

A strong direct product theorem for quantum query complexity

Troy Lee ^{*} J er mie Roland [†]

September 21, 2018

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.

1 Introduction

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.

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,

^{*}Centre for Quantum Technologies

[†]NEC Laboratories America

Špalek and de Wolf [KŠdW07] used the polynomial method [BBC⁺98] to show a strong direct 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 $c \rightarrow 1$, which ends up degrading the resulting direct product theorem into a direct sum theorem. We show that the multiplicative adversary is at least as large as the additive adversary for a value of c bounded away from 1. 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.

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

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

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

In the boolean case, we prove the following XOR lemma which also implies a threshold direct product theorem ([Theorem 5.5](#)).

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

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

1.1 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 ([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 $1 - \epsilon$ ([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 ([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.

2 Preliminaries

Let $\Re(z)$ denote the real part of a complex number z . Let $\delta_{a,b}$ denote the Kronecker delta function. We will refer throughout to a function $f : \mathcal{D} \rightarrow E$ where $\mathcal{D} \subseteq D^n$ for finite sets D, E . We let $f^{(k)} : \mathcal{D}^k \rightarrow E^k$ be the function computing k independent copies of f , namely $f^{(k)}(x^1, \dots, x^k) = (f(x^1), \dots, f(x^k))$. We let $\oplus \circ f^{(k)}$ denote the parity function composed with $f^{(k)}$. We also define some auxiliary matrices associated with f . Let $F(x, y) = \delta_{f(x), f(y)}$, and $\Delta_i(x, y) = \delta_{x_i, y_i}$ for $x, y \in \mathcal{D}$ and $i \in [n]$. For boolean functions, i.e., when $|E| = 2$, we also define the matrix $\sigma_f(x, y) = (-1)^{f(x)+f(y)}$ for $x, y \in \mathcal{D}$. Note that $\sigma_f = 2F - J$, where J is the all-1 matrix. We use $A \circ B$ for the entrywise product between two matrices A, B , also known as the Schur or Hadamard product.

Let ρ, σ be two $|\mathcal{D}| \times |\mathcal{D}|$ positive semidefinite matrices such that $\text{Tr}\rho = \text{Tr}\sigma = 1$ (i.e., quantum states on a $|\mathcal{D}|$ -dim Hilbert space) and p, q be two probability distributions over \mathcal{D} . We will use the notion of fidelity, for both quantum states and classical probability distributions.

Definition 2.1 (Fidelity).

$$\mathcal{F}(\rho, \sigma) = \text{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \qquad \mathcal{F}(p, q) = \sum_{x \in \mathcal{D}} \sqrt{p_x q_x}$$

For $0 \leq \lambda \leq 1$ and $0 < \mu < 1$, we denote by $D(\lambda || \mu)$ the binary relative entropy of λ and μ , defined as follows.

Definition 2.2 (Binary relative entropy).

$$D(\lambda || \mu) = \lambda \ln \frac{\lambda}{\mu} + (1 - \lambda) \ln \frac{1 - \lambda}{1 - \mu}$$

where $0 \ln 0 = 0$.

Finally, for a $|\mathcal{D}| \times |\mathcal{D}|$ matrix A we will also use the factorization norm $\gamma_2(A)$.

Definition 2.3 (Factorization norm).

$$\begin{aligned} \gamma_2(A) &= \min_{\substack{m \in \mathbf{N} \\ |u_x\rangle, |v_x\rangle \in \mathbf{C}^m}} \left\{ \max_{x \in \mathcal{D}} \max \left\{ \| |u_x\rangle \|^2, \| |v_x\rangle \|^2 \right\} : \forall x, y \in \mathcal{D}, A_{x,y} = \langle u_x | v_y \rangle \right\} \\ &= \max_{\substack{|u\rangle, |v\rangle \\ \| |u\rangle \| = \| |v\rangle \| = 1}} \| A \circ |u\rangle \langle v| \|_{\text{tr}} \end{aligned}$$

We will make use of the following basic claims.

Claim 2.4. For any matrices A, B where $A \circ B$ is defined,

1. $\| A \circ B \| \leq \gamma_2(A) \cdot \| B \|$
2. $\{ A \succeq 0 \text{ and } B \succeq 0 \} \Rightarrow A \circ B \succeq 0$

2.1 Quantum query complexity and state generation

The quantum query complexity of f , denoted $Q_\epsilon(f)$ is the minimum number of input queries needed to compute f with error at most ϵ . We refer to the survey [BdW02] for definitions and background on this model.

Although our main interest will be in the query complexity of functions, it will be useful to also talk about 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 . As unitary transformations independent of the input can be made for free in the query model, a state generation problem is wholly determined by the Gram matrix $\sigma(x, y) = \langle \sigma_x | \sigma_y \rangle$ of the target states $\{|\sigma_x\rangle\}_{x \in \mathcal{D}}$. We refer to σ as the target Gram matrix.

State generation problems come in two variations, coherent and non-coherent. An algorithm \mathcal{P} solves the coherent quantum state generation problem σ with error at most ϵ if, for every $x \in \mathcal{D}$, it generates a state $|\mathcal{P}(x)\rangle \in \mathcal{H} \otimes \mathcal{H}'$ such that $\Re(\langle \mathcal{P}(x) | (|\sigma_x\rangle \otimes |\bar{0}\rangle)) \geq \sqrt{1 - \epsilon}$, where \mathcal{H}' denotes the workspace of the algorithm, and $|\bar{0}\rangle$ is a default state for \mathcal{H}' . The coherent quantum query complexity of σ , denoted $Q_\epsilon^c(\sigma)$ is the minimum number of queries needed to generate σ coherently with error at most ϵ .

An algorithm \mathcal{P} solves the non-coherent state generation problem σ with error at most ϵ if there exists a set of states $|\phi_x\rangle \in \mathcal{H}'$ such that $\Re(\langle \mathcal{P}(x) | (|\sigma_x\rangle \otimes |\phi_x\rangle)) \geq \sqrt{1 - \epsilon}$ for all $x \in \mathcal{D}$. We denote by $Q_\epsilon(\sigma)$ the non-coherent query complexity of generating σ with error ϵ .

Evaluating a function f can be seen as a special case of non-coherent state generation where the target Gram matrix is $F(x, y) = \delta_{f(x), f(y)}$. In other words, $Q_\epsilon(f) = Q_\epsilon(F)$ where $F(x, y) = \delta_{f(x), f(y)}$, justifying our abuse of notation. For state generation problems corresponding to functions the coherent and non-coherent complexities are closely related.

