

# The Adversary Bound Revisited: From Optimal Query Algorithms to Optimal Control

Duyal Yolcu

<https://github.com/qudent>

This note complements the upcoming paper "One-Way Ticket to Las Vegas and the Quantum Adversary" by Belovs and Yolcu, to be presented at QIP 2023 [BY23]. I develop the ideas behind the adversary bound - universal algorithm duality therein in a different form. This form may be faster to understand for a general quantum information audience: It avoids defining the "unidirectional filtered  $\gamma_2$ -bound" and relating it to query algorithms explicitly. This proof is also more general because the lower bound (and universal query algorithm) apply to a class of optimal control problems rather than just query problems. That is in addition to advantages to be discussed in [BY23], namely the more elementary algorithm and correctness proof that avoids phase estimation and spectral analysis, and allows for limited treatment of noise.

The approach - not new - starts with considering an optimal *query* problem for state conversion - in which we are given an unknown oracle  $L_a$  for  $a \in A$ , and want to construct an algorithm that transforms initial states  $|\xi_a\rangle$  to acceptable target states  $|\tau_a\rangle$  by invoking that oracle - as an optimal *control* problem, in which  $a \in A$  is stored as a quantum "input state" in another Hilbert space  $\mathcal{A}$ , and we want to transform  $|\xi\rangle = \sum_{a \in A} |a\rangle \otimes |\xi_a\rangle$  to  $|\tau\rangle = \sum_{a \in A} |a\rangle \otimes |\tau_a\rangle$  by invoking

$L = \sum_{a \in A} |a\rangle \langle a| \otimes L_a$  without being allowed to access  $\mathcal{A}$  directly. Then we track

feasible *reduced density matrices* on  $\mathcal{A}$  (which correspond to the transpose of the Gram matrices in the adversary bound literature). This information is sufficient to track the system's state by standard facts on purifications and their unitary equivalence. This is close to [BSS; Bar07].

The adversary bound is the inverse maximal speed we can achieve in reduced density matrix space from any starting RDM, travelling in the desired direction. We describe a new universal control algorithm that matches this speed up to a error-dependent factor by slightly perturbing initial and target state by that ideal starting RDM; by a linearity argument, an algorithm going along a straight line between these perturbed states is feasible. We can then bound the error in the final state if we apply that algorithm to the original initial state, rather than the perturbed one.

Importantly, this approach doesn't assume that  $L$  is "read-only", i.e. block-diagonal in  $\mathcal{A}$ , anymore - as long as there is still an "idle subspace" as defined in the note. We can therefore apply it to problems in which the register  $\mathcal{A}$  is to be manipulated, rather than just read out. The argument also works with problems in which  $L$  is only subunitary, i.e. may correspond to noise occurring and the algorithm "giving up" in some instances.

To follow this text, one only needs basic knowledge in quantum physics including reduced density operators, purifications and their local equivalence. Therefore, I hope it has expository value for a general quantum information

audience that wants to understand adversary bound - universal query algorithm dualities.

### Acknowledgments

I thank Alexander Belov (Aleksandrs Belovs) and Berare Göktürk for helpful discussions while writing the draft.

## Contents

<b>1</b>	<b>The problem - discrete time</b>	<b>2</b>
<b>2</b>	<b>Quantum algorithms as sequences of feasible reduced density matrices on <math>\mathcal{AB}</math></b>	<b>3</b>
<b>3</b>	<b>Adversary bound</b>	<b>4</b>
<b>4</b>	<b>Matching the lower bound by a universal algorithm</b>	<b>5</b>
<b>5</b>	<b>Further remarks</b>	<b>7</b>
5.1	From control to query algorithms . . . . .	7
5.2	Continuous time . . . . .	7
5.3	Other characterizations of quantum processes . . . . .	8
<b>6</b>	<b>Conclusion and outlook</b>	<b>8</b>

