THEORY OF COMPUTING, Volume 6 (2010), pp. 1–25
www.theoryofcomputing.org

A new quantum lower bound method, with an application to a strong direct product theorem for quantum search

Andris Ambainis*

Received: July 6, 2007; revised: July 24, 2009; published: January 12, 2010.

Abstract: We present a new method for proving lower bounds on quantum query algorithms. The new method is an extension of the adversary method, by analyzing the eigenspace structure of the problem.

Using the new method, we prove a strong direct product theorem for quantum search. This result was previously proved by Klauck, Špalek, and de Wolf (FOCS'04) using the polynomials method. No proof using the adversary method was known before.

ACM Classification: F1.2, F2.2

AMS Classification: 81P68, 68Q17

Key words and phrases: quantum computing, quantum algorithms, quantum lower bounds

1 Introduction

Many quantum algorithms (for example, Grover's algorithm [13] and quantum counting [11]) can be analyzed in the query model where the input is accessed via a black box that answers queries about the values of input bits.

There are two main methods for proving lower bounds on quantum query algorithms: the adversary method [3] and the polynomials method [9]. Both of them have been studied in detail. The limits of the adversary method are particularly well understood. The original adversary method [3] has been

*Supported by University of Latvia grant ZP01-100, a Marie Curie International Reintegration Grant (IRG), and ESF project 1DP/1.1.1.2.0/09/APIA/VIAA/044. Most of this work was done at the University of Waterloo and supported by NSERC, CIFAR, ARO, MITACS, and an IQC University Professorship.

DOI: 10.4086/toc.2010.v006a001

generalized in several different ways [4, 18, 8]. Špalek and Szegedy [23] then showed that all the generalizations are equivalent and, for certain problems, cannot improve the best known lower bounds. For example, it was shown in [23, 24] that the adversary methods of [4, 18, 8] cannot prove a lower bound for a total Boolean function that exceeds $O(\sqrt{C_0(f)C_1(f)})$, where $C_0(f)$ and $C_1(f)$ are the certificate complexities of f on 0-inputs and 1-inputs, resp. This implies that the adversary methods of [4, 18, 8] cannot prove a tight lower bound for element distinctness or improve the best known lower bound for triangle finding. (The complexity of element distinctness is $\Theta(N^{2/3})$ [2, 5] but the adversary method cannot prove a bound better than $\Omega(\sqrt{N})$. For triangle finding [19], the best known lower bound is $\Omega(N)$ and it is known that it cannot be improved using the adversary method. It is, however, possible that the bound is not tight, because the best algorithm uses $O(N^{1.3})$ queries.)

In this paper we describe a new version of the quantum adversary method which may not be subject to those limitations. We then use the new method to prove a strong direct product theorem for the K-fold search problem.

In the K-fold search problem, a black box contains $x_1, \ldots, x_N$ such that $|\{i : x_i = 1\}| = K$ and we have to find all the K values of i such that $x_i = 1$. This problem can be solved with $O(\sqrt{NK})$ queries. It can be easily shown, using any of the previously known methods, that $\Omega(\sqrt{NK})$ quantum queries are required. A more difficult problem is to show that $\Omega(\sqrt{NK})$ queries are required, even if the algorithm only has to be correct with an exponentially small probability c^{-K}, $c > 1$. This result is known as the *strong direct product theorem* for k-fold search. Besides being interesting on its own, the strong direct product theorem is useful for proving time-space tradeoffs for quantum sorting [16] and lower bounds on quantum computations that use advice [1].

The strong direct product theorem for quantum search was first shown by Klauck, Špalek, and de Wolf [16], using the polynomials method. No proof using the adversary method has been known and, as we show in Section 3, the previously known adversary methods are insufficient to prove a strong direct product theorem for K-fold search.

Recent developments After the author completed the research presented in this paper, several developments occurred.

1. Together with Špalek and de Wolf [7], we have used the methods from this paper to prove a direct product theorem for t-threshold functions. This implies time-space tradeoffs for the problem of deciding systems of linear inequalities.

   This paper and [7] were merged for publication at STOC'06 [6]. We have decided to publish the journal versions separately.

   The relation between the two papers is as follows. A direct product theorem for k-threshold functions implies a direct product theorem for search. Thus, the result of [7] implies the result in this paper. The proof of our result is, however, substantially simpler than the proof of the more general result in [7]. Because of that, we think that our proof continues to be of interest even though the result in this paper has been generalized by [7].

2. Špalek [22] generalized the results of the current paper and [7], obtaining a *multiplicative adversary method*. This is a general framework for proving lower bounds which includes the results of the current paper and [7] as particular cases.

3. Høyer, Lee, and Špalek [14] generalized the usual adversary method in a different way, by extending the usual weighted adversary method of [4] to negative weights. Reichardt [21] has shown that this method is optimal: if $\mathrm{Adv}^{\pm}(f)$ is the best adversary lower bound that can be proven for a function f, then f can be evaluated using

$$O\left(\mathrm{Adv}^{\pm}(f)\frac{\log \mathrm{Adv}^{\pm}(f)}{\log\log \mathrm{Adv}^{\pm}(f)}\right)$$

queries. Although the negative weight adversary method is guaranteed to provide nearly optimal results, the other lower bound methods also remain interesting because particular lower bounds may follow more easily using different tools.

2 Preliminaries

We consider the following problem.

Search for K marked elements, $\mathrm{SEARCH}_K(N)$: Given a black box containing $x_1,\ldots,x_N \in \{0,1\}$ such that $x_i = 1$ for exactly K values $i \in \{1,2,\ldots,N\}$, find all K values $i_1,\ldots,i_K$ satisfying $x_{i_j} = 1$.

This problem can be viewed as computing an $\binom{N}{K}$-valued function $f(x_1,\ldots,x_N)$ in the variables $x_1,\ldots,x_N \in \{0,1\}$, with values of the function being indices for the $\binom{N}{K}$ sets $S \subseteq [N]$ of size K, in some canonical ordering of those sets.

We study this problem in the quantum query model. (For a survey on the quantum query model, see [12]). In this model, the input bits can be accessed by queries to an oracle X and the complexity of f is the number of quantum queries needed to compute f. A quantum computation with T queries is just a sequence of unitary transformations

$$U_0 \to O \to U_1 \to O \to \cdots \to U_{T-1} \to O \to U_T\,.$$

The U_j can be arbitrary unitary transformations that do not depend on the input bits $x_1,\ldots,x_N$. The transformations O are query (oracle) transformations which depend on $x_1,\ldots,x_N$. To define O, we represent basis states as $|i,z\rangle$ where i consists of $\lceil \log(N+1)\rceil$ bits and z consists of all other bits. Then, O_x maps $|0,z\rangle$ to itself and $|i,z\rangle$ to $(-1)^{x_i}|i,z\rangle$ for $i \in \{1,...,N\}$ (i. e., we change phase depending on x_i, unless $i = 0$ in which case we do nothing).

The computation starts with a state $|0\rangle$. Then we apply $U_0, O_x, \ldots, O_x, U_T$ and measure the final state. The result of the computation is the string of $\lceil \log_2 \binom{N}{K}\rceil$ rightmost bits of the state obtained by the measurement, which is interpreted as a description of one of the $\binom{N}{K}$ subsets $S \subseteq \{1,\ldots,N\}$, $|S| = K$.

3 Overview of the adversary method

We describe the adversary method of [3].

Let X be a subset of the set of possible inputs $\{0,1\}^N$. We run the algorithm on a superposition of inputs in X. More formally, let $\mathcal{H}_A$ be the workspace of the algorithm. We consider a bipartite system

$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_I$ where $\mathcal{H}_I$ is an "input subspace" spanned by basis vectors $|x\rangle$ corresponding to inputs $x \in X$.

Let $U_T\, O\, U_{T-1} \cdots U_0$ be the sequence of unitary transformations on $\mathcal{H}_A$ performed by the algorithm A, where $U_0, \ldots, U_T$ denote the transformations that do not depend on the input and O stands for the query transformations. We transform this sequence into a sequence of unitary transformations on $\mathcal{H}$. A unitary transformation U_i on $\mathcal{H}_A$ corresponds to the transformation $U_i' = U_i \otimes I$ on the whole $\mathcal{H}$. The query transformation O corresponds to a transformation O' that is equal to O_x on the subspace $H_A \otimes |x\rangle$.

We perform the sequence of transformations $U_T'\, O'\, U_{T-1}' \cdots U_0'$ on the starting state

$$|\psi_{\text{start}}\rangle = |0\rangle \otimes \sum_{x \in S} \alpha_x |x\rangle \,.$$

Then, the final state is

$$|\psi_{\text{end}}\rangle = \sum_{x \in X} \alpha_x |\psi_x\rangle \otimes |x\rangle \,,$$

where $|\psi_x\rangle$ is the final state of $A = U_T\, O\, U_{T-1} \ldots U_0$ on input x. This follows from the fact that the restrictions of $U_T', O', U_{T-1}', \ldots, U_0'$ to $\mathcal{H}_A \otimes |x\rangle$ are $U_T, O_x, U_{T-1}, \ldots, U_0$ and these are exactly the transformations of the algorithm A on input x.

Let ρ_{end} be the reduced density matrix of the $\mathcal{H}_I$ register of the state $|\psi_{\text{end}}\rangle$. The adversary method of [3, 4] works by showing the following two statements.

- Let $x \in X$ and $y \in X$ be such that $f(x) \neq f(y)$ (where f is the function that is being computed). If the algorithm outputs the correct answer with probability $1 - \varepsilon$ on both x and y then

$$|(\rho_{\text{end}})_{x,y}| \leq 2\sqrt{\varepsilon(1-\varepsilon)}|\alpha_x||\alpha_y| \,.$$

- For any algorithm that uses T queries, there exist inputs $x, y \in S$ such that $f(x) \neq f(y)$ and

$$(\rho_{\text{end}})_{x,y} > 2\sqrt{\varepsilon(1-\varepsilon)}|\alpha_x||\alpha_y| \,.$$

These two statements together imply that any algorithm computing f must use more than T queries.

An equivalent approach [15, 4] is to consider the inner products $\langle\psi_x|\psi_y\rangle$ between the final states $|\psi_x\rangle$ and $|\psi_y\rangle$ of the algorithm on inputs x and y. Then, $|(\rho_{\text{end}})_{x,y}| \leq 2\sqrt{\varepsilon(1-\varepsilon)}|\alpha_x||\alpha_y|$ is equivalent to $|\langle\psi_x|\psi_y\rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)}$.

As a result, both of the above statements can be described in terms of inner products $\langle\psi_x|\psi_y\rangle$, without explicitly introducing the register $\mathcal{H}_I$. The first statement says that, for the algorithm to succeed on inputs x, y such that $f(x) \neq f(y)$, the states $|\psi_x\rangle$ and $|\psi_y\rangle$ must be sufficiently far apart from one another (so that the inner product $|\langle\psi_x|\psi_y\rangle|$ is at most $2\sqrt{\varepsilon(1-\varepsilon)}$). The second statement says that this is impossible if the algorithm only uses T queries.

