Problem set 7

CSE 534 Autumn 2026

Due date: November 30th 11:59 pm

Instructions: Solutions should be legibly handwritten or typeset. Mathematically rigorous solutions are expected for all problems unless explicitly stated. You are encouraged to collaborate on problems in small teams; however, each team member must write and submit their own individual solution. Read the AI tools policy on the course webpage and adhere to it. For grading purposes, start each problem on a new page.

In this problem set, $\mathbb{Z}_N$ will be the group over $\{0, \ldots, N-1\}$ under addition. Secondly, we use the notation $F_N : \mathbb{C}^N \to \mathbb{C}^N$ to denote the Fourier transform

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{kx} |k\rangle \quad \text{for } x \in \mathbb{Z}_N \text{ and } \omega = \exp\left(\frac{2\pi i}{N}\right).$$

And for $s, t \in \mathbb{Z}_N$, define

$$X_s \stackrel{\text{def}}{=} \sum_{x \in \mathbb{Z}_N} |x+s\rangle\langle x|, \quad Z_t \stackrel{\text{def}}{=} \sum_{x \in \mathbb{Z}_N} \omega^{tx} |x\rangle\langle x|.$$

In all problems, you may assume that the Fourier transform can be implemented with $O(\log^2 N)$ elementary operations.

Practice problems (not graded)

These problems are not graded. Do not submit a solution, but do ensure that you can solve the problem.

Problem 1. Prove that $F_N^2 |x\rangle = |-x\rangle$ for $x \in \mathbb{Z}_N$. Therefore, $F_N^4 = \mathbb{I}$. What does $F_N = F_N^\dagger$ imply about N?

Problem 2. Compute $F_N X_s F_N^\dagger$ and $F_N Z_s F_N^\dagger$ and prove that $X_s Z_t = \omega^{-st} Z_t X_s$.

Problem 3. Consider the subspace $\{|\psi\rangle : X_s |\psi\rangle = |\psi\rangle\}$ — i.e., the +1-eigenspace of X_s. Express its dimension as a function of s and N.

Problem 4. Suppose $r|N$. For any $a \in \mathbb{Z}_N$, define

$$|\psi_a\rangle \stackrel{\text{def}}{=} \sqrt{\frac{r}{N}} \sum_{j=0}^{N/r-1} |a + jr\rangle.$$

1. When does $|\psi_a\rangle = |\psi_{a'}\rangle$?
2. Compute $F_N |\psi_a\rangle$. If this state is measured in the standard basis, what measurement outcomes have non-zero probability?

Problem 5 (Hidden line problem)**.** Let p be a prime. Suppose that we have quantum query access to a function $f : \mathbb{F}_p^2 \to \{0,1\}^m$. We are promised that there exists $a \in \mathbb{F}_p$ such that

$$f(x,y) = f(x',y') \iff ay - x = ay' - x'.$$

Equivalently, for each $\gamma \in \mathbb{F}_p$, the level sets of f are the parallel lines

$$L_\gamma \stackrel{\text{def}}{=} \left\{(x,y) \in \mathbb{F}_p^2 \,:\, x = ay - \gamma\right\}, \qquad \gamma \in \mathbb{F}_p.$$

Our goal is to determine a. The query oracle acts as

$$\mathcal{O}_f \,|x,y,b\rangle = |x,y,b \oplus f(x,y)\rangle\,.$$

1. Suppose a classical algorithm queries f at distinct locations (x_1,y_1) and (x_2,y_2). What do we learn about (a,b) when $f(x_1,y_1)$ and $f(x_2,y_2)$ are equal, and what do we learn when they are not equal? Conclude that any deterministic classical algorithm requires $\Omega(\sqrt{p})$ queries.

2. Show that

   $$H_a \stackrel{\text{def}}{=} \left\{(at,t) \,:\, t \in \mathbb{F}_p\right\}$$

   is a subgroup of the additive group $\mathbb{F}_p^2$, and that each L_γ is a coset of H_a. Explain why finding a is an instance of the abelian hidden subgroup problem.

