CPSC 536W: Homework 3

Due on Gradescope by 11:59pm on 12th April 2024

Rules.

1. Please try to solve the problems yourself first. If you get stuck, you may consult any resources (books, internet, peers, office hours, etc.) for solutions. Provided you *acknowledge* these resources in detail, no marks will be deducted.
2. Please write legibly, work that is illegible will be marked as incorrect. Latex is strongly recommended for legibility. (I also recommend using `https://www.overleaf.com/` if you're new to Latex.)
3. All answers should be justified.
4. The total number of points for non-bonus questions is $T = 32$. Credit policy for the bonus question: suppose you receive x points for the bonus question and y points for the non-bonus questions, then the total number of points you receive for this homework is $\min(x + y, T)$.

Homework

1. **Consolidation of lecture material.**

   (a) Recall that for $M \in \mathbb{N}$, the quantum Fourier transform on $\mathbb{C}^M$ is the unitary $\mathrm{QFT}_M \in \mathbb{C}^{M\times M}$ defined by

   $$\mathrm{QFT}_M |j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{jk} |k\rangle , \tag{1}$$

   for all $j \in \{0, 1 \ldots, M-1\}$, where $w_M \coloneqq \exp(2\pi i/M)$.
   (1 point) Show that QFT_M is unitary, using Dirac notation throughout. That is, show that

   $$\mathrm{QFT}_M^\dagger \mathrm{QFT}_M = \mathbb{1}_M = \mathrm{QFT}_M \mathrm{QFT}_M^\dagger .$$

   (b) Recall the following lemma that we used in the proof of the query complexity of HSP:
   Lemma 1. *Let G be a finite group, $H, H' \leq G$ (subgroups of G), and $g, g' \in G$. Then*

   $$|gH \cap g'H'| = \begin{cases} |H \cap H'| & \text{if } g^{-1}g' \in HH', \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

   Here is a sketch proof of the lemma.

   Sketch proof.

   $$|gH \cap g'H'| = |\{(h, h') \in H \times H' \colon gh = g'h'\}| \tag{3}$$

   $$= \begin{cases} |H \cap H'| & \text{if } g^{-1}g' \in HH', \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

   □

   This question is about filling in the details of this sketch proof.
   (2 points) Justify eq. (3) in the proof by defining a map

   $$\phi_1 \colon \{(h, h') \in H \times H' \colon gh = g'h'\} \to gH \cap g'H'$$

   and showing that it is a bijection. (You first need to show that ϕ_1 is well-defined.) (Hint: you need to use properties of (sub)groups.)
   (3 points) Justify eq. (4) in the proof. In the case $g^{-1}g' \in HH'$, do this by defining a map

   $$\phi_2 \colon \{(h, h') \in H \times H' \colon gh = g'h'\} \to H \cap H'$$

   and showing that it is a bijection. (You first need to show that ϕ_2 is well-defined.) (Hint: this question is worth an entire mark more than the previous question, so you may need to be more careful.)

(c) Symmetry of the fidelity function.

Let $d \in \mathbb{N}$. Let $X \in \mathbb{C}^{d\times d}$.

(1 point) Show that there exist two sets of orthonormal bases $\{|u_1\rangle, \ldots, |u_d\rangle\}$ and $\{|v_1\rangle, \ldots, |v_d\rangle\}$ of $\mathbb{C}^d$ such that

$$X = \sum_{i=1}^{\operatorname{rank}(X)} \sigma_i |u_i\rangle\langle v_i|, \tag{5}$$

where the σ_is are the non-zero singular values of X, using Dirac notation as much as possible. (Hint: You may assume the singular value decomposition of X.)

(1 point) Show that $\operatorname{tr}[|X|] = \operatorname{tr}[|X^\dagger|]$, where $|X| \coloneqq \sqrt{X^\dagger X}$.

(1 point) Given two d-dimensional density matrices $\rho, \sigma \in \mathbb{C}^{d\times d}$, recall their fidelity is defined to be

$$F(\rho, \sigma) \coloneqq \|\sqrt{\rho}\sqrt{\sigma}\|_1, \tag{6}$$

where $\|\cdot\|_1$ is the Schatten 1-norm (aka the trace norm). Show that $F(\rho, \sigma) = F(\sigma, \rho)$.

