Highly Composite: Papers in Number Theory, RMS-Lecture Notes Series No. 23, 2016, pp. 77–85.

Some Remarks on the Discrete Uncertainty Principle

M. Ram Murty

Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada
e-mail: murty@mast.queensu.ca

Abstract. We give a survey of recent results related to the uncertainty principle for finite groups. We begin by discussing the abelian case, and give a simplified proof of a theorem of Tao in the case of cyclic groups. We then discuss variations of this theme and make some remarks in the non-abelian case.

Keywords. Uncertainty principle, Chebotarev's theorem, Tao's theorem, Descartes rule of signs.

Subject Classification: 11B30, 11B50, 11B75

Dedicated to Professor R. Balasubramanian on the occasion of his 60th birthday.

1. Introduction

The classical uncertainty principle of quantum mechanics asserts that the position of a particle and its momentum cannot both be measured accurately. More precisely, if σ_x denotes the standard deviation of position of a particle, and σ_p the standard deviation of its momentum, then

$$\sigma_x \sigma_p \geq \frac{\hbar}{2},$$

where $\hbar$ denotes Planck's constant. This result can be reformulated in the terminology of harmonic analysis and it translates into the assertion that a function and its Fourier transform cannot simultaneously be sharply localised. For an excellent survey on the classical uncertainty principle, we refer the reader to [2]. In this paper, we will discuss versions of the uncertainty principle as they apply to finite groups both abelian and non-abelian. In 2005, Tao [8] gave a remarkable improvement of this in the case of (cyclic) groups of prime order. Below, we give a simplified treatment due to the author and Whang [5]. Here, we will also discuss generalizations to the non-cyclic and non-abelian cases as well as amplify the Lie-theoretic perspective enunciated in [5].

2. The uncertainty principle for finite abelian groups

Let G be a finite abelian group and let $f : G \to \mathbb{C}$ be a complex-valued function not identically zero. To each character χ of G, we define

$$\widehat{f}(\chi) := \sum_{a \in G} \overline{\chi(a)} f(a).$$

The support of f, denoted $S(f)$, is defined as the set of elements $a \in G$ for which $f(a)$ is non-zero. Similarly, the support of $\widehat{f}$, denoted $S(\widehat{f})$, is the set of characters χ for which $\widehat{f}(\chi)$ is non-zero. Then, the uncertainty principle for G takes the form:

Theorem 1. *For any $f : G \to \mathbb{C}$, not identically zero,*

$$|S(f)||S(\widehat{f})| \geq |G|.$$

Proof. First, we note that f is identically zero if and only if $\widehat{f}$ is identically zero. So we may suppose $\widehat{f} \not\equiv 0$. From the definition of $\widehat{f}$, we have

$$\sup_{\chi} |\widehat{f}(\chi)| \leq \left(\sup_{a \in G} |f(a)| \right) |S(f)|. \tag{1}$$

By Fourier inversion,

$$f(a) = \frac{1}{|G|} \sum_{\chi} \chi(a) \widehat{f}(\chi),$$

so that

$$|f(a)| \leq \frac{1}{|G|} \left(\sup_{\chi} |\widehat{f}(\chi)| \right) |S(\widehat{f})|.$$

Hence

$$\sup_{a \in G} |f(a)| \leq \frac{1}{|G|} \left(\sup_{\chi} |\widehat{f}(\chi)| \right) |S(\widehat{f})|.$$

Putting these together in (1), we get

$$\sup_{\chi} |\widehat{f}(\chi)| \leq \frac{1}{|G|} \left(\sup_{\chi} |\widehat{f}(\chi)| \right) |S(f)||S(\widehat{f})|,$$

which gives the result as $\widehat{f}$ is not identically zero so that $\sup_{\chi} |\widehat{f}(\chi)| \neq 0$. □

We remark that Tao's proof [8] of the above uses Plancherel's theorem and the Cauchy-Schwarz inequality. The proof above uses neither.

