideal with norm p in the p-th cyclotomic field (see [8]). Note that $\det(\zeta_p^{ij})_{i \in A, j \in B} = 0$ is equivalent to saying that there exist $c_j, j \in B$, not all zero, such that $P(x) = \sum_{j \in B} c_j x^j$ vanishes at $x = \zeta_p^i$, for all $i \in A$. We can choose $c_j \in \mathbb{Z}[\zeta_p]$ and assume that not all c_j are divisible by $1 - \zeta_p$. Since $P(x) = \prod_{i \in A}(x - \zeta_p^i)G(x)$ where $G(x) \in \mathbb{Z}[\zeta_p][x]$, we see that $P(x) \mod (1 - \zeta_p)$ has a zero of order $|A|$ at $x = 1$. Thus

$$\sum_{j \in B} c_j (j)_t \equiv 0 \mod (1 - \zeta_p), \quad \forall t = 0, \ldots, |A| - 1,$$

where $(j)_t := j(j-1)\cdots(j-t+1)$. By easy induction, this implies that

$$\sum_{j \in B} c_j j^t \equiv 0 \mod (1 - \zeta_p).$$

But since the Vandermonde determinant $\det(j^t)_{j \in B, t \in \{0, \ldots, |A|-1\}}$ is nonzero, it follows that $c_j \equiv 0 \mod (1 - \zeta_p)$ for all $j \in B$, contradicting our assumption. It follows that $\det(\zeta_p^{ij})_{i \in A, j \in B} \neq 0$. □

The connection between minors of the Vandermonde matrix and representations of the unitary group, considered in the main sections of this paper, may be exploited further. Here we present another result exemplifying this idea, weakly analogous to Chebotarev's theorem.

Proposition 7. *Let $m > 1$ be an integer. For $1 \leqslant n \leqslant m$, let $\omega_1, \ldots, \omega_n$ be distinct mth roots of unity. Let $\kappa_1, \ldots, \kappa_n$ be an arithmetic progression of integers with common difference r, where $(m, r) = 1$. Then* $\det(\omega_i^{\kappa_j}) \neq 0$.

Proof. Since $(m, r) = 1$, we have $rs \equiv -1 \mod m$ for some integer s. Recalling the notation $\omega_i = \omega^{\iota_i}$ where ι_i are distinct modulo m, we have

$$(\omega_i^{\kappa_j}) = (\omega^{\iota_i(\kappa_1 + r(j-1))}) = (\omega^{-rs\iota_i(\kappa_1 + r(j-1))}) = ((\omega^{-r\iota_i})^{s\kappa_1 - (j-1)}).$$

Since ω^r is also a primitive mth root of unity, it follows that $\omega^{-r\iota_1}, \ldots, \omega^{-r\iota_n}$ are distinct. Replacing $\kappa_1, \ldots, \kappa_n$ by $s\kappa_1, s\kappa_1 - 1, \ldots, s\kappa_1 - (n-1)$, we may therefore assume that $r = -1$. Then κ is a strictly dominant weight, so it suffices to show that $\chi_{\kappa - \rho}(\omega_1, \ldots, \omega_n) \neq 0$. But we see that

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009

$$\deg(\chi_{\kappa-\rho}) = \frac{\prod_{1\leqslant i<j\leqslant n}(\kappa_i - \kappa_j)}{\prod_{1\leqslant i<j\leqslant n}(j-i)} = \frac{\prod_{1\leqslant i<j\leqslant n}(j-i)}{\prod_{1\leqslant i<j\leqslant n}(j-i)} = 1$$

by the dimension formula, so $\chi_{\kappa-\rho}$ is a group homomorphism from $\mathbf{U}(n)$ to $\mathbb{C}^\times$; in particular, it is zero nowhere. The desired result follows. □

Arguing as in the proof of the main theorem, we obtain the following result as an immediate corollary of Proposition 7. For any subset $X \subseteq \mathbb{Z}/m\mathbb{Z}$, let $Q(X)$ denote the property: X is represented by an arithmetic progression $\kappa_1, \ldots, \kappa_n$ with common difference coprime to m.

Corollary 8. *Let $m > 1$ be an integer, and let $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ a nonzero function. If $Q(\mathrm{supp}(f))$ or $Q(\mathrm{supp}(\hat{f}))$ holds, then*

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geqslant m + 1.$$

Arguing as before, one may obtain a partial converse to the corollary above and results on zeros of scarce polynomials and the Cauchy–Davenport inequality, analogous to those derived in Section 4.

Based on the connection we have expounded in this paper, it seems evident that nonvanishing results for irreducible characters of $\mathbf{U}(n)$ on points of finite order may lead to further generalizations of Tao's theorem for finite cyclic groups.

A different generalization of Tao's theorem was given by Meshulam [3] for arbitrary finite abelian groups. Let G be a finite abelian group of order m, and let $f : G \to \mathbb{C}$ be a nonzero function. If $d_1 < d_2$ are consecutive divisors of m such that $d_1 \leqslant |\mathrm{supp}(f)| \leqslant d_2$, then Meshulam's result states that

$$|\mathrm{supp}(\hat{f})| \geqslant \frac{n}{d_1 d_2}(d_1 + d_2 - |\mathrm{supp}(f)|).$$

In the case of cyclic groups, our results give more precise bounds in certain cases, especially when $|\mathrm{supp}(f)|$ is near a divisor of the group order. It seems reasonable to conjecture that, for general finite abelian groups, there will be conditions similar to those in Theorem 4 or Corollary 8 which imply inequalities of Tao's type.

Acknowledgements

We thank Mike Roth and D. Suryaramana for some useful remarks on a previous version of this paper. We also thank the referees for their helpful comments.

References

[1] W. Fulton, J. Harris, Representation Theory, A First Course, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, 2001.
[2] T.Y. Lam, K.H. Leung, On vanishing sums of roots of unity, J. Algebra 109 (1995) 91–109.
[3] R. Meshulam, An uncertainty inequality for finite abelian groups, European J. Combin. 27 (1) (2006) 37–63.
[4] J.P. Serre, Linear Representations of Finite Groups, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, 1977.
[5] R.P. Stanley, Enumerative Combinatorics, vol. 2, Cambridge Studies in Advanced Mathematics, 62, Cambridge University Press, 1999.
[6] T. Tao, An uncertainty principle for cyclic groups of prime order, Math. Res. Lett. 12 (1) (2005) 121–127.
[7] A. Terras, Fourier Analysis on Finite Groups and Applications, London Mathematical Society Student Texts, 43, Cambridge University Press, 1999.
[8] L.C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, 83, Springer-Verlag, 1982.
[9] H. Weyl, The Classical Groups, Their Invariants and Representations, Princeton Landmarks in Mathematics, Princeton University Press, 1997.

Please cite this article in press as: M.R. Murty, J.P. Whang, The uncertainty principle and a generalization of a theorem of Tao, Linear Algebra Appl. (2012), doi:10.1016/j.laa.2012.02.009