Claim 2.5. *Let f be a function. Then*

$$Q_\epsilon(F) \leq Q_\epsilon^c(F) \leq 2Q_{1-\sqrt{1-\epsilon}}(F) .$$

Proof. The lower bound holds for a general target Gram matrix σ , as the success condition in the coherent case implies the non-coherent one.

For the upper bound, let A_x be an algorithm computing $f(x)$ with success probability $1 - \eta$. Thus the algorithm applied on $|0\rangle|\bar{0}\rangle$, where the first register is the output register and the second register corresponds to some workspace initialized in a default state, prepares a state

$$A_x|0\rangle|\bar{0}\rangle = \sum_j \alpha_j |j + f(x)\rangle |\psi_j\rangle,$$

where by assumption $|\alpha_0| \geq \sqrt{1 - \eta}$, and the states $|\psi_j\rangle$ describe the final state of the workspace register. Let us now copy the output register into an additional register initialized in the state $|0\rangle$ using an addition gate G , and finally uncompute the original output register together with the workspace by using the algorithm A_x in reverse.

We analyze the overlap of $A_x^{-1}GA_x|0\rangle|\bar{0}\rangle|0\rangle$ with $|0\rangle|\bar{0}\rangle|f(x)\rangle$. After applying G on $A_x|0\rangle|\bar{0}\rangle|0\rangle$, we have the state $|v\rangle = \sum_j \alpha_j |j + f(x)\rangle |\psi_j\rangle |j + f(x)\rangle$. Now we look at the overlap of $|0\rangle|\bar{0}\rangle|f(x)\rangle$ with $A_x^{-1}|v\rangle$ or, equivalently, the overlap of $A_x|0\rangle|\bar{0}\rangle|f(x)\rangle$ with $|v\rangle$. Since

$$A_x|0\rangle|\bar{0}\rangle|f(x)\rangle = \sum_j \alpha_j |j + f(x)\rangle |\psi_j\rangle |f(x)\rangle,$$

we have

$$\langle 0|\langle \bar{0}|\langle f(x)|A_x^{-1}|v\rangle = \sum_j |\alpha_j|^2 \langle f(x)|j + f(x)\rangle \geq 1 - \eta.$$

Therefore, this algorithm coherently computes $f(x)$ with success probability $1 - \epsilon \geq (1 - \eta)^2$. Inverting this relation, we obtain $\eta \geq 1 - \sqrt{1 - \epsilon}$. \square

We will also consider another type of state generation problem associated with a function, that of computing the function in the phase. For a boolean function $f : \mathcal{D} \rightarrow \{0, 1\}$ let $\sigma_f(x, y) = (-1)^{f(x)+f(y)}$. While the non-coherent complexity of σ_f is trivial, the coherent complexity of σ_f is closely related to that of F .

Claim 2.6.

$$Q_{(1-\sqrt{1-\epsilon})/2+\epsilon/4}^c(F) \leq Q_\epsilon^c(\sigma_f) \leq 2Q_{(1-\sqrt{1-\epsilon})/2}(F)$$

Proof. For the lower bound, we turn an algorithm for σ_f into an algorithm for $F = (J + \sigma_f)/2$ by using the SWAP test. The error dependence then follows from the joint concavity of the fidelity:

$$\mathcal{F}\left(\frac{J+\rho}{2} \circ uu^*, \frac{J+\sigma_f}{2} \circ uu^*\right) \geq \frac{1}{2} + \frac{1}{2}\mathcal{F}(\rho \circ uu^*, \sigma_f \circ uu^*).$$

for any u .

For the upper bound, let us consider an algorithm A_x computing $f(x)$ (in a register) with success probability $1 - \eta$. Thus, the algorithm applied on $|0\rangle|\bar{0}\rangle$, where the first register is the output register and the second register corresponds to some workspace initialized in a default state, prepares a state

$$A_x|0\rangle|\bar{0}\rangle = \sum_{j=0,1} \alpha_j |j \oplus f(x)\rangle |\psi_j\rangle,$$

where by assumption $|\alpha_0| \geq \sqrt{1 - \eta}$, and the states $|\psi_j\rangle$ describe the final state of the workspace register. Let Φ be a phase gate acting on the output register as $|b\rangle \mapsto (-1)^{f(x)}|b\rangle$. We can turn an algorithm A_x computing in a register into an algorithm computing in the phase by first applying A_x to compute the output, then applying the phase gate Φ , and finally applying A_x^{-1} to uncompute the output.

After applying Φ on $A_x|0\rangle|\bar{0}\rangle$, we have the state $\Phi A_x|0\rangle|\bar{0}\rangle = \sum_{j=0,1} (-1)^{j+f(x)} \alpha_j |j \oplus f(x)\rangle |\psi_j\rangle$. Now we look at the overlap of $(-1)^{f(x)}|0\rangle|\bar{0}\rangle$ with $A_x^{-1}\Phi A_x|0\rangle|\bar{0}\rangle$ or, equivalently, the overlap of $(-1)^{f(x)}A_x|0\rangle|\bar{0}\rangle$ with $\Phi A_x|0\rangle|\bar{0}\rangle$. We have

$$(-1)^{f(x)}\langle 0|\langle \bar{0}|A_x^{-1}\Phi A_x|0\rangle|\bar{0}\rangle = \sum_j (-1)^j |\alpha_j|^2 \geq 1 - 2\eta.$$

Therefore we obtain a success probability $1 - \epsilon \geq (1 - 2\eta)^2$. Inverting this relation, we obtain $\eta \geq (1 - \sqrt{1 - \epsilon})/2$. \square

3 Adversary methods

In this section we introduce both the additive and multiplicative adversary lower bound methods. Even when one is only interested in the functional case, it is useful to view these methods as lower bounds on quantum state generation as this allows the separation of the method into two distinct parts. The first part is a lower bound on exact coherent quantum state generation. This is where the two methods differ. The second part is the output condition, a minimization of the bound for exact coherent quantum state generation over all valid output Gram matrices. The set of valid output Gram matrices is determined by the target Gram matrix σ , the error parameter ϵ , and if one is considering coherent or non-coherent state generation. This second step is common to both the additive and multiplicative methods. Finally, we show that the multiplicative bound is at least as large as the additive bound.

3.1 Additive method

We first review the derivation of the additive adversary method to compare it with the multiplicative method in the next section. We will actually present a generalization of the additive adversary method due to [LMR⁺11].

Consider an algorithm that exactly coherently computes σ by making T queries. Let $|\psi_x^t\rangle$ be the state of this algorithm on input x after t queries, and $\rho^t(x, y) = \langle \psi_x^t | \psi_y^t \rangle$ be the corresponding Gram matrix. Note that $\rho^0 = J$ the all ones matrix and, by assumption, $\rho^T = \sigma$.

