A complexity theory for non-local quantum computation

Andreas Bluhm[1], Simon Höfer[1], Alex May[2,3], Mikka Stasiuk[2], Philip Verduyn Lunel[4], and Henry Yuen[5]

[1]Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
[2]Perimeter Institute for Theoretical Physics
[3]Institute for Quantum Computing, Waterloo, Ontario
[4]Sorbonne Université, Paris
[5]Columbia University

Non-local quantum computation (NLQC) replaces a local interaction between two systems with a single round of communication and shared entanglement. Despite many partial results, it is known that a characterization of entanglement cost in at least certain NLQC tasks would imply significant breakthroughs in complexity theory. Here, we avoid these obstructions and take an indirect approach to understanding resource requirements in NLQC, which mimics the approach used by complexity theorists: we study the relative hardness of different NLQC tasks by identifying resource efficient reductions between them. Most significantly, we prove that f-measure and f-route, the two best studied NLQC tasks, are in fact equivalent under $O(1)$ overhead reductions. This result simplifies many existing proofs in the literature and extends several new properties to f-measure. For instance, we obtain sub-exponential upper bounds on f-measure for all functions, and efficient protocols for functions in the complexity class $\mathsf{Mod}_k\mathsf{L}$. Beyond this, we study coherently controlled applications of Pauli operators and more general unitaries. We find relationships among coherent protocols, and show the coherently controlled NLQCs imply classically controlled protocols, suggesting they are harder NLQC tasks.

Andreas Bluhm: andreas.bluhm@univ-grenoble-alpes.fr
Simon Höfer: simon.hofer@univ-grenoble-alpes.fr
Alex May: amay@perimeterinstitute.ca
Mikka Stasiuk: mstasiuk@perimeterinstitute.ca
Philip Verduyn Lunel: philip.verduyn-lunel@lip6.fr
Henry Yuen: hyuen@cs.columbia.edu

Contents

1 Introduction

A non-local quantum computation (NLQC) replaces a local interaction of two systems with a single round of communication and shared entanglement (see Figure 1). Non-local quantum computation has many applications, including to quantum position-verification (QPV) [1, 2], AdS/CFT [3–6], information-theoretic cryptography [7–9], uncloneable secret sharing [10], and Hamiltonian complexity [11]. In all these applications, a key quantity of interest is the amount of entanglement necessary to implement a given computation as a NLQC. Despite the need to understand this, a clear and general characterization of the entanglement cost of a NLQC is still lacking.

There are fundamental obstructions to obtaining a complete understanding of entanglement cost in NLQC. In particular, entanglement cost in certain NLQC tasks can be upper bounded by complexity measures. Consequently, placing lower bounds on entanglement would imply lower bounds on these measures of complexity, which is a notoriously hard problem. For instance, in the context of a specific scheme known as f-route, there is an upper bound on entanglement cost which is exponential in the memory needed to compute the Boolean function f [12]. Super-polynomial bounds on f-route for a given function f therefore imply super-logarithmic lower bounds on memory. Thus such lower bounds face complexity barriers: a super-polynomial lower bound for a function in P

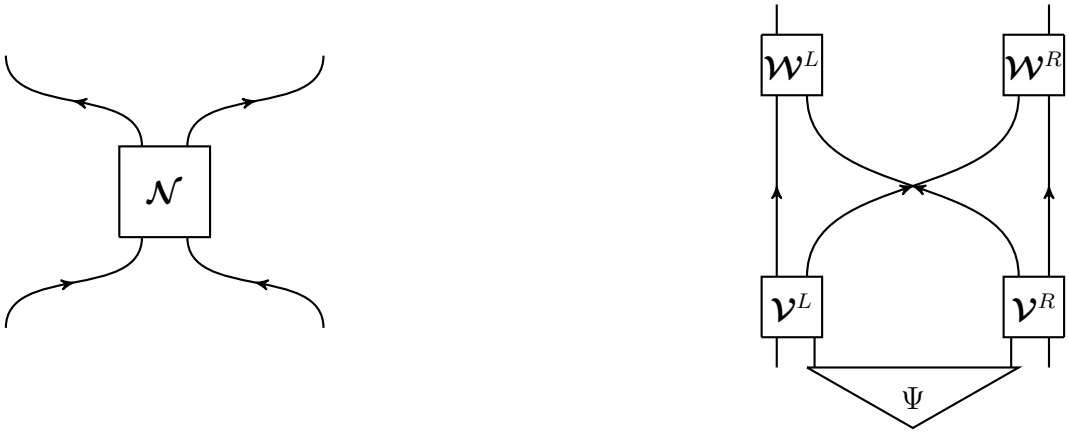

Figure 1: (a) Circuit diagram showing the local implementation of a channel $\mathcal{N}$. Physically, systems A and B are brought together spatially and interacted. (b) Circuit diagram showing the form of a non-local quantum computation. $\mathcal{V}^L$, $\mathcal{V}^R$, $\mathcal{W}^L$, and $\mathcal{W}^R$ are quantum channels. The triangle labelled Ψ represents the shared, in general entangled, resource state. The goal is to simulate the local channel $\mathcal{N}$.

(poly-time) would separate L (logspace) and P, a long-standing problem in complexity theory.[1]

In this work we take a new approach to elucidating how entanglement cost is determined in non-local quantum computation. We focus on the question: *when is one computation harder to implement non-locally than another?* To understand this, we study the relationships among different NLQC tasks, looking for reductions among them. Whenever we find that a protocol for implementing a non-local computation A can be transformed, without too much overhead, into a protocol for implementing a computation B, we know that B is no harder than A. By introducing this notion of a reduction we lay the groundwork for a more complete notion of complexity theory for NLQC.

