1 Unitarity of a Fourier Transform

The Fourier transform mod N is the $N \times N$ matrix given by

$$FT_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \quad , \tag{1}$$

where $\omega = e^{2\pi i/N}$ is a primitive Nth root of unity. That is, the i, j'th element of FT_N is $\frac{1}{\sqrt{N}}\omega^{ij}$, for $i, j = 0, \ldots, N-1$.

Equivalently, in ket notation, for $j \in \{0, 1, \ldots, N-1\}$, $FT_N|j\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \omega^{ij}|i\rangle$.

We need to check the inner product between the ith and jth columns of FT_N, that $\langle i|FT_N^\dagger FT_N|j\rangle = \delta_{ij} \equiv \left\{ \begin{smallmatrix} 1 \text{ if } i=j \\ 0 \text{ if } i \neq j \end{smallmatrix} \right.$. Indeed, this inner product is

$$\frac{1}{N} \sum_{k=0}^{N-1} \overline{\omega^{ik}} \omega^{jk} = \frac{1}{N} \sum_{k=0}^{N-1} \omega^{k(j-i)} \tag{2}$$

This is a geometric series with ratio between terms ω^{j-i} and so can easily be evaluated. If $i = j \mod N$, then each term is $\omega^0 = 1$, so the inner product is $N/N = 1$. If $i \neq j$, then the sum is

$$1 + \omega^{j-i} + \omega^{2(j-i)} + \cdots + \omega^{(N-2)(j-i)} + \omega^{(N-1)(j-i)} \quad . \tag{3}$$

Multiplying the sum by $\omega^{i-j} \neq 1$ gives

$$\omega^{j-i} + \omega^{2(j-i)} + \omega^{3(j-i)} + \cdots + \omega^{(N-1)(j-i)} + \omega^{N(j-i)} \quad . \tag{4}$$

But $\omega^{N(j-i)} = (\omega^N)^{j-i} = 1$, so we have just rearranged the terms of the summation; the sum itself doesn't change when multiplied by ω^{j-i}. Therefore the sum is zero, as claimed.

2 Fourier Transforms and the uncertainty principle

a) Prove that for any quantum state $|\psi\rangle$ on n qubits, $S(|\psi\rangle) \leq 2^{n/2}$.

Answer: We need to show that if $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$, then $\sum_x |\alpha_x| \leq 2^{n/2}$. Using the Cauchy-Schwarz inequality $\langle v|w\rangle \leq ||v|| \cdot ||w||$, we get

$$\begin{aligned}\sum_x |\alpha_x| =& \sum_x (|\alpha_x| \cdot 1) \\ \leq& \left(\sum_x |\alpha_x|^2\right)^{1/2} \left(\sum_x 1^2\right)^{1/2} \\ =& 1 \cdot 2^{n/2} = 2^{n/2} \ ,\end{aligned}$$

with equality iff $|\alpha_x| = 1/2^{n/2}$ for all x.

(b) **Answer**: Using the normalization condition, $1 = \sum_x |\alpha_x|^2 \leq \sum_x a|\alpha_x| = aS(|\psi\rangle)$. (Notice that this inequality is an equality iff all α_x are zero or exactly a – that is, to minimize the spread, concentrate the probability mass as much as possible while still satisfying the constraint $|\alpha_x| \leq a$.)

(c)

$$\begin{aligned}H^{\otimes n}|x\rangle &= \bigotimes_{i=1}^{n} \begin{pmatrix} |0\rangle + |1\rangle \text{ if } x_i = 0 \\ |0\rangle - |1\rangle \text{ if } x_i = 1 \end{pmatrix} \\ &= \sum_z \left(\bigotimes_{i=1}^{n} \begin{matrix} |z_i\rangle \text{ if } x_i = 0 \text{ or } z_i = 0 \\ -|z_i\rangle \text{ if } x_i = 1 \text{ and } z_i = 1 \end{matrix} \right) \\ &= \sum_z (\prod_{i=1}^{n} (-1)^{x_i z_i})|z\rangle \\ &= \sum_z (-1)^{x\cdot z}|z\rangle\end{aligned}$$

(d) Use (c) to prove that for all y, $|\beta_y| \leq \frac{1}{2^{n/2}} S(|\psi\rangle)$.

Answer: Using the triangle inequality $|a + b| \leq |a| + |b|$,

$$\begin{aligned}|\beta_y| &= \tfrac{1}{2^{n/2}} |\sum_y (-1)^{x\cdot y} \alpha_y| \\ &\leq \tfrac{1}{2^{n/2}} \sum_y |(-1)^{x\cdot y} \alpha_y| \\ &= \tfrac{1}{2^{n/2}} \sum_y |\alpha_y| \\ &= \tfrac{1}{2^{n/2}} S(|\psi\rangle) \ .\end{aligned}$$

(e) Prove the uncertainty relation $S(|\psi\rangle)S(H^{\otimes n}|\psi\rangle) \geq 2^{n/2}$. Justify why it makes sense to call this an uncertainty relation.

Answer: By part d, $|\beta_y| \leq \frac{1}{2^{n/2}} S(|\psi\rangle)$ for all y. So by part b, $S(H^{\otimes n}|\psi\rangle) \geq 2^{n/2}/S(|\psi\rangle)$, which is the desired inequality.

This is an uncertainty relation because it gives a tradeoff between the spread in one basis and the spread in another. For example, if a state is well-concentrated in the standard basis, then it has high spread – and therefore high uncertainty – in the Fourier basis.