Now let Γ be a matrix, v a vector, and consider the potential function $\Phi(t) = \text{Tr}((\Gamma \circ \rho^t)vv^*)$. The additive change in this potential function from the beginning to the end of the protocol is

$$\begin{aligned} \text{Tr}((\Gamma \circ (J - \sigma))vv^*) &= \sum_{t=0}^{T-1} \text{Tr}((\Gamma \circ (\rho^t - \rho^{t+1}))vv^*) \\ &\leq T \max_t \text{Tr}((\Gamma \circ (\rho^t - \rho^{t+1}))vv^*) . \end{aligned}$$

A standard argument (see, for example, [HLŠ07]) then goes that if we impose the condition on Γ that

$$I \pm \Gamma \circ (J - \Delta_i) \succeq 0 \text{ for all } i \in [n],$$

then $\text{Tr}((\Gamma \circ (\rho^t - \rho^{t+1}))vv^*) \leq 2$, for all t and v .

As this argument holds for any Γ and v , we can maximize over them leading to the following definition.

Definition 3.1 (Additive adversary method [LMR⁺11]).

$$\begin{aligned} \text{Adv}^*(\sigma) &= \underset{\Gamma}{\text{maximize}} \quad \|\Gamma \circ (J - \sigma)\| \\ &\text{subject to} \quad I \pm \Gamma \circ (J - \Delta_i) \succeq 0 \text{ for all } i \in [n], \end{aligned}$$

where the maximization is over $|\mathcal{D}| \times |\mathcal{D}|$ hermitian matrices Γ .

The preceding argument shows the following.

Theorem 3.2 ([LMR⁺11]). *For any target Gram matrix σ ,*

$$Q_0^c(\sigma) \geq \frac{\text{Adv}^*(\sigma)}{2}$$

[LMR⁺11] have also shown that this lower bound is tight for the bounded-error query complexity of functions.

Theorem 3.3 ([LMR⁺11]). *For any function f ,*

$$Q_{1/4}(f) \leq 1000 \cdot \text{Adv}^*(F)$$

Up to the constant factor, this upper bound holds more generally for *well-behaved* state generation problems, where the query complexity $Q_\epsilon(\sigma)$ does not depend dramatically on the error ϵ (i.e., $Q_\epsilon(\sigma) = \Theta(Q_{\epsilon'}(\sigma))$ for small ϵ, ϵ').

Remark 3.4. *The adversary bound Adv^\pm from [HLŠ07] was originally defined in the functional case, that is, for target Gram matrices F of the form $F(x, y) = \delta_{f(x), f(y)}$ for a function F . This definition had an additional constraint that $\Gamma \circ F = 0$. This constraint only affects the bound up to a multiplicative factor of two [LMR⁺11].*

$$\text{Adv}^\pm(F) \leq \text{Adv}^*(F) \leq 2\text{Adv}^\pm(F) . \quad (3.1)$$

The constraint $\Gamma \circ F = 0$ allows one to show that $\text{Adv}^\pm(F)/2$ is a lower bound even on the non-coherent complexity of generating F . One can see that $\text{Adv}^(F)/4$ is a lower bound on the non-coherent complexity of generating F either by Eq. (3.1) or by Claim 2.5 showing that the coherent and non-coherent state generation complexities of functions are related by a factor of two.*

3.2 Multiplicative adversary method

The multiplicative bound is derived by considering the same potential function $\Phi(t)$, but looks at the ratio of this function at the beginning and end of the protocol, rather than the difference. Equivalently, one can consider the logarithmic potential function $\ln(\Phi(t))$ and again look at the additive change over the course of the protocol. As the argument to the logarithm should be positive, we already see that a new constraint on Γ is needed, namely $\Gamma \succ 0$.

Definition 3.5 (Multiplicative adversary method).

$$\begin{aligned} \text{Madv}(\sigma) = \underset{c}{\text{maximize}} \quad & \frac{1}{\ln(c)} \underset{\Gamma \succ 0, v}{\text{maximize}} \quad \ln(\text{Tr}((\Gamma \circ \sigma)vv^*)) \\ & \text{subject to} \quad \text{Tr}(\Gamma vv^*) = 1 \\ & \quad \quad \quad c^{-1}\Gamma \preceq \Gamma \circ \Delta_i \preceq c \Gamma \text{ for all } i \in [n], \end{aligned}$$

where the maximization is over $|\mathcal{D}| \times |\mathcal{D}|$ positive definite matrices Γ and unit vectors v .

Theorem 3.6 ([Špa08, AMRR11]). *For any state generation problem σ ,*

$$Q_0^c(\sigma) \geq \frac{\text{Madv}(\sigma)}{2} .$$

Proof. Consider an algorithm that coherently generates σ by making T queries, and define a potential function $\Phi(t) = \text{Tr}((\Gamma \circ \rho^t)vv^*)$, where $\Gamma \succ 0$. Then

$$\begin{aligned} \frac{\Phi(T)}{\Phi(0)} &= \frac{\text{Tr}((\Gamma \circ \sigma)vv^*)}{\text{Tr}((\Gamma \circ J)vv^*)} = \prod_{t=0}^{T-1} \frac{\text{Tr}((\Gamma \circ \rho^{t+1})vv^*)}{\text{Tr}((\Gamma \circ \rho^t)vv^*)} \\ &\leq \left(\max_t \frac{\text{Tr}((\Gamma \circ \rho^{t+1})vv^*)}{\text{Tr}((\Gamma \circ \rho^t)vv^*)} \right)^T . \end{aligned}$$

Analogously to the additive bound, we now show that the constraint $c^{-1}\Gamma \preceq \Gamma \circ \Delta_i \preceq c\Gamma$ for all $i \in [n]$ implies

$$\max_t \frac{\text{Tr}((\Gamma \circ \rho^{t+1})vv^*)}{\text{Tr}((\Gamma \circ \rho^t)vv^*)} \leq c .$$

This argument is very similar to proofs in [Špa08, AMRR11] so we only sketch the idea here. Recall from [AMRR11] that we can assume that there are only two types of queries, called computing and uncomputing queries (this restriction can only increase the query complexity by a factor at most 2, hence the factor 1/2 in the final lower bound). Let us first consider a computing query. Let $|\psi_{x,i}^t\rangle = P_i|\psi_x^t\rangle$, where P_i is a projector onto the query register containing index i , and $\rho_i^t(x, y) = \langle \psi_{x,i}^t | \psi_{y,i}^t \rangle$. We can decompose the state before the t -th query as $\rho^t = \sum_i \rho_i^t$, and the state after the query as $\rho^{t+1} = \sum_i \rho_i^t \circ \Delta_i$. The condition $\Gamma \circ \Delta_i \preceq c\Gamma$ then immediately implies that

$$\text{Tr}((\Gamma \circ \rho^{t+1})vv^*) \leq c \text{Tr}((\Gamma \circ \rho^t)vv^*).$$