3. Prepare a uniform superposition over $(x,y) \in \mathbb{F}_p^2$, query f into an output register initialized to $|0^m\rangle$, and discard that register. Show that the resulting density matrix is

   $$\rho = \frac{1}{p} \sum_{\gamma \in \mathbb{F}_p} |L_\gamma\rangle\langle L_\gamma|\,, \qquad |L_\gamma\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{F}_p} |ay - \gamma, y\rangle\,.$$

4. Compute $(F_p \otimes \mathbb{I})\rho(F_p \otimes \mathbb{I})^\dagger$. Express your answer in the form

   $$\frac{1}{p} \sum_{k \in \mathbb{F}_p} |k\rangle\langle k| \otimes |\phi_k\rangle\langle\phi_k|\,,$$

   giving an explicit expression for $|\phi_k\rangle$. If we measure the first register, what is the distribution of the outcome k, and what is the conditional state of the second register?

5. Give a measurement of the second register that, together with k, allows you to determine a whenever $k \neq 0$. What is the probability that one run of this procedure determines a? If we repeat until $k \neq 0$, what is the expected number of oracle queries?

Graded problems

Problem 6 (Uncertainty principle)**. (6 points)** Let $|\psi\rangle \in \mathbb{C}^N$ be a unit vector and $S \subset \mathbb{Z}_N$ be a subset such that $|\psi\rangle$ is entirely supported on S. Meaning that for any $y \in \mathbb{Z}_N \setminus S$, $\langle y|\psi\rangle = 0$. Similarly, let T be a subset such that $F_N|\psi\rangle$ is entirely supported on T.

Prove that $|S| \cdot |T| \geq N$. This is a simplified form of the uncertainty principle, which says a quantum state is uncertain in either the standard or Fourier basis (or both).

Hint: Prove using Cauchy-Schwarz that for all $z \in \mathbb{Z}_N$, $|\langle z|F_N|\psi\rangle| \leq \sqrt{|S|/N}$.

Problem 7. (4 points) Assume N is prime. Let $|\widehat{x}\rangle \stackrel{\text{def}}{=} F_N|x\rangle$. It follows that $\{|\widehat{x}\rangle\}_{x\in\mathbb{Z}_N}$ forms a basis for $\mathbb{C}^N$ called the Fourier basis. Prove that for any matrix $\rho \in \mathbb{C}^{N\times N}$ and any $s \neq 0$,

$$X_s \rho X_s^\dagger = \rho \iff \rho \text{ is diagonal in the Fourier basis.}$$

Problem 8 (Hidden parabola problem)**.** Consider a variant of the Simons problem where, instead of a hidden linear function, we have a hidden parabola. Specifically, suppose we have query access to a function $f : \mathbb{F}_p^2 \to \{0,1\}^m$ where p is a prime number > 2 and m is some integer.