## 1 The problem - discrete time

We consider a tripartite quantum system  $\mathcal{ABC}$ , assumed to be finite-dimensional for convenience. We want to construct an algorithm that transforms an initial state  $|\xi\rangle \in \mathcal{ABC}$  to a target state  $|\tau\rangle \in \mathcal{ABC}$  (or similar, e.g. allowing a range of acceptable target states). The catch is that the algorithm is not allowed to arbitrarily act on  $\mathcal{A}$ . Instead, there is a fixed subunitary interaction operator  $L$  (i.e. fulfilling  $\|L|\varphi\rangle\| \leq 1$  whenever  $\|\varphi\| \leq 1$ ) that acts on  $\mathcal{AB}$  (not  $\mathcal{C}$ ) once per timestep. On the other hand, we are allowed to apply arbitrarily complex unitaries on  $\mathcal{BC}$  at any time, without cost. We also assume that  $\mathcal{C}$  is "as large as the algorithm could need it to be"; in Section 5.1, we'll see that  $\dim \mathcal{C} \geq \dim(\mathcal{AB})$  works for any algorithm.

Finally, we fix a designated normalized state  $|\text{idle}\rangle \in \mathcal{B}$ . We assume that  $L$  acts trivially on  $|\text{idle}\rangle$ , i.e.  $L(|\varphi\rangle|\text{idle}\rangle) = |\varphi\rangle|\text{idle}\rangle$  for all  $|\varphi\rangle \in \mathcal{A}$ . This is equivalent to assuming that  $L$  can be applied in a "controlled" way, and the algorithm can always choose to do nothing.

Allowing subunitary, rather than only unitary,  $L$  allows a limited discussion of **noise**: If the true transformation a physical system undergoes involves a noisy quantum channel, one can choose  $L$  to be one Kraus operator of that quantum channel and consider it the "successful" Kraus operator. The other

Kraus operators can be considered "errors", and one stops tracking the computation in case one of them is applied. Then the norm of the state will decay over time - corresponding to losing probability mass in case an error occurs - but one can still define sets of acceptable, sub-normalized target states, and achieving them with that  $L$  is sufficient to solve the entire problem. However, it is necessary for our universal algorithm that  $L$  preserves the norm when acting on  $|\text{idle}\rangle$ .

As mentioned in the abstract, we can encode a query complexity problem by choosing  $L$  block-diagonal. For a more thorough introduction to query problems, see [Bel15].

## 2 Quantum algorithms as sequences of feasible reduced density matrices on $\mathcal{AB}$

We now define quantum algorithms in terms of the feasible intermediate reduced density matrices on  $\mathcal{AB}$ . This section uses essentially the same ideas as [BSS; Bar07] (aside from pointing out that they apply to a wider class of  $L$ ).

**Definition 1.** *In our discussion, a  $T$ -step **quantum algorithm** is a list of positive semidefinite operators  $(\pi^0, \pi^1, \dots, \pi^{T-1})$  representing (non-normalized) reduced density matrices on  $\mathcal{AB}$  such that for all  $j$ ,*

$$\text{tr}_{\mathcal{B}} \pi^{j+1} = \text{tr}_{\mathcal{B}} (L \pi^j L^\dagger). \quad (1)$$

**Proposition 1.** *In the model of Section 1, it is possible to transform  $|\xi\rangle \mapsto |\tau\rangle$  in  $T$  timesteps iff such a list exists with  $\text{tr}_{\mathcal{BC}} |\xi\rangle \langle \xi| = \text{tr}_{\mathcal{B}} \pi^0$  and  $\text{tr}_{\mathcal{BC}} |\tau\rangle \langle \tau| = \text{tr}_{\mathcal{B}} (L \pi^{T-1} L^\dagger)$ .*

*Proof.* First suppose that such a transformation is possible and let  $|\Phi^j\rangle \in \mathcal{ABC}$  be the system's state directly before the  $j + 1$ th application of  $L$  (counting from 1). Then set  $\pi^j := \text{tr}_{\mathcal{C}} |\Phi^j\rangle \langle \Phi^j|$ . As reduced density operators of a non-normalized state, these are positive semidefinite. Directly after the  $j + 1$ th application of  $L$ , the reduced density matrix on  $\mathcal{A}$  is  $\text{tr}_{\mathcal{B}} (L \pi^j L^\dagger)$  by standard quantum physics. Similarly, directly before the  $j + 2$ nd application, the RDM is  $\text{tr}_{\mathcal{B}} (\pi^{j+1})$ . But these matrices must be equal because between the  $j + 1$ th and the  $j + 2$ nd application, the quantum computer may only act on  $\mathcal{BC}$ , and not on  $\mathcal{A}$ .