For uncomputing queries, the roles of ρ^t and ρ^{t+1} are interchanged, and we obtain the same conclusion from the constraint $\Gamma \preceq c\Gamma \circ \Delta_i$. \square

Remark 3.7. *The constraints on Γ given here are expressed differently from [Špa08, AMRR11], the latter using the constraint $\|\Gamma^{1/2}(\Gamma \circ \Delta_i)^{-1/2}\|^2 \leq c$ and $\|(\Gamma \circ \Delta_i)^{1/2}\Gamma^{-1/2}\|^2 \leq c$. It is straightforward to show, however, that these conditions are equivalent to $c^{-1}\Gamma \preceq \Gamma \circ \Delta_i \preceq c\Gamma$.*

When the value of c is fixed, the multiplicative bound becomes a semidefinite program. Indeed, setting $W = \Gamma \circ vv^*$, we have:

$$\begin{aligned} \text{Madv}(\sigma) = \maximize_c \frac{1}{\ln(c)} \maximize_{W \succ 0} & \ln(\text{Tr}(W\sigma)) \\ \text{subject to} & \text{Tr}(WJ) = 1 \\ & c^{-1}W \preceq W \circ \Delta_i \preceq cW \text{ for all } i \in [n]. \end{aligned}$$

Thus we can view the multiplicative adversary bound as a maximization over semidefinite programs.

3.3 Output condition

Thus far, we have seen lower bounds on the problem of *exact coherent* state generation. To obtain a lower bound in the bounded-error setting—coherent or non-coherent—one can minimize the exact coherent bound over the set of valid final Gram matrices of a successful algorithm.

We will restrict our discussion to the coherent output condition. As our main results are for functions, by showing lower bounds on the coherent state generation problems F and σ_f associated with a function f , we obtain lower bounds on the query complexity of f by Claim 2.5 and Claim 2.6.

Recall that a successful coherent ϵ -error algorithm \mathcal{P} for the set of target vectors $\{\sigma_x\}$ must satisfy $\Re(\langle \mathcal{P}(x) | (\sigma_x \otimes |\bar{0}\rangle) \rangle) \geq \sqrt{1-\epsilon}$. We can equivalently rephrase this as $\Re(\langle \mathcal{P}(x) | V(|\sigma_x\rangle \otimes |\bar{0}\rangle) \rangle) \geq \sqrt{1-\epsilon}$ for some unitary V . This can be done as the unitary V can be appended to the algorithm at no extra cost, and this formulation has the advantage that it only depends on the Gram matrix σ of the vectors $\{\sigma_x\}$ and the Gram matrix $\sigma'(x, y) = \langle \mathcal{P}(x) | \mathcal{P}(y) \rangle$, rather than the vectors themselves.

The set of σ' satisfying this condition can be hard to deal with, so previous works have typically relaxed this condition and used an output condition that defines a larger, simpler set. For example,

the original Ambainis output condition minimized over σ' satisfying $\ell_\infty(\sigma - \sigma') \leq 2\sqrt{\epsilon}$ for error parameter ϵ . A stronger output condition based on the γ_2 norm that $\gamma_2(\sigma - \sigma') \leq 2\sqrt{\epsilon}$ was introduced in [HLŠ07]. As $\gamma_2(v) \geq \ell_\infty(v)$, this output condition defines a smaller set. The γ_2 output condition was later shown to be approximately tight in the sense that if $\gamma_2(\sigma - \sigma') \leq \epsilon$, then there is a unitary V such that $\langle \sigma_x | V | \sigma'_x \rangle \geq 1 - 2\sqrt{\epsilon}$ for all x [LMR⁺11]. While approximately tight in the bounded-error setting, this condition is not strong enough for proving strong direct product theorems, where we need to obtain non-trivial bounds for exponentially small success probabilities.

Here we work with the full output condition and express it in an alternative form that is easier to handle. As a side effect, our new characterization provides an alternative proof that the γ_2 output condition is tight in the bounded-error setting, and improves the parameters given in [LMR⁺11].

Claim 3.8. *Let $\{|a_x\rangle\}, \{|b_x\rangle\}$ be two sets of vectors, and ρ, σ their corresponding Gram matrices.*

$$\max_V \min_x \Re(\langle a_x | V | b_x \rangle) = \min_{u: \|u\|=1} \mathcal{F}(\rho \circ uu^*, \sigma \circ uu^*) , \quad (3.2)$$

where the maximization is taken over all unitaries V .

Proof. By writing the left hand side as a semidefinite program and taking the dual one can show that

$$\max_V \min_x \Re(\langle a_x | V | b_x \rangle) = \min_{u: \|u\|=1} \max_V \Re(\text{Tr}(V \sum_x |u_x|^2 |a_x\rangle\langle b_x|)) .$$

Letting $D(u)$ be a diagonal matrix with entries given by u , we can rewrite the right hand side of this last expression as

$$\max_V \min_x \Re(\langle a_x | V | b_x \rangle) = \min_{u: \|u\|=1} \|AD(u)(BD(u))^*\|_{\text{tr}} ,$$

where $A = \sum_x |a_x\rangle\langle x|$ and $B = \sum_x |b_x\rangle\langle x|$. Since $\rho = A^*A$, $\sigma = B^*B$ and $\rho \circ uu^* = D(u)^*\rho D(u)$, the claim follows using

$$\|XY^*\|_{\text{tr}} = \|(X^*X)^{1/2}(Y^*Y)^{1/2}\|_{\text{tr}}$$

and the definition of the fidelity $\mathcal{F}(X^*X, Y^*Y) = \|(X^*X)^{1/2}(Y^*Y)^{1/2}\|_{\text{tr}}$. \square

The following quantities then give lower bounds for ϵ -error coherent quantum state generation:

Definition 3.9 (Additive and multiplicative bounds).

$$\begin{aligned} \text{Adv}_\epsilon(\sigma) &= \min_\rho \text{Adv}^*(\rho) \\ \text{Madv}_\epsilon(\sigma) &= \min_\rho \text{Madv}(\rho), \end{aligned}$$

where both minimizations are over Gram matrices ρ such that

$$\min_{u: \|u\|=1} \mathcal{F}(\rho \circ uu^*, \sigma \circ uu^*) \geq \sqrt{1 - \epsilon}.$$

In light of Claim 3.8, we can slightly improve one of the bounds in [LMR⁺11, Lemma 4.8], which compares the tight output condition based on the fidelity to the output condition based on the factorization norm γ_2 .