3. Chebotarev's determinant theorem

Tao's improvement of the uncertainty principle in the case of cyclic groups of prime order relies on an old result of Chebotarev which we state and prove here. N. G. Chebotarev is most famous for his density theorem in algebraic number theory (see for example, [4]). However, there is a lesser known result of his proved in 1926 (see [6]) which is central to Tao's argument.

Theorem 2. *Let p be a prime number and let ζ_p be a primitive p-th root of unity. Let $A, B \subseteq \{0, 1, 2, \ldots, p-1\}$ such that $|A| = |B|$. Then, $\det(\zeta_p^{ij})_{i \in A, j \in B} \neq 0$.*

Tao's proof of this result is combinatorial. As noted in [5] a suggestion of D. Surya Ramana leads to an exceedingly simple proof provided we make use of a basic fact from algebraic number theory. More precisely, we employ the result that $(1 - \zeta_p)$ is a prime ideal with norm p in the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. With this result in hand, we suppose that Chebotarev's theorem is not true and arrive at a contradiction. Indeed, if the determinant of the matrix is zero, then there exist complex numbers c_b (not all zero) such that the polynomial

$$P(x) = \sum_{b\in B} c_b x^b$$

vanishes at $x = \zeta_p^a$ for all $a \in A$. Moreover, from elementary linear algebra, we can choose $c_b \in \mathbb{Z}[\zeta_p]$ and assume that not all the c_b are divisible by $1 - \zeta_p$. By the division algorithm, we have

$$P(x) = G(x) \prod_{a\in A} (x - \zeta_p^a),$$

where $G(x)$ lies in the polynomial ring $\mathbb{Z}[\zeta_p][x]$. Since $1 \equiv \zeta_p \pmod{(1-\zeta_p)}$, we see that $1 \equiv \zeta_p^a \pmod{(1-\zeta_p)}$ for any a. Thus we see that $P(x) \pmod{(1-\zeta_p)}$ has a zero of order $|A|$ at $x = 1$. Thus, all the $|A| - 1$ derivatives of $P(x)$ evaluated at $x = 1$ vanish (mod $1 - \zeta_p$). In other words,

$$\sum_{b\in B} c_b (b)_t \equiv 0 \bmod (1 - \zeta_p), \qquad \forall t = 0, 1, \ldots, |A| - 1,$$

where the notation $(b)_t$ means $b(b-1)(b-2)\cdots(b-t+1)$. An easy induction leads to

$$\sum_{b\in B} c_b b^t \equiv 0 \bmod (1 - \zeta_p).$$

But now, the determinant of the matrix $(b^t)_{b\in B, 0\le t\le |A|-1}$ is a classical Vandermonde and is clearly non-zero (mod p) since the entries of B are distinct residue classes mod p. In particular, the matrix is invertible mod $(1 - \zeta_p)$ so we deduce that all the c_b's are $\equiv 0 \pmod{(1 - \zeta_p)}$, a contradiction.

4. Tao's theorem

In 2003, Tao [8] proved the following sharpening for groups of prime order.

Theorem 3. *If p is prime and $G = \mathbb{Z}/p\mathbb{Z}$, and $f : G \to \mathbb{C}$ is not identically zero, then*

$$|S(f)| + |S(\widehat{f})| \ge p + 1.$$

Proof. Suppose not. Then $|S(f)| \le p - |S(\widehat{f})|$ so that we can find a set of residue classes B disjoint from $S(\widehat{f})$ such that $|S(f)| = |B|$. In particular, $\widehat{f}|_B = 0$. Put $A = S(f)$. By the definition of the Fourier transform and $\zeta_p = e^{-2\pi i/p}$, we have

$$\widehat{f}(b) = \sum_{a\in A} \zeta_p^{ab} f(a) = 0 \qquad \forall\, b \in B.$$

But the left hand side is zero for all $b \in B$ since $\widehat{f}|_B = 0$. Now the matrix

$$(\zeta_p^{ab})_{a\in A, b\in B}$$

is invertible by Theorem 2, so that we conclude that f is identically zero, a contradiction. □

5. Chebotarev's theorem via the Weyl character formula

In [5], we proposed another perspective of Chebotarev's theorem using representation theory of the unitary group over the complex numbers. This allowed us to derive a generalization of Tao's theorem for cyclic groups of composite order. To describe this, we present here a short review of the basic representation theory of the unitary group.

