

Exercises

Instructor: Fermi Ma

All of these exercises are **optional**. Feel free to email me with questions if you get stuck.

1. (Properties of the Quantum Fourier Transform.) Let q be prime and let $\omega_q := e^{2\pi i/q}$. Define the Quantum Fourier Transform over $\mathbb{Z}_q$ to be the unitary that maps

$$\text{QFT}_q |x\rangle = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{Z}_q} \omega_q^{xy} |y\rangle. \quad (1)$$

for all $x \in \mathbb{Z}_q$. More generally, its n -fold tensor product acts on $x \in \mathbb{Z}_q^n$ as

$$\text{QFT}_q^{\otimes n} |x\rangle = \frac{1}{\sqrt{q^n}} \sum_{y \in \mathbb{Z}_q^n} \omega_q^{\langle x, y \rangle} |y\rangle. \quad (2)$$

where $\langle x, y \rangle = \sum_i x_i y_i \pmod{q}$.

Prove the following properties:

- (a) (Subspaces map to their orthogonal complements) For a subspace $V \subset \mathbb{Z}_q^n$, the uniform superposition over V is denoted as

$$|V\rangle = \frac{1}{\sqrt{|V|}} \sum_{x \in V} |x\rangle.$$

Denote the orthogonal complement of V as

$$V^\perp = \{y : \langle x, y \rangle = 0 \pmod{q} \text{ for all } x \in V\}.$$

Show that

$$\text{QFT}_q^{\otimes n} |V\rangle = |V^\perp\rangle.$$

- (b) (Shifts maps to phases) For each $s \in \mathbb{Z}_q^n$, define

- the shift operator X_s to be the unitary that maps $X_s |x\rangle = |x + s\rangle$ for all $x \in \mathbb{Z}_q^n$.
- the phase operator Z_s to be the unitary that maps $Z_s |x\rangle = \omega_q^{\langle s, x \rangle} |x\rangle$ for all $x \in \mathbb{Z}_q^n$.

Prove that

$$\text{QFT}_q^{\otimes n} \cdot X_s = Z_s \cdot \text{QFT}_q^{\otimes n}.$$

- (c) (Fourier transforms of cosets) For $s \in \mathbb{Z}_q^n$ and a subspace $V \subset \mathbb{Z}_q^n$, define

$$|s + V\rangle = \frac{1}{\sqrt{|V|}} \sum_{x \in V} |s + x\rangle.$$

Show that applying $\text{QFT}_q^{\otimes n}$ to $|s + V\rangle$ and measuring in the computational basis gives a uniformly random element of $V^\perp$.

2. (The Convolution Theorem) Let $|\psi\rangle = \sum_{x \in \mathbb{Z}_q^n} \alpha_x |x\rangle$ and $|\phi\rangle = \sum_{x \in \mathbb{Z}_q^n} \beta_x |x\rangle$ be two quantum states. Denote their fourier transforms as

$$\text{QFT}_q^{\otimes n} |\psi\rangle = \sum_{z \in \mathbb{Z}_q^n} \hat{\alpha}_z |z\rangle, \quad \text{QFT}_q^{\otimes n} |\phi\rangle = \sum_{z \in \mathbb{Z}_q^n} \hat{\beta}_z |z\rangle. \quad (3)$$

Define their convolution by the un-normalized state

$$|\psi\rangle * |\phi\rangle := \sum_{x, y \in \mathbb{Z}_q^n} \alpha_x \beta_y |x + y\rangle \quad (4)$$

Prove that for some constant c ,

$$\text{QFT}_q^{\otimes n} (|\psi\rangle * |\phi\rangle) = c \sum_{z \in \mathbb{Z}_q^n} \hat{\alpha}_z \hat{\beta}_z |z\rangle.$$

3. (Bernstein–Vazirani and Quantum Goldreich–Levin.) Let $s \in \mathbb{Z}_2^n$ be an unknown string. **Note:** This problem (especially parts c and d) is tricky! Feel free to search the internet or ask an LLM for help if you get stuck.

- (a) (Bernstein–Vazirani) Suppose you are given oracle access to function $f_s : \{0, 1\}^n \mapsto \{0, 1\}$, defined as $f_s(x) = \langle x, s \rangle$, where $\langle x, s \rangle$ denotes inner product mod 2.
- How many classical oracle calls to f_s do you need to recover s ?
 - How many quantum oracle calls to f_s (defined as calls to the unitary that maps $|x\rangle |b\rangle \mapsto |x\rangle |b \oplus \langle x, s \rangle\rangle$) do you need to recover s ?
- (b) (Quantum Goldreich–Levin) Suppose you are given oracle access to a function $\hat{f}_s$ that agrees with $\langle x, s \rangle$ mod 2 on $1/2 + \varepsilon$ of all inputs x (you can think of the previous problem as the case where $\varepsilon = 1/2$). That is,

$$\Pr_{x \leftarrow \mathbb{Z}_2^n} [\hat{f}_s(x) = \langle x, s \rangle] \geq \frac{1}{2} + \varepsilon. \quad (5)$$

Show that you can recover s given a constant number of quantum oracle calls to $\hat{f}_s$ with probability at least $\Omega(\varepsilon^2)$.

Note: there is a famous result in classical cryptography called the Goldreich-Levin theorem which says that you can recover s given polynomially-many classical oracle calls to $\hat{f}_s$.

- (c) (Quantum Goldreich-Levin over $\mathbb{Z}_q$) Now suppose our unknown string is $s \in \mathbb{Z}_q^n$ for some prime q . You are given quantum oracle access to a function $\hat{f}_s$ that agrees with $\langle x, s \rangle$ mod q on $1/q + \varepsilon$ of all inputs x . That is,

$$\Pr_{x \leftarrow \mathbb{Z}_q^n} [\hat{f}_s(x) = \langle x, s \rangle] \geq \frac{1}{q} + \varepsilon. \quad (6)$$

i.e., the algorithm predicts inner products w.r.t. s with probability ε better than random guessing, over a random x . Show that you can recover s with probability at least $\Omega(\varepsilon^2)$.

- (d) (Quantum Search-To-Decision Reduction for LWE.) Using your solution to the problem above, give a quantum search-to-decision reduction for LWE, with prime modulus $q = \text{poly}(n)$. That is, show that if there is a polynomial-time algorithm D that distinguishes LWE samples from uniform with non-negligible advantage, you can turn this into a quantum polynomial-time algorithm A that solves search LWE.

Hint: First use the LWE distinguisher to construct a predictor for $\langle x, s \rangle$ on a random input x . Then apply quantum Goldreich–Levin.