Claim 3.10. Let $\{|a_x\rangle\}, \{|b_x\rangle\}$ be two sets of vectors, and ρ, σ their corresponding Gram matrices. Say that $\sqrt{1-\epsilon} = \max_V \min_x \Re(\langle a_x | V | b_x \rangle)$, where the maximization is taken over all unitary matrices V . Then

$$1 - \sqrt{1-\epsilon} \leq \frac{1}{2} \gamma_2(\rho - \sigma) \leq \sqrt{\epsilon},$$

Proof. This directly follows from [Claim 3.8](#) and the relation between the trace distance and fidelity.

$$1 - \mathcal{F}(\rho \circ uu^*, \sigma \circ uu^*) \leq \frac{1}{2} \|(\rho - \sigma) \circ uu^*\|_{\text{tr}} \leq \sqrt{1 - \mathcal{F}(\rho \circ uu^*, \sigma \circ uu^*)^2}.$$

□

Note that an adversary matrix Γ yields a good zero-error multiplicative adversary bound if $\text{Tr}(\Gamma(\sigma \circ vv^*))$ is large. To obtain a bound for ϵ -error algorithms, we need to show that $\text{Tr}(\Gamma(\rho \circ vv^*))$ remains large for any Gram matrix ρ such that $\mathcal{F}(\rho \circ uu^*, \sigma \circ uu^*) \geq \sqrt{1-\epsilon}$ for all unit vectors u . The following lemma will be useful.

Lemma 3.11. Let p, q be two distributions for a discrete random variable A taking values in \mathbf{R}_0^+ . If $\mathcal{F}(p, q) \geq \sqrt{\delta}$, then

$$E_q(A) \geq \delta [E_p(A^{-1})]^{-1}.$$

Proof. Let $p_i = \Pr_p[A = a_i]$ and $q_i = \Pr_q[A = a_i]$. We need to lower bound the value of the following optimization program:

$$\text{minimize}_{q_i \geq 0: \sum_i q_i = 1} \sum_i q_i a_i \text{ subject to } \mathcal{F}(p, q) \geq \sqrt{\delta}.$$

Introducing vectors $|u\rangle = \sum_i \sqrt{p_i} |i\rangle$ and $|v\rangle = \sum_i \sqrt{q_i} |i\rangle$, and letting $D(A)$ be a diagonal matrix with the support of A along the diagonal, this can be rewritten as

$$\begin{aligned} & \text{minimize}_{|v\rangle: \|v\|=1} \langle v | D(A) | v \rangle \text{ subject to } |\langle u | v \rangle|^2 \geq \delta \\ & = \text{minimize}_{\rho \succeq 0: \text{Tr} \rho = 1} \text{Tr}[D(A)\rho] \text{ subject to } \text{Tr}[|u\rangle\langle u| \rho] \geq \delta. \end{aligned}$$

This is a semidefinite program, whose dual can be written as

$$\text{maximize}_{\lambda \geq 0, \mu} \lambda \delta + \mu \text{ subject to } D(A) \succeq \lambda |u\rangle\langle u| + \mu I.$$

Setting $\mu = 0$, this is at least

$$\delta \text{ maximize}_{\lambda \geq 0} \lambda \text{ subject to } D(A) \succeq \lambda |u\rangle\langle u|.$$

Let $|w\rangle = \sum_i \sqrt{p_i/a_i} |i\rangle$. The constraint is equivalent to $I \succeq \lambda |w\rangle\langle w|$, which in turn is equivalent to $\lambda \| |w\rangle\langle w| \| = \lambda \|w\|^2 \leq 1$. The lemma then follows from $\|w\|^2 = \sum_i p_i a_i^{-1}$. □

To apply this lemma, we need an upper bound on $E_p[A^{-1}]$. In our applications, we usually do not know explicitly the distribution p , but we do know its expectation and the extremal values in its support. The next claim allows us to upper bound $E_p[A^{-1}]$ in terms of these quantities.

Claim 3.12. Let $0 < a_0 \leq \bar{a} \leq a_1$, and A be a random variable taking values in $S \subseteq [a_0, a_1]$. If $E_p(A) = \bar{a}$, then $E_p(A^{-1}) \leq \frac{a_0 + a_1 - \bar{a}}{a_0 a_1}$.

Proof. $E_p(A^{-1})$ is at most the value of the following linear program:

$$\text{maximize}_{p_a \geq 0} \sum_{a \in S} p_a a^{-1} \text{ subject to } \sum_{a \in S} p_a a = \bar{a}, \quad \sum_{a \in S} p_a = 1.$$

The dual program can be written as

$$\text{minimize}_{\lambda, \mu} \lambda - \bar{a}\mu \text{ subject to } \mu a^2 - \lambda a + 1 \leq 0 \quad \forall a \in S.$$

Since $a_0 \leq a \leq a_1$, the constraint is satisfied for $\lambda = \frac{a_0 + a_1}{a_0 a_1}$ and $\mu = \frac{1}{a_0 a_1}$, which leads to $E_p(A^{-1}) \leq \frac{a_0 + a_1 - \bar{a}}{a_0 a_1}$. \square

Putting the last two claims together, we get the following corollary which is key to our strong direct product theorem.

Corollary 3.13. Let $a_1 \geq a_0 > 0$ and p be a distribution for a random variable A taking values in $[a_0, a_1]$. If $E_p[A] = \bar{a}$ and q is a distribution over $(\mathbf{R}_0^+)^k$ such that $\mathcal{F}(p^{\otimes k}, q) \geq \sqrt{\delta^k}$, then

$$E_q(\Pi_{l=1}^k A_l) \geq \left(\frac{\delta a_0 a_1}{a_0 + a_1 - \bar{a}} \right)^k.$$

3.4 Comparison of the adversary bounds

Let us first prove a variation of the result by [AMRR11] that the multiplicative adversary bound is stronger than the additive bound. The main difference with [AMRR11] is that this claim relies on the bound $\text{Adv}^*(\sigma)$ which is potentially stronger for general quantum state generation problems.