First, an n-tuple of integers $(r_1, \ldots, r_n)$ will be called a *weight*. It is convenient to consider $\mathbb{R}^n/\mathbb{Z}^n$ and understand that all characters of this group are parametrized by weights $r := (r_1, \ldots, r_n) \in \mathbb{Z}^n$ corresponding to the character suggestively denoted as

$$e^r(t_1, \ldots, t_n) = e^{2\pi i(r_1t_1+\cdots+r_nt_n)}.$$

Thus, there is a one-to-one correspondence between weights and characters of $\mathbb{R}^n/\mathbb{Z}^n$. A weight will be called *dominant* if $r_1 \geq r_2 \geq \cdots \geq r_n$ and *strictly dominant* if $r_1 > r_2 > \cdots > r_n$. This terminology and notation is convenient to describe representations of any compact Lie group over the complex numbers.

The representation theory of compact Lie groups is an aesthetically complete chapter in the annals of mathematics. Given a compact Lie group G and an irreducible representation V of G with character χ, the standard procedure to understand χ is to restrict it to a maximal torus T of G, since every conjugacy class of G is represented by an element of T. Now T is an abelian group and as a group is isomorphic to $\mathbb{R}^n/\mathbb{Z}^n$ where n is the *rank* of G. One can describe $\chi|_T$ in terms of one dimensional characters of T (called *weights* associated with χ). The Weyl character formula gives an explicit expression for this character.

In the case of the group of $n \times n$ unitary matrices $U(n)$, we may take T to be the set of matrices

$$t = \operatorname{diag}(t_1, \ldots, t_n), \qquad t_j = e^{2\pi i\theta_j}.$$

Note that $T \simeq \mathbb{R}^n/\mathbb{Z}^n$. The characters of T are parametrized by n-tuples of integers $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ from which we define the character (suggestively denoted as)

$$e^u(t) := t_1^{u_1} \cdots t_n^{u_n}.$$

When V is restricted to T, it decomposes as a finite direct sum of irreducible representations. Thus,

$$V|_T = \oplus_{u\in\mathbb{Z}^n} n_u V_u, \qquad n_u \in \mathbb{N}$$

where

$$V_u = \{v \in V : t \cdot v = e^u(t)v \quad \forall\, t \in T\}.$$

The u's that occur in this decomposition are called the *weights* of V. A weight is called *dominant* if $u_1 \geq u_2 \geq \cdots \geq u_n$ and *strictly dominant* if $u_1 > u_2 > \cdots > u_n$. There is a distinguished dominant weight called the *highest weight* which occurs with multiplicity one and we denote this by λ:

$$\lambda = (f_1, \ldots, f_n) \qquad f_1 \geq f_2 \geq \cdots \geq f_n.$$

The symmetric group S_n acts on the weights in the obvious way: for $\sigma \in S_n$,

$$\sigma \cdot (f_1, \ldots, f_n) = (f_{\sigma^{-1}(1)}, \ldots, f_{\sigma^{-1}(n)}).$$

Let χ_λ be the character attached to V and $\rho = (n-1, n-2, \ldots, 1, 0) = (\rho_1, \rho_2, \ldots, \rho_n)$ (say). In the setting of $U(n)$, the Weyl character formula is given by

$$\chi_\lambda(t) = \frac{\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) e^{\sigma \cdot (\lambda+\rho)}(t)}{\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) e^{\sigma \cdot \rho}(t)}.$$

By the definition of the determinant, we see that this can be written as

$$\chi_\lambda(t) = \frac{\det(t_i^{\lambda_j+\rho_j})}{\det(t_i^{\rho_j})}.$$

It is not difficult to show that $\chi_\lambda(t) \in \mathbb{Z}[t_1, \ldots, t_n]$. The Weyl dimension formula shows that writing $\mu = \lambda + \rho = (\mu_1, \ldots, \mu_n)$,

$$\chi_\lambda(1) = \frac{\prod_{i<j}(\mu_i - \mu_j)}{\prod_{i<j}(j-i)}.$$

Conversely, given a dominant weight λ, there is an irreducible representation V such that the highest weight attached to V is λ. That is, there is a one-to-one correspondence between dominant weights and irreducible representations. Though we have given an explicit description for $U(n)$, the results hold in the general context of any compact Lie group over the complex numbers. (See [3] for more details.)