This approach breaks down if we consider computing a function f with success probability $p < 1/2$. (f has to have more than 2 values for this task to be nontrivial.) Then, $|\psi_x\rangle$ and $|\psi_y\rangle$ could be the same and the algorithm may still succeed on both inputs, if it outputs x with probability 1/2 and y with probability 1/2. In the case of strong direct product theorems, the situation is even more difficult. Since the algorithm only has to be correct with probability c^{-K}, the algorithm could have almost the same final state on c^K different inputs and still "succeed" on every one of them.

In this paper, we present a new method that does not suffer from this problem. Our method, described in the next section, uses the idea of augmenting the algorithm with an input register $\mathcal{H}_I$, together with two new ingredients:

1. **Symmetrization.** We symmetrize the algorithm by applying a random permutation $\pi \in S_N$ to the input $x_1, \ldots, x_N$.

2. **Eigenspace analysis.** We study the eigenspaces of ρ_{start}, ρ_{end} and density matrices describing the state of $\mathcal{H}_I$ at intermediate steps and use them to bound the progress of the algorithm.

The eigenspace analysis is the main new technique. Symmetrization is necessary to simplify the structure of the eigenspaces, to make the eigenspace analysis possible.

4 Our result

Theorem 4.1. *There exist ε and c satisfying $\varepsilon > 0$, $0 < c < 1$ such that, for any $K \leq N/2$, solving SEARCH$_K(N)$ with probability at least c^K requires $(\varepsilon - o(1))\sqrt{NK}$ queries.*

4.1 General framework

We first give a high-level overview of the new method, in a form that may be applicable to a variety of problems. After that, in Section 4.2, we will describe how to adapt this general method to the K-fold search problem.

As before, let $X \subseteq \{0,1\}^N$ be a subset of the set of inputs for the function $f(x_1, \ldots, x_N)$. Let G be the group of all permutations π on $\{1, \ldots, N\}$ that fix X:

$$\{(x_{\pi(1)}, \ldots, x_{\pi(N)}) : (x_1, \ldots, x_N) \in X\} = X\,.$$

Additionally we assume for all $\pi \in G$ that $f(x_{\pi(1)}, \ldots, x_{\pi(N)})$ and π uniquely determine $f(x_1, \ldots, x_N)$.

We choose X so that X consists of "hard" inputs (inputs on which f is difficult to evaluate with few queries) and the symmetry group G is as large as possible. For example, in the case of K-fold search, X is the set of all $x \in \{0,1\}^N$, $|x| = K$ and G consists of all permutations on $\{1, \ldots, N\}$.

Let $\mathcal{A}$ be an algorithm for $f(x_1, \ldots, x_N)$ and let $\mathcal{H}_A$ be the workspace on which $\mathcal{A}$ operates.

We first "symmetrize" $\mathcal{A}$ by adding an extra register $\mathcal{H}_S$ holding a permutation $\pi \in G$. Initially, $\mathcal{H}_S$ holds a uniform superposition of all permutations π:

$$\frac{1}{\sqrt{|G|}} \sum_{\pi \in G} |\pi\rangle\,.$$

Before each query O, we insert a transformation $|i\rangle|\pi\rangle \mapsto |\pi^{-1}(i)\rangle|\pi\rangle$ on the part of the state containing the index i to be queried and $\mathcal{H}_S$. After the query, we insert a transformation $|i\rangle|\pi\rangle \mapsto |\pi(i)\rangle|\pi\rangle$. The effect of the symmetrization is that, on the subspace $|s\rangle \otimes |\pi\rangle$, the algorithm is effectively running on the input $x_{\pi(1)}, \ldots, x_{\pi(N)}$. At the end of algorithm, we apply a unitary transformation that replaces the answer for $f(x_{\pi(1)}, \ldots, x_{\pi(N)})$ with the corresponding answer for $f(x_1, \ldots, x_N)$. (This is possible because of our requirement that $f(x_{\pi(1)}, \ldots, x_{\pi(N)})$ and π uniquely determine $f(x_1, \ldots, x_N)$.)

If the original algorithm $\mathcal{A}$ succeeds on every input $(x_1,\dots,x_N)$ with probability at least ε, the symmetrized algorithm also succeeds with probability at least ε, since its success probability is just the average of the success probabilities of $\mathcal{A}$ over all $(x_{\pi(1)},\dots,x_{\pi(N)})$, $\pi \in G$. Next, we recast $\mathcal{A}$ into a different form, using a register that stores the input $x_1,\dots,x_N$, as in Section 3.

Let $\mathcal{H}_I$ be an $|X|$-dimensional Hilbert space whose basis states correspond to inputs $(x_1,\dots,x_N) \in X$. We transform the symmetrized version of $\mathcal{A}$ into a sequence of transformations on a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_S \otimes \mathcal{H}_I$. As before, a non-query transformation U on $\mathcal{H}_A \otimes \mathcal{H}_S$ is replaced by $U \otimes I$ on $\mathcal{H}$. A query is replaced by a transformation O that is equal to $O_{x_1,\dots,x_N} \otimes I$ on the subspace consisting of states of the form $|s\rangle_{A,S} \otimes |x_1 \dots x_N\rangle_I$. The starting state of the algorithm on Hilbert space $\mathcal{H}$ is $|\varphi_0\rangle = |\psi_{\text{start}}\rangle_{A,S} \otimes |\psi_0\rangle_I$ where $|\psi_{\text{start}}\rangle_{A,S}$ is the starting state of $\mathcal{A}$ as an algorithm acting on $\mathcal{H}_A \otimes \mathcal{H}_S$ and $|\psi_0\rangle_I$ is some fixed superposition of states $|x_1 \dots x_N\rangle$, $(x_1,\dots,x_N) \in X$.

Let $|\psi_t\rangle$ be the state of the algorithm $\mathcal{A}$, as a sequence of transformations on $\mathcal{H}$, after the t^{th} query. Let ρ_t be the mixed state obtained from $|\psi_t\rangle$ by tracing out the $\mathcal{H}_A \otimes \mathcal{H}_S$ register and let $\lambda_1,\lambda_2,\dots$ be all the distinct eigenvalues of ρ_t. Let S_i be the subspace of $\mathcal{H}_I$ consisting of all eigenvectors with the eigenvalue λ_i and let P_i be the projector to the subspace S_i. Then,

$$\rho_t = \sum_i \lambda_i P_i \,.$$

For a permutation $\pi \in G$, let U_π be the unitary transformation on the register $\mathcal{H}_I$ defined by

$$U_\pi |x_1 \dots x_N\rangle = |x_{\pi(1)} \dots x_{\pi(N)}\rangle \,.$$

Then, because of the symmetrization step, ρ_t is invariant under U_π: $\rho_t = U_\pi \rho_t U_\pi^{-1}$. This means that every eigenspace S_i is fixed by U_π, for every $\pi \in G$.

Let $\mathcal{V}$ be the collection of all invariant subspaces $S \le \mathcal{H}_A$ (subspaces S that are fixed by all $\pi \in G$). Then, we can always express ρ_t as

$$\rho_t = \sum_{S \in \mathcal{V}} \lambda_S P_S$$

where P_S is a projector to the subspace S. This means that the state of the algorithm can be fully described by the vector $(\lambda_S)_{S \in \mathcal{V}}$. (For some symmetry groups G, there could be infinitely many invariant subspaces. Then $\mathcal{V}$ will be infinite but only finitely many of the λ_S will be nonzero.)

We divide $\mathcal{V}$ into a set $\mathcal{V}_{\text{good}}$ of "good" subspaces and a set $\mathcal{V}_{\text{bad}}$ of "bad" subspaces so that, if the algorithm $\mathcal{A}$ succeeds, a non-negligible part of the final state ρ_T must consist of P_S, $S \in \mathcal{V}_{\text{good}}$.

To prove a lower bound on the number of queries, we show that the initial state of $\mathcal{H}_I$ is in $\mathcal{V}_{\text{bad}}$ and then prove that T_0 queries are not enough to move a non-negligible part of the state to $S \in \mathcal{V}_{\text{good}}$. That is done by bounding the change in $(\lambda_S)_{S \in \mathcal{V}}$ in one query, as follows. Let ρ_t be the state of $\mathcal{H}_I$ before the $(t+1)^{\text{st}}$ query. We decompose

$$\rho_t = \sum_{i=0}^{N} \rho_{t,i} \,,$$

with $\rho_{t,i}$ being the part of the state in which the query register of $\mathcal{A}$ contains i. Let $G^{(i)}$ consist of all $\pi \in S$ with $\pi(i) = i$. Then $\rho_{t,i}$ is fixed by U_π for all $\pi \in G^{(i)}$. Let $\mathcal{V}^{(i)}$ consist of all subspaces S that are fixed by all $U_\pi, \pi \in G^{(i)}$. Then

$$\rho_{t,i} = \sum_{S \in \mathcal{V}^{(i)}} \lambda_S P_S \,.$$

We use this decomposition to describe the effect of a query on $\rho_{t,i}$. Then we relate subspaces $S \in \mathcal{V}^{(i)}$ to subspaces $S \in \mathcal{V}$. This allows us to bound the change in $(\lambda_S)_{S\in\mathcal{V}}$.

Specialization to k-fold search In the case of k-fold search (described in the next section), there are just $K+1$ invariant subspaces $S_0, \ldots, S_K$ with S_i intuitively corresponding to the algorithm knowing locations of i out of K items j with $x_j = 1$. The state of the algorithm can then be described by a vector $(\lambda_0, \ldots, \lambda_K)$ of length $K+1$, where λ_i describes the probability that the algorithm knows locations of i out of the K items.

The bad subspaces that make up $\mathcal{V}_{\text{bad}}$ are $S_0, \ldots, S_{K/2}$ which correspond to A knowing at most $K/2$ of the K locations j with $x_j = 1$. The good subspaces that make up $\mathcal{V}_{\text{good}}$ are $S_{K/2+1}, \ldots, S_K$ which correspond to A knowing more than $K/2$ of the K locations j with $x_j = 1$.

4.2 K-fold search

We now prove Theorem 4.1. Let $\mathcal{A}$ be an algorithm for $\text{SEARCH}_K(N)$ that uses $T \le \varepsilon\sqrt{NK}$ queries.

As described in the previous subsection, we first "symmetrize" $\mathcal{A}$ by adding an extra register $\mathcal{H}_S$ holding a permutation $\pi \in S_N$. Initially, $\mathcal{H}_S$ holds a uniform superposition of all permutations π:

$$\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |\pi\rangle .$$

The result of this step is that, on the subspace consisting of all states $|s\rangle \otimes |\pi\rangle$, the algorithm runs on the input $x_{\pi(1)}, \ldots, x_{\pi(N)}$. At the end of the algorithm, we apply the transformation

$$|i_1\rangle \ldots |i_K\rangle |\pi\rangle \mapsto |\pi^{-1}(i_1)\rangle \ldots |\pi^{-1}(i_K\rangle |\pi\rangle$$

on the part of $\mathcal{H}_A$ that holds the output of the algorithm and $\mathcal{H}_S$. This converts the answer for the input $x_{\pi(1)}, \ldots, x_{\pi(N)}$ into the answer for the actual input $x_1, \ldots, x_N$.

