My [algebraic] methods are really methods of working and thinking; this is why they have crept in everywhere anonymously. - Emmy Noether

Problem Set 8

PCMI USS, Summer 2023

1. (a) Let $V = \mathbf{C}^4$ with basis $|0\rangle, |1\rangle, |2\rangle, |3\rangle$. Write down the matrix (yellow) for the Fourier transform F_4.

   (b) Let $\alpha, \beta \in \mathbf{C}$. Consider the vector

   $$|\psi\rangle = x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + x_3|3\rangle,$$

   where $x_0 = \alpha$, $x_1 = \beta$, $x_2 = \alpha$, $x_3 = \beta$. You might say that $|\psi\rangle$ has *period 2* since its coefficients satisfy

   $$x_j = x_{j+2}$$

   for $j = 0, \ldots, 3$, with addition of indices is taken modulo 4. Compute $F_4|\psi\rangle$. What is special about it?

   (c) Now take a vector $|\psi\rangle \in \mathbf{C}^4$ with period 1. Explain why this means $x_0 = x_1 = x_2 = x_3$. Compute $F_4|\psi\rangle$.

   (d) Can you have a vector $|\psi\rangle \in \mathbf{C}^4$ with period 3? Explain why you might rather say that such a vector has period 1.

   (e) Now let $N = 8$. For $|\psi\rangle \in \mathbf{C}^8$, what are the possible periods for $|\psi\rangle$? For each period p, apply the Fourier transform F_8 to a vector of that period, and make observations about the vector you get. (If you're working in a group, different group members could try different periods.)

   (f) Suppose you're given a state $|\psi\rangle \in \mathbf{C}^8$ and told that this state (a) might be a random state, or (b) might have period 4. What might you do quantumly to have a good shot at finding out which? Probabilitywise, how good can you do?

   (g) (For thought) What do you think happens when $N = 2^n$ for a general n. What about N that are not powers of 2?

2. (**Character Basics**) Let G be a finite abelian group. Recall that a character of G is a homomorphism from G into $\mathbf{C}^\star$, the group of nonzero complex numbers under multiplication. That is

   Definition 1 *Let G be an abelian group. A function $\chi : G \to \mathbf{C}^\star$ is called a character of G if*

   $$\chi(g_1 + g_2) = \chi(g_1) + \chi(g_2)$$

   for all $g_1, g_2 \in G$.

(a) Show that if χ is a character of G, then $\chi(0) = 1$. (0 denotes the additive identity of G.)

(b) Show that $\chi(-g) = 1/\chi(g)$ for all $g \in G$.

(c) For a positive integer n and $g \in G$, we use ng to denote the result of adding g to itself n times. If χ is a character of G, explain why

$$\chi(ng) = \chi(g)^n.$$

Does this equation make sense for negative values of n?

(d) Show that if $g \in G$ has order n, then $\chi(g)$ is an nth root of unity.

(e) Show that for any $g \in G$, $\chi(-g) = \overline{\chi(g)}$.

(f) Let $G = \mathbb{Z}_N$ be group of integers mod N under addition. Let $\omega = e^{2\pi i/N}$. Show that for any $k \in \{0, \ldots, N-1\}$, the function χ_k defined for $j \in \mathbb{Z}_N$ by

$$\chi_k(j) = \omega^{kj}$$

is a character of Z_N.

(g) Show conversely that if χ is any character of Z_N, then $\chi = \chi_k$ for some k.

(h) Can you find all the characters of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$?

(i) (For thought) How about $G = (\mathbb{Z}_2)^n$? Other abelian groups?

3. **(Orthogonality of Characters)**

(a) Prove the Orthogonality of Characters:

Theorem 2 *Let G be a finite abelian group, and let χ_1, χ_2 be characters of G. Then*

$$\frac{1}{|G|}\sum_{g\in G}\chi_1(g)\overline{\chi_2(g)} = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2 \\ 1 & \text{if } \chi_1 = \chi_2. \end{cases}$$

(b) Use this theorem to prove that an abelian group G with n elements can have at most n distinct characters.

(c) It turns out that if G has n elements, then G has exactly n distinct characters! This is harder to prove. Try it if you're good at group theory and up for a challenge.

4. **(Uncertainty Principle for the Fourier Transform)** In this problem, you will prove a version of the Uncertainty Principle for the Fourier Tranform. Roughly, the idea is that it is impossible for both $|\psi\rangle$ and its Fourier transform $F|\psi\rangle$ to be highly concentrated on a small number of basis states. To this end, we define the *support* of a state $|\psi\rangle \in \mathbf{C}^N$ as follows: if $|\psi\rangle = \sum_j x_j|j\rangle$, then $\mathrm{Supp}(|\psi\rangle)$ is the set of indices j such that $x_j \neq 0$. Thus the size $|\mathrm{Supp}(|\psi\rangle)|$ is the number of nonzero coordintates of $|\psi\rangle$ in the standard basis. The uncertainty principle then states that

Theorem 3 *For any state $|\psi\rangle \in \mathbf{C}^N$,*

$$|Supp(|\psi\rangle)| \cdot |Supp(F|\psi\rangle)| \geq N$$

See if you can prove this. Find your own proof, or use the following outline as a guide.

(a) The ∞-norm

$$||w||_\infty$$

of a vector $w \in \mathbf{C}^n$ is the maximum absolute value of the components of v. Prove that

$$||F|\psi\rangle||_\infty \leq \frac{1}{\sqrt{N}} |\text{Supp}(|\psi\rangle)| \cdot |||\psi\rangle||_\infty.$$

(b) Now prove the same inequality with $|\psi\rangle$ and $F|\psi\rangle$ reversed.

(c) Combine your inequalities to bring it home.

(d) What properies of F did you use? Does you proof actually yield an uncertainty principle for other unitary operators?

(e) Explain why the theorem shows that it is impossible for both $|\psi\rangle$ and its Fourier transform $F|\psi\rangle$ to be highly concentrated on a small number of basis states. How does this ressemble any other form of the Uncertainty Principle that you know? It is actually true, but quite a bit harder to show (and a more recent result), that the sum of the supports is at least $N+1$. Is this stronger than the above theorem in all cases? If you generalaized to other unitaries U in part (d), does the stronger additive statement apply to all such U?