In our setting, we can deduce Chebotarev's theorem from this viewpoint as follows. We are interested in the determinant of $(\zeta_p^{a_i b_j})$ where the a_i's are in A and the b_j's are in B. Since we are interested in the absolute value of this determinant, we may, without any loss of generality suppose that $a_1 > a_2 > \cdots > a_n$ and $b_1 > b_2 > \cdots > b_n$. With $\rho = (n-1, n-2, \ldots, 1, 0)$ as before, it is now easy to see that setting $\lambda_j = b_j - \rho_j$, the weight $\lambda := (\lambda_1, \ldots, \lambda_n)$ is dominant. Consequently, there is an irreducible representation V of $U(n)$ with character given by χ_λ. Now let

$$t = \operatorname{diag}(\zeta_p^{a_1}, \ldots, \zeta_p^{a_n}).$$

Then, the Weyl character gives

$$\chi_\lambda(t) = \frac{\det(\zeta_p^{a_i b_j})}{\det(\zeta_p^{a_i \rho_j})}.$$

The denominator is a standard Vandermonde determinant and is non-zero since the $\zeta_p^{a_i}$ are all distinct. The numerator is the determinant we want to evaluate and so we see it vanishes if and only if $\chi_\lambda(t) = 0$. If $\chi_\lambda(t) = 0$, then the same is true mod $(1 - \zeta_p)$. Thus, as $\chi_\lambda(t) \in \mathbb{Z}[\zeta_p]$, we deduce

$$0 = \chi_\lambda(t) \equiv \chi_\lambda(1) \pmod{(1 - \zeta_p)}.$$

By the Weyl dimension formula,

$$\chi_\lambda(1) = \frac{\prod_{i<j}(b_i - b_j)}{\prod_{i<j}(j-i)}$$

which is a positive integer. If $(1 - \zeta_p)$ divides $\chi_\lambda(1)$, then $p|\chi_\lambda(1)$, which is a contradiction. This completes our proof of Chebotarev's theorem.

6. Variation of Tao's theorem

The discrete Fourier transform is a special case of a matrix transform. Indeed, let (a_{ij}) be an $n \times n$ matrix. Given any sequence $f(1), f(2), \ldots, f(n)$ we may define a new sequence

$$\widetilde{f}(j) = \sum_{i=1}^{n} a_{ij} f(i).$$

It is clear that our proof of Theorem 3 extends to establish the following.

Theorem 4. *Suppose that for any two subsets A, B of $\{1, 2, \ldots, n\}$ with $|A| = |B|$, the matrix $(a_{ij})_{i\in A, j\in B}$ has non-zero determinant, then*

$$|S(f)| + |S(\widetilde{f})| \geq n + 1.$$

Based on density considerations, we can see that with probability one, a random non-singular matrix has the property required by the theorem. Indeed, if we view the a_{ij} as variables, each vanishing determinant determines a subspace of dimension at most $n^2 - 1$. The Fourier transform corresponds to the matrix in which $a_{ij} = \zeta_n^{ij}$ where ζ_n is a primitive n-th root of unity.

