CO 781/QIC 823/CS 867 Assignment 2

You are permitted to complete this assignment in groups of at most two (collaboration with other students aside from your partner is not permitted). Your completed assignment should include an acknowledgment of any sources (research papers, textbooks, etc) consulted. If you decide to work with a partner then (a) you must choose a partner that you have not worked with on another assessment in this course and (b) the completed assignment (one per group) should clearly state both group members names. The assignment must be submitted by Tuesday, July 13 at 9pm.

Problem 1 (Pretty good measurement)**.** In this problem you will derive the bound on the success probability of the pretty good measurement, following Ref. [4]. Suppose we are given a set $\{\rho_1, \rho_2, \ldots, \rho_N\}$ of quantum states to discriminate. Let $M = \sum_{i=1}^{N} \rho_i$ and suppose for simplicity that M is full rank. Recall that the pretty good measurement is defined by POVM elements

$$E_i = M^{-1/2} \rho_i M^{-1/2} \qquad 1 \leq i \leq N.$$

(i) For each i, write $\rho_i = \sum_j \lambda_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$ where $\{|\psi_{ij}\rangle\}_j$ form an orthonormal basis. Consider matrices G and P defined by

$$G_{ij,kl} = \sqrt{\lambda_{ij}\lambda_{kl}} \langle\psi_{ij}|\psi_{kl}\rangle \qquad P_{ij,kl} = \sqrt{\lambda_{ij}\lambda_{kl}} \langle\psi_{ij}|M^{-1/2}|\psi_{kl}\rangle.$$

Show that G, P are positive semidefinite matrices and that $P = \sqrt{G}$.

(ii) Show that the worst case success probability of the pretty good measurement is

$$p = \min_{1 \leq i \leq N} \sum_{l,s} |(\sqrt{G})_{il,is}|^2.$$

(iii) Show that the above expression is equal to

$$p = 1 - \max_{1 \leq i \leq N} \sum_{j \neq i} \sum_{l,s} |(\sqrt{G})_{il,js}|^2.$$

(iv) Read the proof of Lemma 3 in Ref. [4] which (in less than half a page) shows that

$$\max_{1 \leq i \leq N} \sum_{j \neq i} \sum_{l,s} |(\sqrt{G})_{il,js}|^2 \leq \sum_{k,l} F(\rho_k, \rho_l)$$

and therefore the worst case success probability is lower bounded as

$$p \geq 1 - \sum_{k,l} F(\rho_k, \rho_l) \geq 1 - N^2 \max_{k \neq l} F(\rho_k, \rho_l)$$

as we discussed in class. (For this part we are only asking you to confirm that you have read the proof from Montanaro's paper)

Problem 2 (Quantum walk on even-weight bit strings)**.** Consider the set of even weight n-bit strings:

$$S = \left\{ z \in \{0,1\}^n : \sum_{i=1}^{n} z_i \text{ is even} \right\}.$$

Consider a graph G with vertices labeled by elements of S and an edge between $x, y \in S$ whenever x and y differ in exactly two bits. Suppose you are given oracle access to a function $f : S \to \{0,1\}$ and asked to distinguish between the case where (A) $f(x) = 0$ for all $x \in S$ or (B) there is a unique $x \in S$ such that $f(x) = 1$. Design a quantum walk algorithm (on the graph G) which decides between these two cases and give an upper bound on its runtime.

Problem 3 (Query complexity lower bounds)**.** Consider a function

$$f_T(x) = \begin{cases} 0, \sum_{i=1}^{n} x_i \leq T \\ 1, \sum_{i=1}^{n} x_i > T \end{cases}$$

Establish lower bounds on the query complexity $Q(f_T)$ using (a) the polynomial method, and (b) the adversary method.

Problem 4 (Approximate degree of OR)**.** Consider the n-bit OR function

$$\mathrm{OR}_n(x_1, x_2, \ldots, x_n) = 1 - (1 - x_1)(1 - x_2) \ldots (1 - x_n).$$

(i) Describe a simple variant of Grover search which uses $O(\sqrt{n} \log(1/\epsilon))$ quantum queries and computes OR_n with probability at least $1 - \epsilon$. Describe how this implies an upper bound on the ϵ-approximate degree of OR_n.

Let $F(k)$ be the univariate function which is associated with OR_n, defined by $F(0) = 0$ and $F(k) = 1$ for all $1 \leq k \leq n$. The above

bound implies that there exists a univariate polynomial $p(x)$ of degree $O(\sqrt{n}\log(1/\epsilon))$ such that

$$|p(k) - F(k)| \leq \epsilon \qquad \text{for all } k = 0, 1, 2, \ldots, n. \tag{1}$$

In the remainder of this question you will explicitly construct a polynomial which approximates F in this sense.