We then add an input register $\mathcal{H}_I$ which initially, holds the starting state

$$|\psi_0\rangle = \frac{1}{\sqrt{\binom{N}{K}}} \sum_{\substack{x_1,\ldots,x_N: \\ x_1+\cdots+x_N=K}} |x_1 \ldots x_N\rangle .$$

Let $|\psi_t\rangle$ be the state of the algorithm $\mathcal{A}$, as a sequence of transformations on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_S \otimes \mathcal{H}_I$, after the t^{th} query. Then,

$$|\psi_t\rangle = \frac{1}{\sqrt{\binom{N}{K} N!}} \sum_{\substack{x_1,\ldots,x_N: \\ x_1+\cdots+x_N=K}} \sum_{\pi \in S_N} |\psi_t^{x_{\pi(1)},\ldots,x_{\pi(N)}}\rangle_A |\pi\rangle_S |x_1, \ldots, x_N\rangle_I$$

where $|\psi_t^{x_{\pi(1)},\ldots,x_{\pi(N)}}\rangle$ denotes the state of $\mathcal{H}_A$ after t steps, on the input $x_{\pi(1)}, \ldots, x_{\pi(N)}$.

Let ρ_t be the mixed state obtained from $|\psi_t\rangle$ by tracing out the $\mathcal{H}_A$ register. We claim that the states ρ_t have a special form, due to our symmetrization step.

Lemma 4.2. *The entries $(\rho_t)_{x,y}$ are the same for all $x = (x_1, \ldots, x_N)$, $y = (y_1, \ldots, y_N)$ with the same cardinality of the set $\{\ell : x_\ell = y_\ell = 1\}$.*

Proof. Since ρ_t is independent of the way how the $\mathcal{H}_A \otimes \mathcal{H}_S$ is traced out, we first measure $\mathcal{H}_S$ (in the $|\pi\rangle$ basis) and then measure $\mathcal{H}_A$ (arbitrarily). When measuring $\mathcal{H}_S$, every π is obtained with an equal probability. Let $\rho_{t,\pi}$ be the reduced density matrix of $\mathcal{H}_I$, conditioned on the measurement of $\mathcal{H}_S$ giving π. Then

$$\rho_t = \sum_{\pi} \frac{1}{N!} \rho_{t,\pi} \,.$$

The entry $(\rho_{t,\pi})_{x,y}$ is the same as the entry $(\rho_{t,\mathrm{id}})_{\pi^{-1}(x),\pi^{-1}(y)}$ because the symmetrization by π maps $\pi^{-1}(x), \pi^{-1}(y)$ to x, y. Let x, y, x', y' be such that $|\{i : x_i = y_i = 1\}| = |\{i : x'_i = y'_i = 1\}|$. Then there is a permutation $\tau \in S_N$ such that $\tau(x) = x'$, $\tau(y) = y'$. Therefore,

$$\begin{aligned}
(\rho_t)_{x,y} &= \frac{1}{N!} \sum_{\pi \in S_N} (\rho_{t,\pi})_{x,y} = \frac{1}{N!} \sum_{\pi \in S_N} (\rho_{t,\mathrm{id}})_{\pi^{-1}(x),\pi^{-1}(y)} \\
&= \frac{1}{N!} \sum_{\pi \in S_N} (\rho_{t,\mathrm{id}})_{\pi^{-1}\tau(x),\pi^{-1}\tau(y)} = (\rho_t)_{\tau(x),\tau(y)} = (\rho_t)_{x',y'} \,.
\end{aligned}$$

This means that $(\rho_t)_{x,y}$ only depends on $|\{\ell : x_\ell = y_\ell = 1\}|$. □

Any $\binom{N}{K} \times \binom{N}{K}$ matrix with this property shares the same eigenspaces. Namely, we have

Lemma 4.3 (Knuth [17]). *Let A be an $\binom{N}{K} \times \binom{N}{K}$ matrix whose rows and columns are indexed by 0-1 sequences $x_1, \ldots, x_N$ with $x_1 + \cdots + x_N = K$. Assume that A is such that $A_{x,y}$ only depends on the number of bits $\{i : x_i = y_i = 1\}$. Then, the eigenspaces of A are $S_0, S_1, \ldots, S_K$ where $T_0 = S_0$ consists of multiples of $|\psi_0\rangle$ and, for $j > 0$, $S_j = T_j \cap (T_{j-1})^\perp$, with T_j being the space spanned by all states*

$$|\psi_{i_1,\ldots,i_j}\rangle = \frac{1}{\sqrt{\binom{N}{K-j}}} \sum_{\substack{x_1,\ldots,x_N: \\ x_1+\cdots+x_N=K, \\ x_{i_1}=\cdots=x_{i_j}=1}} |x_1, \ldots, x_N\rangle \,.$$

Let τ_j be the completely mixed state over the subspace S_j.

Lemma 4.4. *There exist $p_{t,0} \geq 0, \ldots, p_{t,K} \geq 0$ such that $\rho_t = \sum_{j=0}^{K} p_{t,j} \tau_j$.*

Proof. By Lemma 4.3, $S_0, \ldots, S_K$ are the eigenspaces of ρ_t. Therefore, ρ_t is a linear combination of the projectors to $S_0, \ldots, S_K$. Since τ_j is a multiple of the projector to S_j, we have

$$\rho_t = \sum_{j=0}^{K} p_{t,j} \tau_j \,.$$

Since ρ_t is a density matrix, it must be positive semidefinite. This means that $p_{t,0} \geq 0, \ldots, p_{t,K} \geq 0$. □

Informally, we can interpret $p_{t,j}$ as the probability that, after t queries, the algorithm $\mathcal{H}_A$ knows the locations for t out of the K items j with $x_j = 1$. Let $q_{t,j} = p_{t,j} + p_{t,j+1} + \cdots + p_{t,K}$. The theorem now follows from the following lemmas.

Lemma 4.5. *$p_{0,0} = 1$, $p_{0,j} = 0$ for $j > 0$.*

Proof. In the starting state, $\mathcal{H}_I$ contains the state $|\varphi_0\rangle$, independent of $\mathcal{H}_A$ and $\mathcal{H}_P$. Therefore, tracing out $\mathcal{H}_A \otimes \mathcal{H}_P$ leaves the state $\rho_0 = |\psi_0\rangle\langle\psi_0|$. □

Lemma 4.6. *For all $j \in \{1,\dots,K\}$ and all t we have $q_{t+1,j+1} \le q_{t,j+1} + \frac{4\sqrt{K}}{\sqrt{N}} q_{t,j}$.*

Proof. In Section 5. □

Lemma 4.7. $q_{t,j} \le \binom{t}{j}\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^j$.

Proof. By induction on t. The base case, $t=0$ follows immediately from $p_{0,0}=1$ and

$$p_{0,1} = \cdots = p_{0,K} = 0\,.$$

For the induction step, we have

$$\begin{aligned} q_{t+1,j} \le q_{t,j} + \frac{4\sqrt{K}}{\sqrt{N}} q_{t,j-1} &\le \binom{t}{j}\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^j + \frac{4\sqrt{K}}{\sqrt{N}}\binom{t}{j-1}\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^{j-1} \\ &= \left(\binom{t}{j} + \binom{t}{j-1}\right)\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^j = \binom{t+1}{j}\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^j, \end{aligned}$$

where the first inequality follows from Lemma 4.6 and the second inequality follows from the inductive assumption. □

Lemma 4.8. *If $t \le 0.03\sqrt{NK}$ then $q_{t,j} < 0.66^j$ for all $j > K/2$.*

Proof. By the well known inequality $\binom{t}{j} < (\mathrm{e}t/j)^j$ for $j \ge 1$, we have

$$q_{t,j} \le \binom{t}{j}\left(\frac{4\sqrt{K}}{\sqrt{N}}\right)^j \le \left(\frac{4\sqrt{K}\mathrm{e}t}{\sqrt{N}j}\right)^j.$$

Let $j > K/2$ and $t \le 0.03\sqrt{NK}$. Then

$$\frac{4\sqrt{K}\mathrm{e}t}{\sqrt{N}j} \le \frac{0.12\mathrm{e}\sqrt{K}\sqrt{NK}}{\sqrt{N}K/2} < 0.66\,,$$

implying the lemma. □

Lemma 4.9. *The success probability of $\mathcal{A}$ is at most*

$$\frac{\binom{N}{K/2}}{\binom{N}{K}} + 4\sqrt{q_{t,K/2+1}}\,.$$

Proof. In Section 6. □

To complete the proof, given the two Lemmas, we choose a constant $c > \sqrt[4]{0.66} = 0.90133\ldots$ and set $\varepsilon = 0.03$. Then, by Lemma 4.9, the success probability of $\mathcal{A}$ is at most

$$\frac{\binom{N}{K/2}}{\binom{N}{K}} + 4\sqrt{0.66^{K/2}}\,.$$

The first term is equal to

$$\begin{aligned}\frac{\binom{N}{K/2}}{\binom{N}{K}} &= \frac{K!(N-K)!}{(K/2)!(N-K/2)!} = \frac{K(K-1)\ldots(K/2+1)}{(N-K/2)(N-K/2-1)\ldots(N-K+1)} \\ &\le \left(\frac{K}{N-K/2}\right)^{K/2} \le \left(\frac{N/2}{3N/4}\right)^{K/2} = \left(\frac{2}{3}\right)^{K/2} = o(c^K)\,,\end{aligned}$$

where the last two inequalities follow from $K < N/2$. The second term is $4\sqrt{0.66^{K/2}} = o(c^K)$. □

5 Proof of Lemma 4.6

Let $|\psi_t\rangle$ be the state before $(t+1)^{\text{st}}$ query. We decompose $|\psi_t\rangle$ as $\sum_{i=0}^{N} a_i|\psi_{t,i}\rangle$, where $|\psi_{t,i}\rangle$ is the part in which the query register contains $|i\rangle$. Because of symmetrization, we must have $|a_1| = |a_2| = \cdots = |a_N|$. Also, we can choose the relative phases so that $a_1, \cdots, a_N$ are all positive reals and, thus, $a_1 = a_2 = \cdots = a_N$. Let $\rho_{t,i} = |\psi_{t,i}\rangle\langle\psi_{t,i}|$. Then

$$\rho_t = \sum_{i=0}^{N} a_i^2 \rho_{t,i}\,. \tag{5.1}$$

Claim 5.1. Let $i \in \{1,\ldots,N\}$. The entry $(\rho_{t,i})_{x,y}$ only depends on x_i, y_i, and the cardinality of $\{\ell : \ell \neq i, x_\ell = y_\ell = 1\}$.

Proof. The main idea is similar to Lemma 4.2.

