The Multiplicative Quantum Adversary

Robert Špalek*
spalek@eecs.berkeley.edu

Abstract

We present a new variant of the quantum adversary method. All adversary methods give lower bounds on the quantum query complexity of a function by bounding the change of a progress function caused by one query. All previous variants upper-bound the *difference* of the progress function, whereas our new variant upper-bounds the *ratio* and that is why we coin it the multiplicative adversary. Our new method generalizes the quantum lower-bound method by Ambainis [Amb05, AŠW06], based on the analysis of eigenspaces of the density matrix, to all functions. We prove a strong direct product theorem for all functions that have a multiplicative adversary lower bound.

1 Introduction

We consider the problem of proving a lower bound on the number of quantum queries needed to compute a function with bounded error. One of the most successful method for proving quantum query lower bounds is the adversary method [BBBV97, Amb02, HNS02, BS04, BSS03, Amb06, LM04, Zha05, ŠS06, HLŠ07]; see the survey [HŠ05] for the history of the method. It intuitively works as follows: The computation starts in a fixed quantum state independent of the input. The quantum algorithm consecutively applies arbitrary unitary transformations on its workspace and the input oracle operator. The quantum state corresponding to two different inputs x, y gradually diverges to two output states $|\psi_x^T\rangle, |\psi_y^T\rangle$. Since the algorithm has bounded error, there exists a measurement on the output state that gives the right outcome with high probability, hence the scalar product $|\langle\psi_x^T|\psi_y^T\rangle|$ must be low whenever $f(x) \neq f(y)$ [BV97]. We define a *progress function* in time t as a weighted average of these scalar products over many input pairs:

$$W^t = \sum_{\substack{x,y \\ f(x)\neq f(y)}} w_{x,y}\langle\psi_x^t|\psi_y^t\rangle. \tag{1}$$

Since the scalar products are all one at the beginning and below a constant at the end, the value of the progress function must drop a lot. On the other hand, one can show that one query only causes little *additive* change to the progress function, hence the algorithm must ask many queries. The quality of the lower bound depends on the adversary matrix w—one typically has to put more weight on input pairs that are hard to distinguish to get a good bound.

The progress function can be equivalently formulated in terms of density matrices. If we run the quantum algorithm on a superposition of inputs instead of a fixed input, then during the computation the algorithm register becomes entangled with the input register. We trace out the algorithm and input register and look at the reduced density matrix ρ_I^t of the input register. We define the progress function as a scalar product

$$W^t = \langle\Gamma, \rho_I^t\rangle \tag{2}$$

for some Hermitian matrix Γ with $\Gamma[x, y] = 0$ if $f(x) = f(y)$. This definition is equivalent with Eqn. (1) (see Section 2), and since it is easier to work with, we will stick to it in the whole paper.

*University of California, Berkeley. Supported by NSF Grant CCF-0524837 and ARO Grant DAAD 19-03-1-0082.

The (additive) adversary method suffers one severe limitation: the lower bound is proportional to the success probability of the algorithm and hence is negligible for exponentially small success probabilities. Several many-output functions, such as t-fold search, however, have strong lower bounds even with exponentially small success (proved first in [KŠW07] using the polynomial method [BBC+01]). These bounds are useful for proving quantum time-space tradeoffs.

Ambainis reproved [Amb05] and extended [AŠW06] these polynomial lower bounds using a new quantum lower-bound method based on the analysis of subspaces of the reduced density matrix of the input register. His method seemed tailored to the problem of quantum search, and is quite complicated.

In this paper, we reformulate Ambainis's new method in the adversary framework, generalize it to all functions, and provide some additional intuition. We use syntactically the same progress function Eqn. (2), but in a different way: (1) we require different conditions on the adversary matrix Γ, and (2) we show that one query can only *multiply* the value of the progress function by a small constant—whence the name *multiplicative adversary*. Surprisingly, the final formula for the multiplicative adversary lower bound is quite similar to the additive adversary. Unfortunately, the similarity is only illusive, and our new formula is significantly harder to bound than the old one and we thus don't simplify Ambainis's calculations much.

We, however, split Ambainis's original proof into several independent logical blocks and dovetail them together: upper-bounding the success probability based on the structure of the subspaces, upper-bounding the change caused by one query, simultaneous block-diagonalization of Γ and the query operator, and simplification of the final formula into a form similar to the additive adversary. This simplification allows us to generalize the method to all functions. Furthermore, we separate the quantum part and the combinatorial part of the proof—the quantum part is hidden inside the proof of the general lower-bound theorem (Section 3), and the user of the method who wants to get a lower bound for some function only has to evaluate its combinatorial properties (see Section 4 for new proofs of all known bounds in our new framework).

Finally, we show that the multiplicative adversary bound inherently satisfies the *strong direct product theorem* (DPT). Roughly speaking it says that to compute k independent instances of a function we need $\Omega(k)$ times more queries even if we are willing to decrease the (worst-case) success probability exponentially. It is not clear whether this theorem holds for all functions or not. Ambainis proved a (more complicated) DPT for all symmetric functions directly, whereas we show that it is sufficient to prove just a (simpler) multiplicative adversary lower bound, and the DPT then automatically follows (Section 5).

The biggest open problem, not addressed here, is to find a new stronger lower bound using the multiplicative adversary. A promising function is the element distinctness problem (tight $\Omega(n^{2/3})$ bound due to the polynomial method [AS04], but only $\Omega(\sqrt{n})$ adversary lower bound). It also doesn't seem completely unlikely that one could find a reduction from the additive adversary to the multiplicative adversary—if a lower bound for some function can be proved using one method, then it can be proved also using the other one. If this is true, then many extensive computations could be avoided. The multiplicative adversary method may also have potential to prove a quantum time-space tradeoff for some Boolean function (again, element distinctness), because small workspace implies small Schmidt-rank of the reduced density matrix. It would be interesting to look at the dual of the multiplicative adversary bound. The bound is not described by a semidefinite program, however one may be able to use general Lagrange multipliers.

2 Adversary framework

2.1 Quantum query complexity

As with the classical model of decision trees, in the quantum query model we wish to compute some function f and we access the input through queries. Let $f : X \to \Sigma_O$ be a function, with $X \subseteq \Sigma_I^n$ the set of inputs. We assume $\Sigma_I = \{0, 1, \ldots, \sigma - 1\}$ with $\sigma = |\Sigma_I|$, and call this the input alphabet and Σ_O the output alphabet. The complexity of f is the number of queries needed to compute f on a worst-case input x. Unlike the classical case, however, we can now make queries in superposition.

The memory of a quantum query algorithm is described by three registers: the input register, $\mathcal{H}_I$, which holds the input $x \in X$, the query register, $\mathcal{H}_Q$, which holds two integers $1 \leq i \leq n$ and $0 \leq p < \sigma$, and the

working memory, $\mathcal{H}_W$, which holds an arbitrary value. The query register and working memory together form the accessible memory, denoted $\mathcal{H}_A$.

The accessible memory of a quantum query algorithm is initialized to a fixed state. For convenience, on input x we assume the state of the algorithm is $|x\rangle_I|1,0\rangle_Q|0\rangle_W$ where all qubits in the working memory are initialized to 0. The state of the algorithm then evolves through queries, which depend on the input register, and accessible memory operators which do not. We now describe these operations.

We will model a query by a unitary operator where the oracle answer is given in the phase. This operator O is defined by its action on the basis state $|x\rangle|i,p\rangle$ as

$$\mathsf{O} : |x\rangle|i,p\rangle \rightarrow e^{\frac{2\pi \mathbf{i}}{\sigma} p x_i}|x\rangle|i,p\rangle,$$

where $1 \leq i \leq n$ is the index of the queried input variable and $0 \leq p < \sigma$ is the phase multiplier. This operation can be extended to act on the whole space by interpreting it as $\mathsf{O} \times \mathsf{I}_W$, where I_W is the identity operation on the workspace $\mathcal{H}_W$. In the sequel, we will refer to the action of O both on $\mathcal{H}_I \otimes \mathcal{H}_Q$ and the full space $\mathcal{H}_I \otimes \mathcal{H}_Q \otimes \mathcal{H}_W$, and let context dictate which we mean.

For a function with Boolean input $\Sigma_I = \{0,1\}$, the query operator simply becomes

$$\mathsf{O} : |x\rangle|i,p\rangle \rightarrow (-1)^{p x_i}|x\rangle|i,p\rangle,$$

An alternative, perhaps more common, way to model a quantum query is through an operator $\mathsf{O}' : |x\rangle|i,p\rangle \rightarrow |x\rangle|i,(x_i+p) \mod \sigma\rangle$ that encodes the result in a register. These two query models are equivalent, as can be seen by conjugating with the quantum Fourier transform on $|p\rangle$. For our results, it is more convenient to work with the phase oracle.

An accessible memory operator is an arbitrary unitary operation U on the accessible memory $\mathcal{H}_A$. This operation is extended to act on the whole space by interpreting it as $\mathsf{I}_I \otimes \mathsf{U}$, where I_I is the identity operation on the input space $\mathcal{H}_I$. Thus the state of the algorithm on input x after t queries can be written

$$|\phi_x^t\rangle = \mathsf{U}_t \mathsf{O} \mathsf{U}_{t-1} \cdots \mathsf{U}_1 \mathsf{O} \mathsf{U}_0 |x\rangle|1,0\rangle|0\rangle.$$

As the input register is left unchanged by the algorithm, we can decompose $|\phi_x^t\rangle$ as $|\phi_x^t\rangle = |x\rangle|\psi_x^t\rangle$, where $|\psi_x^t\rangle$ is the state of the accessible memory after t queries.

The output of a T-query algorithm on input x is chosen according to a probability distribution which depends on the final state of the accessible memory $|\psi_x^T\rangle$. Namely, the probability that the algorithm outputs some $b \in \Sigma_O$ on input x is $\|\Pi_b|\psi_x^T\rangle\|^2$, for a fixed set of projectors $\{\Pi_b\}$ which are orthogonal and complete, that is, sum to the identity. The ϵ-error quantum query complexity of a function f, denoted $Q_\epsilon(f)$, is the minimum number of queries made by an algorithm which outputs $f(x)$ with probability at least $1-\epsilon$ for every x.

2.2 Progress function

Imagine that we run some quantum algorithm on a superposition of inputs $|\delta\rangle = \sum_{x \in X} \delta_x |x\rangle|1,0\rangle|0\rangle$. The quantum state after t queries is

$$|\Psi^t\rangle = \mathsf{U}_t \mathsf{O} \mathsf{U}_{t-1} \cdots \mathsf{U}_1 \mathsf{O} \mathsf{U}_0 |\delta\rangle = \sum_x \delta_x |x\rangle|\psi_x^t\rangle.$$

The reduced density matrix of the input register is

$$\rho_I^t = \operatorname*{Tr}_{Q,W} |\Psi^t\rangle\langle\Psi^t| = \sum_{x,y} \delta_x \delta_y^* \langle\psi_y^t|\psi_x^t\rangle \cdot |x\rangle\langle y|.$$

We define a progress function in terms of the reduced density matrix of the input register and a special Hermitian matrix Γ, coined the *adversary matrix*. We then present two kinds of adversary method, each using the progress function in a different way to get a quantum query lower bound.