(ii) Let T_j be the degree-j Chebyshev polynomial of the first kind, which is the unique j-th degree polynomial satisfying $T_j(\cos(\theta)) = \cos(j\theta)$. Show that $|T_j(x)| \in [-1, 1]$ for $x \in [-1, 1]$ and that $|T_j(1+\delta)| \geq c \cdot e^{c' j\sqrt{\delta}}$ for $\delta \in (0, 2)$, where $c, c' > 0$ are constants.

(iii) Consider the degree-j univariate polynomial $p(x)$ defined below. Show that $p(0) = 0$ and $|p(x) - 1| \leq e^{-\Omega(j/\sqrt{n})}$ for $1 \leq x \leq n$. Use this to establish that Eq. (1) holds for some $j = O(\sqrt{n}\log(1/\epsilon))$.

$$p(x) = 1 - \frac{T_j\left(\frac{2(1-x/n)}{1-1/n} - 1\right)}{T_j\left(\frac{2}{1-1/n} - 1\right)}.$$

Problem 5 (Quantum search with small error probability)**.** In this problem we will discuss variations of Grover's search algorithm with a focus on the runtime scaling with error probability ϵ [2]. In the following we are given oracle access to a function $f : \{0,1\}^n \to \{0,1\}$. Let $M = \{x : f(x) = 1\}$ be the set of marked items. Our goal is to determine if M is empty or not. You have seen already that this problem can be solved with a small constant error probability (say 1/3) using $O(\sqrt{2^n})$ quantum queries to f.

(i) Suppose we are given $k = |M|$. Show that there is an exact version of Grover's algorithm, call it Exact_k which uses $O(\sqrt{2^n/k})$ quantum queries to f and finds a bit string $x \in M$ with certainty. It may be helpful to refer to Ref. [1].

(ii) Now consider the original task which is to determine whether or not M is empty. Let $T = \lceil \log(1/\epsilon) \rceil$. Consider an algorithm which first runs $\text{Exact}_1, \text{Exact}_2, \ldots, \text{Exact}_T$. If any of these subroutines find an $x \in M$ then we are done (otherwise, we may assume that $|M| > T$ if M is nonempty). If the subroutines do not return $x \in M$, the algorithm

then runs T repetitions of standard Grover search assuming $|M| \geq T$ with error probability 1/3 which uses $O(\sqrt{2^n/T})$ queries. Show that this algorithm decides if M is nonempty with error probability at most ϵ and using only $O(\sqrt{2^n \log(1/\epsilon)})$ queries.

(iii) From (ii), infer an upper bound on the approximate degree $\widetilde{deg}_\epsilon(\mathrm{OR}_n)$. Show that this upper bound is better than the explicit one obtained in problem 4. (a refinement of the explicit polynomial is given in Ref. [3])

Problem 6 (Different formulations of the adversary method)**.** Let $f : S \to \{0,1\}$ where $S \subseteq \{0,1\}^n$. In class we discussed the adversary lower bound

$$Q(f) \geq \Omega(\mathrm{Adv}(f)) \qquad \text{where } \mathrm{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{1 \leq i \leq n} \|\Gamma_i\|} \tag{2}$$

where the maximum is over adversary matrices $\Gamma \in \mathbb{R}^{|S| \otimes |S|}$. In KLM there is another version of the adversary lower bound which is described by Theorem 9.7.4. In fact, the latter version of the adversary method is weaker than the one described by Eq. (2). In this problem you are asked to provide a proof of Theorem 9.7.4 by showing that it follows from Eq. (2). You may (with attribution) wish to provide a simplified version of the proof in Theorem 4.4 in Ref. [5], which is specialized to the case at hand.

References

[1] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum counting. In *International Colloquium on Automata, Languages, and Programming*, pages 820–831. Springer, 1998.

[2] Harry Buhrman, Richard Cleve, Ronald De Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*, pages 358–368. IEEE, 1999.

[3] Jeff Kahn, Nathan Linial, and Alex Samorodnitsky. Inclusion-exclusion: Exact and approximate. *Combinatorica*, 16(4):465–477, 1996.

[4] Ashley Montanaro. Pretty simple bounds on quantum state discrimination. *arXiv preprint arXiv:1908.08312*, 2019.

[5] Robert Spalek and Mario Szegedy. All quantum adversary methods are equivalent. *arXiv preprint quant-ph/0409116*, 2004.