On the additive and multiplicative adversary methods

Loïck Magnin*,† Martin Roetteler† Jérémie Roland†

The quantum adversary method is a powerful technique to prove lower bounds on quantum query complexity [BBBV97, Amb00, HNS01, BS04, Amb03, LM08]. The idea is to define a progress function varying from an initial value (before any query) to a final value (depending on the success probability of the algorithm) with one main property: the value of the progress function varies only when the oracle is queried. Then, a lower bound on the quantum query complexity of the problem can be obtained by bounding the amount of progress done by one query.

Initially, different adversary methods were introduced, but they were later proved to be all equivalent [ŠS06]. This unified method relied on optimizing an adversary matrix assigning weights to different pairs of inputs to the problem. While the original method only considered positive weights, it was later shown that negative weights also lead to a lower bound, which can actually be stronger in some cases [HLŠ07]. The relevance of this new adversary method with negative weights was made even clearer when it was shown that it is (almost) tight for Boolean functions [Rei09].

For non-Boolean functions, however, the situation is not so clear. For some problems, it is known that the adversary method gives weaker bounds than the so-called polynomial method [BBC+98, Amb03, KŠdW07], or some other ad-hoc techniques [Amb05, AŠW07]. For this reason, outside of the realm of Boolean functions, the quest for an all-powerful lower bound technique is not over. In [Špa08], Špalek introduced the *multiplicative* adversary method, generalizing previous ad-hoc methods for a set of problems. In particular, he showed that this method did not suffer from one particular limitation of the usual adversary method (which we will from now on call *additive*), the fact that it cannot prove lower bounds for very small success probabilities (this is not an issue for Boolean functions where the success probability is always at least 1/2). However, he left unanswered the question of how multiplicative and additive methods relate in the case of high success probability.

While these methods have been designed to prove lower bounds on the quantum query complexity of *classical* functions, in a quantum context it might be interesting to consider quantum problems, such as quantum state generation. For example, this approach has been considered in [AT03] as an attempt to tackle the Graph Isomorphism problem, as it is well known that it reduces to generating the state $(1/\sqrt{N!})\sum_{\pi\in S_N}|\pi(G)\rangle$ for a graph

*Université Paris-Sud - Université Libre de Bruxelles
†NEC Laboratories America

G with N vertices. Therefore, an extension of the adversary method to quantum state generation might prove to be a very useful tool.

The usual approach for proving lower bounds for a problem $\mathcal{P}$ by the adversary method is to assign weights to pairs of functions f and g such that $\mathcal{P}(f) \neq \mathcal{P}(g)$ and to look how fast the state ρ^t of any algorithm for $\mathcal{P}$ diverges for the inputs f and g. The progress function is then defined as: $W^t = \mathrm{Tr}[\Gamma\rho^t]$ where $\Gamma_{f,g} = 0$ if $\mathcal{P}(f) = \mathcal{P}(g)$. In this work we interpret the method slightly differently with a geometric interpretation: we are interested in the eigenspaces of ρ^t. We study how an oracle call transfer some weight from the eigenspaces of the initial state ρ^0 to the one of the final state ρ^T (this is reminiscent of the approach of [Amb05, Špa08], where this is done for classical problems). This view motivates a new definition of the adversary matrix: it is a Hermitian matrix Γ such that for all normalized Gram matrix M, $\mathrm{Tr}[\Gamma(\rho^\infty \circ M)] = 0$ where ρ^∞ is the target state (zero-error algorithm) and $\circ$ denotes the Hadamard product. By giving this interpretation which is closer to the quantum structure of the problem, we give elementary and highly intuitive proofs of the additive and multiplicative methods, contrasting with some rather technical proofs e.g. in [HLŠ07, Špa08].

To solve the open problem of comparing the power of the additive and multiplicative adversary methods [Špa08], we introduce yet another flavor of adversary method: an additive adversary method for small success probability.