Definition 1 *Let Γ be an $|X| \times |X|$ Hermitian matrix. Let $\langle A, B\rangle = \mathrm{Tr}(A^*B)$. Define the progress function*

$$W^t = \langle \Gamma, \rho_I^t \rangle.$$

Note that W^t is a real number, because both Γ and ρ_I^t are Hermitian.

In the paper, we will use the following matrices.

Definition 2 *Define the following set of $|X| \times |X|$ matrices indexed by $i \in [n]$, $p \in \Sigma_I$, and $z \in \Sigma_O$:*

$$D_i[x,y] = \begin{cases} 1 & x_i \neq y_i \\ 0 & x_i = y_i \end{cases}, \qquad \mathsf{O}_{i,p}[x,x] = e^{\frac{2\pi \mathbf{i}}{\sigma} p x_i}, \qquad \text{and } \mathsf{F}_z[x,x] = \begin{cases} 1 & f(x) = z \\ 0 & f(x) \neq z \end{cases}.$$

D_i's are real (zero-one) symmetric matrices. $\mathsf{O}_{i,p}$'s are diagonal unitary matrices decomposing the query operator $\mathsf{O} = \bigoplus_{i=1}^n \bigoplus_{p \in \Sigma_I} \mathsf{O}_{i,p}$. $\{\mathsf{F}_z\}_{z \in \Sigma_O}$ is a complete set of diagonal orthogonal projectors, that is $\sum_z \mathsf{F}_z = \mathsf{I}$, $\mathsf{F}_{z_1}\mathsf{F}_{z_2} = 0$ for $z_1 \neq z_2$, and $\mathsf{F}_z^2 = \mathsf{F}_z$.

2.3 Additive adversary

In this version of the adversary method, one upper-bounds the difference of the value of the progress function caused by one query. This method is the original adversary method, developed in a series of papers [BBBV97, Amb02, HNS02, BS04, BSS03, Amb06, LM04, Zha05, ŠS06, HLŠ07].

Theorem 1 ([HLŠ07]) *Let Γ be a nonzero $|X| \times |X|$ Hermitian matrix such that $\Gamma[x,y] = 0$ for $f(x) = f(y)$. Consider a quantum algorithm with error probability at most ε and query complexity T. We run it on the superposition of inputs $|\delta\rangle$, where δ is a normalized principal eigenvector of Γ, i.e. corresponding to the spectral norm $\|\Gamma\|$. Then*

1. $W^0 = \|\Gamma\|$
2. $W^t - W^{t+1} \leq 2 \max_i \|\Gamma \circ D_i\|$ *for every time step* $t = 0, 1, \ldots, T-1$
3. $W^T \leq 2(\sqrt{\varepsilon(1-\varepsilon)} + \varepsilon) \cdot \|\Gamma\|$

The third item can be strengthened to $2\sqrt{\varepsilon(1-\varepsilon)}\|\Gamma\|$ if f has Boolean output [HLŠ07].

Corollary 2 ([BSS03, HLŠ07]) *For every sufficiently small ε,*

$$Q_\varepsilon(f) \geq \mathrm{ADV}_\varepsilon(f) \stackrel{\text{def.}}{=} \left(\frac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)} - \varepsilon\right) \max_\Gamma \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}.$$

If all coefficients of the adversary matrix Γ are nonnegative, then Γ corresponds to a hard distribution over input pairs and its principal eigenvector δ to a hard distribution over inputs. The initial value of the progress function W is large, because all scalar products are one in the beginning, and it must decrease a lot. This is because the weight is only put on input pairs evaluating to different outputs, whose scalar product must be low at the end, otherwise one would not be able to distinguish them. This intuition does not tell the whole truth if some coefficients are negative, but the adversary bound still holds.

3 Multiplicative adversary

In this version of the adversary method, one upper-bounds the ratio of the value of the progress function before and after a query. This method is a simplification and generalization of the new adversary method developed by Ambainis [Amb05, AŠW06]. Here, Γ has a different semantics. We require the eigenspaces of Γ corresponding to small eigenvalues to be spanned by vectors (superpositions of inputs) that do not determine

the function value with high probability. The algorithm is then run on a superposition $|\delta\rangle$ corresponding to the smallest eigenvalue (which is typically a uniform superposition of all inputs), and the progress function W is slowly increasing (instead of decreasing) in time. To achieve good success probability, most of the quantum amplitude must move to the higher subspaces.

Theorem 3 *Let Γ be positive definite with smallest eigenvalue 1; then $W^t \geq 1$. Fix a number $1 < \lambda \leq \|\Gamma\|$. Let Π_{bad} be the projector onto the eigenspaces of Γ corresponding to eigenvalues smaller than λ. Assume that $\|\mathsf{F}_z \Pi_{\text{bad}}\|^2 \leq \eta$ for every output letter $z \in \Sigma_O$. Consider a quantum algorithm with success probability at least $\eta + 4\zeta$ and query complexity T. We run it on the superposition of inputs $|\delta\rangle$, where δ is a normalized eigenvector of Γ with $\Gamma\delta = \delta$. Then*

1. $W^0 = 1$
2. $\frac{W^{t+1}}{W^t} \leq \max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\|$, *where* $\Gamma_{i,p} \stackrel{\text{def.}}{=} \mathsf{O}_{i,p}^* \Gamma \mathsf{O}_{i,p}$
3. $W^T \geq \zeta^2 \lambda$

Corollary 4

$$Q_{1-\eta-4\zeta}(f) \geq \text{MADV}_{\eta,4\zeta}(f) \stackrel{\text{def.}}{=} \max_{\Gamma,\lambda} \frac{\log(\zeta^2\lambda)}{\log(\max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\|)}.$$

Proof of Theorem 3(1) Trivial, because $\langle\psi_x^0|\psi_y^0\rangle = 1$ and thus $W^0 = \langle\Gamma, \rho_I^0\rangle = \delta^*\Gamma\delta = 1$. □

Proof of Theorem 3(2) After the $(t+1)$-st query, the quantum state is $|\Psi^{t+1}\rangle = \mathsf{U}_{t+1}\mathsf{O}|\Psi^t\rangle$ and thus

$$\rho_I^{t+1} = \operatorname*{Tr}_{Q,W}(\mathsf{U}_{t+1}\mathsf{O}|\Psi^t\rangle\langle\Psi^t|\mathsf{O}^*\mathsf{U}_{t+1}^*) = \operatorname*{Tr}_{Q,W}(\mathsf{O}|\Psi^t\rangle\langle\Psi^t|\mathsf{O}^*),$$

because the unitary operator U_{t+1} acts as identity on the input register. The oracle operator O only acts on the input register and the query register, hence we can trace out the working memory. Denote $\rho = \text{Tr}_W |\Psi^t\rangle\langle\Psi^t|$ and $\rho' = \mathsf{O}\rho O^*$. Then $\rho_I^t = \text{Tr}_Q(\rho)$ and $\rho_I^{t+1} = \text{Tr}_Q(\rho')$. We re-express the progress function in terms of ρ, ρ'. Define a block-diagonal matrix on $\mathcal{H}_I \otimes \mathcal{H}_Q$:

$$G = \Gamma \otimes \mathsf{I}_n \otimes \mathsf{I}_\sigma = \bigoplus_{i=1}^n \bigoplus_{p\in\Sigma_I} \Gamma.$$

Then

$$\begin{aligned} W^t &= \langle\Gamma, \rho_I^t\rangle = \langle G, \rho\rangle \\ W^{t+1} &= \langle\Gamma, \rho_I^{t+1}\rangle = \langle G, \rho'\rangle = \langle G, \mathsf{O}\rho\mathsf{O}^*\rangle \\ &= \langle\mathsf{O}^*G\mathsf{O}, \rho\rangle = \langle G', \rho\rangle, \end{aligned}$$

where $G' = \mathsf{O}^*G\mathsf{O} = \bigoplus_{i,p} \Gamma_{i,p}$ is a block-diagonal matrix with $\Gamma_{i,p}$'s on the main diagonal.

We upper-bound the change of the progress function as follows. We show that

$$\langle G', \rho\rangle \leq \max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\| \cdot \langle G, \rho\rangle. \tag{3}$$

Since the scalar products $\langle G, \rho\rangle$ and $\langle G', \rho\rangle$ are linear in ρ and mixed states are convex combinations of pure states, it suffices to show this inequality for pure states $\rho = |\rho\rangle\langle\rho|$. Since both Γ and all $\Gamma_{i,p}$'s are positive definite, both G and G' are also positive definite. Let $|\tau\rangle = \sqrt{G}|\rho\rangle$, that is $|\rho\rangle = G^{-\frac{1}{2}}|\tau\rangle$.

$$\begin{aligned} \frac{\langle G', \rho\rangle}{\langle G, \rho\rangle} = \frac{\langle\rho|G'|\rho\rangle}{\langle\rho|G|\rho\rangle} = \frac{\langle\tau|G^{-\frac{1}{2}}G'G^{-\frac{1}{2}}|\tau\rangle}{\langle\tau|\tau\rangle} = \left(\frac{\|\sqrt{G'G^{-1}}|\tau\rangle\|_2}{\|\tau\|_2}\right)^2 \\ \leq \|\sqrt{G'G^{-1}}\|^2 = \|G'G^{-1}\| = \max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\| \end{aligned}$$

We conclude that Eqn. (3) holds for pure states and consequently also for all density matrices. □

Since the spectral norm of $\Gamma_{i,p}\Gamma^{-1}$ is hard to upper-bound, we simplify it to a form similar to the additive adversary.

Lemma 5 *Fix the index of the queried bit i. Assume that Γ and $\mathsf{O}_{i,1}$ are simultaneously block-diagonal in some "basis", that is there exists a complete set of orthogonal projectors $\Pi = \{\Pi_\ell\}_\ell$ such that $\Gamma = \sum_\ell \Gamma^{(\ell)}$ and $\mathsf{O}_{i,1} = \sum_\ell \mathsf{O}_{i,1}^{(\ell)}$, where $\Gamma^{(\ell)}$ denotes $\Pi_\ell\Gamma\Pi_\ell$. Note that since $\mathsf{O}_{i,p} = (\mathsf{O}_{i,1})^p$, all $\mathsf{O}_{i,p}$ are block-diagonal in this basis, too. Then*

$$\|\Gamma_{i,p}\Gamma^{-1}\| = \max_\ell \|\Gamma_{i,p}^{(\ell)}(\Gamma^{(\ell)})^{-1}\| \le 1 + 2\max_\ell \frac{\|\Gamma^{(\ell)} \circ D_i\|}{\lambda_{\min}(\Gamma^{(\ell)})},$$

where $\lambda_{\min}(M)$ denotes the smallest eigenvalue of M.