Our strategy mimics the study of reductions among computational problems. Indeed, since we face some of the same obstructions that appear in the study of complexity theory, it is natural to adopt a similar strategy. We can also hope to gain many of the same insights. For instance, studying examples and comparing their hardness gives insight into what makes a problem hard or easy as a NLQC.

We can also then try to identify the hardest NLQCs, which provide useful candidates for position-based cryptography. Further, by building a scaffolding of examples and relating them to one another, any new NLQC of interest can be related to these problems and some of its properties understood without studying each new example from scratch. Finally, we can hope to gain insight into complexity theory itself via NLQC: since upper bounds for different NLQC tasks are characterized in terms of different complexity measures, we can hope to learn about these complexity measures by studying reductions among the tasks, or even hope to find lower bounds on complexity measures by lower bounding NLQC tasks.

Among the many applications of NLQC, our results are most immediately relevant for the understanding of the security of quantum position-verification. We briefly review the relevance of NLQC to QPV here. In a position-verification scheme, the verifier sends the prover quantum and classical systems and asks for a reply at a set of designated spacetime locations. See Figure 2 for a standard set-up in a spacetime with one spatial dimension. Unfortunately, there is no unconditionally secure QPV scheme; the cheating strategy is exactly to implement a non-local quantum computation in order to simulate

[1] In fact, somewhat more is true: in [13] an upper bound which is efficient for functions in $Mod_k L$ is given, so that a super-polynomial lower bound on f-route for a function in P would separate $Mod_k L$, which contains L, and P.

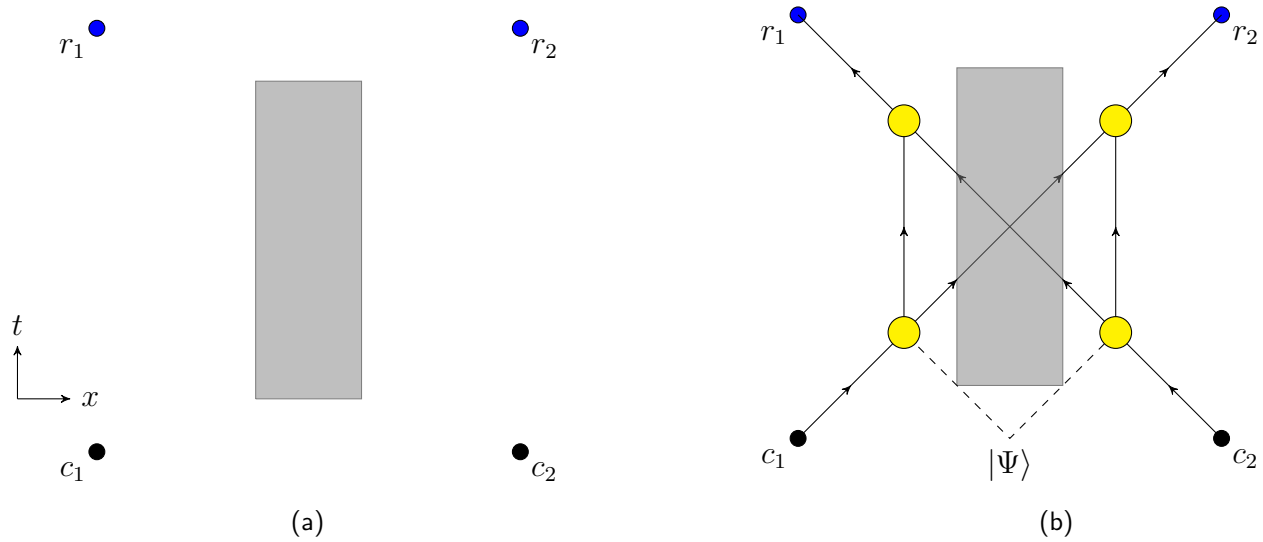

Figure 2: A standard QPV set-up in $1+1$ dimensions. Inputs are given at spacetime locations c_1, c_2. The prover should apply a designated quantum operation to these inputs, then return the outputs to points r_1, r_2. a) An honest prover enters the designated spacetime region (grey) to apply the needed quantum operation. b) A dishonest prover attempts to reproduce the same operation while acting outside the spacetime region; their actions take the form of a non-local quantum computation. Figure reproduced from [3].

the actions of an honest player. Since all computations can be implemented in the NLQC form, it follows that QPV is not secure without making further assumptions.

Rather than look for unconditional security, we can ask if some computations are much easier to implement in the local, honest, form rather than the non-local, dishonest form. Attention has focused on the case where we limit the entanglement shared by Alice and Bob, where the goal is to show that some computation which is reasonably easy to implement locally requires large entanglement to implement non-locally. See for example [5, 14–19].

In this bounded entanglement setting, particular attention has been paid to classes of protocols where most of the input is classical, with just $O(1)$ quantum bits, and in particular to schemes where an honest prover need only compute a classical function and do $O(1)$ quantum operations. The two natural protocols of this form are f-routing and f-measure[2], which are leading candidates for practical schemes. In f-route, Alice receives a classical string $x \in \{0,1\}^n$ along with a quantum system Q described by Hilbert space $\mathcal{H}_Q$, while Bob receives a classical string $y \in \{0,1\}^n$. Q is in an arbitrary unknown state. Their goal is to bring Q to Alice's side if $f(x,y) = 0$, or Q to Bob's side if $f(x,y) = 1$. In f-measure, again Alice receives a classical string $x \in \{0,1\}^n$ along with a quantum system Q, while Bob receives a classical string $y \in \{0,1\}^n$. Now however, Q is one of the BB84 states $H^{f(x,y)}|b\rangle$, $q, b \in \{0,1\}$. Alice and Bob's goal is to both output the bit b at the end of the NLQC.