Conversely, suppose there is an algorithm as in 1 and consider a sequence of purifications of the  $\pi^j$  on  $\mathcal{C}$ , i.e.  $|\Phi^j\rangle \in \mathcal{ABC}$  such that  $\text{tr}_{\mathcal{C}} |\Phi^j\rangle \langle \Phi^j| = \pi^j$ . By standard quantum physics again, these always exist if  $\dim \mathcal{AB} \leq \dim \mathcal{C}$  [NC02]. Then by Equations (1),  $(L \otimes I_{\mathcal{C}}) |\Phi^j\rangle$  and  $|\Phi^{j+1}\rangle$  are purifications of the same reduced density matrix on  $\mathcal{A}$ . The same is true for  $|\Phi^0\rangle$  and  $|\xi\rangle$ , as well as  $(L \otimes I_{\mathcal{C}}) |\Phi^{T-1}\rangle$  and  $|\tau\rangle$ . As all such purifications are related by local unitaries acting only on  $\mathcal{BC}$  [Ozo12], a valid quantum algorithm exists that starts with  $|\xi\rangle$  and applies these connecting unitaries between applications of  $L$ .  $\square$

As promised in the abstract, this argument essentially works by tracking the reduced density matrix on  $\mathcal{A}$ . This set of lists of operators is also a convex set in a natural way, which gives rise to nice properties - see [BY23] for details.

### 3 Adversary bound

Now consider a  $T$ -step quantum query algorithm transforming  $|\xi\rangle \mapsto |\tau\rangle$  and consider the sum of all  $\pi^j$ ,

$$\bar{\pi} := \sum_{j=0}^{T-1} \pi^j \in \mathbb{S}_{\mathcal{AB}}, \quad (2)$$

where  $\mathbb{S}_{\mathcal{AB}}$  denotes the set of positive semidefinite operators on  $\mathcal{AB}$ . Then

$$\begin{aligned} \text{tr}_{\mathcal{B}} (L\bar{\pi}L^\dagger) &= \sum_{j=0}^{T-1} \text{tr}_{\mathcal{B}} (L\pi^jL^\dagger) = \sum_{j=0}^{T-2} \text{tr}_{\mathcal{B}} \pi^{j+1} + \text{tr}_{\mathcal{BC}} (|\tau\rangle\langle\tau|) \\ &= \text{tr}_{\mathcal{B}} \bar{\pi} + \text{tr}_{\mathcal{BC}} (|\tau\rangle\langle\tau| - |\xi\rangle\langle\xi|). \end{aligned} \quad (3)$$

Furthermore,

$$\text{tr}(\bar{\pi}) \leq T \langle\xi|\xi\rangle : \quad (4)$$

If we turn the sequence of  $\pi^j$  into a quantum algorithm involving a sequence of  $|\Phi^j\rangle$  as in 2,  $\text{tr}(\pi^j) = \|\Phi^j\|^2 \leq \|\xi\|^2$  by subunitarity of  $L$ ; Equation (4) is the result of adding these inequalities.

If a  $T$ -query algorithm exists, *some*  $\bar{\pi}$  must exist, which yields the following bound:<sup>1</sup>

**Definition 2.** (*Adversary bound*) The **adversary bound** of a state conversion problem, denoted  $\text{Adv}(|\xi\rangle \rightarrow |\tau\rangle)$ , is the optimal value of the minimization problem (which we call the **primal problem**)

$$\begin{aligned} &\text{minimize } \text{tr}(\bar{\pi}) / \langle\xi|\xi\rangle \\ &\text{subject to } \text{tr}_{\mathcal{B}} (L\bar{\pi}L^\dagger - \bar{\pi}) = \text{tr}_{\mathcal{BC}} (|\tau\rangle\langle\tau| - |\xi\rangle\langle\xi|), \\ &\bar{\pi} \in \mathbb{S}_{\mathcal{AB}}. \end{aligned}$$

By the discussion above,  $\text{Adv}(|\xi\rangle \rightarrow |\tau\rangle)$  lower-bounds the number of queries of quantum query algorithms solving the state conversion problem exactly.

