A strong direct product theorem for quantum query complexity

[arXiv:1104.4468]

Troy Lee [*] Jérémie Roland [†]

Abstract

We show that quantum query complexity satisfies a strong direct product theorem. This means that computing k copies of a function with less than k times the quantum queries needed to compute one copy of the function implies that the overall success probability will be exponentially small in k. For a boolean function f we also show an XOR lemma—computing the parity of k copies of f with less than k times the queries needed for one copy implies that the advantage over random guessing will be exponentially small.

We do this by showing that the multiplicative adversary method, which inherently satisfies a strong direct product theorem, is always at least as large as the additive adversary method, which is known to characterize quantum query complexity.

Direct product theorems. We show that quantum query complexity satisfies a strong direct product theorem. A strong direct product theorem states that to compute k copies of a function with less than k times the resources needed to compute one copy of the function implies that the success probability will be exponentially small in k. For boolean functions, we further show an XOR lemma. XOR lemmas are closely related to strong direct product theorems and state that computing the parity of k copies of a boolean function with less than k times the resources needed to compute one copy implies that the advantage over random guessing will be exponentially small. XOR lemmas can be shown quite generally to imply strong direct product theorems and even threshold direct product theorems [Ung09], which state that one cannot compute a μ fraction of the k copies with less than μk times the resources with better than exponentially small (in μk) success probability. Thus in the boolean case we are also able to obtain a threshold direct product theorem.

Related work. How the resources needed to compute k copies of a function scale with those needed for one copy is a very natural question that has been asked of many computational models. While direct product theorems are intuitively highly plausible, they do not hold in all models [Sha03], and there are relatively few models where strong direct product theorems are known. Notable examples of direct product-type results include Yao's XOR lemma and Raz's parallel repetition theorem [Raz98]. Closer to our setting, strong direct product theorems have been shown for one-way randomized communication complexity [Jai10] and for randomized query complexity [Dru11].

In quantum query complexity strong direct product theorems were previously known for some special classes of functions and bounds shown by particular methods. In the first such result, Klauck, Špalek and de Wolf [KŠdW07] used the polynomial method [BBC$^+$98] to show a strong direct

[*] Centre for Quantum Technologies

[†] NEC Laboratories America

product theorem for the quantum query complexity of the OR function. Via block sensitivity, this gives a polynomially tight strong direct product theorem for all functions—namely, any algorithm using less than a constant fraction times $kQ(f)^{1/6}$ will have exponentially small success probability for computing k copies of f.

Sherstov [She11] recently showed how certain lower bound techniques based on looking at the distance of the function to a convex set inherently satisfy a strong direct product theorem. As an application he was able to show that the polynomial method satisfies a strong direct product theorem *in general*. Thus one obtains a strong direct product theorem for the quantum query complexity of any function where the polynomial method shows a tight lower bound. Super-linear gaps between the polynomial degree and quantum query complexity are known [Amb06], however, so this does not give a tight strong direct product theorem for all functions.

Direct product results have also been shown by the other main lower bound technique in quantum query complexity, the adversary method. The adversary method defines a potential function based on the state of the algorithm after t queries, and bounds the change in this potential function from one query to the next. By developing a new kind of adversary method, Ambainis, Špalek, and de Wolf [AŠdW06] showed a strong direct product theorem for all symmetric functions. Špalek [Špa08] formalized this technique into a generic method, coining it the multiplicative adversary method, and showed that this method inherently satisfies a strong direct product theorem. The name multiplicative adversary contrasts with the additive adversary method, introduced earlier by Ambainis [Amb02] and later extended by Høyer, Lee and Špalek [HLŠ07]. The additive adversary method bounds the difference of the potential function from one step to the next, while the multiplicative adversary method bounds the corresponding ratio.

There have recently been great strides in our understanding of the adversary methods. A series of works [FGG08, CCJY09, ACR$^+$10, RŠ08, Rei09, Rei10, LMRŠ10] has culminated in showing that the additive adversary method characterizes the bounded-error quantum query complexity of any function whatsoever. Ambainis *et al.* [AMRR11], answering an open question of Špalek [Špa08], showed that the multiplicative adversary is at least as large as the additive. Thus the multiplicative adversary bound also characterizes bounded-error quantum query complexity.

This seems like it would close the question of a strong direct product theorem for quantum query complexity. The catch is the following. The multiplicative adversary method can be viewed as a family of methods parameterized by the bound c on the ratio of the potential function from one step to the next. The strong direct product theorem of [Špa08] holds for any value of c sufficiently bounded away from 1. The result of [AMRR11], however, was shown in the limit $c \to 1$, which ends up degrading the resulting direct product theorem into a direct sum theorem.