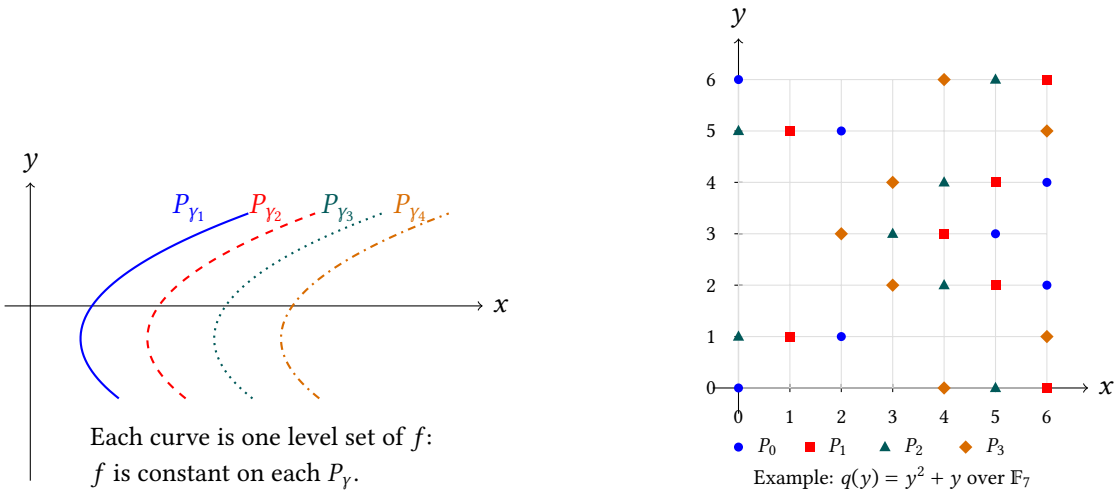


Figure 1: *Two views of the hidden parabola problem. The left panel is a schematic picture over* $\mathbb{R}$*, which is useful for geometric intuition but is not the actual setting of the problem: each level set* P_γ *appears as a horizontal translate of the same parabola. The computation instead takes place over the finite field* $\mathbb{F}_p$*, illustrated in the right panel for* $p = 7$ *and* $q(y) = y^2 + y$*. Here each* P_γ *is a discrete set of points in* $\mathbb{F}_7^2$*.*

We are promised that there exists $\alpha, \beta \in \mathbb{F}_p$ with $\alpha \neq 0$ such that

$$f(x,y) = f(x',y') \iff \alpha y^2 + \beta y - x = \alpha y'^2 + \beta y' - x'.$$

Equivalently, for each $\gamma \in \mathbb{F}_p$, the function f is invariant on the parabola level sets

$$P_\gamma \stackrel{\text{def}}{=} \left\{ (x, y) \in \mathbb{F}_p^2 \,:\, x = q(y) - \gamma \right\} \text{ where } q(y) = \alpha y^2 + \beta y\,.$$

The computational task is to compute (α, β) from query access to the hidden parabola.

1. **(4 points)** Suppose a classical algorithm queries f at distinct locations (x_1, y_1) and (x_2, y_2). What do we learn about (α, β) when $f(x_1, y_1)$ and $f(x_2, y_2)$ are equal, and what do we learn when they are not equal? Conclude that any deterministic classical algorithm requires $\Omega(\sqrt{p})$ queries.

2. **(1 point)** Recall that a query to the function f can be described as

   $$\mathcal{O}_f \left| x, y, b \right\rangle = \left| x, y, b \oplus f(x, y) \right\rangle \text{ for } x, y \in \mathbb{F}_p, b \in \{0,1\}^m.$$

   Define $\left| P_\gamma \right\rangle$ to be the uniform superposition over the parabola level set P_γ What density matrix is generated by preparing a uniform superposition over $(x, y) \in \mathbb{F}_p^2$, then computing the query value (in superposition), and discarding it? Express it in terms of the $\left| P_\gamma \right\rangle$.

3. **(2 points)** Show that ρ is invariant under any shift X_s applied to the first register — i.e., $(X_s \otimes \mathbb{I})\rho(X_s \otimes \mathbb{I})^\dagger = \rho$. By our earlier problem, this proves that ρ is block-diagonal with respect to the first register in the Fourier basis. Compute $(F_p \otimes \mathbb{I})\rho(F_p \otimes \mathbb{I})^\dagger$.

   Hint: First write $F_p \otimes \mathbb{I} \left| P_\gamma \right\rangle$ as $\frac{1}{\sqrt{p}} \sum_{k \in \mathbb{F}_p} \omega^{-k\gamma} \left| k \right\rangle \left| \phi_k \right\rangle$ for some $\left| \phi_k \right\rangle$.

4. **(2 points)** Suppose that we measure the first register after applying $F_p \otimes \mathbb{I}$. Argue that each outcome $k \in \mathbb{Z}_p$ is equally likely, and that the resulting post-measurement state on the second register is $\left| \phi_k \right\rangle$.

5. **(2 points)** Repeat this procedure twice achieving uniformly random outcomes $k, \ell \in \mathbb{Z}_p$ and post-measurement state $\left| \phi_k \right\rangle \otimes \left| \phi_\ell \right\rangle$. Then append two ancilla $\left| 0 \right\rangle \left| 0 \right\rangle$ and apply the transform

   $$V \,:\, \left| x_1, x_2, b_1, b_2 \right\rangle \mapsto \left| x_1, x_2, b_1 + k x_1^2 + \ell x_2^2, b_2 + k x_1 + \ell x_2 \right\rangle.$$

   Argue that the resulting state can be expressed as

   $$\frac{1}{p} \sum_{u,v} \omega^{\alpha u + \beta v} \left| \Phi_{uv} \right\rangle \otimes \left| u, v \right\rangle \text{ where } \left| \Phi_{uv} \right\rangle = \sum_{\substack{x_1, x_2 \,: \\ k x_1^2 + \ell x_2^2 = u, \\ k x_1 + \ell x_2 = v}} \left| x_1, x_2 \right\rangle.$$

6. **(2 points)** Argue that had the resulting state been $\frac{1}{p} \sum_{u,v} \omega^{\alpha u + \beta v} \left| u, v \right\rangle$, we could measure the two registers in the Fourier basis and calculate (α, β).