This time, we trace out all registers, except for $\mathcal{H}_I$ and the query register. This gives us a density matrix ρ whose rows and columns are indexed by pairs (x, j) where x is an input and $j \in \{1,\ldots,N\}$. Let $x \in \{0,1\}^N$, $y \in \{0,1\}^N$, $j \in [N]$, $k \in [N]$ and $x' \in \{0,1\}^N$, $y' \in \{0,1\}^N$, $j' \in [N]$, $k' \in [N]$ be such that there is a permutation $\pi \in S_N$ with $x' = \pi(x)$, $y' = \pi(y)$, $i' = \pi(i)$ and $j' = \pi(j)$. By an argument similar to the proof of Lemma 4.2, we have

$$\rho_{(x,i),(y,j)} = \rho_{(x',i'),(y',j')}\,. \tag{5.2}$$

We now observe that $\rho_{t,i}$ is the submatrix of ρ consisting of rows and columns indexed by pairs (x,i), with all possible $x \in \{0,1\}^N$, $|\{i : x_i = 1\}| = K$.

If we have inputs x, y, x', y' with $x_i = x'_i$, $y_i = y'_i$ and $|\{\ell : \ell \neq i, x_\ell = y_\ell = 1\}| = |\{\ell : \ell \neq i, x'_\ell = y'_\ell = 1\}|$, then we can construct a permutation π with $\pi(i) = i$, $\pi(x) = x'$ and $\pi(y) = y'$. Equation (5.2) then implies $(\rho_{t,i})_{x,y} = (\rho_{t,i})_{x',y'}$. □

We now describe the eigenspaces of matrices $\rho_{t,i}$. The proofs of some claims are postponed to Section 7.

We define the following subspaces of states. Let $i \in [N]$ and $j \in \{0,1,\ldots,K\}$. We define $T_j^{i,0}$ to be the subspace spanned by all states

$$|\psi^{i,0}_{i_1,\ldots,i_j}\rangle = \frac{1}{\sqrt{\binom{N-j-1}{K-j}}} \sum_{\substack{x:|x|=K \\ x_{i_1}=\cdots=x_{i_j}=1, x_i=0}} |x_1 \ldots x_N\rangle ,$$

with $(i_1,\ldots,i_j)$ ranging over all tuples of j distinct elements of $[N]-\{i\}$. Similarly, we define $T_j^{i,1}$ to be the subspace spanned by all states

$$|\psi^{i,1}_{i_1,\ldots,i_j}\rangle = \frac{1}{\sqrt{\binom{N-j-1}{K-j-1}}} \sum_{\substack{x:|x|=K \\ x_{i_1}=\cdots=x_{i_j}=1, x_i=1}} |x_1 \ldots x_N\rangle .$$

Let $S_j^{i,0} = T_j^{i,0} \cap (T_{j-1}^{i,0})^{\perp}$ and $S_j^{i,1} = T_j^{i,1} \cap (T_{j-1}^{i,1})^{\perp}$. Equivalently, we can define $S_j^{i,0}$ and $S_j^{i,1}$ as the subspaces spanned by the states $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ and $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$, respectively, with

$$|\tilde{\psi}^{i,\ell}_{i_1,\ldots,i_j}\rangle = P_{(T^{i,\ell}_{j-1})^{\perp}} |\psi^{i,\ell}_{i_1,\ldots,i_j}\rangle .$$

Let $S^i_{\alpha,\beta,j}$ be the subspace spanned by all states

$$\alpha \frac{|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle}{\| |\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle \|} + \beta \frac{|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle}{\| |\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle \|} . \tag{5.3}$$

where $(i_1,\ldots,i_j)$ again ranges over all tuples of j distinct elements of $[N]-\{i\}$.

Claim 5.2. Every eigenspace of $\rho_{t,i}$ is a direct sum of subspaces $S^i_{\alpha,\beta,j}$ for some α, β, j.

Proof. In Section 7. □

Let $\tau^i_{\alpha,\beta,j}$ be the completely mixed state over $S^i_{\alpha,\beta,j}$. Similarly to Lemma 4.4, we can write $\rho_{t,i}$ as

$$\rho_{t,i} = \sum_{(\alpha,\beta,j)\in A_{t,i}} p^i_{\alpha,\beta,j} \tau^i_{\alpha,\beta,j} , \tag{5.4}$$

where (α,β,j) range over some finite set $A_{t,i}$. (This set is finite because the $\mathcal{H}_I$ register holding $|x_1 \ldots x_N\rangle$ is finite dimensional and, therefore, decomposes into a direct sum of finitely many eigenspaces.) For every pair $(\alpha,\beta,j) \in A_{t,i}$, we normalize α,β by multiplying them by the same constant so that $\alpha^2+\beta^2 = 1$. Querying x_i transforms this state to

$$\rho'_{t,i} = \sum_{(\alpha,\beta,j)\in A_{t,i}} p^i_{\alpha,\beta,j} \tau^i_{\alpha,-\beta,j} ,$$

because $|\tilde{\psi}^{i,\ell}_{i_1,\ldots,i_j}\rangle$ is a superposition of $|x\rangle$ with $x_i = \ell$ and, therefore, a query leaves $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ unchanged and flips a phase on $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$. If $i = 0$, we have $\rho'_{t,0} = \rho_{t,0}$, because, if the query register contains $|0\rangle$, the query maps any state to itself, thus leaving $\rho_{t,0}$ unchanged.

Claim 5.3. Let $\alpha_0 = \sqrt{\frac{N-K}{N-j}}\|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\|$ and $\beta_0 = \sqrt{\frac{K-j}{N-j}}\|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\|$.

(i) $S^i_{\alpha_0,\beta_0,j} \subseteq S_j$;

(ii) $S^i_{\beta_0,-\alpha_0,j} \subseteq S_{j+1}$.

Proof. In Section 7. $\square$

Corollary 5.4. For any α, β we have $S^i_{\alpha,\beta,j} \subseteq S_j \oplus S_{j+1}$.

Proof. We have $S_{\alpha,\beta,j} \subseteq S^{i,0}_j \oplus S^{i,1}_j$, since $S_{\alpha,\beta,j}$ is spanned by linear combinations of states $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ (which belong to $S^{i,0}_j$) and states $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$ (which belong to $S^{i,1}_j$). As shown in the proof of Claim 5.3 above,

$$S^{i,0}_j \oplus S^{i,1}_j \subseteq S_{\alpha_0,\beta_0,j} \oplus S_{-\beta_0,\alpha_0,j} \subseteq S_j \oplus S_{j+1}\,.$$

$\square$

The next claim quantifies the overlap between $S^i_{\alpha,\beta,j}$ and S_{j+1}.

Claim 5.5.

$$\operatorname{Tr} P_{S_{j+1}} \tau^i_{\alpha,\beta,j} = \frac{|\alpha\beta_0 - \beta\alpha_0|^2}{\alpha_0^2+\beta_0^2}\,.$$

Proof. In Section 7. $\square$

To be able to use this bound, we also need to bound α_0 and β_0.

Claim 5.6. $\frac{\beta_0}{\sqrt{\alpha_0^2+\beta_0^2}} \leq \sqrt{\frac{4(K-j)}{N+3K-4j}}$.

Proof. In Section 7. $\square$

We can now complete the proof of Lemma 4.6. By projecting both sides of $\rho_t = \sum_i p_{t,i}\tau_i$ to $(T_j)^\perp = S_{j+1} \oplus \cdots \oplus S_K$ and taking trace, we get

$$\operatorname{Tr} P_{(T_j)^\perp}\rho_t = \sum_{j'=0}^{K} p_{t,j'} \operatorname{Tr} P_{(T^j)^\perp}\tau_{j'} = \sum_{j'=j+1}^{K} p_{t,j'} = q_{t,j}\,, \tag{5.5}$$

with the second equality following because the states $\tau_{j'}$ are uniform mixtures over subspaces $S_{j'}$ and $S_0,\ldots,S_j$ are contained in T_j while $S_{j+1},\ldots,S_K$ are contained in $(T_j)^\perp$. Because of equations (5.1) and (5.4), this means that

$$q_{t,j+1} = a_0^2 \operatorname{Tr} P_{(T_j)^\perp}\rho_{t,0} + \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j')\in A_{t,i}} p^i_{\alpha,\beta,j'} \operatorname{Tr} P_{(T_j)^\perp}\tau^i_{\alpha,\beta,j'}\,. \tag{5.6}$$

Decomposing the state after the query in a similar way, we get

$$q_{t+1,j+1} = a_0^2 \operatorname{Tr} P_{(T_j)^\perp}\rho'_{t,0} + \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j')\in A_{t,i}} p^i_{\alpha,\beta,j'} \operatorname{Tr} P_{(T_j)^\perp}\tau^i_{\alpha,-\beta,j'}\,.$$

By substracting the two sums and using $\rho'_{t,0} = \rho_{t,0}$, we get

$$q_{t+1,j+1} - q_{t,j+1} = \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j')\in A_{t,i}} p^i_{\alpha,\beta,j'} \operatorname{Tr} P_{(T_j)^\perp}(\tau^i_{\alpha,-\beta,j'} - \tau^i_{\alpha,\beta,j'}) \,. \tag{5.7}$$

We now claim that all the terms in this sum with $j' \neq j$ are 0. For $j' < j$, $S_{\alpha,\beta,j'} \subseteq T_{j'+1} \subseteq T_j$, implying that $\operatorname{Tr} P_{(T_j)^\perp} \tau^i_{\alpha,\beta,j'} = 0$ and, similarly, $\operatorname{Tr} P_{(T_j)^\perp} \tau^i_{\alpha,-\beta,j'} = 0$. For $j' > j$, $S_{\alpha,\beta,j'} \subseteq S_{j'} \oplus S_{j'+1} \subseteq (T_j)^\perp$, implying that

$$\operatorname{Tr} P_{(T_j)^\perp} \tau^i_{\alpha,\beta,j'} = 1, \quad \operatorname{Tr} P_{(T_j)^\perp} \tau^i_{\alpha,-\beta,j'} = 1 \,,$$

and the difference of the two is 0. By removing those terms from (5.7), we get

$$q_{t+1,j+1} - q_{t,j+1} = \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j)\in A_{t,i}} p^i_{\alpha,\beta,j} \operatorname{Tr} P_{(T_j)^\perp}(\tau^i_{\alpha,-\beta,j} - \tau^i_{\alpha,\beta,j}) \,. \tag{5.8}$$

We have

$$\operatorname{Tr} P_{(T_j)^\perp}(\tau^i_{\alpha,-\beta,j} - \tau^i_{\alpha,\beta,j}) = \operatorname{Tr} P_{S_{j+1}}(\tau^i_{\alpha,-\beta,j} - \tau^i_{\alpha,\beta,j}) = \frac{|\alpha\beta_0 + \beta\alpha_0|^2}{\alpha_0^2 + \beta_0^2} - \frac{|\alpha\beta_0 - \beta\alpha_0|^2}{\alpha_0^2 + \beta_0^2} \,,$$

where the first equality follows from Corollary 5.4, $S_j \subseteq T_j$, and $S_{j+1} \subseteq (T_j)^\perp$, and the second equality follows from Claim 5.5. This is at most

$$4\frac{|\alpha\beta\alpha_0\beta_0|}{\alpha_0^2+\beta_0^2} \le 2\frac{\alpha_0\beta_0}{\alpha_0^2+\beta_0^2} = 2\frac{\alpha_0}{\sqrt{\alpha_0^2+\beta_0^2}}\frac{\beta_0}{\sqrt{\alpha_0^2+\beta_0^2}} \le 2\sqrt{\frac{4(K-j)}{N+3K-4j}} \le 2\sqrt{\frac{4K}{N}} \,,$$

where the first inequality follows from

$$|\alpha\beta| \le \frac{|\alpha|^2+|\beta|^2}{2} = \frac{1}{2}$$

and the second inequality follows from Claim 5.6 and $\frac{\alpha_0}{\sqrt{\alpha_0^2+\beta_0^2}} \le 1$. Together with equation (5.7), this means

$$q_{t+1,j+1} - q_{t,j+1} \le \frac{4\sqrt{K}}{\sqrt{N}} \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j)\in A_{t,i}} p^i_{\alpha,\beta,j} \,. \tag{5.9}$$