1.1 Related work

Our explorations are in part inspired by a related set of reductions between instances of NLQC and primitives in information-theoretic cryptography [7]. Those relationships have already led to a number of useful results [8, 19], and our work can be seen as extending this to the study of relationships between NLQC tasks themselves. We describe the results of [7] briefly below.

In [7], the f-route task was related to a primitive studied in information-theoretic cryptography known as conditional disclosure of secrets (CDS) [20]. In CDS two players,

[2]This is also referred to as f-BB84 in the literature.

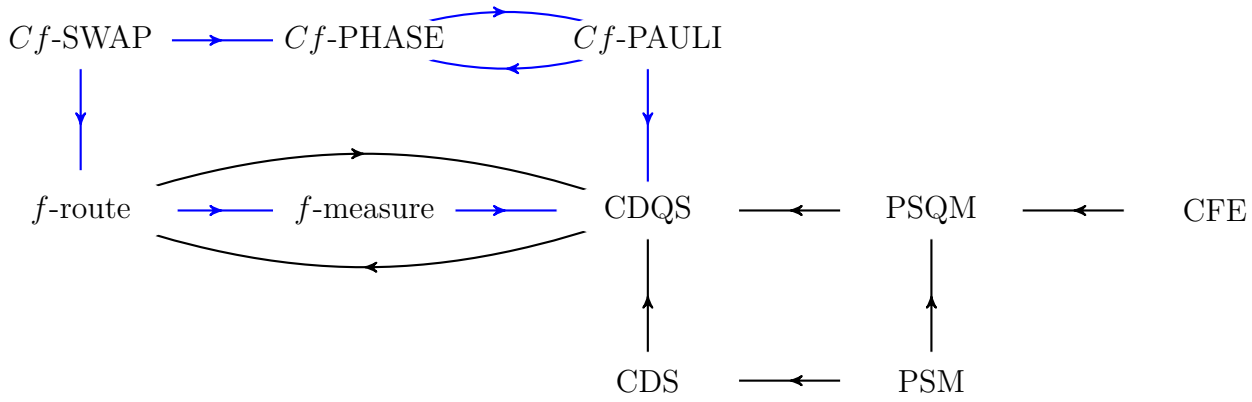

Figure 3: The known reductions among function NLQC tasks and primitives from information-theoretic cryptography. Blue implications are new to this work. Clicking on primitives links to definitions; clicking on blue arrows links to proofs of the corresponding implication. Black arrows are proven in [7].

Alice and Bob, share correlations (in the classical setting) or entanglement (in the quantum setting) but do not communicate. Alice receives a string s, the secret, as well as an input string $x \in \{0,1\}^n$; Bob receives an input string $y \in \{0,1\}^n$. Alice and Bob can each send a message to a third party, the referee. The referee knows x, y and wishes to learn s. Alice and Bob's goal is to allow the referee to learn s if and only if $f(x,y) = 1$ for some Boolean function f. The work [7] proved that CDS with quantum resources is equivalent to f-route: a protocol for quantum CDS can be transformed into one for f-route with only a small overhead in the resources used, and vice versa. Further, classical CDS schemes give quantum CDS schemes using the same resources.

A second result in [7] related another primitive from information-theoretic cryptography and a second instance of NLQC. Private-simultaneous message passing (PSM) [21] is defined by a choice of Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$ played by three parties, Alice, Bob and the referee. Alice receives input $x \in \{0,1\}^n$; Bob receives input $y \in \{0,1\}^n$. In this setting the referee does not know x, y. Alice and Bob will each send a message to the referee, who should learn $f(x,y)$ but no other information about (x,y). PSM with quantum resources, denoted PSQM, is related to an instance of NLQC known as coherent function evaluation (CFE). In CFE, the goal is to implement the isometry

$$\mathbf{V}[f] = \sum_{x,y} |x,y\rangle_Z |f(x,y)\rangle_{Z'} \langle x|_X \langle y|_Y \tag{1}$$

with X starting on Alice's side, Y starting on Bob's side, and Z ending on Alice's side, Z' ending on Bob's side. In [7] a reduction transforming protocols for CFE into protocols for PSQM using similar resources was given.

1.2 Our results

We explore a variety of NLQC tasks, each with different qualitative features whose relationships to their hardness we explore. An overview of the tasks we study and reductions among them appears as Figure 3.

One grouping of NLQCs we study are the *classically controlled* protocols, which require implementing a small quantum operation controlled on a large classical computation. This setting is well studied in the quantum position-verification literature [1, 2, 18, 19, 22–25]. There, the hope is that as we increase the size of the classical control, the entanglement cost of the NLQC will go up, even while the quantum resources used by an honest player do not. The examples of classically controlled NLQCs we study are f-route, CDQS, and f-measure[3]. In an f-measure task, Alice is given $H^{f(x,y)} |b\rangle_Q$ and

[3]In earlier work this task is sometimes referred to as f-BB84.

the string $x \in \{0,1\}^n$ while Bob is given $y \in \{0,1\}^n$. Their goal is for both Alice and Bob to output b. We show the following relationship among these settings.

Theorem 1 *f-route, f-measure and CDQS can all be transformed into one another with constant factor overhead in the entanglement cost.*

This is stated more formally in the main text using our definition of a reduction among NLQCs. The proof leverages the existing result that such a transformation exists between f-route and CDQS, and then we combine this with proofs that f-route $\Rightarrow$ f-measure and f-measure $\Rightarrow$ CDQS. In Section 5 we describe the simplifications of the literature or new results that follow from the equivalence of f-route and f-measure. Indeed, they are the best studied examples of NLQCs, and many properties previously proved for each separately now follow by proving it for only one of the two equivalent primitives. For example, f-measure gains an upper bound of $2^{O(\sqrt{n \log n})}$ via this connection, and efficient protocols for all functions in the complexity class $\mathsf{Mod}_k\mathsf{L}$.

