Problems for
Quantum query complexity and the adversary bound

Alexander Belov

Palmse, 2017

First Lecture

1. Use the basic adversary bound to prove the following lower bounds on quantum query complexity:

   (a) An $\Omega(\sqrt{nm})$ lower bound for evaluating the function

   $$\mathrm{OR}\Big(\mathrm{AND}(x_{11}, x_{12}, \ldots, x_{1m}),\quad \mathrm{AND}(x_{21}, x_{22}, \ldots, x_{2m}),\ \ldots,\ \mathrm{AND}(x_{n1}, \ldots, x_{nm})\Big).$$

   (Note: this follows from the composition theorem, but try to give a basic adversary argument.)

   (b) Graph connectivity problem. You are given oracle access to the adjacency matrix of a simple graph G on n vertices. Prove $\Omega(n^{3/2})$ lower bound for deciding whether G is connected. (Hint: try to distinguish two cases: G consists of a single cycle, and G consists of two disjoing cycles.)

2. Some properties of PSD matrices.

   (a) We already know that linear combinations of PSD matrices with *positive* coefficients are PSD. Nothing to prove here.

   (b) Let A be an $n \times n$ PSD matrix, and $S \subseteq [n]$. Prove that $|S| \times |S|$ submatrix $A[\![S, S]\!]$ of A is PSD.

   (c) Prove that a tensor product $A \otimes B$ of two PSD matrices is PSD.

   (d) Prove that a Hadamard (element-wise) product $A \circ B$ of two PSD matrices is PSD.

3. The goal of this problem is to prove that the adversary bound of the k-threshold function on n variables is $\sqrt{k(n-k+1)}$ *exactly*. We saw the lower bound in lecture, so let us prove the upper bound.

   Consider first the case when each negative input y contains exactly $k-1$ ones, and each positive input x contains exactly k ones. The matrices X_j satisfy $X_j[\![x, y]\!] = 0$ unless $x_j = 1$ and $y_j = 0$. And if $x_j = 1$ and $y_j = 0$, then

   $$X_j[\![x, y]\!] = \frac{1}{\big|\{i \in [n] \mid x_i = 1,\ y_i = 0\}\big|}, \quad X_j[\![x, x]\!] = \sqrt{\frac{n-k+1}{k}}, \quad X_j[\![y, y]\!] = \sqrt{\frac{k}{n-k+1}}. \tag{1}$$

   (a) Verify that these matrices satisfy $\sum_{j: x_j \neq y_j} X_j[\![x, y]\!] = 1$ and give the desired objective value.

It remains to prove that these matrices can be made positive semi-definite.

(b) Prove there exist PSD matrices A_j satisfying
- first, $A_j[\![x, y]\!] = 0$ unless $x_j = 1$ and $y_j = 0$.
- Otherwise, $A_j[\![x, y]\!] = \big|\{i \in [n] \mid x_i = y_i = 1\}\big|$; and
- $A_j[\![x, x]\!] = A_j[\![y, y]\!] = k - 1$.

(c) Assume $k > 0$ is a real number, and a matrix $A \succeq 0$ is such that $\big|A[\![i, j]\!]\big| < k$ for all i and j. Prove that the matrix B, defined by $B[\![i, j]\!] = (k - A[\![i, j]\!])^{-1}$, is also PSD. (Hint: use decomposition in series.)

(d) Prove there exist PSD matrices X_j satisfying (1).

(e) How do we get a dual adversary bound for all inputs without the restriction $|x| = k$ and $|y| = k - 1$?

4. Prove the composition theorem for the adversary bound. (The upper bound is relatively easy, but the lower bound is more challenging, and we won't cover it.)

Second Lecture

1. Find an upper bound on the learning graph complexity of the following certificate structures:

(a) The k-OR certificate structure. Each $M \in \mathcal{C}$ is specified by a subset $A \subseteq [n]$ of size k, where $S \in M$ iff $A \cap S \neq \emptyset$. (And all subsets are used in this way.)

(b) The k-subset certificate structure from the lecture. Each $M \in \mathcal{C}$ is specified by a subset $A \subseteq [n]$ of size k, where $S \in M$ iff $A \subseteq S$.

(c) The shift certificate structure. n is even and the set $[n]$ is split into two halves: $[\frac{n}{2}]$ and $[\frac{n}{2} + 1..n]$. Each $M \in \mathcal{C}$ is specified by a number $d \in [n/2]$. A subset S is in M iff there exists $i \in [n/2]$ such that

$$i \in S \qquad \text{and} \qquad \frac{n}{2} + 1 + (i + d \bmod \frac{n}{2}) \in S.$$

(d) The collision certificate structure. Like in the shift case, n is even. Each $M \in \mathcal{C}$ is specified by a permutation $\pi\colon [n/2] \to [n/2]$. A subset S is in M iff there exists $i \in [n/2]$ such that

$$i \in S \qquad \text{and} \qquad \frac{n}{2} + \pi(i) \in S.$$

(e) 2-path certificate structure. Like in the case of triangle, the input variables are edges of a simple graph. A certificate is given by a 2-path, i.e., two edges uv and vw.

(f) (Open problem) Consider certificates in the form of some fixed graph H (we had H being the triangle, and H being a 2-path).

2. Consider the following learning graph for the triangle certificate structure:

I	Take disjoint subsets $B, C \subseteq [n] \setminus \{a, b, c\}$ of sizes r_2 and r_3, respectively, uniformly at random, and load all the edges between B and C
II	Add a to B and load all the edges between a and C
III	Add b to B and load all the edges between b and C
IV	Choose, uniformly at random, a subset $A \subseteq B \setminus \{a, b\}$ of size r_1 and load all the edges between c and A
V	Load the edge ac, and add a to A
VI	Load the edge bc
VII	Load the edge ab

Analyse this learning graph in terms of lengths and specialities. How does it compare to the one considered in the lecture?

Third Lecture

1. Prove lower bounds for the certificate structures in Problem 1 of Lecture 2.
2. Which of the certificate structures of Problem 1 are boundedly generated? That is, for which certificate structures we can get a quantum lower bound for the corresponding sum problem?
3. Construct a dual learning graph for the triangle certificate structure. It is relatively easy to get complexity $\Omega(n^{5/4})$. Going to $n^{9/7}$ is more challenging. (Compare to Problem 2 of Lecture 2.)

Fourth Lecture

1. Construct an adaptive learning graph for the k-collision problem when k is not necessarily bounded by a constant.
2. Prove a quantum lower bound of $\Omega(\sqrt{k})$ for the group testing problem.
3. (Open problem) What is the quantum query complexity of the graph collision problem?
4. (Open problem) Find applications of the quantum algorithm for the (gapped) group testing problem.