Claim 3.14 ([AMRR11]). For any $\epsilon > 0$ and any state generation problem σ , we have

$$\text{Madv}(\sigma) \geq (1 - \epsilon)\text{Adv}^*(\sigma).$$

Proof. Let Γ be an optimal witness for $\text{Adv}^*(\sigma) = b$, and v be the principal eigenvector of $\Gamma \circ (J - \sigma)$. Note that we may assume without loss of generality that v corresponds to a positive eigenvalue of $\Gamma \circ (J - \sigma)$. Let $\Gamma' = \Gamma - \text{Tr}((\Gamma \circ \sigma)vv^*)I$, and notice that Γ' is also a witness for $\text{Adv}^*(\sigma) = b$, satisfying $\text{Tr}(\Gamma'vv^*) = b$ and $\text{Tr}((\Gamma' \circ \sigma)vv^*) = 0$. Let $d = \|\Gamma'\|$ and note that $d \geq b$. Finally, define $\Gamma_m = (I + \gamma(dI - \Gamma'))/(1 + \gamma(d - b))$. Therefore, we have $\text{Tr}(\Gamma_m vv^*) = 1$ and $\text{Tr}((\Gamma_m \circ \sigma)vv^*) = (1 + \gamma d)/(1 + \gamma(d - b))$.

We now show that the condition $c^{-1}\Gamma_m \preceq \Gamma_m \circ \Delta_i \preceq c\Gamma_m$ is satisfied for $c = 1 + \gamma$. We show $(1 + \gamma(d - b))(\Gamma_m \circ (c\Delta_i - J)) \succeq 0$ which implies $\Gamma_m \circ (c\Delta_i - J) \succeq 0$ as $1 + \gamma(d - b) > 0$.

$$\begin{aligned} (1 + \gamma(d - b))(\Gamma_m \circ (c\Delta_i - J)) &= \left((1 + \gamma d)I - \gamma\Gamma' \right) \circ \left((\Delta_i - J) + \gamma\Delta_i \right) \\ &= \gamma(I + \Gamma' \circ (J - \Delta_i)) + \gamma^2(dI - \Gamma') \circ \Delta_i. \end{aligned}$$

From the constraint of the additive metric we know that $I + \Gamma' \circ (J - \Delta_i) \succeq 0$ for all $i \in [n]$. Also as $dI - \Gamma' \succeq 0$, taking the Hadamard product with $\Delta_i \succeq 0$ gives $(dI - \Gamma') \circ \Delta_i \succeq 0$, by Property 2

in Claim 2.4. Therefore, we have $\Gamma_m \circ (c\Delta_i - J) \succeq 0$. One can show $\Gamma_m \circ (cJ - \Delta_i) \succeq 0$ in a similar fashion. This implies that Γ_m is a witness for

$$\text{Madv}(\sigma) \geq \frac{\ln\left(\frac{1+\gamma d}{1+\gamma(d-b)}\right)}{\ln(1+\gamma)}.$$

The right hand side tends to $b = \text{Adv}^*(\sigma)$ in the limit $\gamma \rightarrow 1$, therefore, by continuity, for any $\epsilon > 0$ there exists γ such that $\text{Madv}(\sigma) \geq (1 - \epsilon)\text{Adv}^*(\sigma)$. \square

Adapting results from [Špa08, AMRR11], this implies a strong direct product theorem for $\text{Madv}(\sigma)$ as long as the bound is obtained for $c = 1 + \Omega(1/\text{Adv}^*(\sigma))$. Unfortunately, showing that we can take c bounded away from 1 requires bounding $d = \|\Gamma'\|$, which we do not know how to do for a general state generation problem σ . In general, we can only use this statement in the limit $c \rightarrow 1$, in which case the direct product theorem degrades into a direct sum theorem. This is why [AMRR11] were not able to conclude a strong direct product theorem.

We observe that for interesting cases such as F or σ_f , we can bound the norm of the witness Γ' using the following claim.

Claim 3.15. *Suppose that $(J - \sigma) \circ (J - \sigma) = \lambda(J - \sigma)$. Then there is a matrix Γ' witnessing $\lambda \frac{\text{Adv}^*(\sigma)}{\gamma_2(J - \sigma)}$ such that $\|\Gamma'\| \leq \frac{\text{Adv}^*(\sigma)}{\gamma_2(J - \sigma)}$ and $\Gamma' \circ (J - \sigma) = \lambda\Gamma'$.*

Proof. Let Γ be an optimal witness for $\text{Adv}^*(\sigma)$. Define $\Gamma' = \gamma_2(J - \sigma)^{-1}(\Gamma \circ (J - \sigma))$. By assumption, we then have $\Gamma' \circ (J - \sigma) = \lambda\Gamma'$. This is a feasible witness as

$$\|\Gamma' \circ (J - \Delta_i)\| \leq \frac{\gamma_2(J - \sigma)}{\gamma_2(J - \sigma)} \|\Gamma \circ (J - \Delta_i)\| \leq 1$$

by Property 1 in Claim 2.4. Furthermore, $\|\Gamma'\| = \gamma_2(J - \sigma)^{-1}\text{Adv}^*(\sigma)$ and Γ' witnesses a bound of $\lambda\|\Gamma'\| = \lambda\gamma_2(J - \sigma)^{-1}\text{Adv}^*(\sigma)$. \square

For certain state generation problems including F and σ_f we are thus able to obtain a quantitative version of Claim 3.14.

Claim 3.16. *Suppose that $(J - \sigma) \circ (J - \sigma) = \lambda(J - \sigma)$, and let $d = \gamma_2(J - \sigma)^{-1}\text{Adv}^*(\sigma)$. Then, for any $\gamma > 0$, there is a multiplicative witness Γ_m and a vector v such that*

$$\begin{aligned} \text{Tr}(\Gamma_m v v^*) &= 1 \\ \text{Tr}(\Gamma_m(\sigma \circ v v^*)) &= 1 + \lambda\gamma d \\ I &\preceq \Gamma_m \preceq (1 + 2\gamma d)I, \\ c^{-1}\Gamma_m &\preceq \Gamma_m \circ \Delta_i \preceq c\Gamma_m \text{ for all } i, \end{aligned}$$

where $c = 1 + \gamma$. Therefore Γ_m satisfies the constraints of Definition 3.5 and witnesses that

$$\text{Madv}(\sigma) \geq \frac{\ln(1 + \lambda\gamma d)}{\ln(1 + \gamma)}$$

Proof. From Claim 3.15, there exists a witness Γ witnessing $\text{Adv}^*(\sigma) \geq \lambda d$ such that $\|\Gamma\| = d$. Let v be the principal eigenvector of Γ , and $\Gamma_m = I + \gamma(dI - \Gamma)$. Note that we may assume without loss of generality that v corresponds to a positive eigenvalue of Γ . Therefore, we have $\Gamma_m \succeq I$ and $\text{Tr}(\Gamma_m vv^*) = 1$. As $\Gamma \circ (J - \sigma) = \lambda \Gamma$, it follows that v is also a principal eigenvector of $\Gamma \circ (J - \sigma)$, and the objective value achieved by Γ is $\text{Tr}(\Gamma((J - \sigma) \circ vv^*)) = \lambda d$. Thus $\text{Tr}(\Gamma(\sigma \circ vv^*)) = (1 - \lambda)d$ and $\text{Tr}(\Gamma_m(\sigma \circ vv^*)) = 1 + \lambda \gamma d$. The third condition follows from $-dI \preceq \Gamma \preceq dI$.