Corollary 6 *Let $\Gamma \succeq \mathsf{I}$ and $1 < \lambda \le \|\Gamma\|$. Assume that $\|\mathsf{F}_z\Pi_{\text{bad}}\|^2 \le \eta$ for every $z \in \Sigma_O$, where Π_{bad} is the projector onto the eigenspaces of Γ smaller than λ. For a fixed i, block-diagonalize simultaneously Γ and $\mathsf{O}_{i,1}$, and let $\Gamma^{(\ell)}$ denote the ℓ-th block.*

$$\mathrm{MADV}_{\eta,4\zeta}(f) \ge \max_{\Gamma,\lambda} \log(\zeta^2\lambda) \cdot \min_{i,\ell} \frac{\lambda_{\min}(\Gamma^{(\ell)})}{2\|\Gamma^{(\ell)} \circ D_i\|}.$$

Note that for most functions, one typically does not want to apply this statement using the trivial block-diagonalization $\Pi = \{\mathsf{I}\}$ with just one projector onto the whole space. In this case, $\|\Gamma \circ D_i\|$ is way too large compared to $\lambda_{\min}(\Gamma)$ and the final bound is too weak. For some functions, such as unordered search, however, even this approach gives a reasonable bound; see Lemma 7.

Proof of Lemma 5 Denote $Y_{i,p} = \mathsf{O}_{i,p}^* E \mathsf{O}_{i,p}$, where E is the all-ones matrix; then $\Gamma_{i,p} = \mathsf{O}_{i,p}^*\Gamma\mathsf{O}_{i,p} = \Gamma \circ Y_{i,p}$. Note that $Y_{i,0} - \frac{1}{\sigma}\sum_{p=0}^{\sigma-1} Y_{i,p} = D_i$ (by summing a geometrical sequence depending on $x_i - y_i$). Since Γ and all $\mathsf{O}_{i,p}$ are block-diagonal in Π, it follows that $\Gamma_{i,p}$, $\Gamma_{i,p}\Gamma^{-1}$, and $\Gamma \circ D_i$ are block-diagonal in Π, too. Therefore it suffices to compute an upper bound on $\|\Gamma_{i,p}/\Gamma^{-1}\|$ in each subspace of Π separately and take the maximum as the total upper bound. This proves the first part of the lemma that $\|\Gamma_{i,p}\Gamma^{-1}\| = \max_\ell \|\Gamma_{i,p}^{(\ell)}(\Gamma^{(\ell)})^{-1}\|$.

Henceforth, fix the index ℓ of one such subspace and let $\Gamma := \Gamma^{(\ell)}$ denote the matrix projected onto Π_ℓ.

$$\begin{aligned}
\|\Gamma_{i,p}\Gamma^{-1}\| &= \max_{v\in\Pi_\ell} \frac{\|\Gamma_{i,p}\Gamma^{-1}v\|_2}{\|v\|_2} && v = \Gamma w \\
&= \max_{w\in\Pi_\ell} \frac{\|\Gamma_{i,p}w\|_2}{\|\Gamma w\|_2} \\
\frac{\|\Gamma_{i,p}w\|_2}{\|\Gamma w\|_2} &= \frac{\|\Gamma w + (\Gamma_{i,p} - \Gamma)w\|_2}{\|\Gamma w\|_2} \\
&\le 1 + \frac{\|(\Gamma_{i,p} - \Gamma)w\|_2}{\|\Gamma w\|_2} && \|\Gamma w\|_2 \ge \underbrace{\lambda_{\min}(\Gamma)}_{\mu}\|w\|_2 \\
&\le 1 + \frac{1}{\mu}\cdot\frac{\|(\Gamma_{i,p} - \Gamma)w\|_2}{\|w\|_2} && \Gamma_{i,p} - \Gamma = (\Gamma_{i,p} - \Gamma) \circ D_i \\
&= 1 + \frac{1}{\mu}\cdot\frac{\|(\Gamma_{i,p} \circ D_i)w - (\Gamma \circ D_i)w\|_2}{\|w\|_2} && \Gamma_{i,p} = \Gamma \circ Y_{i,p} \\
&\le 1 + \frac{1}{\mu}\cdot\frac{\|(\Gamma \circ Y_{i,p} \circ D_i)w\|_2 + \|(\Gamma \circ D_i)w\|_2}{\|w\|_2} && (\Gamma \circ D_i) \circ Y_{i,p} = \mathsf{O}_{i,p}^*(\Gamma \circ D_i)\mathsf{O}_{i,p} \\
&\le 1 + \frac{\|\mathsf{O}_{i,p}^*(\Gamma \circ D_i)\mathsf{O}_{i,p}\| + \|\Gamma \circ D_i\|}{\mu} && \mathsf{O}_{i,p} \text{ is unitary} \\
&= 1 + 2\frac{\|\Gamma \circ D_i\|}{\lambda_{\min}(\Gamma)},
\end{aligned}$$

which proves the second part of the lemma, because Γ here denotes $\Gamma^{(\ell)}$. □

Proof of Theorem 3(3) At the end of the computation, we measure the input register in the computational basis and the accessible memory according to the output projectors $\{\Pi_b\}$. Denote the outcomes $x \in X$ and $b \in \Sigma_O$. Since the algorithm has good success probability, $f(x) = b$ with probability at least $\eta + 4\zeta$. Let us prove an upper bound on this success probability in terms of the progress function.

Let $\Pi_{\text{good}} = \mathsf{I} - \Pi_{\text{bad}}$ denote the projector onto the orthogonal complement of the bad subspace, coined the good subspace. We upper-bound the success probability in the bad subspace by η and in the good subspace by 1. Consider the final state of the computation $|\Psi^T\rangle$; recall that $\rho_I^T = \text{Tr}_{Q,W} |\Psi^T\rangle\langle\Psi^T|$. Let $|\Psi_{\text{bad}}\rangle = \frac{\Pi_{\text{bad}}|\Psi^T\rangle}{\|\Pi_{\text{bad}}|\Psi^T\rangle\|_2}$, $|\Psi_{\text{good}}\rangle = \frac{\Pi_{\text{good}}|\Psi^T\rangle}{\|\Pi_{\text{good}}|\Psi^T\rangle\|_2}$, and $\beta = \langle\Pi_{\text{good}}, \rho_I^T\rangle = \|\Pi_{\text{good}}|\Psi^T\rangle\|_2^2$. (When using a projector on a larger Hilbert space than defined, we first extend it by a tensor product with identity. For example, $|\Psi_{\text{bad}}\rangle = \frac{(\Pi_{\text{bad}} \otimes \mathsf{I}_A)|\Psi^T\rangle}{\|(\Pi_{\text{bad}} \otimes \mathsf{I}_A)|\Psi^T\rangle\|_2}$, where A is the accessible memory.) Decompose

$$|\Psi^T\rangle = \sqrt{1-\beta}|\Psi_{\text{bad}}\rangle + \sqrt{\beta}|\Psi_{\text{good}}\rangle.$$

Assume for a moment that the final state was $|\Psi_{\text{bad}}\rangle$ instead of $|\Psi^T\rangle$. We measure the accessible memory first and fix the output of the computation $b \in \Sigma_O$, then we trace out the accessible memory completely and end up with a mixed state ρ over the input register (not necessarily equal to ρ_I^T, because we remember b). We then measure the input register according to the projectors $\{\mathsf{F}_z\}$ (set of inputs x such that $f(x) = z$) and test whether $z = b$. Now, for every $z \in \Sigma_O$, including the right result $z = b$,

$$\begin{aligned}
\Pr[\text{obtaining } z] &= \langle \mathsf{F}_z, \rho \rangle && \rho \text{ is only supported on } \Pi_{\text{bad}} \\
&= \langle \mathsf{F}_z, \Pi_{\text{bad}} \rho \Pi_{\text{bad}} \rangle \\
&= \langle \Pi_{\text{bad}} \mathsf{F}_z \Pi_{\text{bad}}, \rho \rangle && \langle A, B \rangle \leq \|A\| \cdot \|B\|_{tr} \\
&\leq \|\Pi_{\text{bad}} \mathsf{F}_z \Pi_{\text{bad}}\| \cdot \|\rho\|_{tr} && \|\rho\|_{tr} = 1 \\
&= \|\Pi_{\text{bad}} \mathsf{F}_z \Pi_{\text{bad}}\| && \mathsf{F}_z = \mathsf{F}_z^2 \\
&= \|\Pi_{\text{bad}} \mathsf{F}_z \mathsf{F}_z \Pi_{\text{bad}}\| && \|AB\| \leq \|A\| \cdot \|B\| \\
&\leq \|\Pi_{\text{bad}} \mathsf{F}_z\| \cdot \|\mathsf{F}_z \Pi_{\text{bad}}\| && \mathsf{F}_z, \Pi_{\text{bad}} \text{ are Hermitian} \\
&= \|\mathsf{F}_z \Pi_{\text{bad}}\|^2 \\
&\leq \eta.
\end{aligned}$$

Therefore the success probability of the algorithm would be at most η, had the input register been in the state $|\Psi_{\text{bad}}\rangle$. The real output state is $|\Psi^T\rangle$. Since the trace distance of these two states is

$$\||\Psi^T\rangle - |\Psi_{\text{bad}}\rangle\|_2 \leq (1 - \sqrt{1-\beta}) + \sqrt{\beta} \leq 2\sqrt{\beta},$$

by [BV97], the success probability on $|\Psi^T\rangle$ could be at most $\eta + 4\sqrt{\beta}$. On the other hand, we assumed that the algorithm has success probability at least $\eta + 4\zeta$, hence $\beta \geq \zeta^2$. The progress function at the end takes value

$$W^T = \langle \Gamma, \rho_I^T \rangle \geq \langle \lambda \cdot \Pi_{\text{good}}, \rho_I^T \rangle = \beta\lambda \geq \zeta^2\lambda,$$

which is what we had to prove. □

4 Applications

In this section, we reprove all known bounds obtained by the subspace-analysis technique of Ambainis. We only consider functions with Boolean input. The input oracle rotates the phase by a factor of $(-1)^{px_i}$ and the only nontrivial case is $p = 1$. We thus omit p and write just O_i, Γ_i instead of $\mathsf{O}_{i,1}, \Gamma_{i,1}$.

4.1 Search

Let $X = \{x \in \{0,1\}^n : |x| = 1\}$ and $\mathrm{Search}_n(x) = i$ such that $x_i = 1$. In other words, there is exactly one 1 in an n-bit string and we have to find it. One can quickly estimate the multiplicative adversary bound as follows.

Lemma 7 $\mathrm{MADV}_{n^{-1},4\zeta}(\mathrm{Search}_n) = \Omega(\zeta^2\sqrt{n})$.