The inverse of this problem's optimal solution is also the answer to the question "In the space of reduced density matrices on  $\mathcal{A}$ , what is the maximum fraction of the desired change  $\text{tr}_{\mathcal{BC}} (|\tau\rangle\langle\tau| - |\xi\rangle\langle\xi|)$  achievable, starting from *any* state with the correct normalization?"

---

<sup>1</sup>The motivation for this term is clearer in other expositions, such as Childs's lecture notes [Chi].

Subsection 5.1 discusses a strengthening relevant for query problems, omitted here to reduce technicality.

The following remark uses semidefinite programming duality; the result isn't necessary for the remainder of the discussion, and a reader unfamiliar with the technique may take it on faith. The optimal value of the problem is lower-bounded by the optimal value of the maximization problem (the dual problem)

$$\begin{aligned} & \text{maximize } (\langle \tau | \Gamma \otimes I_{\mathcal{BC}} | \tau \rangle - \langle \xi | \Gamma \otimes I_{\mathcal{BC}} | \xi \rangle) / \langle \xi | \xi \rangle \\ & \text{subject to } L^\dagger (\Gamma \otimes I_{\mathcal{B}}) L - \Gamma \otimes I_{\mathcal{B}} \preceq I_{\mathcal{AB}}, \\ & \Gamma \in \mathbb{H}_{\mathcal{A}}, \end{aligned}$$

where  $\mathbb{H}_{\mathcal{A}}$  denotes the space of Hermitian matrices on  $\mathcal{A}$ . This means that finding any feasible  $\Gamma$  for this problem corresponds to a proof that no algorithm can be faster - which is more convenient for finding lower bounds on the number of steps necessary for a conversion. We can see that *Slater's strong duality condition* is fulfilled by choosing  $\Gamma = 0$  in the dual problem. This means that the best solution to problem (8)-(10) results in a value equal to the best solution of problem (5)-(7).

## 4 Matching the lower bound by a universal algorithm

Now assume we have some feasible solution  $\bar{\pi}$  of (5)-(7), which doesn't have to be optimal. Can we "turn it around" and obtain an algorithm to transform  $|\xi\rangle \rightarrow |\tau\rangle$  in  $\text{tr } \bar{\pi}$  steps? The answer will turn out to be "almost".

**Proposition 2.** *Using the notations above, for any integer  $T' > 0$ , the sequence of  $\pi^j$*

$$(\pi^j)_{0 \leq j < T'} = \left( \left( \frac{T' - j}{T'} \text{tr}_{\mathcal{BC}} |\xi\rangle \langle \xi| + \frac{j}{T'} \text{tr}_{\mathcal{BC}} |\tau\rangle \langle \tau| \right) \otimes |\text{idle}\rangle \langle \text{idle}| + \frac{\bar{\pi}}{T'} \right)_{0 \leq j < T'}$$

*constitutes a  $T'$ -query quantum query algorithm solving the state conversion problem  $|\xi\rangle \otimes |0\rangle + \frac{|v\rangle}{\sqrt{T'}} \otimes |1\rangle \mapsto |\tau\rangle \otimes |0\rangle + \frac{|v\rangle}{\sqrt{T'}} \otimes |1\rangle$ , where  $|v\rangle$  is a purification of  $\bar{\pi}$  on  $\mathcal{C}$  (and we add a qubit to the ancilla space).*

*Proof.* Equation (1) and the final condition follows directly from the optimization constraint (6) and the constraint that  $L$  acts trivially on  $|\text{idle}\rangle$ . Positive semidefiniteness follows from the fact that all reduced density matrices are positive semidefinite.  $\square$