One can actually produce explicitly many matrices with this property as follows. Let $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_n$ and consider the $n \times n$ matrix with $a_{ij} = \alpha_i^j$. We claim that this matrix has the required property. Indeed, this occurs as Problem 48 on p. 43 of the classic problem book Polya and Szego [7]. The proof is quite elegant and uses Descartes theorem (proved in the next section) on the rule of signs. Recall that this theorem says that the number of positive zeros of

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$$

is bounded by the number of sign changes of the sequence of coefficients

$$a_0, a_1, \ldots, a_{n-1}, 1.$$

To apply this in our context, we proceed as in our proof of Chebotarev's lemma. If the submatrix $(\alpha_i^j)_{i\in A, j\in B}$ has zero determinant, we can find real numbers c_b (not all zero), such that

$$P(x) = \sum_{b\in B} c_b x^b$$

has zeros for $x = \alpha_i$, $i \in A$. The number of sign changes is at most $|B| - 1$ so the number of positive zeros is at most $|B| - 1$, a contradiction, since the α_i's are positive and $|A|$ in number.

7. Descartes rule of signs

This elegant theorem finds little mention in standard books of analysis or algebra. The proof found in [7] relies on earlier problems and questions that the elegant proof becomes inelegant after riffling through the many pages of the book. Here we give a proof based on [7] that is short and crisp.

Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x].$$

Let C be the number of sign changes and P the number of positive roots. We need to show that $C \geq P$. Let $\alpha_1, \ldots, \alpha_P$ be the positive roots of $f(x)$ so that

$$f(x) = (\alpha_1 - x)\cdots(\alpha_P - x)Q(x), \qquad Q(x) \in \mathbb{R}[x]. \tag{2}$$

We need to count the number of sign changes of the polynomial on the right hand side. We can do this easily if we have the following:

Lemma 5. *If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ has R sign changes in the sequence of coefficients, and $\alpha > 0$, then the number of sign changes of $(\alpha - x)f(x)$ is at least $R + 1$.*

If we have this, then the theorem is proved by induction. Indeed, if U is the number of sign changes in the sequence of coefficients of $Q(x)$, then applying the lemma inductively, the number of sign changes for $f(x)$ is at least $U + P$, from which the result follows.

To prove the lemma, we need only make a few observations. The number of sign changes of the polynomial $(\alpha - x)f(x)$ is the same if we replace x by αx since $\alpha > 0$. This reduces to the problem of counting the number of sign changes of $(1 - x)g(x)$ for a given polynomial $g(x)$. Writing

$$g(x) = b_0 + b_1x + \cdots + b_nx^n,$$

we see that

$$(1 - x)g(x) = b_0 + (b_1 - b_0)x + \cdots + (b_n - b_{n-1})x^{n-1} - b_nx^{n+1}.$$

We claim that the the number of sign changes of

$$b_0, \quad b_1 - b_0, \quad \ldots, \quad b_n - b_{n-1}, \quad b_n$$

is at least one more than the number of sign changes of

$$b_0, b_1, \ldots, b_n. \tag{3}$$

Indeed, let $\upsilon_1 + 1, \upsilon_2 + 1, \ldots, \upsilon_T + 1$ be the indices of sign change in the sequence (3). Then, each row of the following matrix has at least one sign change:

$$\begin{matrix} b_{\upsilon_1+1} - b_{\upsilon_1} & b_{\upsilon_1+2} - b_{\upsilon_1+1} & \cdots & b_{\upsilon_2+1} - b_{\upsilon_2} \\ b_{\upsilon_2+1} - b_{\upsilon_2} & b_{\upsilon_2+2} - b_{\upsilon_2+1} & \cdots & b_{\upsilon_3+1} - b_{\upsilon_3} \\ \cdots & \cdots & \cdots & \cdots \\ b_{\upsilon_{T-1}+1} - b_{\upsilon_{T-1}} & b_{\upsilon_{T-1}+2} - b_{\upsilon_{T-1}+1} & \cdots & b_{\upsilon_T+1} - b_{\upsilon_T} \end{matrix}$$

Indeed, for the first row, say that $b_{v_1} < 0$ and $b_{v_1+1} > 0$, then $b_{v_1+1} - b_{v_1} > 0$ and if all the entries in the first row are positive, $v_2 + 1$ would not be an index of sign change. The same argument applies to the other rows. Thus, we have $T - 1$ sign changes in the matrix grid. In addition to this, we have the sequences

$$b_0, \quad b_1 - b_0, \quad \ldots, \quad b_{v_1+1} - b_{v_1}$$

and

$$b_{v_T+1} - b_{v_T}, \quad \ldots, \quad b_n - b_{n-1}, \quad -b_n$$

each of which has a sign change. This completes the proof of the claim and Descartes rule.