Proof Let $q > 1$ be a constant whose value we fix later. Define the following unit vectors: $v = \frac{1}{\sqrt{n}}(1,\ldots,1)$ and $v_i = \frac{1}{\sqrt{n(n-1)}}(1,\ldots,1,1-n,1,\ldots,1)$ with $1-n$ on the i-th position. Note that $v \perp v_i$, but $v_i \not\perp v_j$ for $i \neq j$. Define the following adversary matrix:

$$\Gamma = (1-q)|v\rangle\langle v| + q\mathsf{I}, \tag{4}$$

where I is the identity matrix. Γ has two eigenspaces: $\Gamma v = v$, and $\Gamma v_i = q v_i$. The success probability in the subspace of v is $\eta = 1/n$. Let $\lambda = \|\Gamma\| = q$.

We apply Corollary 6 with trivial block-diagonalization $\Pi = \{\mathsf{I}\}$. Then $\lambda_{\min}(\Gamma) = 1$. $\Gamma \circ D_i$ consists of an $1 \times (n-1)$ block $\frac{1-q}{n}(1,\ldots,1)$ and its adjoint, hence $\|\Gamma \circ D_i\| = \sqrt{n-1}\cdot(q-1)/n < (q-1)/\sqrt{n}$. Hence

$$\mathrm{MADV}_{n^{-1},4\zeta}(\mathrm{Search}_n) \geq \frac{\log(\zeta^2 q)}{2(q-1)}\sqrt{n}. \tag{5}$$

We set $q = 2/\zeta^2$ to make the logarithm positive. □

It turns out that the rough analysis in the previous lemma loses a quadratic factor in the success probability. Let us compute exactly the eigenvalues of $\Gamma_i\Gamma^{-1}$. Thanks to the symmetry, it is sufficient to only consider one case $i = 1$.

Theorem 8 $\mathrm{MADV}_{n^{-1},4\zeta}(\mathrm{Search}_n) = \Omega(\zeta\sqrt{n})$.

Proof We use the same adversary matrix Eqn. (4). We could compute $\Gamma_1\Gamma^{-1}$ explicitly, but we instead choose to demonstrate the block-diagonalization process. Define a complete set of orthogonal projectors $\Pi = \{\Pi_2, \Pi_{\mathrm{triv}}\}$ with a 2-dimensional subspace $\Pi_2 = |v\rangle\langle v| + |v_1\rangle\langle v_1|$ and its orthogonal complement $\Pi_{\mathrm{triv}} = \mathsf{I} - \Pi_2$. Define $|w_2\rangle = \Pi_{\mathrm{triv}}|v_2\rangle = |v_2\rangle - \langle v_1|v_2\rangle|v_1\rangle = \sqrt{\frac{n}{(n-1)^3}}(0, 2-n, 1, \ldots, 1)$ for which $v_1 \perp w_2$, and define similarly $w_3, \ldots, w_n$. Then Π_{triv} is spanned by $w_2, \ldots, w_n$. $\mathsf{O}_1 w_i = w_i$ implies $\Pi_{\mathrm{triv}}\mathsf{O}_1 = \Pi_{\mathrm{triv}}$. Since O_1 is unitary, O_1 is block-diagonal in Π. Now,

$$\Pi_2\Gamma = |v\rangle\langle v| + q|v_1\rangle\langle v_1|$$

and $\Pi_{\mathrm{triv}}\Gamma = q(\mathsf{I} - |v\rangle\langle v| - |v_1\rangle\langle v_1|) = q\Pi_{\mathrm{triv}}$, and hence Γ is also block-diagonal in Π. We now analyze the diagonal blocks of $\Gamma_1\Gamma^{-1}$ in this "basis". We already know that $\Pi_{\mathrm{triv}}\mathsf{O}_1 = \Pi_{\mathrm{triv}}$ and hence $\Gamma_1\Gamma^{-1} = \mathsf{I}$ on the trivial subspace. It remains to examine the non-trivial subspace Π_2.

In the orthonormal basis $\{|v\rangle, |v_1\rangle\}$,

$$\Gamma = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}, \qquad \mathsf{O}_1 = \frac{1}{n}\begin{pmatrix} n-2 & 2\sqrt{n-1} \\ 2\sqrt{n-1} & 2-n \end{pmatrix},$$

and the eigenvalues of $\Gamma_1\Gamma^{-1} = \mathsf{O}_1^*\Gamma\mathsf{O}_1\Gamma^{-1}$ are $1 \pm \frac{2(q-1)}{\sqrt{qn}} + O(\frac{1}{n})$. Hence $\|\Gamma_1\Gamma^{-1}\| \approx 1 + \frac{2(q-1)}{\sqrt{qn}}$, and by Corollary 4, the multiplicative adversary bound is

$$\mathrm{MADV}_{n^{-1},4\zeta}(\mathrm{Search}_n) \geq \frac{\log(\zeta^2\lambda)}{\log(1 + 2(q-1)/\sqrt{qn})} \geq \frac{\log(\zeta^2 q)\sqrt{q}}{2(q-1)}\sqrt{n},$$

where we have used that $\log(1+x) \leq x$. This is by a factor of $\sqrt{q}$ larger than the bound given by Eqn. (5). Again, we set $q = 2/\zeta^2$ and finish the proof. □

4.2 t-fold search

This is a generalization of the search problem, where we have to find t ones. Let $X = \{x \in \{0,1\}^n : |x| = t\}$ and $\mathrm{Search}_{t,n}(x) = J$ such that $J \subseteq [n]$, $|J| = t$, and $x_J = 1$. The additive adversary implies that the bounded-error quantum query complexity of $\mathrm{Search}_{t,n}$ is $\Omega(\sqrt{tn})$. The multiplicative adversary gives the same bound even for an exponentially small success probability! A part of this section is based on the analysis by Ambainis [Amb05] translated to our framework.

4.2.1 Combinatorial matrices

The additive adversary matrix for $\mathrm{Search}_{t,n}$ is very simple [Amb02]: $\Gamma_{\mathrm{add}} = J_{n,t,t-1}$, where $J_{n,t,d}$ is a zero-one $\binom{n}{t} \times \binom{n}{t}$ matrix indexed by subsets of $[n]$ of size t such that $J_{n,t,d}[x,y] = 1$ iff $|x \cap y| = d$. The intuition is that we only put the weight on input pairs that are hardest to distinguish (because they have the smallest possible Hamming distance).

The matrices $J_{n,t,d}$ are called *combinatorial matrices* [Knu03]. For fixed n, t, the matrices $J_{n,t,d}$ commute and they thus all diagonalize in the same basis. This basis can be written in the bracket syntax as follows.

Definition 3 ([Amb05]) *Let Π_{S_j} denote the projector onto the subspace S_j, where $S_j = T_j \cap T_{j-1}^{\perp}$, and T_j is the space spanned by*

$$|\psi_J\rangle = \frac{1}{\sqrt{\binom{n-j}{t-j}}} \sum_{\substack{x:|x|=t \\ x_J=1}} |x\rangle \qquad \text{for } J \subseteq [n] \text{ with } |J| = j.$$

Intuitively, $|\psi_J\rangle$ is a superposition of input states compatible with fixing the input bits from J to 1, T_j is the subspace where we "know" at most j ones, and S_j is the subspace where we "know" exactly j ones. Denote $|\tilde{\psi}_J\rangle = \Pi_{T_{j-1}^{\perp}} |\psi_J\rangle$. Note that these projected states are neither normalized nor orthogonal for $j > 0$. Denote $|\ddot{\psi}_J\rangle = \frac{|\tilde{\psi}_J\rangle}{\|\tilde{\psi}_J\|_2}$. Note that S_j is spanned by $|\ddot{\psi}_J\rangle$.

Claim 9 ([Knu03, Eqn. (4.4)]) *$J_{n,t,d}$ has eigenspaces $\{S_j\}_{j=0}^{t}$ with eigenvalues*

$$e_d(j) = \sum_{r=0}^{j} (-1)^{j-r} \binom{j}{r} \binom{t-r}{d-r} \binom{n-t-j+r}{t-d-j+r}.$$

The eigenvalues of $J_{n,t,t-1}$ can be expressed explicitly as

$$e_{t-1}(j) = (n-t-j)(t-j+1) - (n-t). \tag{6}$$

4.2.2 Multiplicative adversary matrix for constant ζ

Let us utilize the knowledge of the best known additive adversary matrix $\Gamma_{\mathrm{add}} = J_{n,t,t-1} = \sum_{j=0}^{t} e_{t-1}(j)\, S_j$ to design a good multiplicative adversary matrix for the same function. Note that e_{t-1} is a quadratic polynomial in j, decreasing in the range of interest $j \in [0,t]$, and $e_{t-1}(t) = -t$. It follows that, assuming $t < \frac{n}{2}$, $\Gamma' = \Gamma_{\mathrm{add}} + (n-t)I$ is a positive definite matrix with smallest eigenvalue $n - 2t$ and principal eigenvalue $(n-t)(t+1)$.

We want to assign higher weights to higher eigenspaces (because the success probability is higher there), whereas the eigenvalues of Γ' are decreasing in j. Let us thus compute its inverse and renormalize the outcome. We will show that

$$\Gamma'' = \|\Gamma'\| \cdot (\Gamma')^{-1} = (n-t)(t+1)\Big(\Gamma_{\mathrm{add}} + (n-t)I\Big)^{-1} \tag{7}$$

gives rise to a good multiplicative adversary matrix for $\mathrm{Search}_{t,n}$, in the range $\zeta \geq 0.78$ and exponentially small η. The only change we have to do to get this bound, is *compressing* the high eigenspaces of Γ'' by

decreasing their eigenvalues. Unfortunately, $4\zeta > 1$, which makes the final lower bound trivial. However, we show in the next section how to amplify ζ to roughly ζ^t and thus get a lower bound for an exponentially small success probability.

Theorem 10 *For every $t \le \frac{n}{4e}$ and $\zeta \ge 0.78$, $\mathrm{MADV}_{2^{-t/2},4\zeta}(\mathrm{Search}_{t,n}) = \Omega(\sqrt{tn})$.*

Proof Denote the eigenvalues of Γ'' by $q_j = \frac{(n-t)(t+1)}{e_{t-1}(j)+(n-t)} = \frac{(n-t)(t+1)}{(n-t-j)(t-j+1)}$ and set $\lambda = q_{t/2}$. Take the matrix $\Gamma'' = \sum_{j=0}^{t} q_j \Pi_{S_j}$ from Eqn. (7) and change it to

$$\Gamma = \sum_{j=0}^{t/2-1} q_j \Pi_{S_j} + \lambda \sum_{j=t/2}^{t} \Pi_{S_j}, \tag{8}$$

i.e., *compress* the eigenspaces for $j \ge t/2$ into one eigenspace with the lowest eigenvalue among them.