Similarly to equation (5.5) we have

$$p_{t,j+1} + p_{t,j} = \operatorname{Tr} P_{(S_j \oplus S_{j+1})} \rho_t \,.$$

We can then express the right hand side, similarly to equation (5.6), as a sum of terms $p^0_{j'} \operatorname{Tr} P_{(S_j\oplus S_{j+1})} \tau_{j'}$ and $p^i_{\alpha,\beta,j'} \operatorname{Tr} P_{(S_j\oplus S_{j+1})} \tau^i_{\alpha,\beta,j'}$. Since $S^i_{\alpha,\beta,j} \subseteq S_j \oplus S_{j+1}$ (by Corollary 5.4), we have

$$\operatorname{Tr} P_{(S_j\oplus S_{j+1})} \tau^i_{\alpha,\beta,j} = 1 \,.$$

This means that

$$p_{t,j+1}+p_{t,j} \geq \sum_{i=1}^{N} a_i^2 \sum_{(\alpha,\beta,j)\in A_{t,i}} p^i_{\alpha,\beta,j}\,.$$

Together with equation (5.9), this implies

$$q_{t+1,j+1}-q_{t,j+1} \leq \frac{4\sqrt{K}}{\sqrt{N}}(p_{t,j}+p_{t,j+1}) \leq \frac{4\sqrt{K}}{\sqrt{N}} \sum_{j'=j}^{K} p_{t,j'} = \frac{4\sqrt{K}}{\sqrt{N}} q_{t,j}\,.$$

□

6 Proof of Lemma 4.9

We start with the case when $p_{T,K/2+1} = \cdots = p_{T,K} = 0$.

Lemma 6.1. *If $p_{T,K/2+1} = \cdots = p_{T,K} = 0$, the success probability of $\mathcal{A}$ is at most $\frac{\binom{N}{K/2}}{\binom{N}{K}}$.*

Proof. Let $|\psi\rangle$ be the final state. The state of register $\mathcal{H}_I$ lies in $T_{K/2}$, which is an $\binom{N}{K/2}$-dimensional space. Therefore, there is a Schmidt decomposition for $|\psi\rangle$ with at most $\binom{N}{K/2}$ terms. This means that the state of $\mathcal{H}_A$ lies in an $\binom{N}{K/2}$-dimensional subspace of $\mathcal{H}_A \otimes H_S$.

We express the final state as

$$|\psi\rangle = \sum_{x:|x|=K} \frac{1}{\sqrt{\binom{N}{K}}} |\psi_x\rangle |x\rangle\,.$$

We can think of $|\psi_x\rangle$ as a quantum encoding for x and the final measurement as a decoding procedure that takes $|\psi_x\rangle$ and produces a guess for x. The probability that algorithm $\mathcal{A}$ succeeds is then equal to the average success probability of the encoding. We now use

Theorem 6.2. *[20] For any encoding $|\psi_x\rangle$ of M classical values by quantum states in d dimensions, the probability of success is at most d/M.*

In our case, $M = \binom{N}{K}$ and $d = \binom{N}{K/2}$ because the states $|\psi\rangle$ all lie in a $\binom{N}{K/2}$-dimensional subspace of $\mathcal{H}_A \otimes \mathcal{H}_S$. Therefore, Theorem 6.2 implies Lemma 6.1. □

We decompose the state $|\psi_T\rangle$ as $\sqrt{1-\delta}|\psi'_T\rangle + \sqrt{\delta}|\psi''_T\rangle$ where $|\psi'_T\rangle$ is in the subspace $\mathcal{H}_A \otimes T_{K/2}$ and $|\psi''_T\rangle$ is in $\mathcal{H}_A \otimes (T_{K/2})^{\perp}$. We have

$$\delta = \sum_{j=K/2+1}^{K} p_{T,j}\,.$$

The success probability of $\mathcal{A}$ is the probability that, if we measure both the register of $\mathcal{H}_A$ containing the result of the computation and $\mathcal{H}_I$ then we get $i_1,\ldots,i_K$ and $x_1,\ldots,x_N$ such that $x_{i_1} = \cdots = x_{i_K} = 1$.

Consider the probability of getting $i_1, \ldots, i_K$ and $x_1, \ldots, x_N$ such that $x_{i_1} = \cdots = x_{i_K} = 1$, when measuring $|\psi'_T\rangle$ (instead of $|\psi_T\rangle$). By Lemma 6.1, this probability is at most $\binom{N}{K/2}/\binom{N}{K}$. We have

$$\|\psi_T - \psi'_T\| \leq (1-\sqrt{1-\delta^2})\|\psi'_T\| + \sqrt{\delta}\|\psi''_T\| = (1-\sqrt{1-\delta^2}) + \sqrt{\delta} \leq 2\sqrt{\delta}\,.$$

We now apply

Lemma 6.3. *[10] For any states $|\psi\rangle$ and $|\psi'\rangle$ and any measurement, the total variation distance between the probability distributions obtained by applying M to $|\psi\rangle$ and to $|\psi'\rangle$ is at most $2\|\psi - \psi'\|$.*

By Lemma 6.3, the probabilities of getting $i_1, \ldots, i_K$ and $x_1, \ldots, x_N$ such that $x_{i_1} = \cdots = x_{i_K} = 1$, when measuring $|\psi_T\rangle$ and $|\psi'_T\rangle$ differ by at most $4\sqrt{\delta} = 4\sqrt{q_{T,K/2+1}}$. Therefore, the success probability of $\mathcal{A}$ is at most

$$\frac{\binom{N}{K/2}}{\binom{N}{K}} + 4\sqrt{q_{T,K/2+1}}\,.$$

7 Structure of the eigenspaces of $\rho_{t,i}$

In this section, we prove Claims 5.2, 5.3, 5.5, and 5.6 describing the structure of the eigenspaces of $\rho_{t,i}$. Before giving the proofs, we briefly summarize the results in this section.

1. Let $\rho_{t,i}$ be a matrix whose rows and columns are indexed by $(x_1, \ldots, x_N)$, $x_i \in \{0,1\}$ with $x_1 + \ldots + x_N = K$. By Claim 5.2, if $\rho_{t,i}$ is symmetric w. r. t. any permutation $\pi \in S_N$ that fixes i, then its eigenspaces are of the form $S^i_{\alpha,\beta,j}$, which is the subspace spanned by the states of the form

$$\alpha \frac{|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle\|} + \beta \frac{|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle\|}$$

   where $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ and $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$ are the states defined at the beginning of Section 5.

2. We then relate the eigenspaces $S^i_{\alpha,\beta,j}$ to the subspaces $S_0, \ldots, S_K$ defined in Section 4.2. In Claim 5.3 we show that, for certain α_0 and β_0, we have

   - $S^i_{\alpha_0,\beta_0,j} \subseteq S_j$;
   - $S^i_{-\beta_0,\alpha_0,j} \subseteq S_{j+1}$;

   A corollary of this is that, for any α, β, we have

$$S^i_{\alpha,\beta,j} \subseteq S^i_{\alpha_0,\beta_0,j} \oplus S^i_{-\beta_0,\alpha_0,j} \subseteq S_j \oplus S_{j+1}\,.$$

   This is shown in Corollary 5.4.

3. Next, in Claim 5.5, we quantify how close $S^i_{\alpha,\beta,j}$ is to S_j and S_{j+1}. The result is an expression for $\operatorname{Tr} P_{S_{j+1}} \tau^i_{\alpha,\beta,j}$ (where $\tau^i_{\alpha,\beta,j}$ is the maximally mixed state over $S^i_{\alpha,\beta,j}$) that involves α, β and α_0, β_0. To use that expression, we also need a bound on the ratio of α_0 and β_0 (Claim 5.6).

Proof of Claim 5.2. We rearrange the rows and the columns of $\rho_{t,i}$ so that all rows and columns corresponding to $|x_1 \dots x_N\rangle$ with $x_i = 0$ are before the rows and the columns corresponding to $|x_1 \dots x_N\rangle$ with $x_i = 1$. We then express $\rho_{t,i}$ as

$$\rho_{t,i} = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A is an $\binom{N-1}{K} \times \binom{N-1}{K}$ square matrix indexed by $|x_1 \dots x_N\rangle$ with $x_i = 0$, D is an $\binom{N-1}{K-1} \times \binom{N-1}{K-1}$ square matrix indexed by $|x_1 \dots x_N\rangle$ with $x_i = 1$, and B and C are rectangular matrices with rows (columns) indexed by $|x_1 \dots x_N\rangle$ with $x_i = 0$ and columns (rows) indexed by $|x_1 \dots x_N\rangle$ with $x_i = 1$.

We claim that

$$\begin{aligned} \rho_{t,i}|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle &= a_{11}|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle + a_{12}|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle \quad \text{and} \\ \rho_{t,i}|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle &= a_{21}|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle + a_{22}|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle, \end{aligned} \tag{7.1}$$

where $a_{11}, a_{12}, a_{21}, a_{22}$ are independent of $i_1, \dots, i_j$. To prove that, we first note that A and D are matrices where A_{xy} and D_{xy} only depend on $|\{t : x_t = y_t\}|$. Therefore Lemma 4.3 applies. This means that $S^{i,0}_j$ and $S^{i,1}_j$ are eigenspaces for A and D, respectively, and

$$\begin{aligned} A|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle &= a_{11}|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle \quad \text{and} \\ D|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle &= a_{22}|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle, \end{aligned}$$

where a_{11} and a_{22} are the eigenvalues of A and D for the eigenspaces $S^{i,0}_j$ and $S^{i,1}_j$. It remains to prove that

$$B|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle = a_{12}|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle \quad \text{and} \tag{7.2}$$

$$C|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle = a_{21}|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle. \tag{7.3}$$

Let M be a rectangular matrix, with entries indexed by x, y, with $|x| = |y| = K$ and $x_i = 1$ and $y_i = 0$. The entries of M are $M_{xy} = 1$ if x and y differ in two places, with $x_i = 1$, $y_i = 0$ and $x_l = 0$, $y_l = 1$ for some $l \neq i$ and $M_{xy} = 0$ otherwise. We claim

$$M|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle = c|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle \tag{7.4}$$

for some c that may depend on N, k, and j but not on $i_1, \dots, i_j$. To prove that, we need to prove two things. First,

$$M|\psi^{i,0}_{i_1,\dots,i_j}\rangle = c|\psi^{i,1}_{i_1,\dots,i_j}\rangle. \tag{7.5}$$

