Optimal quantum adversary lower bounds for ordered search

Andrew M. Childs[*] Troy Lee[†]

Abstract

The goal of the ordered search problem is to find a particular item in an ordered list of n items. Using the adversary method, Høyer, Neerbek, and Shi proved a quantum lower bound for this problem of $\frac{1}{\pi}\ln n + \Theta(1)$. Here, we find the exact value of the best possible quantum adversary lower bound for a symmetrized version of ordered search (whose query complexity differs from that of the original problem by at most 1). Thus we show that the best lower bound for ordered search that can be proved by the adversary method is $\frac{1}{\pi}\ln n + O(1)$. Furthermore, we show that this remains true for the generalized adversary method allowing negative weights.

1 Introduction

Search is a fundamental computational task. In a general search problem, one is looking for a distinguished item in a set, which may or may not have some structure. At one extreme, in the *unstructured search problem*, we assume the set has no additional structure whatsoever. In this setting, a classical search requires $\Omega(n)$ queries in the worst case to find the distinguished item. Grover's well-known search algorithm shows that a quantum computer can find the distinguished item with high probability in only $O(\sqrt{n})$ queries [16]. A lower bound based on a precursor to the adversary method shows this is optimal up to a constant factor [6].

At the other extreme of search problems, in the *ordered search problem*, we assume our set comes equipped with a total order, and we are able to make comparison queries, i.e., queries of the form '$w \leq z$?'. Classically, we can apply binary search to find the desired item in $\lceil \log_2 n \rceil$ queries, and an information theoretic argument shows this is tight.

Quantum computers can speed up the solution of the ordered search problem by a constant multiplicative factor. Farhi, Goldstone, Gutmann, and Sipser developed a class of translation-invariant ordered search algorithms and showed that one such algorithm, applied recursively, gives an exact ordered search algorithm using $3\log_{52} n \approx 0.526\log_2 n$ quantum queries [14]. Brookes, Jacokes, and Landahl used a gradient descent search to find an improved translation-invariant algorithm, giving an upper bound of $4\log_{550} n \approx 0.439\log_2 N$ queries [8]. Childs, Landahl, and Parrilo used numerical semidefinite optimization to push this approach still further, improving the upper bound to $4\log_{605} n \approx 0.433\log_2 n$ [11]. Ben-Or and Hassidim gave an algorithm based on adaptive learning that performs ordered search with probability of error $o(1)$ using only about $0.32\log_2 n$ queries [7].

In fact, the quantum speedup for ordered search is not more than a constant multiplicative factor. Using the quantum adversary method [2], Høyer, Neerbek, and Shi showed a lower bound of $\frac{1}{\pi}(\ln n - 1) \approx 0.221\log_2 n$ queries [18], improving on several previous results [1, 9, 13]. However, the exact value of the best possible speedup factor, a fundamental piece of information about the power of quantum computers, remains undetermined.

[*] Department of Combinatorics & Optimization and Institute for Quantum Computing, University of Waterloo; amchilds@uwaterloo.ca

[†] Laboratoire de Recherche en Informatique, Université Paris-Sud; troyjlee@gmail.com

In this paper, we give some evidence that the asymptotic quantum query complexity of ordered search is $\frac{1}{\pi}\ln n + O(1)$. Specifically, we show that the best lower bound given by the adversary method, one of the most powerful techniques available for showing lower bounds on quantum query complexity, is $\frac{1}{\pi}\ln n + O(1)$. We show this both for the standard adversary method [2] and the recent strengthening of this method to allow negative weights [17]. In particular, we prove the following:

Theorem 1. *Let* $\mathrm{ADV}(f)$ *be the optimal bound given by the adversary method for the function* f*, let* $\mathrm{ADV}^{\pm}(f)$ *be the optimal value of the adversary bound with negative weights, and let* OSP_n *the ordered search problem on* n *items (symmetrized as discussed in Section 4). Then*

$$\mathrm{ADV}(\mathrm{OSP}_{2m}) = 2\sum_{i=0}^{m-1}\left(\frac{\binom{2i}{i}}{4^i}\right)^2$$

$$\mathrm{ADV}(\mathrm{OSP}_{2m+1}) = 2\sum_{i=0}^{m-1}\left(\frac{\binom{2i}{i}}{4^i}\right)^2 + \left(\frac{\binom{2m}{m}}{4^m}\right)^2.$$

Furthermore,

$$\mathrm{ADV}^{\pm}(\mathrm{OSP}_n) \le \mathrm{ADV}(\mathrm{OSP}_n) + O(1).$$

The bounds described in Theorem 1 are asymptotically $\frac{2}{\pi}\ln n + O(1)$, but are always strictly larger than the Høyer-Neerbek-Shi bound. Understanding the best possible adversary bound for small n could be useful, since the best exact algorithms for ordered serach have been found by discovering a good algorithm for small values of n and using this algorithm recursively. Furthermore, since the adversary quantity can be viewed as a simplification of the quantum query complexity, we hope that our analytic understanding of optimal adversary bounds will provide tools that are helpful for determining the quantum query complexity of ordered search.

The remainder of this article is organized as follows. In Section 2, we briefly review the quantum adversary method. In Section 3, we define the basic ordered search problem as well as a extended version that is more symmetric, and hence easier to analyze. In Section 4, we apply the adversary method to the symmetrized ordered search problem and present semidefinite programs characterizing it, both in primal and dual formulations. In Section 5, we find the optimal non-negative adversary lower bound for ordered search and compare it to the bound of [18]. Then we show in Section 6 that negative weights do not substantially improve the bound. Finally, we conclude in Section 7 with a brief discussion of the results.