Theorem 1 *Consider a quantum algorithm solving $\mathcal{P}$ with success at least $1-\varepsilon$. Let $\tilde{\Gamma}$ be any additive adversary matrix, S_{bad} be the direct sum of eigenspaces of $\tilde{\Gamma}$ with eigenvalue strictly larger than $\tilde{\lambda} < 1$, and assume that for all ρ having support only on S_{bad} the quantity $\eta(\rho) = \max_M [\mathcal{F}(\rho, \rho^\infty \circ M)]^2$ satisfies $\eta(\rho) \leq \eta$ with $0 \leq \eta \leq 1-\varepsilon$. We have*

1. $\tilde{W}^0 = 1$,
2. $|\tilde{W}^{t+1} - \tilde{W}^t| \leq \max_x \left\|\tilde{\Gamma}_x - \tilde{\Gamma}\right\|$,
3. $\tilde{W}^T \leq 1 - \tilde{K}(\tilde{\Gamma}, \tilde{\lambda}, \varepsilon)$, *where* $\tilde{K}(\tilde{\Gamma}, \tilde{\lambda}, \varepsilon) = (1-\tilde{\lambda})(\sqrt{1-\varepsilon} - \sqrt{\eta})^2$.

Therefore, $Q_\varepsilon(\mathcal{P}) \geq \widetilde{\mathrm{ADV}}_\varepsilon(\mathcal{P}) = \max_{\tilde{\Gamma},\tilde{\lambda}} \frac{\tilde{K}(\tilde{\Gamma},\tilde{\lambda},\varepsilon)}{\max_x \left\|\tilde{\Gamma}_x - \tilde{\Gamma}\right\|}$.

This adversary method is equivalent to the additive method for large success probability, but is also able to prove non-trivial lower-bounds for small success probability, contradicting the statement in [Špa08] that the additive adversary method fails in this case.

The notion of success probability we use here is the square of the fidelity between the output of the algorithm and the desired state (when $\mathcal{P}$ consists in computing a classical function, this definition coincides with the usual one). Hence, this method can also be applied to prove lower bounds on quantum state generation. In fact, we are able to extend the usual additive and multiplicative methods in a similar way.

We can now compare the strength of the 3 methods. We denote by $\widetilde{\mathrm{ADV}}_\varepsilon(\mathcal{P})$ our new bound, by $\mathrm{ADV}^{\pm}_\varepsilon(\mathcal{P})$ the usual additive adversary bound (with negative weights as in [HLŠ07]) and by $\mathrm{MADV}_\varepsilon(\mathcal{P})$ the multiplicative adversary bound [Špa08]. We then have:

Theorem 2 $\mathrm{MADV}_\varepsilon(\mathcal{P}) \geq \widetilde{\mathrm{ADV}}_\varepsilon(\mathcal{P}) \geq \mathrm{ADV}^{\pm}_\varepsilon(\mathcal{P})/60$.

We also show that all these inequalities are strict by considering the search problem (Grover):

Lemma 3 *For any* $0 < \varepsilon < 1 - \frac{1}{n}$*, we have*

$$\mathrm{ADV}^{\pm}_\varepsilon(\mathrm{Search}_n) = \Omega\left((1-\varepsilon-2\sqrt{\varepsilon(1-\varepsilon)})\sqrt{n}\right)$$
$$\widetilde{\mathrm{ADV}}_\varepsilon(\mathrm{Search}_n) = \Omega\left((\sqrt{1-\varepsilon}-1/\sqrt{n})^2\sqrt{n}\right)$$
$$\mathrm{MADV}_\varepsilon(\mathrm{Search}_n) = \Omega\left((\sqrt{1-\varepsilon}-1/\sqrt{n})\sqrt{n}\right).$$

In particular, for $\varepsilon > 1/5$*, we have* $\mathrm{MADV}_\varepsilon(\mathrm{Search}_n) > \widetilde{\mathrm{ADV}}_\varepsilon(\mathrm{Search}_n) > \mathrm{ADV}^{\pm}_\varepsilon(\mathrm{Search}_n)$*.*

Two major difficulties of using the adversary method are to choose a good adversary matrix $\tilde{\Gamma}$ and to compute the spectral norm of $\tilde{\Gamma}_x - \tilde{\Gamma}$. As it has been previously noted many interesting problems have strong symmetries [Amb05, AŠW07, Špa08]. Following the *automorphism principle* of [HLŠ07], we define the automorphism group of $\mathcal{P}$:

Definition 1 *We call a group* $G \subseteq S_M \times S_N$ *an* automorphism group *of a problem* $\mathcal{P}$ *if: 1) For any* $(\pi,\tau) \in G$ *and* $f \in \mathcal{F}$*, we have* $\pi \circ f \circ \tau \in \mathcal{F}$*; and 2) For any* $(\pi,\tau) \in G$*, there exists a unitary* $V_{\pi,\tau}$ *such that* $V_{\pi,\tau}|\mathcal{P}(f)\rangle = |\mathcal{P}(\pi \circ f \circ \tau)\rangle$ *for all* $f \in \mathcal{F}$*. (where* M *and* N *are the size of the input and output alphabets of* $f \in \mathcal{F}$*). We also define* $G_x = \{(\pi,\tau) \in G : \tau(x) = x\}$*.*

A similar approach has been used before to help designing $\tilde{\Gamma}$. We push this approach further to show how it can be explicitly used to compute the adversary bound itself.

Theorem 4 $\left\|\tilde{\Gamma}_x - \tilde{\Gamma}\right\|^2 = \max_l \left\|\tilde{\Delta}^l_x\right\|$,

where the maximum is over irreps l of G_x and $\tilde{\Delta}^l_x$ is a matrix of size $m_l \times m_l$ (the multiplicity of l) depending only on irreps of G and G_x. Theses matrices are indeed a lot smaller than $\tilde{\Gamma}$ since they typically have size at most 2×2 [Amb05, AŠW07, Špa08]. We therefore reduced the adversary method from an algebraic problem to the study of the representations of the automorphism group.

From these results, we can conclude that the multiplicative adversary method is a good candidate for a unified framework of lower bound techniques: it generalizes the usual adversary method which is (almost) tight for Boolean functions, as well as other ad-hoc lower bounds, and it can also be used to prove lower bounds on quantum state generation.

References

[Amb00] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 636–643, Portland, Oregon, United States, 2000. ACM.

[Amb03] Andris Ambainis. Polynomial degree vs. quantum query complexity. In *Foundations of Computer Science, Annual IEEE Symposium on*, volume 0, page 230, Los Alamitos, CA, USA, 2003. IEEE Computer Society.

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

[AŠW07] Andris Ambainis, Robert Špalek, and Ronald Wolf. A new quantum lower bound method, with applications to direct product theorems and Time-Space tradeoffs. *Algorithmica*, 55(3):422–461, 2007.

[AT03] Dorit Aharonov and Amnon Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 20–29, San Diego, CA, USA, 2003. ACM.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[BBC+98] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, page 352. IEEE Computer Society, 1998.

[BS04] Howard Barnum and Michael Saks. A lower bound on the quantum query complexity of read-once functions. *J. Comput. Syst. Sci.*, 69(2):244–258, 2004.

[HLŠ07] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *STOC '07: Proceedings of the thirty-ninth annual ACM Symposium on Theory of Computing*, pages 526–535, New York, NY, USA, 2007. ACM.

[HNS01] Peter Høyer, Jan Neerbek, and Yaoyun Shi. Quantum complexities of ordered searching, sorting, and element distinctness. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming,*, pages 346–357. Springer-Verlag, 2001.

[KŠdW07] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. Quantum and classical strong direct product theorems and optimal Time-Space tradeoffs. *SIAM Journal on Computing*, 36(5):1472–1493, January 2007.

[LM08] Sophie Laplante and Frédéric Magniez. Lower bounds for randomized and quantum query complexity using kolmogorov arguments. *SIAM Journal on Computing*, 38(1):46–62, 2008.

[Rei09] Ben W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function. In *Annual IEEE Symposium on Foundations of Computer Science,*, pages 544–551, Los Alamitos, CA, USA, 2009. IEEE Computer Society.

[Špa08] Robert Špalek. The multiplicative quantum adversary. In *CCC '08: Proceedings of the 2008 IEEE 23rd Annual Conference on Computational Complexity*, pages 237–248, Washington, DC, USA, 2008. IEEE Computer Society.

[ŠS06] Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006.