We also explore several classes of *coherently controlled* operations, which implement $O(1)$ size gates controlled on inputs that may be in superposition. In particular we focus on NLQC implementations of the following three unitaries,

$$\begin{aligned} Cf\text{-SWAP}_{AA'BB'} &= \sum_{x,y} \text{SWAP}^{f(x,y)}_{A'B'} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \\ Cf\text{-PHASE}_{AA'BB'} &= \sum_{x,y} (-1)^{f(x,y)} \ |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \\ Cf\text{-}\mathbf{Z}_{AA'BB'} &= \sum_{x,y} \mathbf{Z}^{f(x,y)}_{A'} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \,. \end{aligned} \tag{2}$$

Note that by acting with local unitaries before and after implementing the NLQC protocol, we can convert a coherently controlled protocol for a unitary $\mathbf{U}_{A'B'}$ into one for $(\mathbf{V}_A \otimes \mathbf{V}_B)\mathbf{U}_{A'B'}(\mathbf{V}_A^\dagger \otimes \mathbf{V}_B^\dagger)$ for any choice of $\mathbf{V}_{A'}, \mathbf{V}_{B'}$. This means we can view the above unitaries as representatives of a class of equivalent NLQCs. With this in mind, we will refer also to the Cf-PAULI, which requires we implement Cf-$\mathbf{Z}$ or any unitary of the form $\mathbf{V}_{A'}\mathbf{Z}_{A'}\mathbf{V}_{A'}^\dagger$ (which includes Pauli $\mathbf{X}$ and $\mathbf{Y}$).

We prove reductions among the coherently controlled NLQC tasks. To start out, we observe that a Cf-SWAP protocol implies a Cf-PHASE protocol for the same function using similar resources. This follows by running the Cf-SWAP operation with the $A'B'$ system chosen to be in the -1 eigenstate of the SWAP operator. We were not able to find an implication from Cf-PHASE to Cf-SWAP, so Cf-SWAP may be stronger.

In a similar spirit, choosing A' to be in the state $|1\rangle_{A'}$ shows Cf-$\mathbf{Z}$ (and hence Cf-PAULI) implies Cf-PHASE. Conversely, we show that a Cf-PHASE protocol for the function $f \wedge z_1$ for z_1 a single bit gives a protocol for Cf-PAULI for the same function. We can add controls to the implemented unitary by concatenating with the AND operation further: CZ controlled on function f is implied by a Cf-PHASE protocol for $f \wedge z_1 \wedge z_2$, CCZ controlled on f is implied by a Cf-PHASE protocol for $f \wedge z_1 \wedge z_2 \wedge z_3$, etc. These observations raise the question of whether f and $f \wedge z_1$ have similar costs in Cf-PHASE. We show that indeed this is the case: a Cf-PHASE protocol for $f \wedge z_1$ costs at most 1 additional EPR pair compared to f. This establishes that NLQCs for Cf-$CC...CZ$ for any constant number of controls are all equivalent under constant entanglement overhead reductions.

We defined Cf-SWAP as a natural choice of coherent NLQC task which is strong enough to imply f-route. Cf-PHASE appears to be weaker than Cf-SWAP, but we can ask if it is strong enough to recover the incoherent NLQC tasks. We find that indeed Cf-PHASE actually suffices to obtain the classically controlled tasks f-route, f-measure and CDQS. We do this by proving an implication from the equivalent task Cf-PAULI to

CDQS. We leave open understanding if all (non-trivial) coherent tasks are stronger than all incoherent tasks.

As a final additional result, we show that in the NLQC context the ability to efficiently implement a unitary that interchanges between two states $|\psi_0\rangle, |\psi_1\rangle$ implies the ability to efficiently distinguish between the two "Fourier" states $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle \pm |\psi_1\rangle)$. This is inspired by a similar result which holds in the computational complexity context [26]. Note that in the complexity context the ability to apply interchange efficiently implies the ability to distinguish the Fourier states efficiently, and vice versa. We were motivated to study if this result also holds in the NLQC context. This is because, for instance, it has been conjectured [5] that the complexity of a unitary controls its entanglement cost as an NLQC. According to this conjecture, interchange and distinguish should have similar entanglement costs. We were able to establish this, but only in one direction. This is our only result relating classes of NLQCs which are not characterized by Boolean functions; we find this result suggestive that there may be other interesting reductions among state transformations or unitaries, though we do not explore this in depth here.

2 Background and preliminaries

2.1 Tools from quantum information theory

We label the maximally entangled state on $\mathcal{H}_A \otimes \mathcal{H}_B$ by Ψ^+_{AB}. When we don't specify the Hilbert spaces, Ψ^+ denotes a maximally entangled state on two qubits.

Let $\mathcal{D}(\mathcal{H}_A)$ be the set of density matrices on the Hilbert space $\mathcal{H}_A$. Given two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$, define the fidelity,

$$F(\rho, \sigma) \equiv \left(\operatorname{tr}\left(\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)\right)^2 \tag{3}$$

which is related to the trace distance $\frac{1}{2}\|\rho - \sigma\|_1$ by the Fuchs-van de Graaf inequalities,

$$1 - \sqrt{F(\rho,\sigma)} \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho,\sigma)}. \tag{4}$$

The fidelity and trace distance allow us to characterize distances between quantum states. To characterize distances between quantum channels, define the diamond norm distance [27, 28].