The fact that the condition $c^{-1}\Gamma_m \preceq \Gamma_m \circ \Delta_i \preceq c\Gamma_m$ is satisfied for $c = 1 + \gamma$ follows by the same argument as in the proof of Claim 3.14. \square

Taking $\gamma = 1/(d\lambda)$ gives the following corollary.

Corollary 3.17. *Suppose that $(J - \sigma) \circ (J - \sigma) = \lambda(J - \sigma)$. Then,*

$$\text{Madv}(\sigma) \geq \lambda \frac{\text{Adv}^*(\sigma)}{2}.$$

Note that in this statement $\text{Madv}(\sigma)$ is proved with $c = 1 + 1/(\lambda \cdot \text{Adv}^*(\sigma))$, which is what we need for the strong direct product theorem.

Now we have shown that the multiplicative bound is a constant fraction of the additive bound in the exact case. Thus the same will be true with respect to any output condition.

4 Strong direct product theorem

We first prove the following theorem, which will lead to both the strong direct product theorem and the XOR lemma in the boolean case.

Theorem 4.1. *Let σ be a Gram matrix for a state generation problem satisfying $(J - \sigma) \circ (J - \sigma) = \lambda(J - \sigma)$ for some $\lambda > 0$, and let $d = \gamma_2(J - \sigma)^{-1} \text{Adv}^*(\sigma)$. Then for any $\gamma > 0$*

$$Q_{1-\delta^k}^c(\sigma^{\otimes k}) \geq \frac{k \ln \left(\delta \frac{1+2\gamma d}{1+\gamma d(2-\lambda)} \right)}{2 \ln(1 + \gamma)}.$$

Proof. Let v, Γ_m satisfy the conditions in Claim 3.16. As a witness for $\sigma^{\otimes k}$ we take $\Gamma_m^{\otimes k}$. Let us first see that this matrix satisfies the multiplicative constraint with the same value $c = 1 + \gamma$.

We label the constraint matrices $\Delta_{p,q}$ for $\sigma^{\otimes k}$ by $p \in [k]$ and $q \in [n]$. These are $|\mathcal{D}|^k$ -by- $|\mathcal{D}|^k$ matrices where $\Delta_{p,q}((x^1, \dots, x^k), (y^1, \dots, y^k)) = \delta_{x_q^p, y_q^p}$. In other words, $\Delta_{p,q} = J^{\otimes p-1} \otimes \Delta_q \otimes J^{\otimes k-p}$. Thus $\Gamma^{\otimes k} \circ \Delta_{p,q} = \Gamma_m^{\otimes p-1} \otimes \Gamma_m \circ \Delta_q \otimes \Gamma_m^{\otimes k-p}$. Since $c^{-1}\Gamma_m \preceq \Gamma_m \circ \Delta_q \preceq c\Gamma_m$ for all $p \in [n]$, and obviously $c^{-1}\Gamma_m \preceq \Gamma_m \preceq c\Gamma_m$ for $c > 1$, we immediately have

$$c^{-1}\Gamma_m^{\otimes k} \preceq \Gamma_m^{\otimes k} \circ \Delta_{p,q} \preceq c\Gamma_m^{\otimes k}$$

for any $p \in [k], q \in [n]$.

To lower bound the objective value we lower bound

$$\text{Madv}_{1-\delta^k}(\sigma^{\otimes k}) \geq \min_{\rho} \text{Tr}(\Gamma_m^{\otimes k}(\rho \circ (vv^*)^{\otimes k})),$$

where the minimum is over psd matrices ρ such that $\rho \circ I = I$ and

$$\min_u \mathcal{F}(\rho \circ uu^*, \sigma^{\otimes k} \circ uu^*) \geq \delta^{k/2}.$$

In particular, this will hold for $u = v^{\otimes k}$ and we can apply [Corollary 3.13](#) with p being the distribution arising from measuring Γ_m on $\sigma \circ vv^*$, and q the distribution arising from measuring $\Gamma_m^{\otimes k}$ on $\rho \circ (vv^*)^{\otimes k}$. Since $\mathcal{F}(\rho \circ (vv^*)^{\otimes k}, (\sigma \circ vv^*)^{\otimes k}) \geq \delta^{k/2}$, we also have $\mathcal{F}(p^{\otimes k}, q) \geq \delta^{k/2}$. The parameters in [Corollary 3.13](#) are $a_0 = 1$, $a_1 = 1 + 2\gamma d$, and $\bar{a} = 1 + \lambda\gamma d$ thus

$$\mathrm{Tr}(\Gamma_m^{\otimes k}(\rho \circ (vv^*)^{\otimes k})) \geq \delta^k \left(\frac{1 + 2\gamma d}{1 + \gamma d(2 - \lambda)} \right)^k.$$

and in turn

$$\mathrm{Madv}_{1-\delta^k}(\sigma^{\otimes k}) \geq \frac{k \ln(\delta \frac{1+2\gamma d}{1+\gamma d(2-\lambda)})}{\ln(1+\gamma)}.$$

□

We then obtain the following strong direct product theorem for the quantum query complexity of any function (boolean or not).

Theorem 4.2. *For any function f , any $(2/3) \leq \delta \leq 1$ and any integer $k > 0$, we have*

$$Q_{1-\delta^{k/2}}(f^{(k)}) \geq \frac{k \ln(3\delta/2)}{8} \mathrm{Adv}^*(F).$$

Proof. Notice that $(J - F) \circ (J - F) = J - F$ and $\gamma_2(J - F) \leq 2$. Thus applying [Theorem 4.1](#) with $\lambda = 1$ and $\gamma = 1/d$, we obtain

$$Q_{1-\delta^k}^c(F^{\otimes k}) \geq \frac{k \ln(3\delta/2)}{4} \mathrm{Adv}^*(F).$$

This lower bound is for computing $f^{(k)}$ coherently, and we obtain the lower bound for $f^{(k)}$ using [Claim 2.5](#). □

5 Boolean functions

5.1 XOR Lemma

We now focus on boolean functions. Before proving the XOR lemma, we prove a strong direct product theorem for the problem of computing a function in the phase.