This follows by

$$\begin{aligned}
M|\psi^{i,0}_{i_1,\dots,i_j}\rangle &= \frac{1}{\sqrt{\binom{N-j-1}{k-j}}} \sum_{\substack{x:x_{i_1}=\dots=x_{i_j}=1,\\ x_i=0}} M|x\rangle \\
&= \frac{1}{\sqrt{\binom{N-j-1}{K-j}}} \sum_{\substack{x:x_{i_1}=\dots=x_{i_j}=1\\ x_i=0}} \sum_{\ell:x_\ell=1} |x_1\dots x_{\ell-1}0x_{\ell+1}\dots x_{i-1}1x_{i+1}\dots x_N\rangle \\
&= \frac{1}{\sqrt{\binom{N-j-1}{K-j}}}(N-K) \sum_{\substack{y:y_{i_1}=\dots=y_{i_j}=1\\ y_i=1}} |y\rangle = \sqrt{(K-j)(N-K)}|\psi^{i,1}_{i_1,\dots,i_j}\rangle\,.
\end{aligned}$$

Second, $M(T^{i,0}_j) \subseteq T^{i,1}_j$ and $M(T^{i,0}_j)^\perp \subseteq (T^{i,1}_j)^\perp$. The first statement immediately follows from equation (7.5), because the subspaces $T^{i,0}_j$ and $T^{i,1}_j$ are spanned by the states $|\psi^{i,0}_{i_1,\dots,i_j}\rangle$ and $|\psi^{i,1}_{i_1,\dots,i_j}\rangle$, respectively. To prove the second statement, let $|\psi\rangle \in (T^{i,0}_j)^\perp$ and $|\psi\rangle = \sum_x a_x|x\rangle$. We would like to prove $M|\psi\rangle \in (T^{i,1}_j)^\perp$. This is equivalent to $\langle\psi^{i,1}_{i_1,\dots,i_j}|M|\psi\rangle = 0$ for all $i_1,\dots,i_j$. We have

$$\begin{aligned}
\langle\psi^{i,1}_{i_1,\cdots,i_j}|M|\psi\rangle &= \frac{1}{\sqrt{\binom{N-j-1}{K-j-1}}} \sum_{y:y_{i_1}=\dots=y_{i_j}=1} \langle y|M|\psi\rangle \\
&= \frac{1}{\sqrt{\binom{N-j-1}{K-j-1}}} \sum_{\substack{x:x_{i_1}=\dots=x_{i_j}=1,\\ x_i=0}} \sum_{\substack{l:x_l=1,\\ l\notin\{i_1,\dots,i_j\}}} a_x \\
&= \frac{1}{\sqrt{\binom{N-j-1}{K-j-1}}}(K-j) \sum_{x:x_{i_1}=\dots=x_{i_j}=1} a_x = 0\,.
\end{aligned}$$

The first equality follows by writing out $\langle\psi^{i,1}_{i_1,\dots,i_j}|$, the second equality follows by writing out M. The third equality follows because, for every x with $|x| = K$ and $x_{i_1} = \dots = x_{i_j} = 1$, there are $K-j$ more $l \in [N]$ satisfying $x_l = 1$. The fourth equality follows because $\sum_{x:x_{i_1}=\dots=x_{i_j}=1} a_x$ is a constant times $\langle\psi^{i,0}_{i_1,\dots,i_j}|\psi\rangle$ and $\langle\psi^{i,0}_{i_1,\dots,i_j}|\psi\rangle = 0$, because $|\psi\rangle \in (T^{i,0}_j)^\perp$.

Furthermore, BM is an $\binom{N-1}{K} \times \binom{N-1}{K}$ matrix, with $(BM)_{x,y}$ only depending on $|\{\ell : x_\ell = y_\ell = 1\}|$. Therefore, $S^{i,1}_j$ is an eigenspace of BM and, since $|\tilde\psi^{i,1}_{i_1,\dots,i_j}\rangle \in S^{i,1}_j$, we have

$$BM|\tilde\psi^{i,1}_{i_1,\dots,i_j}\rangle = \lambda|\tilde\psi^{i,1}_{i_1,\dots,i_j}\rangle$$

for an eigenvalue λ independent of $i_1,\dots,i_j$. Together with equation (7.4), this implies equation (7.2) with $a_{12} = \lambda/c$.

Equation (7.3) follows by proving

$$M^T|\tilde\psi^{i,1}_{i_1,\dots,i_j}\rangle = c|\tilde\psi^{i,0}_{i_1,\dots,i_j}\rangle \quad\text{and}\quad CM^T|\tilde\psi^{i,0}_{i_1,\dots,i_j}\rangle = \lambda|\tilde\psi^{i,0}_{i_1,\dots,i_j}\rangle\,,$$

in a similar way.

We now diagonalize the matrix

$$M' = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

It has two eigenvectors: $\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$ and $\begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$. Equation (7.1) implies that, for any $i_1, \ldots, i_j$,

$$\alpha_1 |\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle + \beta_1 |\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$$

is an eigenvector of $\rho_{t,i}$ with the same eigenvalue λ. Therefore, $S^i_{\alpha_1,\beta_1,j}$ is an eigenspace of $\rho_{t,i}$. Similarly, $S^i_{\alpha_2,\beta_2,j}$ is an eigenspace of $\rho_{t,i}$. Vectors $\alpha_1|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle + \beta_1|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$ and $\alpha_2|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle + \beta_2|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$ together span the same space as vectors $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ and $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$. Since the vectors $|\tilde{\psi}^{i,\ell}_{i_1,\ldots,i_j}\rangle$ span $S^{i,\ell}_j$, this means that

$$S^{i,0}_j \oplus S^{i,1}_j \subseteq S_{\alpha_1,\beta_1,i} \oplus S_{\alpha_2,\beta_2,i}.$$

Therefore, repeating this argument for every j gives a collection of eigenspaces that span the entire state space for $\mathcal{H}_I$. This means that any eigenspace of $\rho_{t,i}$ is a direct sum of some of eigenspaces $S^i_{\alpha,\beta,j}$. □

Proof of Claim 5.3. For part (i), consider the states $|\psi_{i_1,\ldots,i_j}\rangle$ spanning T_j. We have

$$|\psi_{i_1,\ldots,i_j}\rangle = \sqrt{\frac{N-k}{N-j}}|\psi^{i,0}_{i_1,\ldots,i_j}\rangle + \sqrt{\frac{K-j}{N-j}}|\psi^{i,1}_{i_1,\ldots,i_j}\rangle \tag{7.6}$$

because an $(N-K)/(N-j)$ fraction of the states $|x_1 \ldots x_N\rangle$ with $|x| = K$ and $x_{i_1} = \cdots = x_{i_j} = 1$ have $x_i = 0$ and the rest have $x_i = 1$. The projection of these states to $(T^{i,0}_{j-1} \oplus T^{i,1}_{j-1})^\perp$ are

$$\sqrt{\frac{N-K}{N-j}}|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle + \sqrt{\frac{K-j}{N-j}}|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$$

which, by equation (5.3) are exactly the states spanning $S^i_{\alpha_0,\beta_0,j}$. Furthermore, we claim that

$$T_{j-1} \subseteq T^{i,0}_{j-1} \oplus T^{i,1}_{j-1} \subseteq T_j. \tag{7.7}$$

The first containment is true because T_{j-1} is spanned by the states $|\psi_{i_1,\ldots,i_{j-1}}\rangle$ which either belong to $T^{i,1}_{j-2} \subseteq T^{i,1}_{j-1}$ (if one of $i_1, \ldots, i_{j-1}$ is equal to i) or are a linear combination of states $|\psi^{i,0}_{i_1,\ldots,i_{j-1}}\rangle$ and $|\psi^{i,1}_{i_1,\ldots,i_{j-1}}\rangle$ which belong to $T^{i,0}_{j-1}$ and $T^{i,1}_{j-1}$. The second containment follows because the states $|\psi^{i,1}_{i_1,\ldots,i_{j-1}}\rangle$ spanning $T^{i,1}_{j-1}$ are the same as the states $|\psi_{i,i_1,\ldots,i_{j-1}}\rangle$ which belong to T_j and the states $|\psi^{i,0}_{i_1,\ldots,i_{j-1}}\rangle$ spanning $T^{i,0}_{j-1}$ can be expressed as linear combinations of $|\psi_{i_1,\ldots,i_{j-1}}\rangle$ and $|\psi_{i,i_1,\ldots,i_{j-1}}\rangle$ which both belong to T_j.

The first part of (7.7) now implies

$$S^i_{\alpha_0,\beta_0,j} \subseteq (T^{i,0}_{j-1} \oplus T^{i,1}_{j-1})^\perp \subseteq (T_{j-1})^\perp.$$

We also have $S^i_{\alpha_0,\beta_0,j} \subseteq T_j$, because, $S^i_{\alpha_0,\beta_0,j}$ is spanned by the states

$$P_{(T^{i,0}_{j-1}\oplus T^{i,1}_{j-1})^\perp}|\psi_{i_1,\ldots,i_j}\rangle = |\psi_{i_1,\ldots,i_j}\rangle - P_{T^{i,0}_{j-1}\oplus T^{i,1}_{j-1}}|\psi_{i_1,\ldots,i_j}\rangle$$

and $|\psi_{i_1,\ldots,i_j}\rangle$ belongs to T_j by the definition of T_j and $P_{T^{i,0}_{j-1}\oplus T^{i,1}_{j-1}}|\psi_{i_1,\ldots,i_j}\rangle$ belongs to T_j because of the second part of (7.7). Therefore, $S^i_{\alpha_0,\beta_0,j} \subseteq T_j \cap (T_{j-1})^\perp = S_j$.

For the part (ii), we have

$$S^i_{\alpha_0,\beta_0,j} \subseteq S^{i,0}_j \oplus S^{i,1}_j \subseteq T^{i,0}_j \oplus T^{i,1}_j \subseteq T_{j+1}\,,$$

where the first containment is true because $S^i_{\alpha_0,\beta_0,j}$ is spanned by linear combinations of vectors $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ (which belong to $S^{i,0}_j$) and vectors $|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle$ (which belong to $S^{i,1}_j$) and the last containment is true because of the second part of equation (7.7).

Let

$$|\psi\rangle = \beta_0 \frac{|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle\|} - \alpha_0 \frac{|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle\|} \tag{7.8}$$

be one of the vectors spanning $S^i_{\beta_0,-\alpha_0,j}$. To prove that $|\psi\rangle$ is in $S_{j+1} = T_{j+1} - T_j$, it remains to prove that $|\psi\rangle$ is orthogonal to T_j. This is equivalent to proving that $|\psi\rangle$ is orthogonal to every vector $|\psi_{i'_1,\ldots,i'_j}\rangle$ spanning T_j.