7. **(Optional and tricky part!)** The trouble is that this is not the state and the entanglement with the first two registers prevents us from extracting (α, β) this way. To achieve this, we need to "uncompute" $|\Phi_{uv}\rangle$. This "morally" amounts to calculating the "compute" transform

$$T : |0, 0, u, v\rangle \mapsto \frac{1}{\sqrt{2}} |\Phi_{uv}\rangle \otimes |u, v\rangle .$$

as its inverse is the "uncompute" transform. You can trust me (or verify for yourself) that when $k \neq -\ell$ and $D \stackrel{\text{def}}{=} k\ell((k+\ell)u - v^2) \neq 0$ there are exactly 2 solutions to the system

$$\{x_1, x_2 : kx_1^2 + \ell x_2^2 = u, kx_1 + \ell x_2 = v\}$$

and they are

$$(x_1^{\pm}, x_2^{\pm}) = \left(\frac{kv \pm \sqrt{D}}{k(k+\ell)}, \frac{\ell v \mp \sqrt{D}}{\ell(k+\ell)} \right).$$

Furthermore, for every (u, v) occurring, D is not a square. Come up with a way to implement T.

Hint: First come up with a way to implement the isometry $|u, v, \pm\rangle \mapsto |u, v, x_1^{\pm}, x_2^{\pm}\rangle$.

8. **(Optional)** Argue that the bad events of $k = -\ell$ or $D = 0$ occur with at most probability $3/4$, giving an efficient algorithm for solving the hidden parabola problem!

9. Read the following text about why you studied this problem. No response is required.

Epilogue: Many of the quantum algorithms we have seen so far (such as Simon's problem, period finding, or discrete log) can all be understood as instances of the *abelian hidden subgroup problem*. In each case, a function hides the cosets of a subgroup of an abelian group, and the quantum Fourier transform over that group reveals information about the hidden subgroup. A major unanswered question in quantum algorithms is whether this paradigm can be extended to *nonabelian* groups. This is substantially harder as the simple Fourier-sampling arguments that work in the abelian case no longer suffice.

One particularly important example identified early on is the *dihedral hidden subgroup problem*. The dihedral group $D_N \cong \mathbb{Z}_N \rtimes \mathbb{Z}_2$ (the symmetries of an N-gon) is one of the simplest nonabelian groups, yet no polynomial-time quantum algorithm for its hidden subgroup problem is known. Understanding this problem has long been of interest partly because of its connection to lattice problems: Regev showed that an efficient solution to the dihedral hidden subgroup problem would yield efficient quantum algorithms for certain versions of the unique shortest-vector problem. Lattice problems are also the foundation of modern post-quantum cryptography—most notably Learning With Errors (LWE)—so understanding the limits of quantum algorithms

for these algebraic problems remains an important goal towards constructing post-quantum cryptography.

The hidden parabola problem you studied comes from this broader effort to understand what remains possible beyond the abelian setting. Although it is phrased as a problem about the level sets of a quadratic polynomial, it can be reformulated as a hidden subgroup problem over a special nonabelian group. In fact, for odd p, the relevant group is a p^3-element group closely related to (and isomorphic to) the finite Heisenberg group. This shows that quantum algorithms can solve *some* nonabelian hidden subgroup problems. It can be generalized to notions of a hidden polynomial problem, but we still have not found an efficient quantum algorithm for the dihedral hidden subgroup problem. The algorithm illustrates an idea that does not arise in the abelian algorithms we have studied in class: rather than extracting the answer from a single Fourier sample, we will combine multiple hidden-subgroup states and use their algebraic structure to reveal the hidden parameters.