Definition 2 *Let $\boldsymbol{\mathcal{N}}_{B\to C}, \boldsymbol{\mathcal{M}}_{B\to C} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_C)$ be quantum channels. The **diamond norm distance** is defined by*

$$\|\boldsymbol{\mathcal{N}}_{B\to C} - \boldsymbol{\mathcal{M}}_{B\to C}\|_\diamond = \sup_d \max_{\Psi_{A_d B}} \|\boldsymbol{\mathcal{N}}_{B\to C}(\Psi_{A_d B}) - \boldsymbol{\mathcal{M}}_{B\to C}(\Psi_{A_d B})\|_1 \tag{5}$$

where $\Psi_{A_d B} \in \mathcal{D}(\mathcal{H}_{A_d} \otimes \mathcal{H}_B)$ and $\mathcal{H}_{A_d}$ is a d dimensional Hilbert space.

The diamond norm distance has an operational interpretation in terms of the maximal probability of distinguishing quantum channels.

We also make use of the von Neumann entropy and some related quantities and inequalities. The von Neumann entropy of a density matrix ρ_A is

$$S(A)_\rho = -\operatorname{tr}(\rho_A \log \rho_A) \tag{6}$$

where we use base 2 logarithms here and throughout the paper. The conditional quantum entropy is

$$S(A|B)_\rho = S(AB)_\rho - S(B)_\rho. \tag{7}$$

and the mutual information is

$$I(A:B)_\rho = S(A)_\rho + S(B)_\rho - S(AB)_\rho. \tag{8}$$

We also use the relative entropy, which is given by

$$D(\rho\|\sigma) = \operatorname{tr}\rho\log\rho - \operatorname{tr}\rho\log\sigma \tag{9}$$

when the support of ρ is contained within the support of σ, and defined to be infinity otherwise. Pinsker's inequality relates the relative entropy and the trace distance,

$$\|\rho-\sigma\|_1 \leq \sqrt{(2\ln 2)D(\rho\|\sigma)}. \tag{10}$$

We use the identity

$$I(A:B)_\rho = D(\rho_{AB}\|\rho_A\otimes\rho_B). \tag{11}$$

We exploit the following inequality relating conditional entropies in a tri-partite state.

Theorem 3 (CIT [29, 30]) *Let $|\psi\rangle_{REF}$ be an arbitrary tripartite state, with R a single qubit. Consider measurements on the R system that produce a measurement result we store in register Z. Consider measurements in both the computational and Hadamard basis, and denote the post-measurement state when measuring in the computational basis by ρ^C_{ZEF}, and when measuring in the Hadamard basis by ρ^H_{ZEF}. Then,*

$$S(Z|E)_{\rho^C} + S(Z|F)_{\rho^H} \geq 1 \ .$$

2.2 NLQC reductions

We first define what a NLQC aims to achieve, which is to complete what we call a $2\to 2$ quantum task.

Definition 4 *A $2\to 2$ **quantum task** is defined by a pair of input systems A, B, a pair of output systems A', B', and a set of input/output state pairs $\mathcal{S} = \{(\rho_{RAB}, \sigma_{RA'B'})\}$. We require that there exists a quantum channel $\boldsymbol{\mathcal{M}}_{AB\to A'B'}$ such that $(\mathcal{I}_R\otimes\boldsymbol{\mathcal{M}}_{AB\to A'B'})(\rho_{RAB}) = \sigma_{RA'B'}$ for all ρ_{RAB}.*

This definition of task could be further generalized to the case when multiple outputs are allowed per a given input state (i.e., a quantum analogue of a search problem), but we leave that for future exploration.

We will also be interested in *families* of $2\to 2$ quantum tasks, which are collections of $2\to 2$ tasks parameterized by a natural number n. The parameter n will correspond to an input size with the exact relation specified in the definition of each family of tasks. We will label families of tasks with capital letters F, G, etc., where these denote sets of tasks, so that $F = \{F_n\}_n$, $G = \{G_n\}_n$, etc. As an example, the f-route example mentioned in the introduction with a choice of Boolean function family $\{f_n\}_n$ defines a family of $2\to 2$ task, with each member of the family labelled by an element of $\{f_n\}_n$.

We are interested in implementing $2\to 2$ quantum tasks in the form of NLQCs, which we define more carefully next.

Definition 5 *A **non-local quantum computation (NLQC)** is a channel in the form*

$$\boldsymbol{\mathcal{N}}_{AB\to A'B'}(\,\cdot\,) = (\boldsymbol{\mathcal{W}}_{K_aM_a\to A'}\otimes\boldsymbol{\mathcal{W}}_{K_bM_b\to B'})\circ(\boldsymbol{\mathcal{V}}_{AL\to K_aM_b}\otimes\boldsymbol{\mathcal{V}}_{RB\to M_aK_b})(\,\cdot\,\otimes\Psi_{LR}). \tag{12}$$

We refer to Ψ_{LR} as the resource system, the $\boldsymbol{\mathcal{V}}$ channels as the first round operations, and the $\boldsymbol{\mathcal{W}}$ channels as the second round operations.

We say a NLQC is an ϵ-correct implementation of a $2\to 2$ task F_n if the channel $\boldsymbol{\mathcal{N}}_{AB\to A'B'}$ implemented as a NLQC is ϵ-close in diamond norm to the channel $\boldsymbol{\mathcal{M}}_{AB\to A'B'}$ relating the input and output states in the definition of the $2\to 2$ task.

We also introduce the following convention. When considering a specific $2 \to 2$ task, call it X, and referring to an implementation of this as a non-local quantum computation, we will write "the non-local computation X". This can be understood as shorthand for "implementations of the $2 \to 2$ task X in the form of a non-local quantum computation".