8. The uncertainty principle for finite non-abelian groups

If G is a finite group (not necessarily abelian), then we consider a complex-valued class function f which is not identically zero. We define its Fourier transform as a function on the irreducible characters of G. Thus, for each irreducible character χ of G, set

$$\widehat{f}(\chi) = \sum_C \overline{\chi}(g_C) f(g_C), \tag{4}$$

where the summation is over the conjugacy classes C of G and g_C is any element in C. The definition of the support of f and the support of $\widehat{f}$ need to be modified. We define the support of f as

$$\sum_{C: f(g_C) \neq 0} |C|,$$

and the support of $\widehat{f}$ as

$$\sum_{\chi: \widehat{f}(\chi) \neq 0} \chi(1)^2.$$

Of course, this agrees with our earlier definition in the abelian case. By the orthogonality relations,

$$f(g_C) = \frac{|C|}{|G|} \sum_{\chi} \chi(g_C) \widehat{f}(\chi). \tag{5}$$

Notice that f is identically zero if and only if $\widehat{f}$ is identically zero. Using basic facts about characters of finite groups, we will establish the following non-abelian analog of Theorem 1.

Theorem 6. *Let G be an arbitrary finite group and $f : G \to \mathbb{C}$ a complex-valued class function not identically zero. Then,*

$$|S(f)||S(\widehat{f})| \geq |G|.$$

Proof. We have from (4)

$$\sup_{\chi} \frac{|\widehat{f}(\chi)|}{\chi(1)} \leq \left(\sup_{C} \frac{|f(g_C)|}{|C|}\right) \left(\sum_{C: f(g_C)\neq 0} |C|\right).$$

On the other hand,

$$\frac{|f(g_C)|}{|C|} \leq \frac{1}{|G|} \left(\sup_{\chi} \frac{|\widehat{f}(\chi)|}{\chi(1)}\right) \sum_{\chi: \widehat{f}(\chi)\neq 0} \chi(1)^2.$$

Putting everything together gives

$$\sup_{\chi} \frac{|\widehat{f}(\chi)|}{\chi(1)} \leq \frac{|S(\widehat{f})||S(f)|}{|G|} \left(\sup_{\chi} \frac{|\widehat{f}(\chi)|}{\chi(1)}\right)$$

As f is not identically zero, the desired inequality follows. □

It is unreasonable to expect that the corresponding matrix of character values satisfies the hypothesis of Theorem 4. Indeed, in the non-abelian case, for each irreducible non-abelian character χ there is a conjugacy class on which it vanishes. So the hypothesis of Theorem 4 is never satisfied. However, it would be of interest to investigate to what extent Tao's theorem can be generalized to the non-abelian setting.

References

[1] D. L. Donoho and P. B. Stark, Uncertainty principles and signal recovery, *Siam J. Applied Math.*, **49(3)** (1989) 906–931.

[2] G. B. Folland and A. Sitaram, The uncertainty principle: A mathematical survey, *Journal of Fourier analysis and applications*, **3(3)** (1997) 207–238.

[3] W. Fulton and J. Harris, Representation theory, A first course, Graduate Texts in Mathematics, Springer-Verlag, (1991).

[4] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *American Journal of Mathematics*, **110** (1988) no. 2, 253–281.

[5] M. Ram Murty and J. P. Whang, The uncertainty principle and a generalization of a theorem of Tao, *Linear algebra and its applications*, **437** (2012) 214–220.

[6] P. Stevenhagen and H.W. Lenstra, Chebotarev and his density theorem, *Math. Intelligencer*, **18** (1996) no. 2, 26–37.

[7] G. Polya and G. Szego, Problems and theorems in Analysis, Volume 2, Springer, (1998).

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