Our results. We show that the multiplicative adversary is at least as large as the additive adversary for a value of c bounded away from 1 [LR11, Claim 3.16]. A similar result was independently observed by Belovs [Bel11]. Together with the strong direct product theorem for the multiplicative adversary by [Špa08] this suffices to give a strong direct product theorem for quantum query complexity. Rather than use this "out of the box" strong direct product theorem, however, we prove the strong direct product theorem from scratch using a stronger output condition than those used previously [Špa08, AMRR11]. This results in better parameters, and a better understanding of the multiplicative adversary method [LR11, Theorem 1.1].

Theorem 1.1 (Strong direct product theorem). *Let $f : \mathcal{D} \to E$ where $\mathcal{D} \subseteq D^n$ for finite sets D, E.*

For an integer $k > 0$ define $f^{(k)}(x^1, \ldots, x^k) = (f(x^1), \ldots, f(x^k))$. Then, for any $(2/3) \le \delta \le 1$,

$$Q_{1-\delta^{k/2}}(f^{(k)}) \ge \frac{k \ln(3\delta/2)}{8000} \cdot Q_{1/4}(f) \ .$$

In the boolean case, we prove the following XOR lemma [LR11, Lemma 1.2] which also implies a threshold direct product theorem [LR11, Theorem 5.5].

Lemma 1.2 (XOR Lemma)**.** *Let $f : \mathcal{D} \to \{0,1\}$ where $\mathcal{D} \subseteq D^n$ for finite set D. For an integer $k > 0$ and any $0 \le \delta \le 1$,*

$$Q_{(1-\delta^{k/2})/2}(\oplus \circ f^{(k)}) \ge \frac{k\delta}{8000} \cdot Q_{1/4}(f) \ .$$

Proof technique. While the statement of our main theorems concern functions, a key to our proofs, especially for the XOR lemma, is to consider more general state generation problems, introduced in [AMRR11]. Instead of producing a classical value $f(x)$ on input x, the goal in state generation is to produce a specified target state $|\sigma_x\rangle$, again by making queries to the input x. We will refer to $\sigma(x,y) = \langle \sigma_x | \sigma_y \rangle$ as the target Gram matrix. Evaluating a function f can be viewed as a special case of state generation where the target Gram matrix is $F(x,y) = \delta_{f(x),f(y)}$.

Our most general result [LR11, Theorem 4.1] shows that for a restricted class of target Gram matrices σ, to generate $\sigma^{\otimes k}$ with better than exponentially small success probability requires at least a constant fraction of k times the complexity of σ. The strong direct product theorem is obtained as a special case of this theorem by considering the Gram matrix $F(x,y) = \delta_{f(x),f(y)}$. To obtain the XOR lemma, we apply this theorem with the state generation problem of computing f in the phase, that is to generate $\sigma_f(x,y) = (-1)^{f(x)+f(y)}$. The advantage of considering this state is that $\sigma_f^{\otimes k}$ is the state generation problem corresponding to computing the parity of k copies of f in the phase. We then show that the complexities of f and the state generation problem of computing f in the phase are closely related.

Another key element of our proofs is a new characterization of the set of valid output Gram matrices for an algorithm solving a state generation problem with success probability $1-\epsilon$ [LR11, Claim 3.8]. We call a condition which defines a set containing this set of valid output matrices an output condition. Usually a lower bound uses an output condition which is a relaxation of the true output condition, and shows a lower bound against all Gram matrices satisfying this output condition, and thereby all valid output matrices as well. Examples of output conditions previously used with the adversary bound include being close to the target Gram matrix in distance measured by the l_∞ or γ_2 norms. These conditions, however, do not work for small success probabilities, which is critical to obtain the strong direct product theorem.

We give a new characterization of the true output condition in terms of fidelity. Since the fidelity between two quantum states is bounded by the fidelity between the probability distributions arising from any measurement on those states, a relaxation of this output condition may be obtained by considering the measurement corresponding to an optimal witness for the adversary bound of the problem. A lower bound on the multiplicative bound under this relaxed output condition can be written as a linear program. By taking the dual of this linear program we are able to lower bound the value on $\sigma^{\otimes k}$ in terms of the bound for σ by using a completely classical claim about product probability distributions [LR11, Corollary 3.13]. This approach allows us to obtain a cleaner statement for the strong direct product theorem than what we would obtain from the output condition used in [Špa08, AMRR11], and also clarifies the inner workings of the adversary method, which might be of independent interest.