We are interested in understanding the relative difficulty of implementing different $2 \to 2$ tasks as NLQCs. To do this, we will define a notion of reduction between $2 \to 2$ tasks. Heuristically, our notion of reduction says that the task G reduces to F when (a few copies of) the resources to implement F as a NLQC can be used to implement G as a NLQC.

To formalize our notion of a reduction among $2 \to 2$ tasks, it is helpful to recall the notion of reduction among computational problems. There we say a function family $A = \{a_n\}_n$ is polynomial-time Turing reducible to function family $B = \{b_n\}$ if a poly(n) time machine with oracle access to B can solve A. More generally, we can replace 'poly-time' with any other complexity class, call it $\mathcal{X}$; the notion of reduction is most meaningful when $\mathcal{X}$ is itself too weak to implement A or B. Inspired by this definition, we give the following definition of reduction among NLQC classes.

Definition 6 *Let F and G be families of $2 \to 2$ task, and α, β, δ all be functions of (n, ϵ), with $\delta \to 0$ as $\epsilon \to 0$. Then we say there is a (α, β, δ)-**reduction** from G to F if, for any resource state $|\Psi^{n,\epsilon}\rangle_{LR}$ which implements F_n at least ϵ-correctly, it is possible to implement G_n δ-correctly using α copies of $|\Psi^{n,\epsilon}\rangle_{LR}$ along with β additional qubits of shared resource state.*

When it is necessary to distinguish this notion of a reduction from other similar notions (e.g. Definition 7 below), we refer to it as a *resource state reduction*. When there is a reduction from family F to family G, we will also say there is an **implication** from G to F, and write $G \Rightarrow F$.

Regarding the values of $\alpha(n)$ and $\beta(n)$, in practice we will find reductions that have $\alpha(n) = O(1)$, $\beta(n) = O(1)$. We define an $O(1)$ reduction to be one where $\alpha = O(1)$, $\beta = O(1)$. Weaker reductions that rely on larger values of $\alpha(n), \beta(n)$ can also be meaningful, at least when $\beta(n)$ is smaller than the number of qubits of resource needed to implement F and G. The requirement on δ that $\delta \to 0$ as $\epsilon \to 0$ is needed to ensure our notion of reduction is not trivial. This is because many $2 \to 2$ tasks can be implemented with some non-zero accuracy trivially, without using any resource state, but become non-trivial at a certain threshold of accuracy. For instance in f-route, the quantum system that is being routed can be brought left or right at random, completing the task correctly half the time. Thus a construction showing that some other $2 \to 2$ task can be used to complete f-route with probability $1/2$ is not meaningful, since we don't need to use any resource state at all. Requiring $\delta \to 0$ when $\epsilon \to 0$ ensures the resource state for F is strong enough, at least if F is implemented with high correctness, to implement a highly correct (and hence non-trivial) G.

Other notions of reduction among $2 \to 2$ tasks are also possible, which highlight different aspects of their structure. For instance, we have not required that our resource state reductions are communication efficient, nor that they involve small computational overheads. Both aspects of NLQC could be explored with other notions of reduction.

One further notion of reduction that we make use of requires that the protocol for G_n be given by using the protocol for F_n used as an oracle, meaning it has access only to copies of the implementation of F_n but not access directly to the state $|\Psi^{n,\epsilon}\rangle_{LR}$. We give a definition of this notion of reduction next.

Definition 7 *Let F and G be families of $2 \to 2$ task, and α, β, δ all be functions of (n, ϵ), with $\delta \to 0$ as $\epsilon \to 0$. Then we say that there is a (α, β, δ) **oracle reduction** from G to F if G can be implemented δ correctly by using α parallel implementations of F along with β additional qubits of resource system and communication.*

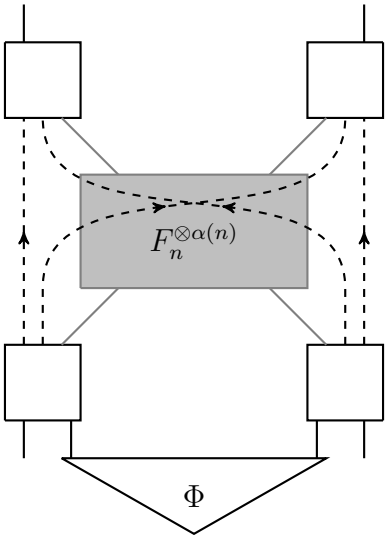

Figure 4: An oracle reduction from a NLQC G to F. The protocol for G_n uses $\alpha(n)$ instances of F_n, plus a $\beta(n)$ qubit resource system Φ and $\beta(n)$ qubits of communication.

The structure of an implementation of G using F as an oracle is shown in Figure 4.

Compared to the notion of resource state reduction in Definition 6, an oracle reduction gives a tighter relationship between task families. This is because in a resource state reduction, we've shown that a resource state that works for F also (up to certain overheads) works for G, while an oracle reduction implies not only that, but that additionally the local operations used in F can also be applied to complete G. Resource state reductions allow greater flexibility in what operations are performed locally to exploit the non-local resources, and reductions under this definition focus on the power of non-local resources for completing NLQCs. For example, some of the reductions described by Theorem 1 are not oracle reductions. Note also that if there is an oracle reduction from F to G then it immediately follows that there is a resource state reduction from F to G in the sense of Definition 6. When not further specified 'reduction' in this article will always mean resource state reduction.

A useful fact is that oracle reductions have convenient error-propagation properties. This follows from the next remark.