Block-diagonalization of Γ and $\mathsf{O}_{i,p}$ [Amb05] Thanks to the symmetry, it is sufficient to only consider the case $i = 1$ of querying the first input bit. As we say above, the only nontrivial case is $p = 1$. We present a complete set of orthogonal projectors Π in which both Γ and O_1 are block-diagonal. Let

$$|\psi_J^b\rangle = \frac{1}{\sqrt{\binom{n-j-1}{t-j-b}}} \sum_{\substack{x:|x|=t \\ x_1=b \\ x_J=1}} |x\rangle \qquad \text{for } J \subseteq [n] \text{ such that } 1 \notin J$$

$$|\tilde{\psi}_J^b\rangle = \Pi_{T_{j-1,b}^{\perp}} |\psi_J^b\rangle \qquad \text{with } T_{j,b} \text{ spanned by } |\psi_J^b\rangle \text{ with } |J| = j$$

$$|\ddot{\psi}_J^b\rangle = \frac{|\tilde{\psi}_J^b\rangle}{\|\tilde{\psi}_J^b\|_2}$$

Let $S_{j,b} = T_{j,b} \cap T_{j-1,b}^{\perp}$. Then the following holds:

- Let $|\ddot{\psi}_J^{a,b}\rangle$ denote the vector $a|\ddot{\psi}_J^0\rangle + b|\ddot{\psi}_J^1\rangle$. Let

$$\alpha'_j = \sqrt{\frac{n-t}{n-j}} \|\tilde{\psi}_J^0\|_2 \qquad \beta'_j = \sqrt{\frac{t-j}{n-j}} \|\tilde{\psi}_J^1\|_2$$

$$\alpha_j = \frac{\alpha'_j}{\sqrt{(\alpha'_j)^2 + (\beta'_j)^2}} \qquad \beta_j = \frac{\beta'_j}{\sqrt{(\alpha'_j)^2 + (\beta'_j)^2}} \tag{9}$$

  We also denote them α, β if the index j is clear from the context. Note that $\alpha^2 + \beta^2 = 1$. Then $|\ddot{\psi}_J^{\alpha,\beta}\rangle \in S_j$ and $|\ddot{\psi}_J^{\beta,-\alpha}\rangle \in S_{j+1}$ [AŠW06, Claim 15]. These two new vectors span the same subspace as $|\ddot{\psi}_J^0\rangle$ and $|\ddot{\psi}_J^1\rangle$.

- [AŠW06, Claim 16] $S_{j,0}$ and $S_{j,1}$ have the same dimension and the mapping

$$M'|0x_2 \dots x_n\rangle \to \sum_{\ell:x_\ell=1} |1x_2 \dots x_{\ell-1} 0 x_{\ell+1} \dots x_n\rangle$$

  is a multiple $M' = c_j \mathsf{M}_j$ of some unitary operation on $S_{j,0} \to S_{j,1}$ that maps $\mathsf{M}_j : |\ddot{\psi}_J^0\rangle \to |\ddot{\psi}_J^1\rangle$.

- Pick any orthonormal basis $\{|\varphi_{j,\ell}\rangle\}_\ell$ for each $S_{j,0}$ (the defining basis $|\ddot{\psi}_J^0\rangle$ is not orthogonal). For $j < t$, define projectors $\Pi_{j,\ell} = |\varphi_{j,\ell}\rangle\langle\varphi_{j,\ell}| + \mathsf{M}_j|\varphi_{j,\ell}\rangle\langle\varphi_{j,\ell}|\mathsf{M}_j^*$. Note that if some $|\varphi_{j,\ell}\rangle = |\ddot{\psi}_J^0\rangle$, then

$$\Pi_{j,\ell} = |\ddot{\psi}_J^0\rangle\langle\ddot{\psi}_J^0| + |\ddot{\psi}_J^1\rangle\langle\ddot{\psi}_J^1| = |\ddot{\psi}_J^{\alpha,\beta}\rangle\langle\ddot{\psi}_J^{\alpha,\beta}| + |\ddot{\psi}_J^{\beta,-\alpha}\rangle\langle\ddot{\psi}_J^{\beta,-\alpha}| \tag{10}$$

due to the basis change mentioned in the first item above. Thus $\Pi_j = \{\Pi_{j,\ell}\}_\ell$ is a complete set of orthogonal projectors for $S_{j,0} \oplus S_{j,1}$, or, equivalently, for the subspace of $S_j \cup S_{j+1}$ spanned by $|\tilde{\psi}_J\rangle$ and $|\tilde{\psi}_{J\cup\{1\}}\rangle$ with $|J| = j$ and $1 \notin J$. It follows that

$$\Pi = \underbrace{\{\Pi_{j,\ell}\}_{j,\ell}}_{\text{2-dim projectors}} \cup \underbrace{\{|\varphi_{t,\ell}\rangle\langle\varphi_{t,\ell}|\}_\ell}_{\text{trivial subspace } S_{t,0}}$$

is a complete set of orthogonal projectors for the whole input space T_t.

Let us verify that Π indeed block-diagonalizes Γ and O_1. To compute the images of the basis states of each projector $\Pi_{j,\ell}$, we use a double decomposition like in Eqn. (10). First, since $|\varphi_{j,\ell}\rangle \in S_{j,0}$ and $\mathsf{M}_j|\varphi_{j,\ell}\rangle \in S_{j,1}$, $\mathsf{O}_1|\varphi_{j,\ell}\rangle = |\varphi_{j,\ell}\rangle$ and $\mathsf{O}_1\mathsf{M}_j|\varphi_{j,\ell}\rangle = -\mathsf{M}_j|\varphi_{j,\ell}\rangle$, hence O_1 is block-diagonal in Π. Second, if we denote $|\varphi^{a,b}_{j,\ell}\rangle = a|\varphi_{j,\ell}\rangle + b\mathsf{M}_j|\varphi_{j,\ell}\rangle$, then $|\varphi^{\alpha,\beta}_{j,\ell}\rangle \in S_j$ and $|\varphi^{\beta,-\alpha}_{j,\ell}\rangle \in S_{j+1}$, because both $|\varphi_{j,\ell}\rangle$ and $\mathsf{M}_j|\varphi_{j,\ell}\rangle$ are just linear combinations with the same coefficients of states $|\ddot{\psi}^0_J\rangle$ and $|\ddot{\psi}^1_J\rangle$ respectively. We conclude that $\Gamma|\varphi^{\alpha,\beta}_{j,\ell}\rangle = q_j|\varphi^{\alpha,\beta}_{j,\ell}\rangle$ and $\Gamma|\varphi^{\beta,-\alpha}_{j,\ell}\rangle = q_{j+1}|\varphi^{\beta,-\alpha}_{j,\ell}\rangle$, hence Γ is also block-diagonal in Π.

Eigenvalues of $\Gamma_1\Gamma^{-1}$ on $\Pi_{j,\ell}$ Consider the orthonormal basis $B_1 = \{|\varphi_{j,\ell}\rangle, \mathsf{M}_j|\varphi_{j,\ell}\rangle\}$ of $\Pi_{j,\ell}$. Let $\mathsf{U} = \left(\begin{smallmatrix}\alpha & \beta\\ \beta & -\alpha\end{smallmatrix}\right)$ denote the self-adjoint unitary operator changing the basis from $B_2 = \{|\varphi^{\alpha,\beta}_{j,\ell}\rangle, |\varphi^{\beta,-\alpha}_{j,\ell}\rangle\}$ to B_1. Then, in the basis B_1,

$$\begin{aligned}\Gamma_1\Gamma^{-1}\Pi_{j,\ell} &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \underbrace{\mathsf{U}\begin{pmatrix}q_j & 0\\ 0 & q_{j+1}\end{pmatrix}\mathsf{U}^*}_{\Gamma} \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \underbrace{\mathsf{U}\begin{pmatrix}q_j^{-1} & 0\\ 0 & q_{j+1}^{-1}\end{pmatrix}\mathsf{U}^*}_{\Gamma^{-1}}\\ &= \left(\left(1 + 2\alpha^2\beta^2\frac{(q-1)^2}{q}\right)\mathsf{I} + 2\alpha\beta\frac{q-1}{q}\begin{pmatrix}0 & \alpha^2+\beta^2 q\\ \beta^2+\alpha^2 q & 0\end{pmatrix}\right),\end{aligned}$$

where $q = \frac{q_{j+1}}{q_j}$ is the ratio of two consecutive eigenvalues of Γ''. Using Eqn. (6) from Claim 9 and $j+1 \le t \le \frac{n}{2} - 1$,

$$\begin{aligned} q = \frac{q_{j+1}}{q_j} &= \frac{e_{t-1}(j) + (n-t)}{e_{t-1}(j+1) + (n-t)}\\ &= 1 + \frac{n-2j}{(n-t-j-1)(t-j)}\\ 1 + \frac{1}{t-j} \le q &\le 1 + \frac{2}{t-j}. \end{aligned} \tag{11}$$

A straightforward calculation shows that $\Gamma_1\Gamma^{-1}\Pi_{j,\ell}$ has eigenvalues

$$\begin{aligned} &1+2\alpha^2\beta^2\frac{(q-1)^2}{q} \pm 2\alpha\beta\frac{q-1}{q}\sqrt{(\alpha^2+\beta^2 q)(\beta^2+\alpha^2 q)}\\ &\le 1 + 2\alpha\beta(q-1) + 2\alpha^2\beta^2(q-1)^2\\ &\le 1 + (2+o(1))\alpha\beta(q-1). \end{aligned} \tag{12}$$

where we have used that $q \ge 1$ and $\alpha^2 + \beta^2 = 1$. (The right expression can be strengthened by a factor of $\sqrt{q}$ for $q = O(\frac{n}{t})$ to get an improvement like in Theorem 8, but we won't need it here.)

To illustrate the bound in the full range of j, assume for a moment a weaker bound $j < t$ instead of $j < \frac{t}{2}$, i.e., forget about the compression of high eigenspaces. We use the expressions $\alpha \le 1$ and $\beta = \sqrt{\frac{t-j}{n-2j}}$ [AŠW06, Claim 19], which easily follow from the (non-trivial) computation of $\|\tilde{\psi}^b_J\|_2 = \sqrt{\frac{(n-t+b-1)^{\underline{j}}}{(n-j)^{\underline{j}}}}$ [AŠW06,

Claim 18], and the bound $q \leq 1 + \frac{2}{t-j}$ from Eqn. (11) above. We obtain

$$\|\Gamma_1 \Gamma^{-1} \Pi_{j,\ell}\| \leq 1 + \frac{4 + o(1)}{\sqrt{(t-j)(n-2j)}}.$$

Note that the bound gets extremely weak for $j \to t$. Since we compress the high eigenspaces for $j \geq \frac{t}{2}$, the norm can be upper-bounded by $1 + 8/\sqrt{tn}$ instead of just $O(1)$.

Eigenvalues of $\Gamma_1\Gamma^{-1}$ on the trivial subspace Let us revisit the trivial subspace $S_{t,0}$ and make sure that the block-diagonalization is right there, too. We claim that $S_{t,0} \subseteq S_t$. Since $|\psi_J^0\rangle = |\psi_J\rangle$ for $|J| = t$ and $1 \notin J$, we get $T_{t,0} \subseteq T_t$, and thus it suffices to prove $S_t = T_{t,0} \cap T_{t-1,0}^{\perp} \subseteq T_{t-1}^{\perp}$. It holds that $T_{t,0} \subseteq T_{t-1,1}^{\perp}$ due to a different value of the first input bit. Also, we know that $T_j \subseteq T_{j,0} \oplus T_{j,1}$, hence $T_{j,0}^{\perp} \cap T_{j,1}^{\perp} \subseteq T_j^{\perp}$ and the proof is finished.