2 Adversary bound

The adversary method, along with the polynomial method [5], is one of the two main techniques for proving lower bounds on quantum query complexity. The adversary method was originally developed by Ambainis [2], with roots in the hybrid method of [6]. It has proven to be a versatile technique, with formulations given by various authors in terms of spectral norms of matrices [4], weight schemes [3, 24], and Kolmogorov complexity [20]. Špalek and Szegedy showed that all these versions of the adversary method are in fact equivalent [23]. Recently, Høyer, Lee, and Špalek developed a new version of the adversary method using negative weights which is always at least as powerful as the standard adversary method, and can sometimes give better lower bounds [17].

We will use the spectral formulation of the adversary bound, as this version best expresses the similarity between the standard and negative adversary methods. In this formulation, the value of the adversary method for a function f is given by

$$\mathrm{ADV}(f) := \max_{\substack{\Gamma\ge 0\\ \Gamma\ne 0}} \frac{\|\Gamma\|}{\max_i \|\Gamma\circ D_i\|},$$

where Γ is a square matrix with rows and columns indexed by the possible inputs $x \in S \subseteq \{0,1\}^n$, constrained to satisfy $\Gamma[x,y] = 0$ if $f(x) = f(y)$; D_i is a zero/one matrix with $D_i[x,y] = 1$ if $x_i \neq y_i$ and 0 otherwise; $A \circ B$ denotes the Hadamard (i.e., entrywise) product of matrices A and B; and $\Gamma \geq 0$ means that the matrix Γ is entrywise non-negative. Note that the set S of possible inputs need not be the entire set $\{0,1\}^n$ of all n-bit strings—in other words, f might be a partial function, as is the case for ordered search.

The negative adversary method is of the same form, but removes the restriction to non-negative matrices in the maximization. Thus the value of the negative adversary method for a function f is given by

$$\mathrm{ADV}^{\pm}(f) := \max_{\Gamma \neq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}.$$

The relation of these adversary bounds to quantum query complexity is given by the following theorem. Let $Q_\epsilon(f)$ denote the minimum number of quantum queries to f needed to compute that function with error at most ϵ. Then we have

Theorem 2 ([2, 17])**.** *Let $S \subseteq \{0,1\}^n$, and let Σ be a finite set. Then for any function $f : S \to \Sigma$,*

$$Q_\epsilon(f) \geq \frac{1 - 2\sqrt{\epsilon(1-\epsilon)}}{2} \mathrm{ADV}(f) \quad \text{and} \quad Q_\epsilon(f) \geq \frac{1 - 2\sqrt{\epsilon(1-\epsilon)} - 2\epsilon}{2} \mathrm{ADV}^{\pm}(f).$$

In particular, $Q_0(f) \geq \frac{1}{2} \mathrm{ADV}^{\pm}(f) \geq \frac{1}{2} \mathrm{ADV}(f)$.

3 Ordered search problem

In the ordered search problem, we are looking for a marked element w in a set Z equipped with a total order. Let the members of Z be $z_1 \leq z_2 \leq \cdots \leq z_n$. We are looking for the marked element $w \in Z$, and are able to ask queries of the form '$w \leq z$?' for $z \in Z$. Notice that if w is the ith element in the list, then the answer to this query will be 'no' for $z = z_j$ with $j < i$, and will be 'yes' otherwise. Thus we can model this problem as finding the first occurence of a '1' in a string $x \in \{0,1\}^n$ where $x_j = 0$ for $j < i$ and $x_j = 1$ otherwise. For example, for $n = 4$, the possible inputs for the ordered search problem are 1111, 0111, 0011, and 0001, corresponding to the marked item being first, second, third, or fourth in the ordered set, respectively. Thus we have transformed the input into a binary string, and the queries are to the bits of this input. The goal is to determine which input we have—in other words, the function takes a different value on each input.

In general, when trying to determine the query complexity of a function f, it is helpful to consider its symmetries, as expressed by its *automorphism group*. We say that $\pi \in S_n$, a permutation of the n bits of the input, is an automorphism of the function f provided it maps inputs to inputs, and $f(x) = f(y) \Leftrightarrow f(\pi(x)) = f(\pi(y))$. The set of automorphisms of any function on n-bit inputs is a subgroup of S_n, called the automorphsim group of that function.

The ordered search problem as formulated above has a trivial automorphism group, because any nontrivial permutation maps some input to a non-input. However, we can obtain a more symmetric function, with only a small change to the query complexity, by putting the input on a circle [14]. Now let the inputs have $2n$ bits, and consist of those strings obtained by cyclically permuting the string of n 1's followed by n 0's. For example, with $n = 4$, the inputs are $11110000, 01111000, 00111100, 00011110, 00001111, 10000111, 11000011, 11100001$. Again, we try to identify the input, so the function OSP_n takes a different value on each of the $2n$ inputs. The automorphism group of OSP_n is isomorphic to $\mathbb{Z}_{2n}$, a fact that we will exploit in our analysis.

The query compexity of this extended function is closely related to that of the original function. Given an n-bit input x, we can simulate a $2n$-bit input by simply querying x for the first n bits, and the complement of x for the second n bits. In the other direction, to simulate an n-bit input using a $2n$-bit input, first query the nth bit of the $2n$-bit input. If it is 1, then we use the first half of the $2n$-bit input; otherwise we use the second half (or, equivalently, the complement of the first half). Thus the query complexity of the extended function is at least that of the original function, and at most one more than that of the original function, a difference that is asymptotically negligible.

4 Adversary bounds for ordered search

Finding the value of the adversary method is as an optimization problem. To analyze the adversary bound for ordered search, we will use symmetry to simplify this problem. The same simplification applies to both the standard and negative adversary bounds, so we treat the two cases simultaneously.

Suppose we are trying to design a good adversary matrix Γ, and are deciding what weight to assign the (x, y) entry. Intuitively, it seems that if (x, y) and (x', y') are related by an automorphism, then they should look the same to an adversary, and hence should be given the same weight. The *automorphism principle* states that there is an optimal adversary matrix with this property. Although this principle does not provide any advice about what weight to give a particular pair (x, y), it can vastly reduce the optimization space by indicating that the adversary matrix should possess certain symmetries.