Case 1 $\{i'_1,\ldots,i'_j\} = \{i_1,\ldots,i_j\}$: Since $|\psi\rangle$ belongs to $(T^{i,0}_{j-1}\oplus T^{i,1}_{j-1})^\perp$, it suffices to prove that $|\psi\rangle$ is orthogonal to the projection of $|\psi_{i_1,\ldots,i_j}\rangle$ to $(T^{i,0}_{j-1}\oplus T^{i,1}_{j-1})^\perp$ which, by the discussion after the equation (7.6), is equal to

$$\alpha_0 \frac{|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle\|} + \beta_0 \frac{|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle}{\||\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\rangle\|}\,. \tag{7.9}$$

¿From equations (7.8) and (7.9) we see that the inner product of the two states is $\alpha_0\beta_0 - \beta_0\alpha_0 = 0$.

Case 2 $\{i'_1,\ldots,i'_j\} \neq \{i_1,\ldots,i_j\}$ but one of $i'_1,\ldots,i'_j$ is equal to i: For simplicity, assume $i = i'_j$. Then $|\psi_{i'_1,\ldots,i'_j}\rangle$ is the same as $|\psi^{i,1}_{i'_1,\ldots,i'_{j-1}}\rangle$ which belongs to $T^{i,1}_{j-1}$. By the definition of $S^i_{\alpha,\beta,j}$, the vector $|\psi\rangle$ belongs to $(T^{i,0}_{j-1}\oplus T^{i,1}_{j-1})^\perp$ and is therefore orthogonal to $|\psi^{i,1}_{i'_1,\ldots,i'_{j-1}}\rangle$.

Case 3 $\{i'_1,\ldots,i'_j\} \neq \{i_1,\ldots,i_j\}$ and none of $i'_1,\ldots,i'_j$ is equal to i: One of $i'_1,\ldots,i'_j$ must be not in $\{i_1,\ldots,i_j\}$. For simplicity, assume it is i'_j. We have

$$|\psi_{i'_1,\ldots,i'_{j-1}}\rangle = \sum_{i'\notin\{i'_1,\ldots,i'_{j-1}\}} |\psi_{i'_1,\ldots,i'_{j-1},i'}\rangle\,.$$

Also, $\langle\psi_{i'_1,\ldots,i'_{j-1}}|\psi\rangle = 0$, because $|\psi_{i'_1,\ldots,i'_{j-1}}\rangle$ is in $T^{i,0}_{j-1}\oplus T^{i,1}_{j-1}$. As proved in the previous case,

$$\langle\psi_{i'_1,\ldots,i'_{j-1},i}|\psi\rangle = 0\,.$$

We therefore have

$$\sum_{i' \notin \{i'_1,\dots,i'_{j-1},i\}} \langle \psi_{i'_1,\dots,i'_{j-1},i'} | \psi \rangle = 0 . \tag{7.10}$$

By symmetry, the inner product $\langle \psi_{i'_1,\dots,i'_{j-1},i'} | \psi \rangle$ is the same for every $i' \notin \{i'_1,\dots,i'_{j-1},i\}$. Therefore, equation (7.10) means $\langle \psi_{i'_1,\dots,i'_{j-1},i'} | \psi \rangle = 0$ for every $i' \notin \{i'_1,\dots,i'_{j-1},i\}$. □

Proof of Claim 5.5. $\tau^i_{\alpha,\beta,j}$ is a mixture of states $|\psi\rangle$ from the subspace $S^i_{\alpha,\beta,j}$. We prove the claim by showing that, for any of those states $|\psi\rangle$, the squared norm of its projection to S_{j+1} is equal to the right hand side of Claim 5.5. Since $|\psi\rangle \in S^i_{\alpha,\beta,j}$ we can write it as

$$|\psi\rangle = \sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j} (\alpha |\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle + \beta |\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle)$$

for some $a_{i_1,\dots,i_j}$. Let

$$|\psi^+\rangle = \sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j} (\beta_0 |\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle - \alpha_0 |\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle) \quad \text{and}$$

$$|\psi^-\rangle = \sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j} (\alpha_0 |\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\rangle + \beta_0 |\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\rangle) .$$

Then, $|\psi\rangle$ is a linear combination of $|\psi^+\rangle$ which belongs to $S^i_{\beta_0,-\alpha_0,j} \subset S_{j+1}$ (by Claim 5.3) and $|\psi^-\rangle$ which belongs to $S^i_{\alpha_0,\beta_0,j} \subseteq S_j$. Moreover, all three states are linear combinations of $|\psi^0\rangle$, $|\psi^1\rangle$ defined by

$$|\psi^\ell\rangle = \sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j} |\tilde{\psi}^{i,\ell}_{i_1,\dots,i_j}\rangle .$$

We have

$$|\psi\rangle = \alpha|\psi^0\rangle + \beta|\psi^1\rangle , \quad |\psi^+\rangle = \beta_0|\psi^0\rangle - \alpha_0|\psi^1\rangle \quad \text{and} \quad |\psi^-\rangle = \alpha_0|\psi^0\rangle + \beta_0|\psi^1\rangle .$$

Since $|\psi^+\rangle$ and $|\psi^-\rangle$ belong to subspaces S_{j+1} and S_j which are orthogonal, we must have $\langle\psi^+|\psi^-\rangle = 0$. This means

$$\alpha_0\beta_0\|\psi^0\|^2 - \beta_0\alpha_0\|\psi^1\|^2 = 0 .$$

By dividing the equation by $\alpha_0\beta_0$, we get $\|\psi^0\|^2 = \|\psi^1\|^2$ and $\|\psi^0\| = \|\psi^1\|$. Since $\|\psi\| = 1$, this means that

$$\|\psi^0\| = \|\psi^1\| = \frac{1}{\sqrt{\alpha^2+\beta^2}} = 1 .$$

Since $|\psi\rangle$ lies in the subspace spanned by $|\psi^+\rangle$ which belongs to S_{j+1} and $|\psi^-\rangle$ which belongs to S_j, the norm of the projection of $|\psi\rangle$ to S_{j+1} is equal to $|\langle\psi|\psi^+\rangle|/\|\psi^+\|$. By expressing $|\psi\rangle$ and $|\psi^+\rangle$ in terms of $|\psi^0\rangle$ and $|\psi^1\rangle$, we get

$$\frac{|\langle\psi|\psi^+\rangle|}{\|\psi^+\|} = \frac{\alpha\beta_0\|\psi^0\|^2 - \alpha_0\beta\|\psi^1\|^2}{\sqrt{\beta_0^2\|\psi^0\|^2 + \alpha_0^2\|\psi^0\|^2}} = \frac{|\alpha\beta_0 - \alpha_0\beta|}{\sqrt{\alpha_0^2+\beta_0^2}} ,$$

proving the claim. □

Proof of Claim 5.6. We will prove $\|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\| \geq \frac{1}{2}\|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\|$, because that means

$$\alpha_0 = \frac{\sqrt{N-K}}{\sqrt{N-j}}\|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\| \geq \frac{1}{2}\frac{\sqrt{N-K}}{\sqrt{K-j}}\frac{\sqrt{K-j}}{\sqrt{N-j}}\|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\| = \frac{\sqrt{N-K}}{2\sqrt{K-j}}\beta_0$$

and

$$\frac{\beta_0}{\sqrt{\alpha_0^2+\beta_0^2}} \leq \frac{\beta_0}{\sqrt{\frac{N-K}{4(K-j)}\beta_0^2+\beta_0^2}} = \frac{1}{\sqrt{1+\frac{N-K}{4(K-j)}}} = \frac{\sqrt{4(K-j)}}{\sqrt{N+3K-4j}}\,.$$

To prove $\|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\| \geq \|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\|$, we calculate the vector

$$|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle = P_{(T^{i,0}_{j-1})^\perp}|\psi^{i,0}_{i_1,\ldots,i_j}\rangle\,.$$

Both the vector $|\psi^{i,0}_{i_1,\ldots,i_j}\rangle$ and the subspace $T^{i,0}_{j-1}$ are fixed by

$$U_\pi|x\rangle = |x_{\pi(1)}\ldots x_{\pi(N)}\rangle$$

for any permutation π that fixes i and maps $\{i_1,\ldots,i_j\}$ to itself. This means that $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ is fixed by any such U_π as well. Therefore, the amplitude of $|x\rangle$, $|x|=K$, $x_i=0$ in $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ only depends on $|\{i_1,\ldots,i_j\}\cap\{t : x_t=1\}|$. This means $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ is of the form

$$|\psi_0\rangle = \sum_{m=0}^{j}\alpha_m \sum_{\substack{x:|x|=K,x_i=0\\ |\{i_1,\ldots,i_j\}\cap\{t:x_t=1\}|=m}}|x\rangle\,.$$

To simplify the following calculations, we multiply $\alpha_0,\ldots,\alpha_j$ by the same constant so that

$$\alpha_j = \frac{1}{\sqrt{\binom{N-j-1}{K-j}}}\,.$$

Then, $|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle$ remains a multiple of $|\psi_0\rangle$ but may no longer be equal to $|\psi_0\rangle$.

The coefficients $\alpha_0,\ldots,\alpha_{j-1}$ should be such that the state is orthogonal to T_{j-1} and, in particular, orthogonal to states $|\psi^{i,0}_{i_1,\ldots,i_\ell}\rangle$ for $\ell\in\{0,\ldots,j-1\}$. By writing out $\langle\psi_0|\psi^{i,0}_{i_1,\ldots,i_\ell}\rangle=0$, we get

$$\sum_{m=\ell}^{j}\alpha_m\binom{N-j-1}{K-m}\binom{j-\ell}{m-\ell}=0\,. \tag{7.11}$$

To show that, we first note that $|\psi^{i,0}_{i_1,\ldots,i_\ell}\rangle$ is a uniform superposition of all $|x\rangle$, $|x|=K$, $x_i=0$, $x_{i_1}=\cdots=x_{i_l}=1$. If we want to choose x subject to those constraints and also satisfying $|\{i_1,\ldots,i_j\}\cap\{t : x_t=1\}|=m$, we have to set $x_t=1$ for $m-\ell$ different $t\in\{i_{\ell+1},\ldots,i_j\}$ and for $K-m$ different $t\notin\{i,i_1,\ldots,i_j\}$. This can be done in $\binom{j-\ell}{m-\ell}$ and $\binom{N-j-1}{K-m}$ different ways, respectively.

