CPSC 536W: Homework 4

Due on Gradescope by 11:59pm on 26th 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 $T = 16$. 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) **Block encoding of a Hamiltonian described as a Pauli decomposition.**
   Suppose H is an n-qubit Hamiltonian of the form

$$H = \sum_{j=1}^{N} a_j P_j, \tag{1}$$

   where the P_js are n-qubit Pauli matrices and $a_j > 0$ are such that $\sum_j a_j = 1$. Suppose Prepare $\in \mathbb{C}^{N\times N}$ is a unitary matrix such that Prepare $|0\rangle = \sum_{j=1}^{N} \sqrt{a_j}\,|j\rangle$ and Select $\in \mathbb{C}^{N2^n \times N2^n}$ is the matrix defined by

$$\text{Select} \coloneqq \sum_{j=1}^{N} |j\rangle\langle j| \otimes P_j. \tag{2}$$

   (1 point) Show that Select is a unitary matrix.
   (1 point) Show that $(\text{Prepare}^{-1} \otimes \mathbb{1}_{2^n}) \cdot \text{Select} \cdot (\text{Prepare} \otimes \mathbb{1}_{2^n})$ is a block encoding of H.

   (b) **Existence of block encoding.** Let $H \in \mathbb{C}^{n\times n}$ be Hermitian.
   (4 points) Show that

$$\text{there exists } N \geq n \text{ and a unitary } U \in \mathbb{C}^{N\times N} \text{ such that the top-left } n \times n \text{ block of } U \text{ equals } H \tag{3}$$

   if and only if

$$\|H\| \leq 1. \tag{4}$$

   (Hint: you need to show this for arbitrary $n \in \mathbb{N}$ but it helps to think about the case $n = 1$ first.)

2. **Combinatorial formulation of the adversary method.** *Source: CMSC 858Q, A3, P3; instructor: Andrew Childs.*
   Let $f\colon \{0,1\}^n \to \{0,1\}$. The original formulation of the adversary method in [Ambainis'00] is as follows. Let $X, Y \subseteq \{0,1\}^n$ be such that $f(x) \neq f(y)$ for all $x \in X, y \in Y$. For any relation $R \subseteq X \times Y$, define

$$m \coloneqq \min_{x\in X} |\{y \in Y : (x,y) \in R\}| \quad l \coloneqq \max_{\substack{x\in X\\ i\in\{1,\dots,n\}}} |\{y \in Y : (x,y) \in R \text{ and } x_i \neq y_i\}| \tag{5}$$

$$m' \coloneqq \min_{y\in Y} |\{x \in X : (x,y) \in R\}| \quad l' \coloneqq \max_{\substack{y\in Y\\ i\in\{1,\dots,n\}}} |\{x \in X : (x,y) \in R \text{ and } x_i \neq y_i\}| \tag{6}$$

Then define $\mathrm{Amb}(f) := \max_{X,Y,R} \sqrt{\frac{mm'}{ll'}}$, where the max is over all X, Y, R such that $ll' \neq 0$.

(6 points) Show that $\mathrm{Adv}(f) \geq \mathrm{Amb}(f)$. (You may find a copy of the definition of $\mathrm{Adv}(f)$ in Question 4(a).)

(Hint: you may use the following result: any $A \in \mathbb{R}^{a\times b}$ satisfies

$$\|A\| \leq \sqrt{r(A)\cdot c(A)}, \tag{7}$$

where the norm is the spectral norm and

$$r(A) := \max_{i\in[a]} \sum_{j=1}^{b} |A_{ij}| \quad \text{and} \quad c(A) := \max_{j\in[b]} \sum_{i=1}^{a} |A_{ij}|.) \tag{8}$$

3. **Adversary lower bound for Majority.**

For $n \in \mathbb{N}$, define

$$\mathrm{MAJORITY}_n \colon \{0,1\}^n \to \{0,1\} \tag{9}$$

by $\mathrm{MAJORITY}_n(x) = 1$ if and only if x contains strictly more 1s than 0s.

(4 points) Show that $\mathrm{Adv}(\mathrm{MAJORITY}_n) \geq \Omega(n)$.

(Hint: you may use the last question.)

4. **Bonus questions.**

(a) **Upper bound on the adversary quantity.**

Let $f\colon \{0,1\}^n \to \{0,1\}$. The adversary quantity of f, $\mathrm{Adv}(f)$, is defined[1] by

$$\begin{aligned} &\text{maximize} && \|\Gamma\| \\ &\text{subject to} && \Gamma \in \mathbb{R}^{2^n\times 2^n} \text{ is symmetric} \\ &&& f(x) = f(y) \implies \Gamma_{xy} = 0 \text{ for all } x, y \in \{0,1\}^n \\ &&& \forall i \in [n], \|\Gamma_i\| \leq 1, \\ &&& \quad \text{where } \Gamma_i \in \mathbb{R}^{2^n\times 2^n} \text{ is defined entrywise by } (\Gamma_i)_{xy} = \mathbb{1}[x_i \neq y_i]\Gamma_{xy} \text{ for all } x, y \in \{0,1\}^n. \end{aligned} \tag{10}$$

(4 points) Show that $\mathrm{Adv}(f) \leq n$.