Theorem 3 (Automorphism principle [17]). *Let G be the automorphism group of f. Then there is an optimal adversary matrix Γ satisfying $\Gamma[x, y] = \Gamma[\pi(x), \pi(y)]$ for all $\pi \in G$ and all pairs of inputs x, y. Furthermore, if G acts transitively on the inputs (i.e., if for every x, y there is an automorphism taking x to y), then the uniform vector (i.e., the vector with each component equal to 1) is a principal eigenvector of Γ.*

The automorphism group for the ordered search problem on a list of size n, extended to a circle of size $2n$ as discussed in the previous section, is isomorphic to $\mathbb{Z}_{2n}$, generated by the element $(1\,2\,3 \ldots 2n)$ that cyclically permutes the list. This group acts transitively on the inputs, so by the automorphism principle, the uniform vector is a principal eigenvector of the adversary matrix. In addition, any pairs (x, y) and (x', y') that have the same Hamming distance are related by an automorphism. Thus we may assume that the adversary matrix has at most n distinct entries, and that the (x, y) entry depends only on the Hamming distance between x and y. As all strings have the same Hamming weight, the Hamming distance between any pair is even. We let $\Gamma[x, y] = \gamma_i$ when x, y have Hamming distance $2i$. For example, with $n = 4$, we have

$$\Gamma = \begin{array}{ccccccccc}
\text{11110000} & \text{01111000} & \text{00111100} & \text{00011110} & \text{00001111} & \text{10000111} & \text{11000011} & \text{11100001} & \\
0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & \text{11110000} \\
\gamma_1 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & \text{01111000} \\
\gamma_2 & \gamma_1 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & \text{00111100} \\
\gamma_3 & \gamma_2 & \gamma_1 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \text{00011110} \\
\gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \text{00001111} \\
\gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & \gamma_1 & \gamma_2 & \text{10000111} \\
\gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & \gamma_1 & \text{11000011} \\
\gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & \text{11100001}
\end{array}$$

Since all rows have the same sum, the uniform vector is indeed an eigenvector, corresponding to the eigenvalue $\gamma_n + 2\sum_{i=1}^{n-1} \gamma_i$.

Transitivity of the automorphism group also implies that all matrices $\Gamma \circ D_i$ have the same norm, so it is sufficient to consider $\Gamma \circ D_{2n}$. Again considering the example of $n = 4$, we have

$$\Gamma \circ D_{2n} = \begin{bmatrix} 0 & 0 & 0 & 0 & \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 \\ 0 & 0 & 0 & 0 & \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 \\ 0 & 0 & 0 & 0 & \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 \\ 0 & 0 & 0 & 0 & \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_4 & \gamma_3 & \gamma_2 & \gamma_1 & 0 & 0 & 0 & 0 \\ \gamma_3 & \gamma_4 & \gamma_3 & \gamma_2 & 0 & 0 & 0 & 0 \\ \gamma_2 & \gamma_3 & \gamma_4 & \gamma_3 & 0 & 0 & 0 & 0 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

This matrix consists of two disjoint, identical blocks, so its spectral norm is simply the spectral norm of one of those blocks. In general, $\Gamma \circ D_{2n}$ consists of two disjoint blocks, where each block is an $n \times n$ symmetric Toeplitz matrix with first row equal to $(\gamma_n, \gamma_{n-1}, \ldots, \gamma_1)$, denoted $\mathrm{Toeplitz}(\gamma_n, \gamma_{n-1}, \ldots, \gamma_1)$. Thus via the automorphism principle we have reduced the adversary bound to the semidefinite program

$$\max\ \gamma_n + 2\sum_{i=1}^{n-1} \gamma_i \quad \text{subject to} \quad \| \mathrm{Toeplitz}(\gamma_n, \gamma_{n-1}, \ldots, \gamma_1) \| \le 1,\ \gamma_i \ge 0 \qquad \text{(P)}$$

in the case of non-negative weights, and

$$\max\ \gamma_n + 2\sum_{i=1}^{n-1} \gamma_i \quad \text{subject to} \quad \| \mathrm{Toeplitz}(\gamma_n, \gamma_{n-1}, \ldots, \gamma_1) \| \le 1 \qquad (\mathrm{P}^{\pm})$$

in the case of the negative adversary method. We emphasize that the automorphism principle ensures there is no loss of generality in considering adversary matrices of this form—this program has the same optimal value as the best possible adversary bound.

We will also use the duals of these semidefinite programs to show upper bounds on the values of the adversary methods. Straightforward dualization shows that the dual of (P) is

$$\min \mathrm{Tr}(P) \quad \text{subject to} \quad P \succeq 0,\ \mathrm{Tr}_i(P) \ge 1 \text{ for } i = 0, \ldots, n-1, \qquad \text{(D)}$$

and that the dual of ($\mathrm{P}^{\pm}$) is

$$\min \mathrm{Tr}(P+Q) \quad \text{subject to} \quad P, Q \succeq 0,\ \mathrm{Tr}_i(P-Q) = 1 \text{ for } i = 0, \ldots, n-1 \qquad (\mathrm{D}^{\pm})$$

where $P \succeq 0$ means that the matrix P is positive semidefinite.

In general, by a *solution* of a semidefinite program, we mean a choice of the variables that satisfies the constraints, but that does not necessarily extremize the objective function. If a solution achieves the optimal value of the objective function, we refer to it as an *optimal solution*.

5 Non-negative adversary

In this section, we consider the standard adversary bound. We first present the lower bound of Høyer, Neerbek, Shi as applied to the symmetrized version of ordered search. Then we construct an improved adversary matrix, giving a solution of (P) that achieves the bound stated in Theorem 1. Finally, we exhibit a solution to (D) with the same value, showing that our construction is optimal.