Let $|w\rangle \in S_{t,0}$. $|w\rangle$ is an eigenvector of Γ, because it lies in S_t. Since $\mathsf{O}_1|w\rangle = |w\rangle$, we conclude that $\Gamma_1\Gamma^{-1}|w\rangle = |w\rangle$ and $S_{t,0}$ is indeed a trivial subspace.

Upper-bounding η [Amb05] Since $\lambda = q_{t/2}$, we have to upper-bound $\|\mathsf{F}_z|\varphi\rangle\|_2^2 \leq \eta$ for all $|\varphi\rangle \in T_{t/2}$. Since the dimension of $T_{t/2}$ is $\binom{n}{t/2}$ and the number of possible outcomes is $\binom{n}{t}$, using [Nay99], the success probability is at most $\eta \leq \binom{n}{t/2}/\binom{n}{t}$. Using the bounds $(\frac{n}{k})^k \leq \binom{n}{k} \leq (e\frac{n}{k})^k$ and assuming $t \leq \frac{n}{4e}$,

$$\eta \leq \frac{\binom{n}{t/2}}{\binom{n}{t}} \leq \frac{(2e\frac{n}{t})^{t/2}}{(\frac{n}{t})^t} = \left(\frac{2et}{n}\right)^{t/2} \leq 2^{-t/2}.$$

By being more careful, one can prove an exponentially small upper bound on η for all $t \leq \frac{n}{2}$. This is the second reason why we compress the high eigenspaces—we would not be able to get an exponentially small upper bound on η otherwise.

Multiplicative adversary bound Since $\lambda = q_{t/2} \geq (1 + \frac{1}{t})^{t/2} \approx \sqrt{e}$ by Eqn. (11) and $\|\Gamma_1\Gamma^{-1}\| = \max_j \|\Gamma_1\Gamma^{-1}\Pi_{j,\ell}\|$, by Corollary 4, the multiplicative adversary bound for $\zeta \geq 0.78$ (to make the logarithm in the numerator positive) is

$$\mathrm{MADV}_{\eta,4\zeta}(\mathrm{Search}_{t,n}) \geq \frac{\log(0.78^2\sqrt{e})}{\log(1 + 8/\sqrt{tn})} > \frac{0.003077}{8/\sqrt{tn}} > \frac{\sqrt{tn}}{2600}.$$

(This bound can be improved to $\frac{1}{20}\sqrt{tn}$ for $\zeta \geq 0.96$.) □

4.2.3 Multiplicative adversary matrix for exponentially small ζ

In this section, we show how to improve the parameter ζ of the multiplicative adversary matrix Γ for $\mathrm{Search}_{t,n}$ to roughly ζ^t, while preserving the bound. The basic idea is to use the matrix power Γ^t instead of Γ.

Theorem 11 *For every $t \leq \frac{n}{4e}$, $\mathrm{MADV}_{2^{-t/2},e^{-t/8}}(\mathrm{Search}_{t,n}) = \Omega(\sqrt{tn})$.*

Proof We use the multiplicative adversary matrix Γ^t, where Γ comes from Eqn. (8), and $\lambda = q_{t/2}^t$. Since all eigenvalues of Γ are just raised to the power of t, Γ^t is positive definite with smallest eigenvalue 1. Most of the proof, such as the common block-diagonalization of Γ^t and $\mathsf{O}_{i,p}$, upper-bounding η, and the symbolic computation of eigenvalues of $\mathsf{O}_{i,p}^*\Gamma^t\mathsf{O}_{i,p}\Gamma^{-t}$ on $\Pi_{j,\ell}$, are conducted in the same way as in Theorem 10. We recompute the upper bound on the spectral norm of a sub-matrix in Eqn. (12), changing $q := q^t$, as follows:

$$\|\mathsf{O}_{i,p}^*\Gamma^t\mathsf{O}_{i,p}\Gamma^{-t}\Pi_{j,\ell}\| \leq 1 + (2 + o(1))\alpha\beta(q^t - 1) \qquad \alpha \leq 1,\ \beta \leq \sqrt{\frac{t}{n}},\ q^t \leq e^4 \text{ for } j \leq \frac{t}{2}$$
$$< 1 + 108\sqrt{\frac{t}{n}}.$$

Since $\log(\lambda) = t\log(q_{t/2}) \geq t\log\sqrt{e} = \frac{t}{2}$, the multiplicative adversary bound is

$$\mathrm{MADV}_{\eta,4\zeta}(\mathrm{Search}_{t,n}) \geq \frac{\log(\zeta^2)+\frac{t}{2}}{\log(1+108\sqrt{t/n})} \geq \frac{t/4}{108\sqrt{t/n}} = \frac{\sqrt{tn}}{432},$$

if $\zeta \geq e^{-t/8}$. □

4.2.4 Other possible multiplicative adversary matrices

Let us conclude this section with a few remarks. Ambainis [Amb05] in his proof (and also we, in the previous versions of this paper) used a different multiplicative adversary matrix:

$$\Gamma = \sum_{j=0}^{t/2-1} q^j \Pi_{S_j} + \sum_{j=t/2}^{t} q^{t/2} \Pi_{S_j},$$

where q is a fixed constant, i.e., each ratio of two consecutive eigenvalues of Γ is equal. It turns out that one has a lot of freedom in this respect and almost any matrix with this ratio close to a constant would give a good bound. We have chosen to use $\Gamma \sim (\Gamma_{\mathrm{add}})^{-t}$ to demonstrate the relationship between the additive adversary matrix and the multiplicative adversary matrix. Note that the additive term $(n-t)I$ in Eqn. (7) is not really necessary, because the high eigenspaces of Γ'' are compressed out and it thus does not matter what their original eigenvalues were. It would be nice if one could prove a simpler upper bound on $\Gamma_1\Gamma^{-1}$ using the explicit expression $\Gamma \sim J^{-t}_{n,t,t-1}$, instead of analyzing the complete structure of the eigenspaces. Is it true for other functions that one can take $\Gamma^{-1}_{\mathrm{add}}$ as a good starting point for the multiplicative adversary matrix?

The powering trick from Theorem 11, lowering the ζ parameter to ζ^t, is applicable to all functions, as long as the spectral norms of the blocks are of the form $1+c_1(q-1)$ with the ratio of eigenvalues $q = 1+\frac{c_2}{t}$. The multiplicative adversary bound given by Γ is $\geq \log(\lambda)\cdot t/(c_1c_2)$, and the one given by Γ^t is $\geq t\log(\lambda)/(c_1e^{c_2})$, which is not much smaller is c_2 is not too large. We are not aware of any other application of this principle, mainly because we do not know the optimal multiplicative adversary matrix for any non-symmetric function.

4.3 t-threshold function

The decision version of the t-fold search problem is the t-threshold function $X = \{x \in \{0,1\}^n : |x| \in \{t-1,t\}\}$ and $\mathrm{Threshold}_{t,n}(x) = |x| - t + 1$. Here one can always achieve success probability $1/2$ by random guess, hence we want to upper-bound the bias from $1/2$. The analysis in this section is based on Ambainis's method [AŠW06] translated to our framework.

Theorem 12 ([AŠW06]) $\mathrm{MADV}_{1/2,4\zeta}(\mathrm{Threshold}_{t,n}) = \Omega(\zeta^2\sqrt{tn})$.

One may think that the true bound is $\Omega(\zeta\sqrt{tn})$, however we are unable to prove it using this method. It is quite hard to analyze the 4×4 matrix in the following proof exactly, and we rather use the simpler bound from Corollary 6, which loses exactly this quadratic factor in Lemma 7. We tried to do exact calculations in Mathematica, but they seem to give the same bound $\Omega(\zeta^2\sqrt{tn})$ even when using Corollary 4.

Proof (sketch) We conduct the proof similarly to Theorem 10, but now we use eigenspaces spanned by uniform superpositions of *both* $(t-1)$-weight and t-weight strings. Define the following adversary matrix with $q = 1+\frac{4\log(2/\zeta)}{t}$ and $\lambda = q^{t/2}$:

$$\Gamma = \underbrace{\sum_{j=0}^{t/2-1} q^j \Pi_{S_{j,+}}}_{\text{bad}} + q^{t/2} \underbrace{\left(\sum_{j=t/2}^{t-1} \Pi_{S_{j,+}} + \sum_{j=0}^{t} \Pi_{S_{j,-}}\right)}_{\text{good}}, \tag{13}$$

where $S_{j,\pm}$ is spanned by $|\ddot{\psi}_{J,\pm}\rangle = \frac{1}{\sqrt{2}}(|\ddot{\psi}_{J,0}\rangle \pm |\ddot{\psi}_{J,1}\rangle)$,

$$|\psi_{J,a}\rangle = \frac{1}{\sqrt{\binom{n-j}{t-1+a-j}}} \sum_{\substack{x:|x|=t-1+a \\ x_J=1}} |x\rangle,$$

and the tilde and double-dot states are defined as usual.

Let us explain the intuition behind this construction. We have to put all minus subspaces inside the good subspace of Γ, otherwise some $|v\rangle = |\ddot{\psi}_{J,0}\rangle = \frac{1}{\sqrt{2}}(|\ddot{\psi}_{J,+}\rangle + |\ddot{\psi}_{J,-}\rangle)$, for which $\|\mathsf{F}_0|v\rangle\|_2 = 1$, lies in $S_{j,+} \oplus S_{j,-} \subseteq T_{\text{bad}}$, and the success probability in the bad subspaces could only be upper-bounded by the trivial $\eta = 1$. This way, all states from bad subspaces lie inside $T_{t/2,+}$ and $\eta = 1/2$. On the other hand, we mark the plus subspaces above $j \geq t/2$ as good instead of bad, because it allows us to prove a stronger bound on the denominator. We do not lose much in the numerator.