(b) **Semidefinite programming formulation of the adversary quantity.** (You do not need to know the definition of a semidefinite program to do this question.)

Let $f\colon \{0,1\}^n \to \{0,1\}$. Consider the formulation of the adversary quantity in eq. (10). We'll first introduce some notation that allows us to rewrite it in a form that makes solving this problem slightly easier.

Notation. Let $J \in \mathbb{R}^{2^n\times 2^n}$ be the all-ones matrix. Let $F \in \mathbb{R}^{2^n\times 2^n}$ be defined entrywise by $F_{xy} = \mathbb{1}[f(x) = f(y)]$ for all $x, y \in \{0,1\}^n$. For $i \in [n]$, let $\Delta_i \in \mathbb{R}^{2^n\times 2^n}$ be defined entrywise by $(\Delta_i)_{xy} = \mathbb{1}[x_i \neq y_i]$ for all $x, y \in \{0,1\}^n$. For two matrices A and B of the same size, we write $A \circ B$ for the component-wise multiplication of A and B (aka Hadamard product).

(1 point) Show that the objective value of eq. (10) is the same as that of eq. (11).

$$\begin{aligned} &\text{maximize} && \|\Gamma\| \\ &\text{subject to} && \Gamma \in \mathbb{R}^{2^n\times 2^n} \text{ is symmetric} \\ &&& \Gamma \circ F = 0 \\ &&& \forall i \in [n], \|\Gamma \circ \Delta_i\| \leq 1. \end{aligned} \tag{11}$$

(3 points) Show that the objective value of eq. (11) is at least that of

$$\begin{aligned} &\text{maximize} && \langle J, W\rangle \\ &\text{subject to} && \beta \in \mathbb{R}^{2^n}, W \in \mathbb{R}^{2^n\times 2^n} \text{ is symmetric} \\ &&& W \circ F = 0 \\ &&& \forall i \in [n], \mathrm{diag}(\beta) - W \circ \Delta_i \geq 0 \text{ and } \mathrm{diag}(\beta) + W \circ \Delta_i \geq 0 \\ &&& \mathrm{diag}(\beta) \geq 0, \sum_{x\in\{0,1\}^n} \beta_x \leq 1, \end{aligned} \tag{12}$$

[1] The following definition is not exactly the same as that given in lectures but it should be clear that they are equivalent.

where $\langle J, W\rangle := \mathrm{tr}[J^\dagger W] = \mathrm{tr}[JW] =$ sum of all entries of W, $\mathrm{diag}(\beta)$ denotes the $2^n \times 2^n$ diagonal matrix defined by $\mathrm{diag}(\beta)_{xx} = \beta_x$ for all $x \in \{0,1\}^n$, and the notation $A \geq 0$ for a square matrix A means that A is positive semidefinite.

(Hint: for a given β, W, consider defining

$$\Gamma := \sum_{x,y \in \{0,1\}^n | W_{xy} \neq 0} \frac{W_{xy}}{\sqrt{\beta_x \beta_y}} |x\rangle\langle y|, \tag{13}$$

explaining why $W_{xy} \neq 0 \implies \beta_x \beta_y \neq 0$ so that this definition makes sense.)

(3 points) Show that the objective value of eq. (11) is at most that of

$$\begin{array}{ll} \text{maximize} & \langle J, W\rangle \\ \text{subject to} & \beta \in \mathbb{R}^{2^n}, W \in \mathbb{C}^{2^n \times 2^n} \text{ is Hermitian} \\ & W \circ F = 0 \\ & \forall i \in [n], \mathrm{diag}(\beta) - W \circ \Delta_i \geq 0 \text{ and } \mathrm{diag}(\beta) + W \circ \Delta_i \geq 0 \\ & \mathrm{diag}(\beta) \geq 0, \displaystyle\sum_{x \in \{0,1\}^n} \beta_x \leq 1. \end{array} \tag{14}$$

(Hint: for a given Γ, explain why we can assume $\|\Gamma\| = \gamma^\dagger \Gamma \gamma$ for some unit vector $\gamma \in \mathbb{C}^{2^n}$ without loss of generality, then consider defining

$$W := \mathrm{diag}(\gamma)^\dagger \cdot \Gamma \cdot \mathrm{diag}(\gamma) \quad \text{and} \quad \beta_x = |\gamma_x|^2 \text{ for all } x \in \{0,1\}^n.) \tag{15}$$

(1 point) Show that the objective values of eq. (12) and eq. (14) are the same.

Remark 1. *This question shows that the adversary quantity of f can be formulated as a semidefinite program since eq.* (14) *is a semidefinite program and the above showed* $\mathrm{Adv}(f)$ *equals the objective value of eq.* (14)*. One useful consequence of this result is that we can efficiently compute* $\mathrm{Adv}(f)$ *for any f with small domain size using software packages for semidefinite programming like CVX; the computational complexity scales polynomially with the domain size (exponentially with n). If you're unfamiliar with semidefinite programming but want to understand why eq.* (14) *is a semidefinite program, I recommend Watrous notes.*