5.1 Høyer, Neerbek, Shi construction

Within the framework described above, the lower bound of [18] can be given very simply. Set $\gamma_i = 0$ if $i > \lfloor n/2 \rfloor$ and $\gamma_i = 1/(\pi i)$ otherwise. This gives an objective function of

$$\frac{2}{\pi} \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{1}{i} \sim \frac{2}{\pi} \ln n.$$

Continuing our example with $n = 4$, consider the matrix $\Gamma \circ D_{2n}$ under this choice of weights:

$$\Gamma \circ D_{2n} = \frac{1}{\pi} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

This matrix consists of four disjoint blocks, so its spectral norm is equal to the largest spectral norm of these blocks. In general, we have four disjoint nonzero blocks (and in the case of n odd, two additional 2×2 zero blocks). Each nonzero block is equivalent up to permutation to $1/\pi$ times $Z_{\lfloor n/2 \rfloor}$, where Z_m is the *half Hilbert matrix* of size $m \times m$, namely the Hankel matrix

$$Z_m := \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{m} \\ \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{m} & 0 \\ \frac{1}{3} & \vdots & \iddots & 0 & 0 \\ \vdots & \frac{1}{m} & \iddots & \iddots & \vdots \\ \frac{1}{m} & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

This may be compared with the usual Hilbert matrix, whose (i, j) entry is $1/(i + j - 1)$. The spectral norm of any finite Hilbert matrix is at most π, so as the half Hilbert matrix is non-negative and entrywise less than the Hilbert matrix, its spectral norm is also at most π. (See the delightful article of Choi for this and other interesting facts about the Hilbert matrix [12].) This shows that the spectral norm of each matrix $\Gamma \circ D_i$ is at most 1, giving a bound on the zero-error quantum query complexity of ordered search of approximately $\frac{1}{\pi} \ln n$.

5.2 Optimal non-negative construction

It turns out that one can do slightly better than the Hilbert weight scheme described above. Here we construct the optimal solution to the adversary bound for OSP_n with non-negative weights.

A key role in our construction will be played by the sequence $\{\xi_i\}$, where

$$\xi_i := \frac{\binom{2i}{i}}{4^i}. \tag{1}$$

This sequence has many interesting properties. First, it is monotonically decreasing. Consider the ratio

$$\frac{\xi_{i+1}}{\xi_i} = \frac{\binom{2(i+1)}{i+1} 4^i}{\binom{2i}{i} 4^{i+1}} = \frac{2(i+1)(2i+1)}{4(i+1)^2} = \frac{i + 1/2}{i + 1} < 1.$$

Indeed, this shows that $\{\xi_i\}$ is a hypergeometric sequence with the generating function

$$g(z) := \sum_{i=0}^{\infty} \xi_i z^i = {}_1F_0(\tfrac{1}{2}; z) = \frac{1}{\sqrt{1-z}}.$$

These observations lead us to the next interesting property of our sequence.

Proposition 4. *For any j,*

$$\sum_{i=0}^{j} \xi_i \xi_{j-i} = 1.$$

Proof. The product $g(z)^2$ is the generating function for the convolution appearing on the left hand side. But $g(z)^2 = (1-z)^{-1}$, which has all coefficients equal to 1, as claimed. (For an alternative proof, using the fact that $\xi_i = (-1)^i \binom{-1/2}{i}$, see [15, p. 187].) □

This proposition shows that the sequence $\{\xi_i\}$ behaves nicely under convolution. We will also consider the behavior of $\{\xi_i\}$ under correlation. Define

$$A_m(j) := \sum_{i=0}^{m-j-1} \xi_i \xi_{i+j}.$$

As $\{\xi_i\}$ is a monotonically decreasing sequence, it follows that $A_m(j)$ is a monotonically decreasing function of j. With these definitions in hand, we are now ready to construct our adversary matrix.

Proof of Theorem 1 (lower bound on non-negative adversary). We first consider the case where $n = 2m$ is even. In (P), let

$$\gamma_i = A_m(i-1) - A_m(i).$$

As $A_m(j)$ is a monotonically decreasing function of j, we have $\gamma_i \geq 0$. Also note that $A_m(i) = 0$ for $i \geq m$, so $\text{Toeplitz}(\gamma_n, \dots, \gamma_1)$ is bipartite.

The objective function is a telescoping series, so the value of the semidefinite program is

$$2A_m(0) = 2\sum_{i=0}^{m-1} \xi_i^2,$$

as claimed. Thus it suffices to show that $\|\text{Toeplitz}(\gamma_n, \dots, \gamma_1)\| \leq 1$.

We will show that, in fact, $\|\text{Toeplitz}(\gamma_n, \dots, \gamma_1)\| = 1$. We do this by exhibiting an eigenvector u with eigenvalue 1, and with strictly positive entries. This will finish the proof by the following argument: As $\text{Toeplitz}(\gamma_n, \dots, \gamma_1)$ is a non-negative, symmetric matrix, its spectral norm is equal to its largest eigenvalue. By the Perron-Frobenius theorem, it has a principal eigenvector with non-negative entries. As the eigenvectors of a symmetric matrix corresponding to distinct eigenvalues are orthogonal, and no non-negative vector can be orthogonal to u, we conclude that the largest eigenvalue must agree with the eigenvalue of u, and so is 1.

The relevant eigenvector of $\text{Toeplitz}(\gamma_n, \dots, \gamma_1)$ is

$$u := (\xi_0, \xi_1, \dots, \xi_{m-1}, \xi_{m-1}, \dots, \xi_1, \xi_0). \tag{2}$$

Computing $\text{Toeplitz}(g_n, \dots, g_1)u$, we see that u is an eigenvector with eigenvalue 1 provided

$$\sum_{i=0}^{m-j-1} \big(A_m(i+j) - A_m(i+j+1)\big)\xi_i = \xi_j \tag{3}$$

for each $j = 0, 1, \ldots, m-1$.