(d) Recall the statement of amplitude amplification.

Proposition 1 (Amplitude amplification)**.** *Let $d \in \mathbb{N}$ and $\theta \in [0, \pi/2]$. Let $|\psi_0\rangle$, $|\psi_1\rangle$ be d-dimensional quantum states. Let $|\psi\rangle$ be the $2d$-dimensional quantum state defined by*

$$|\psi\rangle \coloneqq \cos(\theta)\,|0\rangle\,|\psi_0\rangle + \sin(\theta)\,|1\rangle\,|\psi_1\rangle \in \mathbb{C}^{2d}, \tag{7}$$

where $|0\rangle, |1\rangle \in \mathbb{C}^2$ denote the first and second computational basis states. Let

$$G \coloneqq \mathbb{1}_{2d} - 2|\psi\rangle\langle\psi| \quad \textit{and} \quad U \coloneqq \mathbb{1}_{2d} - 2|1\rangle\langle 1| \otimes \mathbb{1}_d\,. \tag{8}$$

Then, for all $k \in \mathbb{N}$,

$$(GU)^k\,|\psi\rangle = (-1)^k(\cos((2k+1)\theta)\,|0\rangle\,|\psi_0\rangle + \sin((2k+1)\theta)\,|1\rangle\,|\psi_1\rangle). \tag{9}$$

The proof of this proposition is "essentially the same" as the steps leading to Eq. 47 in the posted lecture 3 notes but it's not *exactly* the same.

(4 points) Provide a complete and self-contained proof of the proposition.

(e) Let $n \in \mathbb{N}$ and $M \subseteq [n]$. Let P be a real symmetric stochastic $n \times n$ matrix. Let P' be the variant of P that stops transitioning upon reaching M. That is, for all $i, j \in [n]$,

$$(P')_{ij} = \begin{cases} \delta_{ij} & \text{if } j \in M, \\ P_{ij} & \text{if } j \notin M. \end{cases} \tag{10}$$

Let $U \in \mathbb{C}^{n^2\times n^2}$ denote the Szegedy quantum walk operator corresponding to P'. Let $T \coloneqq \sum_{j=1}^n |\psi_j\rangle\langle j| \in \mathbb{C}^{n^2\times n}$, where

$$\forall j \in [n],\ |\psi_j\rangle \coloneqq |j\rangle \otimes \sum_{i=1}^n \sqrt{P'_{ij}}\,|j\rangle \in \mathbb{C}^{n^2}. \tag{11}$$

Let

$$|\psi\rangle \coloneqq \frac{1}{\sqrt{n - |M|}} \sum_{j\in[n], j\notin M} |j\rangle \in \mathbb{C}^n. \tag{12}$$

We needed the following to analyze the behavior of phase estimation with unitary U and state $T\,|\psi\rangle$.

(2 points) In the case $M = \emptyset$, show that $T\,|\psi\rangle$ is an eigenvector of U with eigenvalue 1.

(2 points) In the case $M \neq \emptyset$, let P_M denote the $(n - |M|) \times (n - |M|)$ submatrix of P corresponding to indices not in M. Suppose $\|P_M\| < 1$. Show that $|\psi\rangle$ lies in the span of vectors of the form $|\lambda\rangle$, where $|\lambda\rangle$ is an eigenvector of the discriminant matrix of P' with eigenvalue not equal to 1. (Hint: recall the discriminant matrix $D \in \mathbb{R}^{n\times n}$ of P' is defined entrywise by $D_{ij} = \sqrt{P'_{ij}P'_{ji}}$.)

(Therefore $T\,|\psi\rangle$ lies in the span of vectors of the form $T\,|\lambda\rangle$, where $|\lambda\rangle$ is an eigenvector of the discriminant matrix of P' with eigenvalue not equal to 1.)

2. **Hidden parabola problem.** *Source: CMSC 858Q, A1, P5; instructor: Andrew Childs.*

Let $p \geq 3$ be a prime and S be a finite set with size $|S| \geq p^2$.