References

[ACR+10] Andris Ambainis, Andrew M. Childs, Ben W. Reichardt, Robert Špalek, and Shengyu Zhang. Any AND-OR Formula of Size N Can Be Evaluated in Time $N^{1/2+o(1)}$ on a Quantum Computer. *SIAM Journal on Computing*, 39(6):2513, 2010. doi:10.1137/080712167.

[Amb02] Andris Ambainis. Quantum Lower Bounds by Quantum Arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. arXiv:quant-ph/0002066, doi:10.1006/jcss.2002.1826.

[Amb06] Andris Ambainis. Polynomial degree vs. quantum query complexity. *Journal of Computer and System Sciences*, 72(2):220–238, 2006. arXiv:quant-ph/0305028, doi:10.1016/j.jcss.2005.06.006.

[AMRR11] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland. Symmetry-assisted adversaries for quantum state generation. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 167–177. IEEE Computer Society, 2011. arXiv:1012.2112.

[AŠdW06] Andris Ambainis, Robert Špalek, and Ronald de Wolf. A new quantum lower bound method with applications to direct product theorems and time-space tradeoffs. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 618–633, Seattle, WA, USA, 2006. ACM. doi:10.1145/1132516.1132604.

[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 IEEE Symposium on Foundations of Computer Science*, page 352. IEEE Computer Society, 1998. arXiv:quant-ph/9802049, doi:10.1109/SFCS.1998.743485.

[Bel11] Aleksandrs Belovs. Personal communication, 2011.

[CCJY09] Andrew M. Childs, Richard Cleve, Stephen P. Jordan, and David Yeung. Discrete-query quantum algorithm for NAND trees. *Theory of Computing*, 5:119–123, 2009. arXiv:quant-ph/0702160, doi:10.4086/toc.2009.v005a005.

[Dru11] Andrew Drucker. Improved Direct Product Theorems for Randomized Query Complexity. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 1–11. IEEE Computer Society, 2011. arXiv:1005.0644.

[FGG08] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A Quantum Algorithm for the Hamiltonian NAND Tree. *Theory of Computing*, 4:169–190, 2008. arXiv:quant-ph/0702144, doi:10.4086/toc.2008.v004a008.

[HLŠ07] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 526–535, New York, NY, USA, 2007. ACM. arXiv:quant-ph/0611054, doi:10.1145/1250790.1250867.

[Jai10] Rahul Jain. Strong direct product conjecture holds for all relations in public coin randomized one-way communication complexity. *SIAM Journal on Computing*, 2010. arXiv:1010.0522.

[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, 2007. arXiv:quant-ph/0402123, doi:10.1137/05063235X.

[LMRŠ10] Troy Lee, Rajat Mittal, Ben W. Reichardt, and Robert Špalek. An adversary for algorithms. 2010. arXiv:1011.3020.

[LR11] Troy Lee and Jérémie Roland. A strong direct product theorem for quantum query complexity. 2011. arXiv:1104.4468.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998. doi:10.1137/S0097539795280895.

[Rei09] Ben W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 544–551, Atlanta, Georgia, 2009. IEEE Computer Society. arXiv:0904.2759, doi:10.1109/FOCS.2009.55.

[Rei10] Ben W. Reichardt. Reflections for quantum query algorithms. 2010. arXiv:1005.1601.

[RŠ08] Ben W. Reichardt and Robert Špalek. Span-program-based quantum algorithm for evaluating formulas. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 103–112, Victoria, British Columbia, Canada, 2008. ACM. doi:10.1145/1374376.1374394.

[Sha03] Ronen Shaltiel. Towards proving strong direct product theorems. *Computational Complexity*, 12(1-2):1–22, 2003. doi:10.1007/s00037-003-0175-x.

[She11] Alexander A. Sherstov. Strong direct product theorems for quantum communication and query complexity. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, pages 41–50, San Jose, CA, USA, 2011. ACM. arXiv:1011.4935.

[Špa08] Robert Špalek. The multiplicative quantum adversary. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 237–248, Washington, DC, USA, 2008. IEEE Computer Society. arXiv:quant-ph/0703237, doi:10.1109/CCC.2008.9.

[Ung09] Falk Unger. A Probabilistic Inequality with Applications to Threshold Direct-Product Theorems. *50th Annual IEEE Symposium on Foundations of Computer Science*, 78(78):221–229, October 2009. doi:10.1109/FOCS.2009.62.