We give two proofs of (3). In the first proof, we use generating functions. Define a complementary function to $g(z)$, namely the polynomial

$$h(z) := \xi_{m-1} + \xi_{m-2} z + \ldots + \xi_0 z^{m-1},$$

and consider the product $g(z)h(z)$. For $i = 0, \ldots, m-1$, the coefficient of z^i in this series is $A_m(m-i-1)$, so the coefficent of z^i in $(1-z)g(z)h(z)$ is $A_m(m-i-1) - A_m(m-i)$. Thus the coefficient of z^{m-j-1} in $(1-z)g(z)h(z)g(z) = h(z)$ is the left hand side of (3). But the coefficient of z^{m-j-1} in $h(z)$ is the coefficient of z^j in $g(z)$, which is simply ξ_j, the right hand side of (3).

Alternatively, we can explicitly expand the left hand side of (3), giving

$$\begin{aligned}\sum_{i=0}^{m-j-1} \big(A_m(i+j) - A_m(i+j+1)\big)\xi_i &= \sum_{i=0}^{m-j-1} \left(\sum_{k=0}^{m-(i+j)-1} \xi_k \xi_{k+i+j} \xi_i - \sum_{k=0}^{m-(i+j)-2} \xi_k \xi_{k+i+j+1} \xi_i \right) \\ &= \sum_{s=0}^{2m-j-1} \sum_{i=0}^{s} \xi_{s-i}\xi_i\xi_{s+j} - \sum_{s=0}^{2m-j-2} \sum_{i=0}^{s} \xi_{s-i}\xi_i\xi_{s+j+1} \\ &= \xi_j,\end{aligned}$$

where in the last step we have used Proposition 4. This completes the proof when n is even.

For $n = 2m+1$ odd, let

$$\gamma_i = \frac{1}{2}\big(A_{m+1}(i-1) - A_{m+1}(i) + A_m(i-1) - A_m(i)\big).$$

Then the objective function is

$$A_{m+1}(0) + A_m(0) = 2\sum_{i=0}^{m-1} \xi_i^2 + \xi_m^2$$

as claimed. Now it suffices to show that

$$u := (\xi_0, \xi_1, \ldots, \xi_{m-1}, \xi_m, \xi_{m-1}, \ldots, \xi_1, \xi_0) \tag{4}$$

is an eigenvector of $\mathrm{Toeplitz}(\gamma_n, \ldots, \gamma_1)$ with eigenvalue 1. (Note that for n odd, $\mathrm{Toeplitz}(\gamma_n, \ldots, \gamma_1)$ is irreducible, so u is actually the unique principal eigenvector.) For all but the middle component of the vector $\mathrm{Toeplitz}(\gamma_n, \ldots, \gamma_1)u$, the required condition is simply the average of (3) and the same equation with m replaced by $m+1$. For the middle component, we require $A_{m+1}(m)\xi_0 = \xi_m$, which holds because $A_{m+1}(m) = \xi_0\xi_m$ and $\xi_0 = 1$. □

In the bound of Høyer, Neerbeck, and Shi, the weight given to a pair (x, y) is inversely proportional to the Hamming distance between x and y. This follows the intuition that pairs which are easier for an adversary to distinguish should be given less weight. It is interesting to note that the optimal weight scheme does *not* have this property—indeed, at large Hamming distances the weights actually increase with increasing Hamming distance, as shown in Figure 1.

5.3 Dual

We now show that this bound is optimal by giving a matching solution to the dual semidefinite program (D).

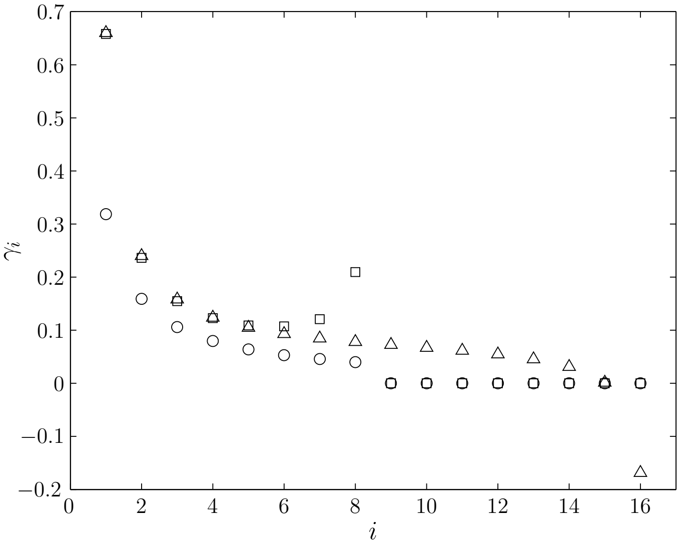

Figure 1. Comparison of the weights γ_i with $n = 16$ for various adversary bounds: the bound of Høyer, Neerbek, and Shi (circles), the optimal non-negative adversary (squares), and the optimal negative adversary (triangles).

Proof of Theorem 1 (upper bound on non-negative adversary). Fix n, and let u be the vector of length n defined by (2) if n is even, or by (4) if n is odd. Notice that in either case, $u_i = u_{n-i+1}$. Let $P = uu^T$, a rank one matrix. This matrix is positive semidefinite, and its trace is $\|u\|^2$, which matches the value of our solution to the primal problem in the previous section. Thus it suffices to verify that $\mathrm{Tr}_i(P) \geq 1$. We have

$$\mathrm{Tr}_i(P) = \sum_{j=1}^{n-i} P[j, i+j] = \sum_{j=1}^{n-i} u_j u_{i+j} = \sum_{j=1}^{n-i} u_j u_{n-i-j+1}.$$

Since $\{\xi_i\}$ is monotonically decreasing in i, we have $u_j \geq \xi_{j-1}$, with equality holding when $j \leq \lceil n/2 \rceil$. Thus

$$\mathrm{Tr}_i(P) \geq \sum_{j=1}^{n-i} \xi_{j-1}\xi_{n-i-j} = 1$$

by Proposition 4. When $i > \lfloor n/2 \rfloor$, this inequality holds with equality. □

Having established the optimal adversary bound for OSP_n, let us examine its asymptotic behavior.