Remark 8 *Suppose that there is a protocol which uses parallel implementations of channels $\boldsymbol{\mathcal{N}}_1, \boldsymbol{\mathcal{N}}_2, ...$ to execute some target channel $\boldsymbol{\mathcal{N}}$, so that*

$$\boldsymbol{\mathcal{N}} = \boldsymbol{\mathcal{F}} \circ \left(\bigotimes_{i=1}^{m} \boldsymbol{\mathcal{N}}_i \right) \circ \boldsymbol{\mathcal{P}}. \tag{13}$$

Then suppose we replace the exact implementations of the $\boldsymbol{\mathcal{N}}_i$ with approximate implementations $\overline{\boldsymbol{\mathcal{N}}}_i$ which satisfy $\|\boldsymbol{\mathcal{N}}_i - \overline{\boldsymbol{\mathcal{N}}}_i\|_\diamond \leq \epsilon_i$. Then

$$\overline{\boldsymbol{\mathcal{N}}} = \boldsymbol{\mathcal{F}} \circ \left(\bigotimes_{i=1}^{m} \overline{\boldsymbol{\mathcal{N}}}_i \right) \circ \boldsymbol{\mathcal{P}} \tag{14}$$

is $\sum_i \epsilon_i$ close in diamond norm to $\boldsymbol{\mathcal{N}}$.

This remark follows from the properties of the diamond norm.

To apply this remark to our oracle reductions, note that any realization of G_n using oracle instances of F_n must be exactly correct when F_n is exactly correct. This is because we require that $\delta \to 0$ as $\epsilon \to 0$. When we instead use ϵ correct realizations of F_n, we get from the remark above that the diamond norm distance to the perfectly correct channel is at most $\alpha \cdot \epsilon$, where α is the number of instances of F_n used.

Finally, we will also discuss sets of $2 \to 2$ tasks which are larger than the families introduced above. These sets have an additional parameter aside from the input size. For example, we can discuss the family of tasks given by routing on a particular function family $\{f_n\}_n$, but we can also go further and consider the set of tasks consisting of routing for any possible choice of Boolean function f. We refer to these larger sets of tasks as classes of $2 \to 2$ task or classes of NLQCs. In this paper these classes are parameterized either by a choice of Boolean function, as in f-routing, or a choice of pair of quantum states. Other sets parameterized differently could also be defined.

3 Some classes and their properties

In this section we collect definitions of NLQC tasks that we study here. Most of these tasks have been studied elsewhere in the literature.

3.1 Classically controlled operations

First we define f-route, introduced in [1, 12].

Definition 9 *An **f-route** NLQC task is defined by a choice of Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$, and a d_Q dimensional Hilbert space $\mathcal{H}_Q$. Inputs $x \in \{0,1\}^n$ and system Q are given to Alice, and input $y \in \{0,1\}^n$ is given to Bob. Alice and Bob exchange one round of communication, with the combined systems received or kept by Bob labelled M and the systems received or kept by Alice labelled M'. Label the combined actions of Alice and Bob in the first round as $\boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'}$. The f-route task is completed ϵ-correctly if there exists a family of channels $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$ such that,*

$$\forall (x,y) \in X \times Y \;\; s.t. \;\; f(x,y) = 1, \;\; \|\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \mathrm{tr}_{M'} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'} - \boldsymbol{\mathcal{I}}_{Q\to Q}\|_\diamond \leq \epsilon \tag{15}$$

and there exists a family of channels $\boldsymbol{\mathcal{D}}^{x,y}_{M'\to Q}$ such that

$$\forall (x,y) \in X \times Y \;\; s.t. \;\; f(x,y) = 0, \;\; \|\boldsymbol{\mathcal{D}}^{x,y}_{M'\to Q} \circ \mathrm{tr}_{M} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to MM'} - \boldsymbol{\mathcal{I}}_{Q\to Q}\|_\diamond \leq \epsilon. \tag{16}$$

In words, Bob can recover Q if $f(x,y) = 1$ and Alice can recover Q if $f(x,y) = 0$.

Remark 10 *f-route is equivalent to f-SWAP, where in f-SWAP the goal is to implement $SWAP^{f(x,y)}_{A_0B_0}$ with A_0 on Alice's side and B_0 on Bob's side. We take the error to be the diamond norm distance between the implemented protocol and implementing $SWAP^{f(x,y)}_{A_0B_0}$ exactly. We can implement f-SWAP by first teleporting system B_0 to Alice, and then playing f-route on A_0 and $\neg f$-route on B_0. This costs twice the resources used for f-route, and $O(1)$ extra entanglement for the teleportation of B_0.*
The maximal error in the two f-route protocols used gives an upper bound on the f-SWAP error. f-SWAP immediately gives f-route with the same error by taking B_0 to be in any fixed state.

f-route was shown to be related to CDQS in [7]; in our language their proof shows a $O(1)$ reduction from f-route to CDQS and vice versa. We define CDQS next, first defined in the quantum context in [8].

Definition 11 *A **conditional disclosure of secrets** task with quantum resources (CDQS) is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$, and a d_Q dimensional Hilbert space $\mathcal{H}_Q$ which holds the secret. The task involves inputs $x \in \{0,1\}^n$ and system Q given to Alice, and input $y \in \{0,1\}^n$ given to Bob. Alice sends message system M_a to the referee, and Bob sends message system M_b. Label the combined message systems as $M = M_aM_b$. Label the quantum channel defined by Alice and Bob's combined actions $\boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}$. We put the following two conditions on a CDQS protocol.*

- ϵ-***correct:*** *There exists a channel* $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$*, called the decoder, such that*

$$\forall (x,y) \in X \times Y \;\; s.t. \; f(x,y) = 1, \;\; \|\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_{Q\to Q}\|_\diamond \leq \epsilon. \tag{17}$$

- δ-***secure:*** *There exists a quantum channel* $\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M}$*, called the simulator, such that*

$$\forall (x,y) \in X \times Y \;\; s.t. \; f(x,y) = 0, \;\; \|\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q - \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}\|_\diamond \leq \delta. \tag{18}$$

We call the log-dimension of M the communication cost of the CDQS protocol. We call the log-dimension of the (possibly entangled) state shared by Alice and Bob at the beginning of the protocol the entanglement cost of the protocol.