Suppose $x_{\alpha,\beta} \colon \mathbb{F}_p^2 \to S$ satisfies the promise that

$$x_{\alpha,\beta}(u,v) = x_{\alpha,\beta}(u',v') \iff \alpha u^2 + \beta u - v = \alpha u'^2 + \beta u' - v' \tag{13}$$

for some unknown $0 \neq \alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p$. In other words, $x_{\alpha,\beta}$ is constant on the parabola

$$P_{\alpha,\beta,\gamma} \coloneqq \{(u,v) \in \mathbb{F}_p^2 \colon v = \alpha u^2 + \beta u + \gamma\} \tag{14}$$

for any fixed $\gamma \in \mathbb{F}_p$, and distinct on parabolas corresponding to different values of γ. The hidden parabola problem is about using (quantum) queries to $x_{\alpha,\beta}$ to determine the values of α and β.

In this exercise, we'll walk through the following description of a quantum query algorithm that can identify the hidden parabola with constant probability using a constant number of queries to $x_{\alpha,\beta}$.

(a) Use one quantum query to $x_{\alpha,\beta}$, i.e., one use of the quantum oracle of $x_{\alpha,\beta}$, to create the state:

$$\frac{1}{p} \sum_{u,v \in \mathbb{F}_p} |u,v\rangle \, |x_{\alpha,\beta}(u,v)\rangle \, . \tag{15}$$

(b) Measure the last register in the computational basis to obtain some $x_0 \in S$. The state of the first two[1] registers becomes

$$\frac{1}{\sqrt{p}} \sum_{u,v \in \mathbb{F}_p | v = \alpha u^2 + \beta u + \gamma_0} |u,v\rangle = \frac{1}{\sqrt{p}} \sum_{u \in \mathbb{F}_p} |u, \alpha u^2 + \beta u + \gamma_0\rangle \tag{16}$$

for some $\gamma_0 \in \mathbb{F}_p$.

(c) Apply QFT_p (as defined in the first question) on the second register gives

$$\frac{1}{p} \sum_{u \in \mathbb{F}_p} |u\rangle \sum_{v \in \mathbb{F}_p} \omega^{v \cdot (\alpha u^2 + \beta u + \gamma_0)} \, |v\rangle \, ,$$

where $\omega \coloneqq \exp(2\pi i / p)$.

(d) Measure the second register in the computational basis to obtain $v_0 \in \mathbb{F}_p$.
(1 point) For each $i \in \mathbb{F}_p$, what is the probability that $v_0 = i$?
The state of the first register then becomes

$$\frac{\omega^{v_0 \gamma_0}}{\sqrt{p}} \sum_{u \in \mathbb{F}_p} \omega^{v_0 \cdot (\alpha u^2 + \beta u)} \, |u\rangle \, , \tag{17}$$

which can be equated to

$$\frac{1}{\sqrt{p}} \sum_{u \in \mathbb{F}_p} \omega^{v_0 \cdot (\alpha u^2 + \beta u)} \, |u\rangle \, , \tag{18}$$

since the "global phase factor" $\omega^{v_0 \gamma_0}$ will not impact any future measurement statistics (this follows from the measurement postulates).

(e) Do all of the above steps another time to obtain the state

$$\begin{aligned}
&\frac{1}{\sqrt{p}} \sum_{u \in \mathbb{F}_p} \omega^{v_0 \cdot (\alpha u^2 + \beta u)} \, |u\rangle \otimes \frac{1}{\sqrt{p}} \sum_{u' \in \mathbb{F}_p} \omega^{v_0' \cdot (\alpha u'^2 + \beta u')} \, |u'\rangle \\
=&\frac{1}{p} \sum_{u,u' \in \mathbb{F}_p} \omega^{v_0 \cdot (\alpha u^2 + \beta u) + v_0' \cdot (\alpha u'^2 + \beta u')} \, |u,u'\rangle \\
=&\frac{1}{p} \sum_{u,u' \in \mathbb{F}_p} \omega^{\alpha (v_0 u^2 + v_0' u'^2) + \beta (v_0 u + v_0' u')} \, |u,u'\rangle
\end{aligned}$$

for some $v_0' \in \mathbb{F}_p$ obtained like v_0.

[1] $|*,\dagger\rangle$ is shorthand for $|*\rangle \otimes |\dagger\rangle = |*\rangle \, |\dagger\rangle$ and so can be viewed as having two registers.