Corollary 5.

$$\mathrm{ADV}(\mathrm{OSP}_n) = \frac{2}{\pi}(\ln n + \gamma + \ln 8) + O(1/n)$$

where $\gamma \approx 0.577$ is the Euler-Mascheroni constant.

Proof. The generating function for the sequence $\{\xi_i^2\}$ is ${}_2F_1(\frac{1}{2}, \frac{1}{2}; 1; z) = \frac{2}{\pi}K(z)$, where $K(z)$ is the complete elliptic integral of the first kind. Thus the generating function for $\{\mathrm{ADV}(\mathrm{OSP}_{2m})\}$, which is twice the mth partial sum of $\{\xi_i^2\}$, is $\frac{4}{\pi}K(z)/(1-z)$. The function $K(z)$ is analytic for $|z| < 1$, and can be analytically continued to the rest of the complex plane, with the only singularities consisting of branch points at $z = 1$ and $z = \infty$ [21, Sec. 5.9.1]. In particular, the logarithmic singularity at $z = 1$ has the expansion [10, Eq. 900.05]

$$K(z) = \ln \frac{4}{\sqrt{1-z}} + \frac{1}{4}(1-z)\left(\ln \frac{4}{\sqrt{1-z}} - 1\right) + O\left((1-z)^2 \ln \frac{1}{1-z}\right).$$

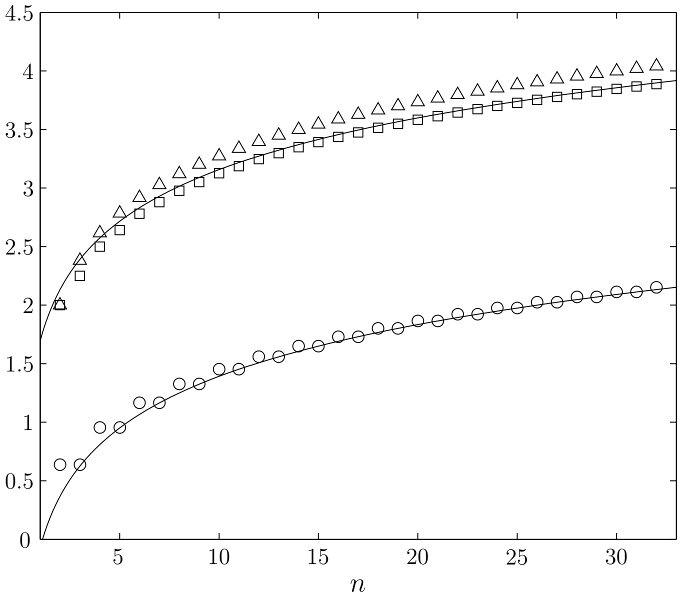

Figure 2. Comparison of adversary lower bounds for ordered search: the bound of Høyer, Neerbek, and Shi (circles), the optimal non-negative adversary (squares), and the optimal negative adversary (triangles). The lower curve shows the asymptotic approximation $\frac{2}{\pi}(\ln n + \gamma - \ln 2)$ of the Høyer-Neerbek-Shi bound, and the upper curve shows the asymptotic approximation $\frac{2}{\pi}(\ln n + \gamma + \ln 8)$ of the non-negative adversary.

Now let $[z^m]f(z)$ denote the coefficient of z^m in $f(z)$. According to Darboux's method (see for example [21, Sec. 8.9]), we have

$$\begin{aligned}
\mathrm{ADV}(\mathrm{OSP}_{2m}) &= [z^m]\frac{4}{\pi} \cdot \frac{K(z)}{1-z} \\
&= [z^m]\frac{4}{\pi}\left(\frac{1}{1-z} \cdot \frac{1}{2} \ln \frac{1}{1-z} + \frac{\ln 4}{1-z}\right) + O(1/m) \\
&= \frac{2}{\pi}(\ln m + \gamma + \ln 16) + O(1/m),
\end{aligned}$$

where we have used [19]

$$[z^m]\frac{1}{1-z} \ln \frac{1}{1-z} = \ln m + \gamma + O(1/m)$$

and the facts that $[z^m](1-z)^{-1} = 1$ and $[z^m] \ln \frac{1}{1-z} = 1/m$. This proves the corollary for $n = 2m$ even. For $n = 2m+1$ odd, we have $\mathrm{ADV}(\mathrm{OSP}_{2m+1}) = \mathrm{ADV}(\mathrm{OSP}_{2m}) + \xi_m^2$, and it suffices to observe that $\xi_m^2 = O(1/m)$ by Stirling's approximation. □

For comparison, the bound of Høyer, Neerbek, and Shi for OSP_n is $\frac{2}{\pi} H_{\lfloor n/2 \rfloor} = \frac{2}{\pi}(\ln n + \gamma - \ln 2) + O(1/n)$, where $H_n := \sum_{i=1}^{n} \frac{1}{i}$ is the nth harmonic number. (Note that for the original, unsymmetrized ordered search problem treated in [18], the bound is $\frac{2}{\pi}(H_n - 1)$.) Indeed, the optimal value of the non-negative adversary is considerably better for small values of n, as shown in Figure 2.

6 Negative adversary

We now turn to the negative adversary method, and give an upper bound on $\mathrm{ADV}^{\pm}(\mathrm{OSP}_n)$ by exhibiting a solution to ($\mathrm{D}^{\pm}$).

Notice that if we find a symmetric matrix R such that $\mathrm{Tr}_i(R) = 1$ for $i = 0, \dots, n-1$, we can translate this into a solution to (D$^\pm$) by decomposing $R = P - Q$ as the difference of two positive semidefinite matrices with disjoint support, letting P be the projection of R onto its positive eigenspace and letting Q be the projection of R onto its negative eigenspace. In this case, $\mathrm{Tr}(P+Q)$ is simply $\|R\|_{\mathrm{Tr}}$, the sum of the absolute values of the eigenvalues of R.