Block-diagonalization of Γ and O_1 Like in the proof of Theorem 10, we naturally decompose the basis states $|\ddot{\psi}_{J,a}\rangle$ with $1 \notin J$ onto $|\ddot{\psi}_{J,a,b}\rangle$ by fixing the first input bit to b. For the same reasons, some linear combinations of these states lie in $S_{j,\pm}$ and $S_{j+1,\pm}$. In particular, if for a $v = (v_{00}, v_{01}, v_{10}, v_{11})$ we let $|\ddot{\psi}^v_J\rangle$ denote $v_{00}|\ddot{\psi}_{J,0,0}\rangle + v_{01}|\ddot{\psi}_{J,0,1}\rangle + v_{10}|\ddot{\psi}_{J,1,0}\rangle + v_{11}|\ddot{\psi}_{J,1,1}\rangle$, then $\Gamma|\ddot{\psi}^v_J\rangle = |\ddot{\psi}^w_J\rangle$ with $w = \mathsf{U}G_j\mathsf{U}^*v$ [AŠW06, Claim 17], where

$$\mathsf{U} = \frac{1}{\sqrt{2}}\begin{pmatrix} \alpha_0 & \beta_0 & \alpha_0 & \beta_0 \\ \beta_0 & -\alpha_0 & \beta_0 & -\alpha_0 \\ \alpha_1 & \beta_1 & -\alpha_1 & -\beta_1 \\ \beta_1 & -\alpha_1 & -\beta_1 & \alpha_1 \end{pmatrix}, \qquad G_j = \begin{pmatrix} q^j & 0 & 0 & 0 \\ 0 & q^{j+1} & 0 & 0 \\ 0 & 0 & q^{t/2} & 0 \\ 0 & 0 & 0 & q^{t/2} \end{pmatrix}, \qquad \mathsf{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

and α_a, β_a for an $a \in \{0,1\}$ (and an implicit index j) are defined by Eqn. (9) with the threshold value $t := t - 1 + a$. In other words, the columns of U are vectors v that put $|\ddot{\psi}^v_J\rangle$ inside $S_{j,+}, S_{j+1,+}, S_{j,-}, S_{j+1,-}$, respectively. Furthermore, the subspaces $S_{j,a,b}$ for $a, b \in \{0,1\}$, spanned by $|\ddot{\psi}_{J,a,b}\rangle$, have the same dimension and there are 3 unitaries that map $|\ddot{\psi}_{J,0,0}\rangle \to |\ddot{\psi}_{J,a,b}\rangle$, hence one can form a complete set of orthogonal projectors $\Pi = \{\Pi_{j,\ell}\}_{j,\ell} \cup \Pi_{\text{triv}}$ that block-diagonalizes Γ. Each projector $\Pi_{j,\ell}$ is 4-dimensional. O_1 is trivially block-diagonal in Π, because $\mathsf{O}_1|\ddot{\psi}_{J,a,b}\rangle = (-1)^b|\ddot{\psi}_{J,a,b}\rangle$, or, equivalently, $\mathsf{O}_1|\ddot{\psi}^v_J\rangle = |\ddot{\psi}^w_J\rangle$ with $w = \mathsf{Z}v$.

Spectral norm of $\Gamma_1\Gamma^{-1}$ on $\Pi_{j,\ell}$ Recall $\Gamma_1 = \mathsf{O}_1^*\Gamma\mathsf{O}_1$ and denote $\Gamma^{(j)} = \Gamma\Pi_{j,\ell} = \mathsf{U}G_j\mathsf{U}^*$ for some ℓ. Then

$$\Gamma_1^{(j)}(\Gamma^{(j)})^{-1} = \Gamma_1\Gamma^{-1}\Pi_{j,\ell} = (\mathsf{Z}\mathsf{U}G_j\mathsf{U}^*\mathsf{Z})(\mathsf{U}G_j^{-1}\mathsf{U}^*).$$

This matrix is too hard to analyze directly, hence we apply Corollary 6 rather than Corollary 4. Compute

$$\frac{2\|\Gamma^{(j)} \circ D_1\|}{\lambda_{\min}(\Gamma^{(j)})} = \frac{2}{q^j}\|(\mathsf{U}G_j\mathsf{U}^*) \circ D_1\|, \qquad \text{where } D_1 = \begin{pmatrix} 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{pmatrix}.$$

Write the matrix $(\mathsf{U}G_j\mathsf{U}^*) \circ D_1$ after swapping the second and third row and column as $-\frac{q^j}{2}\left(\begin{smallmatrix} 0 & H_j \\ H_j^* & 0 \end{smallmatrix}\right)$ with

$$\begin{aligned} H_j &= \begin{pmatrix} \alpha_0\beta_0(q-1) & \alpha_1\beta_0(q^{t/2-j}-1) - \alpha_0\beta_1(q^{t/2-j}-q) \\ \alpha_0\beta_1(q^{t/2-j}-1) - \alpha_1\beta_0(q^{t/2-j}-q) & \alpha_1\beta_1(q-1) \end{pmatrix} \\ &= (q-1)\begin{pmatrix} \alpha_0\beta_0 & \alpha_0\beta_1 \\ \alpha_1\beta_0 & \alpha_1\beta_1 \end{pmatrix} + (q^{t/2-j}-1)(\alpha_1\beta_0 - \alpha_0\beta_1)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \|H_j\| &\leq (q-1)\left\|\begin{pmatrix}\alpha_0 \\ \alpha_1\end{pmatrix}(\beta_0, \beta_1)\right\| + (q^{t/2-j}-1)(\alpha_1\beta_0 - \alpha_0\beta_1)\left\|\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}\right\| \end{aligned}$$

Use $\alpha_a \le 1$, and $\beta_a \le \sqrt{2t/n}$ and $|\alpha_1\beta_0 - \alpha_0\beta_1| = O(1/\sqrt{tn})$ for $j \le t/2$ [AŠW06, Claim 19 and 20]. Then substitute $q = 1 + \frac{4\log(2/\zeta)}{t}$ and bound $\lambda = q^{t/2} \approx e^{2\log(2/\zeta)} = 4/\zeta^2$.

$$\begin{aligned}\|H_j\| &\le 2(q-1)\sqrt{\frac{2t}{n}} + (q^{t/2}-1)O\left(\frac{1}{\sqrt{tn}}\right)\\ &= O(1)\cdot\frac{\log(2/\zeta)+4/\zeta^2}{\sqrt{tn}} = O\Big(\frac{1}{\zeta^2\sqrt{tn}}\Big).\end{aligned}$$

We conclude that

$$\min_j \frac{\lambda_{\min}(\Gamma^{(j)})}{2\|\Gamma^{(j)}\circ D_1\|} = \Omega(\zeta^2\sqrt{tn}).$$

As we say above, this bound is only valid for $j \le t/2$. However, if $j \ge t/2$, then $G_j = q^{t/2}\mathsf{I}$, $\Gamma_1^{(j)}(\Gamma^{(j)})^{-1} = \mathsf{I}$, and the analysis in this subspace is trivial. This is exactly the reason why we mark the subspaces $S_{j,+}$ for $j \ge t/2$ as good.

Analysis of the trivial subspaces For $j \in \{t-1, t\}$, the projectors $\Pi_{j,\ell}$ have smaller dimension than 4×4, because there are not enough basis states. In particular, for $|J| = t-1$, there are only 3 types of basis states $|\ddot{\psi}_{J,0,0}\rangle \in S_{t-1,0,0} \subseteq S_{t-1,0}$, and $|\ddot{\psi}_{J,1,0}\rangle$ and $|\ddot{\psi}_{J,1,1}\rangle$ with $\alpha|\ddot{\psi}_{J,1,0}\rangle + \beta|\ddot{\psi}_{J,1,1}\rangle \in S_{t-1,1}$ and $\beta|\ddot{\psi}_{J,1,0}\rangle - \alpha|\ddot{\psi}_{J,1,1}\rangle \in S_{t,1}$. Hence their linear combinations fall into the following subspaces: $(1,\alpha,\beta) \in S_{t-1,+}$, $(1,-\alpha,-\beta) \in S_{t-1,-}$, and $(0,\beta,-\alpha) \in S_{t,1} = S_{t,-}$. Note that $S_{t,-}$ has a different definition than other $S_{j,-}$, and that there is no subspace $S_{t,+}$. For, $|J| = t$, the situation is simpler, because there are only basis states $|\ddot{\psi}_{J,1,0}\rangle \in S_{t,1,0} \subseteq S_{t,1} = S_{t,-}$. We conclude that even the projectors onto the trivial subspaces block-diagonalize Γ and O_1.

Now, the actual analysis of the norm of $\Gamma_1\Gamma^{-1}$ on these trivial subspaces is not needed, because $\Gamma = q^{t/2}\mathsf{I}$ on $\Pi_{t-1,\ell}$ or $\Pi_{t,\ell}$. We conclude that the norm there is exactly 1.

Multiplicative adversary bound By Corollary 6, using the symmetry over all i and $\zeta^2\lambda = \zeta^2 q^{t/2} \approx 4$,

$$\mathrm{MADV}_{1/2,4\zeta}(\mathrm{Threshold}_{t,n}) \ge \log(\zeta^2\lambda)\cdot\min_j \frac{\lambda_{\min}(\Gamma^{(j)})}{2\|\Gamma^{(j)}\circ D_1\|} = \Omega(\zeta^2\sqrt{tn}).$$

□

4.4 The OR function

Let us consider a special case of the t-threshold function for $t = 1$, the OR function. It is the decision version of the search function from Section 4.1. We show a quadratically better lower bound in terms of the error probability than the one implied by Theorem 12.

Theorem 13 $\mathrm{MADV}_{1/2,4\zeta}(\mathrm{OR}_n) = \Omega(\zeta\sqrt{n})$ *for* $\zeta \ge \sqrt{2/n}$.

Proof We use the same subspaces and the same adversary matrix Γ like in Eqn. (13):

$$\Gamma = \Pi_{S_{0,+}} + q\cdot\big(\Pi_{S_{0,-}} + \Pi_{S_{1,-}}\big),$$

$\lambda = q = 2/\zeta^2$, and the same block-diagonalization like in the proof of Theorem 12. However, we do the analysis more carefully, which is feasible thanks to the fact that we only have one nontrivial 3-dimensional subspace. This subspace is spanned by $|\ddot{\psi}_{\emptyset,0,0}\rangle$, $|\ddot{\psi}_{\emptyset,1,0}\rangle$, and $|\ddot{\psi}_{\emptyset,1,1}\rangle$. In this basis, $\Gamma = \mathsf{U}G\mathsf{U}^*$ and $\Gamma_1 = \mathsf{Z}\Gamma\mathsf{Z}$, where

$$\mathsf{U} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0\\ \alpha & -\alpha & \sqrt{2}\,\beta\\ \beta & -\beta & -\sqrt{2}\,\alpha\end{pmatrix}, \qquad G = \begin{pmatrix}1 & 0 & 0\\ 0 & q & 0\\ 0 & 0 & q\end{pmatrix}, \qquad \mathsf{Z} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}.$$

If we applied Corollary 6 on this adversary matrix, we would obtain the same bound as in Theorem 12. We instead express $\Gamma_1\Gamma^{-1} = (\mathsf{ZU}G\mathsf{U}^*\mathsf{Z})(\mathsf{U}G^{-1}\mathsf{U}^*)$ explicitly and get that its eigenvalues are 1 and

$$1+\gamma \pm \sqrt{\gamma^2+2\gamma}, \quad \text{where } \gamma = \frac{(q-1)^2}{2q}(2\beta^2-\beta^4).$$