Let $\sigma_f = 2F - J$ be the Gram matrix corresponding to computing a boolean function f in the phase.

Claim 5.1. *Let $d = \mathrm{Adv}^*(F)$. For any δ, γ ,*

$$Q_{1-\delta^k}^c(\sigma_f^{\otimes k}) \geq \frac{k \ln(\delta(1 + 2\gamma d))}{2 \ln(1 + \gamma)}.$$

Proof. Notice that $J - \sigma_f = 2(J - F)$, therefore $(J - \sigma_f) \circ (J - \sigma_f) = 2(J - \sigma_f)$, $\gamma_2(J - \sigma_f) = 2$ and $\mathrm{Adv}^*(\sigma_f) = 2\mathrm{Adv}^*(F)$. The claim then follows from [Theorem 4.1](#) with $\lambda = 2$. □

Setting $\gamma = 1/(\delta d)$, we immediately obtain the strong direct product theorem for σ_f .

Corollary 5.2. For any δ ,

$$Q_{1-\delta^k}^c(\sigma_f^{\otimes k}) \geq \frac{k\delta}{4} \text{Adv}^*(F) .$$

Let $\oplus \circ f^{(k)}$ be the function computing the parity of k independent copies of f . Since computing $\oplus \circ f^{(k)}$ in the phase is the same as generating the state $\sigma_f^{\otimes k}$, we obtain the XOR lemma from the strong direct product theorem for σ_f and [Claim 2.6](#).

Corollary 5.3 (XOR Lemma). For any boolean function f , any $0 \leq \delta \leq 1$ and any integer $k > 0$,

$$Q_{(1-\delta^{k/2})/2}(\oplus \circ f^{(k)}) \geq \frac{k\delta}{8} \text{Adv}^*(F) .$$

5.2 Threshold and strong direct product theorems

Finally, we prove a threshold direct product theorem. This will follow from [Claim 5.1](#) together with the following threshold lemma [[Ung09](#), Lemma 2].

Lemma 5.4 ([[Ung09](#)]). Let $Y_1, \dots, Y_k \in \{-1, +1\}$ be random variables, $-1 \leq \beta \leq 1$ and $C > 0$ be such that

$$\mathbb{E} \left[\prod_{i \in S} Y_i \right] \leq C\beta^{|S|}$$

for all $S \subseteq [k]$. Let λ be such that $\beta \leq \lambda \leq 1$. Then

$$\Pr \left[\sum_{i=1}^k Y_i \geq \lambda k \right] \leq C e^{-kD(1/2+\lambda/2||1/2+\beta/2)} .$$

Theorem 5.5. For any function f , any $0 \leq \delta < 1$, any μ such that $\frac{1+\sqrt{\delta}}{2} \leq \mu \leq 1$ and any integers $k, K > 0$, let $\mathcal{P}_i(x_1, \dots, x_k) \in \{-1, 1\}$ be the i -th output of a T -query algorithm for $f^{(k)}$, where

$$T \leq \frac{k\delta}{K(1-\delta)} \text{Adv}^*(F),$$

and let $X = \{i \in [k] : \mathcal{P}_i(x_1, \dots, x_k) = f(x_i)\}$. Then,

$$\Pr[|X| \geq \mu k] \leq e^{\frac{k}{K} - kD\left(\mu || \frac{1+\sqrt{\delta}}{2}\right)} .$$

Proof. Let $d = \text{Adv}^*(F)$ and, for any $i \in [k]$ and any set $S \subseteq [k]$, let us consider the random variables $Y_i = \mathcal{P}_i(x_1, \dots, x_k) \cdot f(x_i) \in \{-1, 1\}$ and the expectations $\beta_S = E(\prod_{i \in S} Y_i)$. By definition, we have

$$Q_{(1-\beta_S)/2}(\oplus \circ f^{(|S|)}) \leq T.$$

Moreover, we also have from [Claims 2.6](#) and [5.1](#):

$$Q_{(1-\beta_S)/2}(\oplus \circ f^{(|S|)}) \geq \frac{1}{2} Q_{1-\beta_S^2}^c(\sigma_f^{\otimes |S|}) \geq \frac{\ln(\beta_S^2(1+2\gamma d)^{|S|})}{4 \ln(1+\gamma)}$$

for any $\gamma > 0$, which together with the previous inequality leads to

$$\beta_S \leq (1 + \gamma)^{2T} (1 + 2\gamma d)^{-|S|/2}.$$

For $\gamma = (1 - \delta)/(2\delta d)$, this implies $\beta_S \leq e^{k/K} \delta^{|S|/2}$. Using Lemma 5.4 with $\beta = \sqrt{\delta}$, $C = e^{k/K}$ and $\lambda = 2\mu - 1$, we then obtain

$$\Pr \left[\sum_{i=1}^k Y_i \geq \lambda k \right] \leq e^{\frac{k}{K} - kD \left(\frac{1+\lambda}{2} \parallel \frac{1+\sqrt{\delta}}{2} \right)}.$$

The theorem then follows from $|X| = (k + \sum_{i=1}^k Y_i)/2$. □

In the special case $\mu = 1$, we obtain the following strong direct product theorem for boolean functions.

Corollary 5.6. *For any function f , any $0 \leq \delta < 1$ and any integers $k, K > 0$,*

$$Q_{1-(e^{1/K}(1+\sqrt{\delta})/2)^k}(f^{(k)}) \geq \frac{k\delta}{K(1-\delta)} \text{Adv}^*(F) .$$

Acknowledgments

JR acknowledges support by ARO/NSA under grant W911NF-09-1-0569. TL would like to thank Ben Reichardt for many insightful conversations on these topics. The authors also thank Oded Regev for interesting comments and in particular for suggesting to prove the XOR lemma. After completion of this work, the authors learned that the quantitative version of the result of Ambainis *et al.* [AMRR11] about the relation between the multiplicative and additive adversary methods, which was the key missing element to prove the strong direct product theorem, was independently proved by Belovs [Bel11].

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.
- [BdW02] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288(1):21–43, 2002. doi:10.1016/S0304-3975(01)00144-X.
- [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.
- [HLS07] 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.
- [LMR⁺11] Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. To appear, 2011.
- [LMRŠ10] Troy Lee, Rajat Mittal, Ben W. Reichardt, and Robert Špalek. An adversary for algorithms. 2010. arXiv:1011.3020.
- [Raz98] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

- [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](#).