As  $T' \rightarrow \infty$ , initial and target states converge to our desired  $|\xi\rangle, |\tau\rangle$  (apart from having redefined the ancilla space. Let  $E: \mathcal{ABC} \rightarrow \mathcal{ABC}$  be the total effective evolution operator applied by the algorithm; this operator must be subunitary. If we apply the algorithm to our true initial state  $|\xi\rangle \otimes |0\rangle$ , and

project to the  $|0\rangle$  subspace in the end (i.e. measures that qubit and outputs "failure" in case the result is 1, generally reducing the norm of the state), the resulting state fulfills

$$\begin{aligned}
& \|P_0 E(|\xi\rangle \otimes |0\rangle) - |\tau\rangle \otimes |0\rangle\| / \|\xi\rangle\| \\
= & \left\| P_0 E(|\xi\rangle \otimes |0\rangle + T'^{-1/2} |\nu\rangle \otimes |1\rangle) - P_0 E(T'^{-1/2} |\nu\rangle \otimes |1\rangle) - |\tau\rangle \otimes |0\rangle \right\| / \|\xi\rangle\| \\
= & \left\| |\tau\rangle \otimes |0\rangle - P_0 E(T'^{-1/2} |\nu\rangle \otimes |1\rangle) - |\tau\rangle \otimes |0\rangle \right\| / \|\xi\rangle\| \\
= & T'^{-1/2} \| -P_0 E(|\nu\rangle \otimes |1\rangle) \| \leq T'^{-1/2} \sqrt{\text{tr} \bar{\pi}} / \|\xi\rangle\|, \tag{5}
\end{aligned}$$

where we used subunitarity of  $E$  and  $P_0$  in the last line. In fact, a similar argument would show that the norm difference would be at most twice that if we were not allowed to throw away part of the state in the last step. For an optimal  $\bar{\pi}$ ,  $\sqrt{\text{tr} \bar{\pi}} / \|\xi\rangle\| = \sqrt{\text{Adv}(|\xi\rangle \mapsto |\tau\rangle)}$ .

For large  $T'$ , each individual step puts most of its amplitude into the  $|\text{idle}\rangle$  subspace. Remarkably, one can show (proof omitted) that for the algorithm's intermediate states  $|\Phi^j\rangle$ , the quantity  $\sum_{j=0}^{T'-1} \langle \Phi^j | I - P_{\text{idle}} | \Phi^j \rangle / \langle \xi | \xi \rangle \leq \text{tr} \bar{\pi} / \langle \xi | \xi \rangle$  independent of  $T'$ . The analogue for query problems - called "Las Vegas complexity" - is defined and studied in [BY23].

In conclusion:

**Theorem 1.**

1. A control algorithm converting  $|\xi\rangle$  to  $|\tau\rangle$  uses at least  $\text{Adv}(|\xi\rangle \rightarrow |\tau\rangle)$  steps,
2. Conversely, for any acceptable error  $\varepsilon$ , we can find an algorithm converting  $|\xi\rangle \otimes |0\rangle$  to  $|\tau'\rangle \otimes |0\rangle + |\Delta\rangle \otimes |1\rangle$ , with  $\| |\tau'\rangle - |\tau\rangle \| / \|\xi\rangle\| \leq \varepsilon$ , that takes

$$T' = \left\lceil \frac{\text{Adv}(|\xi\rangle \rightarrow |\tau\rangle)}{\varepsilon^2} \right\rceil \tag{6}$$

steps and fulfills  $\sum_{j=0}^{T'-1} \langle \Phi^j | I - P_{\text{idle}} | \Phi^j \rangle / \langle \xi | \xi \rangle \leq \text{Adv}(|\xi\rangle \rightarrow |\tau\rangle)$  on the intermediate states.

As remarked in the abstract, this algorithm corresponds to going along a straight line with constant velocity in the space of reduced density operators. As  $\bar{\pi}$  is not "used up" during this transformation, we can interpret it as a "catalyst" in the spirit of catalytic states in LOCC transformations.