(1 point) Explain how we can then create the state (without using any additional queries):

$$\frac{1}{p}\sum_{u,u'\in\mathbb{F}_p}\omega^{\alpha(v_0u^2+v_0'u'^2)+\beta(v_0u+v_0'u')}\left|u,u'\right\rangle\left|v_0u^2+v_0'u'^2\right\rangle\left|v_0u+v_0'u'\right\rangle \tag{19}$$

$$=\frac{1}{p}\sum_{z_2,z_1\in\mathbb{F}_p}\omega^{\alpha z_2+\beta z_1}\sum_{\substack{u,u'\in\mathbb{F}_p|\\ v_0u^2+v_0'u'^2=z_2\\ v_0u+v_0'u'=z_1}}\left|u,u'\right\rangle\left|z_2\right\rangle\left|z_1\right\rangle. \tag{20}$$

(f) (**2 points**) For all 4-tuples $(z_2,z_1,v_0,v_0')\in\mathbb{F}_p^4$ such that $0\notin\{v_0,v_0',v_0+v_0'\}$, solve the following system of equations in the variables (u,u'):

$$\begin{cases} v_0u^2+v_0'u'^2=z_2,\\ v_0u+v_0'u'=z_1. \end{cases} \tag{21}$$

(g) (**1 point**) Assuming $0\notin\{v_0,v_0',v_0+v_0'\}$, explain how to erase the values of the first two registers to zero in the state eq. (20). That is, explain how we can get from eq. (20) to a state of the form

$$\frac{1}{p}\sum_{z_2,z_1\in\mathbb{F}_p}\omega^{\alpha z_2+\beta z_1}c_{z_2,z_1}\left|0,0\right\rangle\left|z_2\right\rangle\left|z_1\right\rangle, \tag{22}$$

where $c_{z_2,z_1}\in\mathbb{C}$. (Hint: use the previous part.)

(h) (**4 points**) Finally, apply $\mathrm{QFT}_p^{-1}\otimes\mathrm{QFT}_p^{-1}$ to the last two registers of eq. (22) and then perform the computational basis measurement on those two registers. Show that the probability of the measurement outcome being $(\alpha,\beta)\in\mathbb{F}_p^2$ is at least a constant. (Note that we are no longer assuming $0\notin\{v_0,v_0',v_0+v_0'\}$.) (Hint: note that $p\geq 3$.)

3. **Spectrum of a product of reflections.** *Source: CMSC 858Q, A2, P4; instructor: Andrew Childs.*

Let $d\in\mathbb{N}$. A reflection on $\mathbb{C}^d$ is a matrix of the form $2P-\mathbb{1}_d$, where P is the projection onto a subspace of $\mathbb{C}^d$. In this language, the Szegedy quantum walk operator is a product of two particular reflections. In lectures, we analyzed the spectrum of the Szegedy quantum walk operator.

In this exercise, we will analyze the spectrum of a product of two *arbitrary* reflections.

Consider two subspaces

$$\mathcal{A}\coloneqq\mathrm{span}\{\left|\psi_1\right\rangle,\ldots,\left|\psi_a\right\rangle\}\quad\text{and}\quad\mathcal{B}\coloneqq\mathrm{span}\{\left|\phi_1\right\rangle,\ldots,\left|\phi_b\right\rangle\} \tag{23}$$

of $\mathbb{C}^d$, where $\langle\psi_j|\psi_k\rangle=\delta_{jk}$ and $\langle\phi_j|\phi_k\rangle=\delta_{jk}$. Let

$$\Pi\coloneqq\sum_{j=1}^{a}\left|\psi_j\right\rangle\!\left\langle\psi_j\right|\quad\text{and}\quad\Sigma\coloneqq\sum_{j=1}^{b}\left|\phi_j\right\rangle\!\left\langle\phi_j\right| \tag{24}$$

denote the projections onto $\mathcal{A}$ and $\mathcal{B}$ respectively. Let $R\coloneqq 2\Pi-\mathbb{1}_d$ and $S\coloneqq 2\Sigma-\mathbb{1}_d$ denote the corresponding reflections. Let $U\coloneqq R\cdot S$. Finally, let D denote the $a\times b$ matrix with entries $D_{jk}=\langle\psi_j|\phi_k\rangle$. We proceed to analyze the spectrum of U in terms of the singular value decomposition of D.