In looking for a matrix R satisfying $\mathrm{Tr}_i(R) = 1$ for all i, a natural starting point is our solution to the non-negative dual (D). Recall that in this construction, for $i > \lceil n/2 \rceil$, the condition $\mathrm{Tr}_i(P) = 1$ held with equality. We imitate that construction by letting

$$R[i,j] = \begin{cases} \xi_i \xi_{n-j+1} & i \leq j \\ \xi_{n-i+1}\xi_j & i > j. \end{cases}$$

Above the diagonal, R looks like a rank one matrix, but it is symmetrized below the diagonal. By the convolution property of the ξ_i's we see that $\mathrm{Tr}_i(R) = 1$ for $i = 0, \dots, n-1$.

To upper bound the trace norm of R, the following lemma will be helpful:

Lemma 6. *Let M be an $n \times n$ matrix with entries*

$$M[i,j] = \begin{cases} v_i w_j & i \leq j \\ v_j w_i & i > j \end{cases} \tag{5}$$

where the vectors $v, w \in \mathbb{R}^n$ have positive components, and satisfy $\frac{v_i}{v_{i+1}} > \frac{w_i}{w_{i+1}}$ for $i = 1, \dots, n-1$. Then M has one positive eigenvalue and $n-1$ negative eigenvalues, and its trace norm satisfies

$$2\|v\|\|w\| - v \cdot w \leq \|M\|_{\mathrm{Tr}} \leq 2\|v\|\|w\| + v \cdot w.$$

Proof. Sylvester's law of inertia states that the triple of the number of positive, zero, and negative eigenvalues of a matrix M and that of a matrix SMS^T are the same, provided S is non-singular. We apply this law with S given by the $n \times n$ upper tridiagonal matrix with entries

$$S[i,j] = \begin{cases} 1 & i = j \\ -v_i/v_j & i = j-1 \\ 0 & \text{otherwise.} \end{cases}$$

Then a straightforward calculation shows that SMS^T is diagonal, with entries

$$(SMS^T)[i,i] = \begin{cases} \frac{v_i}{v_{i+1}}(v_{i+1}w_i - v_i w_{i+1}) & i = 1, \dots, n-1 \\ v_n w_n & i = n. \end{cases}$$

By the assumptions of the lemma, the first $n-1$ diagonal entries are negative, and the last is positive; thus M has one positive eigenvalue and $n-1$ negative eigenvalues.

As M is a symmetric, non-negative matrix, its positive eigenvalue is equal to $\|M\|$, so $\|M\|_{\mathrm{Tr}} + \mathrm{Tr}(M) = 2\|M\|$. Notice that $\mathrm{Tr}(M) = v \cdot w$. Because M is non-negative and entrywise larger than the rank one matrix vw^T, we have $\|M\| \geq \|vw^T\| = \|v\|\|w\|$. Furthermore, because M is entrywise smaller than the rank two matrix $A = vw^T + wv^T$, we have $\|M\| \leq \|vw^T + wv^T\|$. Using the facts that $\mathrm{Tr}(A) = \lambda_1(A) + \lambda_2(A) = 2v \cdot w$ and that $\mathrm{Tr}(A^2) = \lambda_1(A)^2 + \lambda_2(A)^2 = 2(\|v\|^2\|w\|^2 + (v \cdot w)^2)$, we see that the eigenvalues of A are $v \cdot w \pm \|v\|\|w\|$. Thus we conclude that $\|M\| \leq \|v\|\|w\| + v \cdot w$, and the lemma follows. □

Now we are ready to finish the proof of Theorem 1.

Theorem 1 (upper bound on negative adversary). The matrix R defined above is of the form (5) with $v = (\xi_0, \xi_1, \ldots, \xi_{n-1})$ and $w = (\xi_{n-1}, \xi_{n-2}, \ldots, \xi_0)$, the reversal of v. By Proposition 4, $\mathrm{Tr}_i(R) = 1$ for $i = 0, \ldots, n-1$, so R is a solution of (D$^\pm$). Since v is monotonically increasing and w is monotonically decreasing, the conditions of Lemma 6 are satisfied, and thus $\|R\|_{\mathrm{Tr}} \leq 2\|v\|^2 + 1 = \mathrm{ADV}(\mathrm{OSP}_{2n}) + 1$.

Finally, using Corollary 5 we find

$$\mathrm{ADV}(\mathrm{OSP}_{2n}) - \mathrm{ADV}(\mathrm{OSP}_n) \leq \frac{2}{\pi} \ln 2 + O(1/n),$$

so

$$\mathrm{ADV}^{\pm}(\mathrm{OSP}_n) \leq \mathrm{ADV}(\mathrm{OSP}_n) + 1 + \frac{2}{\pi} \ln 2 + O(1/n). \qquad \square$$

Note that the solution of (D$^\pm$) given above is not the optimal one. For fixed n, we can find the optimal solution using a numerical semidefinite program solver. Figure 1 shows the optimal weights for $n = 16$, and Figure 2 shows the value of the optimal negative adversary bound for $n = 2$ through 32. Empirically, we have found that in the optimal solution, $P - Q$ is a rank two matrix in which P, Q are of the form

$$P = pp^T\ ,\ Q = qq^T \quad \text{with} \quad p_i = r_i \cos\theta_i\ ,\ q_i = r_i \sin\theta_i,$$

where

$$\theta_i = \frac{\pi}{2n-1}\left(\frac{n+1}{2} - i\right)$$

and

$$r_i^2 \approx \begin{cases} \frac{1}{n+1} \csc \frac{1}{(n+1)\xi_{i-1}^2} & i = 1, \ldots, \lceil n/2 \rceil \\ r_{n-i+1}^2 & i = \lceil n/2 \rceil + 1, \ldots, n. \end{cases}$$

However, we do not know the exact form of r or the optimal negative adversary value.