## 5 Further remarks

### 5.1 From control to query algorithms

I briefly discuss how to modify this argument for quantum query complexity problems in state conversion problems; I skipped this before because it would have made the discussion more technical. This note completely ignores function evaluation and output conditions - i.e. the question of what final states allow calculating some function of the input in a query problem. See e.g. [BY23], [Bel15], [Bar07] for a more thorough discussion of query complexity problems.

Start directly after Equation (3). Let  $P_{\mathcal{A}'}$  be a projector onto a subspace  $\mathcal{A}' \subseteq \mathcal{A}$  such that  $P_{\mathcal{A}'}L = LP_{\mathcal{A}'}$ . Choosing  $\mathcal{A}' = \mathcal{A}$  and  $P_{\mathcal{A}'} = I$  will always work; when dealing with a query problem and  $L$  is block-diagonal in some basis  $\{|a\rangle\}_{a \in A}$  of  $\mathcal{A}$ , we could choose  $\mathcal{A}' := \text{span}\{|a\rangle\}$  as well for any  $a \in A$ . The argument that shows  $\text{tr}(\bar{\pi}) \leq T \langle \xi | \xi \rangle$  (Equation (4)) is in fact sufficient to show that

$$\text{tr}(P_{\mathcal{A}'}\bar{\pi}) \leq T \langle \xi | P_{\mathcal{A}'} | \xi \rangle \quad (7)$$

for any such  $\mathcal{A}'$ , because we can commute  $P_{\mathcal{A}'}$  through the entire evolution.

So each suitable  $\mathcal{A}'$  yields a lower bound on  $T$ , and we can replace the optimization target  $\text{tr}\bar{\pi}$  of Equation (5) by

$$\sup_{\mathcal{A}' \subseteq \mathcal{A}: P_{\mathcal{A}'}L = LP_{\mathcal{A}'}} (\text{tr}(P_{\mathcal{A}'}\bar{\pi}) / \langle \xi | P_{\mathcal{A}'} | \xi \rangle).$$

We can also fix a set of  $\mathcal{D}'$  that fit, and consider the optimization problem that considers only these. For a block-diagonal  $L$ , choosing the set of subspaces spanned by the computational basis elements of  $\mathcal{A}$ ,  $\{\text{span}\{|a\rangle\} \mid a \in A\}$ , results in an optimization problem equivalent to the unidirectional filtered  $\gamma_2$ -bound of [BY23].

Conversely, suppose we have a optimal solution of that modified optimization problem. Then we can insert any  $P_{\mathcal{A}'}$  we considered into the derivation of Equation (12). Using the fact that it commutes with all operators involved in that derivation, we derive that

$$\frac{\|P_{\mathcal{A}'}P_0A(|\xi\rangle \otimes |0\rangle) - P_{\mathcal{A}'}|\tau\rangle \otimes |0\rangle\|}{\|P_{\mathcal{A}'}|\xi\rangle\|} \leq \sqrt{\frac{\text{Adv}(|\xi\rangle \mapsto |\tau\rangle)}{T'}} \quad (8)$$

for each individual  $P_{\mathcal{A}'}$ , rather than just  $P_{\mathcal{A}'} = I$ . In , this allows us to consider the error bound  $\| |\tau'\rangle - |\tau\rangle \| / \| |\xi\rangle \| \leq \varepsilon$  with  $\| P_{\mathcal{A}'}(|\tau'\rangle - |\tau\rangle) \| / \| P_{\mathcal{A}'}|\xi\rangle \| \leq \varepsilon$  for each individual ones. If we have considered a query problem as a control problem as in the abstract, and want to ensure that the error in the state conversion is small for all possible inputs, such a strengthening is necessary.

### 5.2 Continuous time

This note discusses everything in discrete time, however, quantum physics as we know it is continuous and described by differential equations. In a physical

system, the interaction between  $\mathcal{A}$  and  $\mathcal{B}$  would be described by a Hamiltonian  $H$ ; we may model a situation in which the wavefunction may decohere, and we stop considering the decohered parts, by choosing a non-Hermitian  $H$ .