We plug in the bound $\beta \le \sqrt{2/n}$, expand the Taylor series, and obtain $\|\Gamma_1\Gamma^{-1}\| = 1 + \frac{2(q-1)}{\sqrt{qn}} + O(\frac{q}{n})$. We can neglect the remaining terms when $\zeta \ge \sqrt{2/n}$. By Corollary 4,

$$\mathrm{MADV}_{1/2,4\zeta}(\mathrm{OR}_n) \ge \frac{\log(\zeta^2\lambda)}{\log(1+2(q-1)/\sqrt{qn})} \ge \frac{\log(\zeta^2 q)\sqrt{q}}{2(q-1)}\sqrt{n} = \Omega(\zeta\sqrt{n}).$$

□

The multiplicative adversary bound for OR is stronger than the additive adversary bound for polynomially small success probabilities. Note that success $\frac{1}{2}+\zeta$ corresponds to error $\frac{1}{2}-\zeta$. By Corollary 2, the additive adversary bound for OR is

$$\mathrm{ADV}_{\frac{1}{2}-\zeta}(\mathrm{OR}_n) = \frac{1-\sqrt{(1-2\zeta)(1+2\zeta)}}{2}\sqrt{n} = \frac{1-\sqrt{1-4\zeta^2}}{2}\sqrt{n} \approx \frac{1-(1-2\zeta^2)}{2}\sqrt{n} = \zeta^2\sqrt{n}.$$

4.5 Designing Γ for a general function

After having presented optimal multiplicative adversary matrices for several problems, let us make a note on how to design a good Γ in general. It seems that we don't have too much freedom. All known good multiplicative adversary matrices Γ have the following structure: Γ is a linear combination of projectors S_j, where S_j is spanned by superpositions of input states consistent with fixing exactly j input variables. This matrix is then simultaneously block-diagonalized with the query operator. The diagonal blocks typically overlap with some adjacent subspaces S_j and S_{j+1}. To get a good estimate of the spectral norm of such a block, the minimal and maximal eigenvalue in this block must not differ too much. On the other hand, we want the spectral norm of Γ be as large as possible, hence an optimal choice of the multiplicative coefficients seems to be $q^j\Pi_{S_j}$ for some constant q, or more generally $(\Pi_{i=1}^{j} q_i)\Pi_{S_j}$, with q_i different in each subspace S_i if the subspaces for different i have significantly different properties.

The real difficulty seems to lie not in designing good subspaces S_j, but in their combinatorial analysis.

5 Direct product theorems

In this section we investigate the complexity of evaluating a function f on k independent instances simultaneously. We prove that the multiplicative adversary bound satisfies a *strong direct product theorem (DPT)*. Roughly speaking it says that if we are asked to compute f on k independent inputs in time less than k times the time for one instance, then the success probability goes exponentially down. Ambainis [AŠW06] proved a DPT for t-threshold using these techniques. Here we show that his proof actually gives a DPT for any function that has a multiplicative adversary lower bound.

For a function $f : X \to \Sigma_O$ with $X \subseteq \Sigma_I^n$ and $k \ge 1$, let $f^{(k)} : X^k \to \Sigma_O^k$ such that $f(x_1,\ldots,x_k) = (f(x_1),\ldots,f(x_k))$. An algorithm succeeds with computing $f^{(k)}$ if all individual instances are computed right.

Theorem 14 *For every function f with $\eta \le \frac{1}{2}$, and $k \ge 361$, $\mathrm{MADV}_{\eta^{2k/5},\zeta^{k/10}}(f^{(k)}) \ge \frac{k}{10}\cdot\mathrm{MADV}_{\eta,4\zeta}(f)$.*

Proof Let Γ, λ denote the optimal multiplicative adversary matrix for f with success η, and its threshold value for good subspaces. We construct Γ', λ' for $f^{(k)}$ as follows [AŠW06, Appendix A.1]:

$$\Gamma' = \Gamma^{\otimes k}, \qquad \lambda' = \lambda^{k/10}.$$

We prove that $\max_{i',p} \|\Gamma'_{i',p}(\Gamma')^{-1}\| = \max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\|$. This is because, for an $i' = jn+i$, $\Gamma'_{i',p} = \mathsf{O}^*_{i',p}\Gamma'\mathsf{O}_{i',p}$ with $\mathsf{O}_{i',p} = \mathsf{I}^{\otimes j} \otimes \mathsf{O}_{i,p} \otimes \mathsf{I}^{\otimes(k-1-j)}$, and thus $\Gamma'_{i',p}(\Gamma')^{-1} = \mathsf{I}^{\otimes j} \otimes (\Gamma_{i,p}\Gamma^{-1}) \otimes \mathsf{I}^{\otimes(k-1-j)}$. Therefore, by Corollary 4, if we choose $\zeta' = \zeta^{k/10}$, the multiplicative adversary bound is

$$\mathrm{MADV}_{\eta',4\zeta'}(f^{(k)}) \geq \frac{\log(\zeta'^2\lambda')}{\log(\max_{i,p} \|\Gamma'_{i,p}(\Gamma')^{-1}\|)} = \frac{k}{10} \cdot \frac{\log(\zeta^2\lambda)}{\log(\max_{i,p} \|\Gamma_{i,p}\Gamma^{-1}\|)} = \frac{k}{10} \cdot \mathrm{MADV}_{\eta,4\zeta}(f).$$

It remains to analyze the success η' of the composed function $f^{(k)}$ in the bad subspaces.

Upper-bounding η' Let $T_{\mathrm{bad}}, T_{\mathrm{good}}$ denote the bad and good subspace of Γ. For a $v \in \{\mathrm{bad}, \mathrm{good}\}^k$, let $|\varphi\rangle \in T_{v_1} \otimes \cdots \otimes T_{v_k}$ be a product quantum state such that $\|\Gamma'|\varphi\rangle\|_2 < \lambda'$. Since all eigenvalues of Γ are at least 1, if a subspace of Γ' corresponds to an eigenvalue less than λ', only less than $k/10$ individual subspaces out of k can be the good ones. This means that more than $9k/10$ instances lie in the bad eigenspace of Γ and have thus success probability at most η. Since $|\varphi\rangle$ is a product state, the total success probability of computing all instances right is at most $\eta^{9k/10}$. We, however, have to upper-bound the success probability for all *superposition* states than can come from different combinations of T_{v_i}'s. In general,

$$|\varphi\rangle = \sum_{\substack{v\in\{\mathrm{bad},\mathrm{good}\}^k \\ |v|<k/10}} \alpha_v|\varphi_v\rangle, \text{ where } |\varphi_v\rangle \in T_{v_1} \otimes \cdots \otimes T_{v_k} \text{ and } |v| \text{ denotes \#good subspaces.}$$

Our assumption about f is that $\|\mathsf{F}_z|v\rangle\|_2^2 \leq \eta$ for every z and $|v\rangle \in T_{\mathrm{bad}}$. Thus

$$\begin{aligned}
\|(\mathsf{F}_{z_1} \otimes \cdots \otimes \mathsf{F}_{z_k})|\varphi\rangle\|_2^2 &= \|\sum_v \alpha_v \prod_i \mathsf{F}_{z_i}|\varphi_{v,i}\rangle\|_2^2 \\
&\leq \left(\sum_v \alpha_v \prod_i \|\mathsf{F}_{z_i}|\varphi_{v,i}\rangle\|_2\right)^2 \\
&\leq \left(\sum_v |\alpha_v|^2\right) \cdot \left(\sum_v \prod_i \|\mathsf{F}_{z_i}|\varphi_{v,i}\rangle\|_2^2\right) \\
&\leq 1 \cdot \eta^{9k/10} \sum_{v:|v|<k/10} 1 \\
&= \eta^{9k/10} \sum_{i=0}^{k/10} \binom{k}{i} \leq k\binom{k}{k/10}\eta^{9k/10} && \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k \\
&\leq k(10e)^{k/10}\eta^{9k/10} && \sqrt[5]{10e} < 2 \\
&< 2^{k/2}\eta^{k/2}\eta^{2k/5} && k\sqrt[5]{10e}^{k/2} < 2^{k/2} \text{ for } k \geq 361 \\
&\leq \eta^{2k/5}. && \eta \leq \frac{1}{2}
\end{aligned}$$

Note that in the case of the t-threshold function as the base function, the success probability is $\eta = \frac{1}{2}$ in both bad (plus) and good (minus) subspaces, hence we could use a stronger bound 2^{-k} instead of $\eta^{9k/10}$. There is nothing special about the constant $k \geq 361$; the DPT holds for all k, but we have to take into account the multiplicative factor of k in the success η'.

We conclude that $\mathrm{MADV}_{\eta^{2k/5},\zeta^{k/10}}(f) \geq \frac{k}{10} \cdot \mathrm{MADV}_{\eta,4\zeta}(f)$. □

This technique also allows us to prove the direct product theorem when the k instances are distinct functions.

Acknowledgments

I thank Andris Ambainis, Peter Høyer, Sophie Laplante, Troy Lee, and Mehdi Mhalla for fruitful discussions, and Ronald de Wolf for helpful comments.

References

[Amb02] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. Earlier version in STOC'00.

[Amb05] A. Ambainis. A new quantum lower bound method, with an application to strong direct product theorem for quantum search. quant-ph/0508200, 2005.

[Amb06] A. Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006. Earlier version in FOCS'03.

[AS04] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004.

[AŠW06] 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. of 38th ACM STOC*, pages 618–633, 2006.

[BBBV97] H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. Earlier version in FOCS'98.

[BS04] H. Barnum and M. Saks. A lower bound on the quantum query complexity of read-once functions. *Journal of Computer and System Sciences*, 69(2):244–258, 2004.

[BSS03] H. Barnum, M. Saks, and M. Szegedy. Quantum decision trees and semidefinite programming. In *Proc. of 18th IEEE Complexity*, pages 179–193, 2003.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Earlier version in STOC'93.

[HLŠ07] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proc. of 39th ACM STOC*, pages 526–535, 2007.

[HNS02] P. Høyer, J. Neerbek, and Y. Shi. Quantum complexities of ordered searching, sorting, and element distinctness. *Algorithmica*, 34(4):429–448, 2002. Special issue on Quantum Computation and Cryptography. Earlier version in ICALP'01.

[HŠ05] P. Høyer and R. Špalek. Lower bounds on quantum query complexity. *EATCS Bulletin*, 87:78–103, October, 2005.

[Knu03] D. E. Knuth. Combinatorial matrices. In *Selected Papers on Discrete Mathematics*, volume 106 of *CSLI Lecture Notes*. Stanford University, 2003.

[KŠW07] H. Klauck, R. Špalek, and R. de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. *SIAM Journal on Computing*, 36(5):1472–1493, 2007. Earlier version in FOCS'04.

[LM04] S. Laplante and F. Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. In *Proc. of 19th IEEE Complexity*, pages 294–304, 2004.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proc. of 40th IEEE FOCS*, pages 369–377, 1999.

[ŠS06] R. Špalek and M. Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006. Earlier version in ICALP'05.

[Zha05] S. Zhang. On the power of Ambainis's lower bounds. *Theoretical Computer Science*, 339(2–3):241–256, 2005. Earlier version in ICALP'04.