7 Conclusion

We have given upper bounds on the lower bounds provable by the quantum adversary method for the ordered search problem, showing that both the standard and negative adversary values are $\frac{2}{\pi} \ln n + O(1)$. In particular, we have shown that establishing the quantum query complexity of ordered search will either require a lower bound proved by a different technique, or an improved upper bound. On the lower bound side, one could investigate the bounds given by the recently developed multiplicative adversary technique of Špalek [22]. However, we feel that it is more likely that the $\frac{1}{\pi} \ln n$ lower bound is in fact tight, and that further improvement will come from algorithms. As the current best upper bounds are ad hoc, based on numerical searches, they can almost certainly be improved.

The disagreeable reader may argue that upper bounds on lower bounds are only meta-interesting. We counter this objection as follows. Barnum, Saks, and Szegedy have exactly characterized quantum query complexity in terms of a semidefinite program [4]. The adversary method can be viewed as a relaxation of this program, removing some constraints and focusing only on the output condition. Thus, our results can be viewed as solving a simplification of the quantum query complexity semidefinite program, which might provide insight into the solution of the full program. Indeed, we hope that the results presented here will be a useful step toward determining the quantum query complexity of ordered search.

Acknowledgments

We thank Peter Høyer for stimulating discussions, and in particular, for suggesting the second proof of Equation (3) presented above. This work was done in part while AMC was at the Institute for Quantum Information at the California Institute of Technology, where he received support from NSF Grant PHY-0456720 and ARO Grant W911NF-05-1-0294. TL is supported by a Rubicon grant from the Netherlands Organisation for Scientific Research (NWO) and by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

References

[1] A. Ambainis, *A better lower bound for quantum algorithms searching an ordered list*, Proc. 40th IEEE Sympopsium on Foundations of Computer Science, 1999, pp. 352-357, available at quant-ph/9902053.

[2] ———, *Quantum lower bounds by quantum arguments*, Journal of Computer and System Sciences **64** (2002), no. 4, 750–767, available at quant-ph/0002066. Preliminary version in STOC 2000.

[3] ———, *Polynomial degree vs. quantum query complexity*, Journal of Computer and System Sciences **72** (2006), no. 2, 220–238, available at quant-ph/0305028. Preliminary version in FOCS 2003.

[4] H. Barnum, M. Saks, and M. Szegedy, *Quantum query complexity and semidefinite programming*, Proc. 18th IEEE Conference on Computational Complexity, 2003, pp. 179–193.

[5] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, *Quantum lower bounds by polynomials*, Journal of the ACM **48** (2001), no. 4, 778–797, available at quant-ph/9802049. Preliminary version in FOCS 1998.

[6] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *Strengths and weaknesses of quantum computing*, SIAM Journal on Computing **26** (1997), 1510–1523, available at quant-ph/9701001.

[7] M. Ben-Or and A. Hassidim, *Quantum search in an ordered list via adaptive learning*, quant-ph/0703231.

[8] E. M. Brookes, M. B. Jacokes, and A. J. Landahl, *An improved quantum algorithm for searching an ordered list*, 2004.

[9] H. Buhrman and R. de Wolf, *A lower bound for quantum search of an ordered list*, Information Processing Letters **70** (1999), no. 5, 205-209.

[10] P. F. Byrd and M. D. Friedman, *Handbook of Elliptic Integrals for Engineers and Physicists*, Springer-Verlag, 1954.

[11] A. M. Childs, A. J. Landahl, and P. A. Parrilo, *Improved quantum algorithms for the ordered search problem via semidefinite programming*, Physical Review A **75** (2007), no. 3, 032335, available at quant-ph/0608161.

[12] M.-D. Choi, *Tricks or treats with the Hilbert matrix*, American Mathematical Monthly **90** (1983), no. 5, 301–312.

[13] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, *A limit on the speed of quantum computation for insertion into an ordered list*, quant-ph/9812057.

[14] ———, *Invariant quantum algorithms for insertion into an ordered list*, quant-ph/9901059.

[15] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.

[16] L. K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Physical Review Letters **79** (1997), 325–328, available at quant-ph/9706033. Preliminary version in STOC 1996.

[17] P. Høyer, T. Lee, and R. Špalek, *Negative weights make adversaries stronger*, to appear in Proc. 39th ACM Symposium on Theory of Computing, 2007, available at quant-ph/0611054.

[18] P. Høyer, J. Neerbek, and Y. Shi, *Quantum complexities of ordered searching, sorting, and element distinctness*, Algorithmica **34** (2002), no. 4, 429–448, available at quant-ph/0102078. Preliminary version in ICALP 2001.

[19] R. Jungen, *Sur les séries de Taylor n'ayant que des singularités algébrico-logarithmiques sur leur cercle de convergence*, Commentarii Mathematici Helvetici **3** (1931), no. 1, 266–306.

[20] S. Laplante and F. Magniez, *Lower bounds for randomized and quantum query complexity using Kolmogorov arguments*, Proc. 19th IEEE Conference on Computational Complexity, 2004, pp. 294–304, available at quant-ph/0311189.

[21] F. W. J. Olver, *Asymptotics and Special Functions*, Academic Press, 1974.

[22] R. Špalek, *The multiplicative quantum adversary*, quant-ph/0703237.

[23] R. Špalek and M. Szegedy, *All quantum adversary methods are equivalent*, Theory of Computing **2** (2006), no. 1, 1–18, available at quant-ph/0409116. Preliminary version in ICALP 2005.

[24] S. Zhang, *On the power of Ambainis's lower bounds*, Theoretical Computer Science **339** (2005), no. 2–3, 241–256, available at quant-ph/0311060. Preliminary version in ICALP 2004.