One approach to bridging the gap is to choose  $\epsilon > 0$  and consider a discrete-time query model with  $L_\epsilon := e^{-iH\epsilon}$ . Then  $T$  steps correspond to an elapsed time  $T\epsilon$ . Intuitively, the associated family of lower bounds and algorithms should converge to a description of the continuous-time situation as  $\epsilon \mapsto 0^+$ . However, I didn't succeed in making all associated analysis statements rigorous.

### 5.3 Other characterizations of quantum processes

As mentioned, Section 1 is very similar to the semidefinite programming (SDP) characterization of quantum algorithms by [BSS; Bar07]. Incidentally, an SDP characterization of the success probability is also possible if the transformations aren't subunitaries, but arbitrary quantum channels (e.g. because they introduce errors). This can be done by an application of the frameworks developed independently in [GW07; CDP09]. However, the matrix size necessary here is exponential in  $T$ .

In continuous time, [KBG01] discuss time-optimal control in a still more general setting based on the Pontryagin maximum principle.

## 6 Conclusion and outlook

The main novelty in this note is the universal algorithm, which is simpler than the previous one based on phase detection [Lee+11; Bel15] and shaves another factor of  $\Theta(\log(1/\epsilon))$  off the runtime. The way we obtained this algorithm, and proved its correctness, is also unusual:

- Instead of specifying gates and families of states directly, we considered all inputs at once in an associated control problem and feasible ways to manipulate reduced density matrices involving these inputs,
- Instead of proving correctness starting with the correct initial state, and showing that the final state is not too wrong after application of the algorithm, we started with a slightly wrong initial state, and proved that the final state will be correct when applied to that modified state.

These ideas may be useful to devise other quantum algorithms.

A query-efficient algorithm doesn't necessarily translate into a gate-efficient one in the usual model of quantum complexity, as the algorithm's unitaries may be hard to construct. For example, the query complexity of the  $k$ -distinctness problem was characterized by Belovs in 2012 [Bel12] using the adversary method, but an algorithm matching this complexity (up to a polylogarithmic factor) was only presented in 2022 by Jeffery and Zur [JZ22]. So it would be interesting to find conditions that  $\bar{\pi}$  needs to fulfill so that the unitaries involved in the associated universal algorithm are efficiently representable.



## References

- [KBG01] Navin Khaneja, Roger Brockett, and Steffen J. Glaser. “Time optimal control in spin systems”. In: *Physical Review A* 63.3 (2001).
- [NC02] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.
- [Bar07] Howard Barnum. “Semidefinite programming characterization and spectral adversary method for quantum complexity with noncommuting unitary queries”. In: *CoRR* abs/quant-ph/0703141 (2007).
- [GW07] Gus Gutoski and John Watrous. “Toward a general theory of quantum games”. In: *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing - STOC '07*. ACM Press, 2007.
- [CDP09] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. “Theoretical framework for quantum networks”. In: *Physical Review A* 80.2 (2009).
- [Lee+11] Troy Lee et al. “Quantum Query Complexity of State Conversion”. In: *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*. IEEE, Oct. 2011.
- [Bel12] Aleksandrs Belovs. “Learning-Graph-Based Quantum Algorithm for  $k$ -Distinctness”. In: *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*. 2012, pp. 207–216.
- [Ozo12] Maris Ozols. *Unitary equivalence of purifications*. <https://marozols.wordpress.com/2012/05/09/unitary-equivalence-of-purifications/>. 2012.
- [Bel15] Aleksandrs Belovs. *Variations on Quantum Adversary*. 2015.
- [JZ22] Stacey Jeffery and Sebastian Zur. *Multidimensional Quantum Walks, with Application to  $k$ -Distinctness*. arXiv, 2022.
- [BY23] Aleksandrs Belovs and Duyal Yolcu. “One-Way Ticket to Las Vegas and the Quantum Adversary”. In: *2023 Conference on Quantum Information Processing*. 2023, pp. 207–216.
- [BSS] H. Barnum, M. Saks, and M. Szegedy. “Quantum query complexity and semi-definite programming”. In: *18th IEEE Annual Conference on Computational Complexity, 2003. Proceedings*. IEEE Comput. Soc.
- [Chi] Andrew M Childs. “Lecture notes on quantum algorithms”. In: ().