By solving the system of equations (7.11), we get that the only solution is

$$\alpha_m = (-1)^{j-m} \frac{\binom{N-j-1}{K-j}}{\binom{N-j-1}{K-m}} \alpha_j \,. \tag{7.12}$$

Let $|\psi'_0\rangle = |\psi_0\rangle / \|\psi_0\|$ be the normalized version of $|\psi_0\rangle$. Then

$$\begin{aligned} |\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\rangle &= \langle \psi'_0 | \psi^{i,0}_{i_1,\ldots,i_j}\rangle |\psi'_0\rangle \quad \text{and} \\ \|\tilde{\psi}^{i,0}_{i_1,\ldots,i_j}\| &= \langle \psi'_0 | \psi^{i,0}_{i_1,\ldots,i_j}\rangle = \frac{\langle \psi_0 | \psi^{i,0}_{i_1,\ldots,i_j}\rangle}{\|\psi_0\|} \,. \end{aligned} \tag{7.13}$$

First, we have

$$\langle \psi_0 | \psi^{i,0}_{i_1,\ldots,i_j}\rangle = 1 \,,$$

because $|\psi^{i,0}_{i_1,\ldots,i_j}\rangle$ consists of $\binom{N-j-1}{K-j}$ basis states $|x\rangle$, $x_i = 0$, $x_{i_1} = \cdots = x_{i_j} = 1$, each of which has amplitude $1/\sqrt{\binom{N-j-1}{K-j}}$ in both $|\psi_0\rangle$ and $|\psi^{i,0}_{i_1,\ldots,i_j}\rangle$. Second,

$$\begin{aligned} \|\psi_0\|^2 &= \sum_{m=0}^{j} \binom{j}{m} \binom{N-j-1}{K-m} \alpha_m^2 = \sum_{m=0}^{j} \binom{j}{m} \frac{\binom{N-j-1}{K-j}^2}{\binom{N-j-1}{K-m}} \alpha_j^2 \\ &= \sum_{m=0}^{j} \binom{j}{m} \frac{\binom{N-j-1}{K-j}}{\binom{N-j-1}{K-m}} = \sum_{m=0}^{j} \binom{j}{m} \frac{(K-m)!(N-K+m-j-1)!}{(K-j)!(N-K-1)!} \\ &= \sum_{m=0}^{j} \binom{j}{m} \frac{(K-m)\cdots(K-j+1)}{(N-K-1)\cdots(N-K+m-j)} \end{aligned} \tag{7.14}$$

with the first equality following because there are $\binom{j}{m}\binom{N-j-1}{K-m}$ vectors x such that $|x| = K$, $x_i = 0$, $x_t = 1$ for m different $t \in \{i_1, \ldots, i_j\}$ and $K - m$ different $t \notin \{i, i_1, \ldots, i_j\}$, the second equality following from equation (7.12) and the third equality following from our choice $\alpha_j = 1/\sqrt{\binom{N-j-1}{K-j}}$.

We can similarly calculate $\|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\|$. We omit the details and just state the result. The counterpart of equation (7.13) is

$$\|\tilde{\psi}^{i,1}_{i_1,\ldots,i_j}\| = \frac{\langle \psi_1 | \psi^{i,1}_{i_1,\ldots,i_j}\rangle}{\|\psi_1\|} \,,$$

with $|\psi_1\rangle$ being the counterpart of $|\psi_0\rangle$:

$$|\psi_1\rangle = \sum_{m=0}^{j} \alpha_m \sum_{\substack{x:|x|=K, x_i=1 \\ |\{i_1,\ldots,i_j\}\cap\{\ell:x_\ell=1\}|=m}} |x\rangle \,,$$

with $\alpha_0 = 1/\sqrt{\binom{N-j-1}{K-j-1}}$. Similarly as before, we get $\langle \psi_1 | \psi^{i,1}_{i_1,\dots,i_j} \rangle = 1$ and

$$\|\psi_1\|^2 = \sum_{m=0}^{j} \binom{j}{m} \frac{\binom{N-j-1}{K-j-1}}{\binom{N-j-1}{K-m-1}} = \sum_{m=0}^{j} \binom{j}{m} \frac{(K-m-1)\dots(K-j)}{(N-K)\dots(N-K+m-j+1)}\,. \tag{7.15}$$

Each term in (7.14) is

$$\frac{(K-m)(N-K+m-j)}{(K-j)(N-K)}$$

times the corresponding term in equation (7.15). We have

$$\frac{K-m}{K-j}\,\frac{N-K+m-j}{N-K} \le \frac{K}{K/2} \cdot 2 = 4\,,$$

because $j \le K/2$ and $N-K+m-j \le N-K$ (because of $m \le j$). Therefore, $\|\psi_0\|^2 \le 4\|\psi_1\|^2$ which implies

$$\|\tilde{\psi}^{i,0}_{i_1,\dots,i_j}\| = \frac{1}{\|\psi_0\|} \ge \frac{1}{\sqrt{4}\|\psi_1\|} = \frac{1}{2}\|\tilde{\psi}^{i,1}_{i_1,\dots,i_j}\|\,. \qquad \square$$

Acknowledgment. I would like to thank Frederic Magniez, Robert Špalek, Ronald de Wolf, and several anonymous referees for very helpful comments on a draft of this paper.

References

[1] S. AARONSON: Limitations of quantum advice and one-way communication. *Theory of Computing*, 1:1–28, 2005. Conference version in CCC'2004. [ToC:v001/a001, arXiv:quant-ph/0402095]. 2

[2] S. AARONSON AND Y. SHI: Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, 2004. [JACM:1008731.1008735]. 2

[3] A. AMBAINIS: Quantum lower bounds by quantum arguments. *J. Comput. System Sci.*, 64(4):750–767, 2002. Conference version in STOC'00. [JCSS:10.1006/jcss.2002.1826, STOC:335305.335394, arXiv:quant-ph/0002066]. 1, 3, 4

[4] A. AMBAINIS: Polynomial degree vs. quantum query complexity. *J. Comput. System Sci.*, 72(2):220–238, 2006. Conference version in FOCS'03. [JCSS:10.1016/j.jcss.2005.06.006, FOCS:10.1109/SFCS.2003.1238197, arXiv:quant-ph/0305028]. 2, 3, 4

[5] A. AMBAINIS: Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007. Conference version in FOCS'04. [SICOMP:10.1137/S0097539705447311, arXiv:quant-ph/0311001]. 2

[6] A. AMBAINIS, R. ŠPALEK, AND R. DE WOLF: A new quantum lower bound method, with applications to direct product theorems and time-space tradeoffs. In *Proc. 38th STOC*, pp. 618–633. ACM Press, 2006. [STOC:10.1145/1132516.1132604]. 2

[7] A. AMBAINIS, R. ŠPALEK, AND R. DE WOLF: Quantum direct product theorems for symmetric functions and time-space tradeoffs. *Algorithmica*, 55(3):422–461, 2009. 2

[8] H. BARNUM, M. SAKS, AND M. SZEGEDY: Quantum decision trees and semidefinite programming. In *Proc. 18th IEEE Conf. on Comput. Complex. (CCC'03)*, pp. 179–193. IEEE Press, 2003. [CCC:10.1109/CCC.2003.1214419]. 2

[9] R. BEALS, H. BUHRMAN, R. CLEVE, M. MOSCA, AND R. DE WOLF: Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. Conference version in FOCS'98. [JACM:502090.502097, FOCS:10.1109/SFCS.1998.743485, arXiv:quant-ph/9802049]. 1

[10] E. BERNSTEIN AND U. VAZIRANI: Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997. [SICOMP:10.1137/S0097539796300921]. 15

[11] G. BRASSARD, P. HØYER, AND A. TAPP: Quantum counting. In *Proc. 25th Intern. Conf. Automata, Languages and Programming (ICALP'98)*, volume 1443 of *LNCS*, pp. 820–831. Springer, 1998. [ICALP:ap2mrf08d8gcqppe, arXiv:quant-ph/9805082]. 1

[12] H. BUHRMAN AND R. DE WOLF: Complexity measures and decision tree complexity: A survey. *Theoret. Comput. Sci.*, 288:21–43, 2002. [TCS:10.1016/S0304-3975(01)00144-X]. 3

[13] L. GROVER: A fast quantum mechanical algorithm for database search. In *Proc. 28th STOC*, pp. 212–219. ACM Press, 1996. [STOC:237814.237866, arXiv:quant-ph/9605043]. 1

[14] P. HØYER, T. LEE, AND R. ŠPALEK: Negative weights make adversaries stronger. In *Proc. 39th STOC*, pp. 526–535. ACM Press, 2007. [STOC:10.1145/1250790.1250867]. 3

[15] P. HOYER, J. NEERBEK, AND Y. SHI: Quantum lower bounds of ordered searching, sorting and element distinctness. *Algorithmica*, 34:429–448, 2002. Conference version at ICALP'01. [Algorithmica:25gl9elr5rxr3q6a, arXiv:quant-ph/0102078]. 4

[16] H. KLAUCK, R. ŠPALEK, AND R. DE WOLF: Quantum and classical strong direct product theorems and optimal time-space tradeoffs. *SIAM J. Comput.*, 36(5):1472–1493, 2007. Conference version at FOCS'04. [SICOMP:10.1137/05063235X, FOCS:10.1109/FOCS.2004.52, arXiv:quant-ph/0402123]. 2

[17] D. KNUTH: Combinatorial matrices. In *Selected Papers on Discrete Mathematics, CSLI Lecture Notes, no. 106*. University of Chicago Press, 2003. 8

[18] S. LAPLANTE AND F. MAGNIEZ: Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. *SIAM J. Comput.*, 38(1):46–62, 2008. Conference version at CCC'04. [SICOMP:10.1137/050639090, CCC:10.1109/CCC.2004.1313852, arXiv:quant-ph/0311189]. 2

[19] F. MAGNIEZ, M. SANTHA, AND M. SZEGEDY: Quantum algorithms for the triangle problem. *SIAM J. Comput.*, 37(2):413–424, 2007. Conference version at SODA'05. [SICOMP:10.1137/050643684, arXiv:quant-ph/0310134]. 2

[20] A. NAYAK: Optimal lower bounds for quantum automata and random access codes. In *Proc. 40th FOCS*, pp. 369–377. IEEE Press, 1999. [FOCS:10.1109/SFFCS.1999.814608, arXiv:quant-ph/9904093]. 14

[21] B. REICHARDT: Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean functionnote. Quant-ph, arXiv:0904.2759, 2009. [arXiv:0904.2759]. 3

[22] R. ŠPALEK: The multiplicative quantum adversary. In *Proc. 23rd IEEE Conf. on Comput. Complex.*, pp. 237–248. IEEE Press, 2008. [CCC:10.1109/CCC.2008.9]. 2

[23] R. ŠPALEK AND M. SZEGEDY: All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006. Conference version at ICALP'05. [ToC:v002/a001, arXiv:quant-ph/0409116]. 2

[24] S. ZHANG: On the power of Ambainis's lower bounds. *Theoret. Comput. Sci.*, 339(2–3):241–256, 2005. Conference version in ICALP'04. [TCS:10.1016/j.tcs.2005.01.019, ICALP:gm2ff6wpc0q39v3x, arXiv:quant-ph/0311060]. 2

AUTHOR

Andris Ambainis
professor
University of Latvia
Raina bulv. 19, Riga, LV-1586, Latvia
andris.ambainis@lu.lv
http://home.lanet.lv/~ambainis

ABOUT THE AUTHOR

ANDRIS AMBAINIS received his Ph. D. from the University of California, Berkeley in 2001, supervised by Umesh Vazirani. After that, he was a postdoc at the Institute for Advanced Study, Princeton and at the University of California, Berkeley, and a faculty member at the University of Waterloo, Canada. In 2007, Andris returned to his native Latvia and became Professor at the University of Latvia. His research interests include many areas of quantum computing and quantum information theory (quantum algorithms, quantum complexity theory, quantum cryptography, pseudorandom quantum states, etc.), as well as the classical theory of computation.