(a) **(2 points)** Let $\left|\alpha\right\rangle$ and $\left|\beta\right\rangle$ denote left and right singular vectors of D, respectively, with the same singular value σ. The left singular vector $\left|\alpha\right\rangle\in\mathbb{C}^a$ can be mapped to a vector $A\left|\alpha\right\rangle\in\mathbb{C}^d$ by applying the isometry $A\coloneqq\sum_{j=1}^{a}\left|\psi_j\right\rangle\!\left\langle j\right|$. Similarly, the right singular vector $\left|\beta\right\rangle\in\mathbb{C}^b$ can be mapped to a vector $B\left|\beta\right\rangle\in\mathbb{C}^d$ by the isometry $B\coloneqq\sum_{j=1}^{b}\left|\phi_j\right\rangle\!\left\langle j\right|$. Show that the subspace $\mathrm{span}\{A\left|\alpha\right\rangle,B\left|\beta\right\rangle\}$ is invariant under the action of U.

(b) **(2 points)** Diagonalize the action of U within this subspace to obtain one or two linearly independent eigenvectors of U. When do you obtain one, and when do you obtain two? Compute the eigenvalues of U corresponding to these eigenvectors.

(c) **(2 points)** How many eigenvectors of U are obtained by the procedure outlined above? What are the remaining eigenvectors of U and their corresponding eigenvalues?

4. **Bonus question.**

Let $n,t\in\mathbb{N}$ be such that $t\leq n$. For $\sigma\colon[t]\to[t]$ a bjiection, define $\chi_\sigma\in\mathbb{C}^{n^t\times n^t}$ by

$$\chi_\sigma\coloneqq\sum_{i_1,\ldots,i_t\in[n]}\left|i_1,i_2,\ldots,i_t\right\rangle\!\left\langle i_{\sigma(1)},i_{\sigma(2)},\ldots,i_{\sigma(t)}\right|. \tag{25}$$

Then, define

$$\chi \coloneqq \sum_{\sigma \in S_t} \chi_\sigma, \tag{26}$$

where S_t denotes the set of all bijections from $[t]$ to $[t]$.

Observe that χ is a Hermitian matrix.

(**3 points**) Completely characterize the spectrum of χ. That is, determine all the eigenvalues of χ together with the dimensions of their corresponding eigenspaces.

(Hint: it may help to consider the case $t = 2$ first, in which case χ_σ may be familiar from lectures.)

Now, define

$$\rho \coloneqq \frac{(n-1)!}{(n+t-1)!}\chi. \tag{27}$$

For $x \in \{0,1\}^n$, define

$$|\phi_x\rangle \coloneqq \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{28}$$

and

$$\sigma \coloneqq \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (|\phi_x\rangle\langle\phi_x|)^{\otimes t} \in \mathbb{C}^{n^t \times n^t}. \tag{29}$$

(**5 points**) Show that

$$\|\sigma - \rho\|_1 \leq 100 \cdot \frac{t^2}{n}, \tag{30}$$

for all $n, t \in \mathbb{N}$ with $t \leq n$, where the norm on the l.h.s is the Schatten 1-norm (aka the trace norm).

(Hints:

(a) you may take for granted the fact that $\|A\|_1$ of a Hermitian matrix A is the sum of the absolute values of the eigenvalues of A,

(b) it may help to consider the action of σ on the eigenspaces of ρ (which are the same as those of χ since ρ and χ differ by a scalar factor),

(c) in particular, it may help to consider the action of σ (and ρ) on states of the form

$$\frac{1}{\sqrt{t!}} \sum_{\sigma \in S_t} |i_{\sigma(1)}, \cdots, i_{\sigma(t)}\rangle \in \mathbb{C}^{n^t}, \tag{31}$$

where $i_1, \ldots, i_t \in [n]$ and $|\{i_1, \ldots, i_t\}| = t$, i.e., the i_js are all distinct,

(d) the factor of 100 on the r.h.s. of eq. (30) is not too significant; a better constant is possible, but we don't particularly care about optimizing the constant for this question so I'm giving you some leeway with 100.

)