The correctness parameter ϵ captures how well the secret can be recovered by the referee in $f^{-1}(1)$ instances; the security parameter δ captures how close the message M (seen by the referee) is to a state that doesn't depend on the input at all. Thus when $\delta = 0$, the message system is a fixed state independent of the secret, and hence doesn't reveal the secret.

CDQS was introduced in [7], where its equivalence to f-route was shown. Note that CDQS is not formally an NLQC task, though it is closely related and serves as a useful intermediate setting in our proofs. The same reference also showed that classical CDS protocols also give CDQS protocols, which allowed results on classical CDS to be applied to f-route. CDQS was studied further in [8, 9], where a number of properties are established. One property which we will make use of is amplification, stated formally next, which allows the ϵ, δ parameters in a given CDQS protocol to be reduced.

Theorem 12 ***CDQS amplification:*** *Let F_Q be a* CDQS *for a function f that supports one qubit secrets with correctness error $\delta = 0.09$ and privacy error $\epsilon = 0.09$, has communication cost c, and entanglement cost E. Then for every integer k, there exists a* CDQS *G_Q for f with k-qubit secrets, privacy and correctness errors of $2^{-\Omega(k)}$, and communication and entanglement complexity of size $O(kc)$ and $O(kE)$, respectively.*

This theorem was proven in [8].

We will make use of a variant of CDQS where the secret is assumed to be classical, which we label CDQS'. Since our proofs will relate other primitives to CDQS' (and then CDQS' to CDQS), we give a careful definition of CDQS' as well.

Definition 13 *A* ***conditional disclosure of secrets*** *task with quantum resources and classical secret (CDQS') is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$ and a classical variable $S \in \{0,1\}^{|s|}$ which records the secret. The task involves inputs $x \in \{0,1\}^n$ and system Q given to Alice, and input $y \in \{0,1\}^n$ given to Bob. Alice sends message system M_a to the referee, and Bob sends message system M_b. Label the combined message systems as $M = M_a M_b$. Label the quantum channel defined by Alice and Bob's combined actions $\boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}$. We put the following two conditions on a CDQS' protocol.*

- ϵ-***correct:*** *There exists a channel* $\boldsymbol{\mathcal{D}}^{x,y}_{M\to S}$*, called the decoder, which outputs a classical string in S such that*

$$\forall (x,y) \in X \times Y \;\; s.t. \; f(x,y) = 1, \;\; \forall s \in S, \;\; \Pr\left[\boldsymbol{\mathcal{D}}^{x,y}_{M\to S}(\rho_M(x,y,s)) = s\right] \geq 1 - \epsilon. \tag{19}$$

- δ-***secure:*** *There exists a family of density matrices $\{\sigma_M(x,y)\}_{x,y}$, called the simulator distribution, such that*

$$\forall (x,y) \in X \times Y \;\; s.t. \; f(x,y) = 0, \;\; \forall s \in S, \;\; \|\sigma_M(x,y) - \rho_M(s,x,y)\|_1 \leq \delta. \tag{20}$$

Entanglement and communication costs of CDQS and CDQS' are equivalent up constant factor overheads; the proof is similar to the proof of Theorem 22 in [7]. We adapt their proof to our setting here and give it for completeness in Section A. The two directions of the equivalence are given as Theorem 39 and Theorem 40.

We will make use of the following simple property of CDQS' protocols.

Theorem 14 *Suppose we have a CDQS' protocol which hides a uniformly random classical secret r. Then, using the same resource state but adding $|r|$ bits of communication, we can build a protocol that hides a secret s with $|s| = |r|$ and an arbitrary distribution P_S.*

This is proved in Section A.

Our contribution to the study of these NLQC classes will be to show that CDQS and f-route are equivalent under $O(1)$ reductions to f-measure, defined next.

Definition 15 *A f-**measure** task is defined by a choice of Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$, and a 2 dimensional Hilbert space $\mathcal{H}_Q$. Inputs $x \in \{0,1\}^n$ and system Q are given to Alice, and input $y \in \{0,1\}^n$ is given to Bob. The system Q is in the maximally entangled state with a reference system R.[4] Alice and Bob exchange one round of communication, with the combined systems received or kept by Alice labelled M and the systems received or kept by Bob labelled M'. Define projectors*

$$\Pi^{q,b} = H^q |b\rangle\langle b| H^q \ .$$

The referee will measure $\{\Pi^{f(x,y),0}, \Pi^{f(x,y),1}\}$ on the R system and find measurement outcome $b \in \{0,1\}$. The qubit f-measure task is completed ϵ-correctly on input (x,y) if Alice and Bob both output b. More formally, Alice and Bob succeed if there exist POVM's $\{\Lambda_M^{x,y,0}, \Lambda_M^{x,y,1}\}$, $\{\Lambda_{M'}^{x,y,0}, \Lambda_{M'}^{x,y,1}\}$ such that,

$$\sum_b \mathrm{tr}\left(\Pi_R^{f(x,y),b} \otimes \Lambda_M^{x,y,b} \otimes \Lambda_{M'}^{x,y,b} \rho_{RMM'}\right) \geq 1 - \epsilon \ . \tag{21}$$

f-measure is well studied as a candidate protocol for secure quantum position-verification [1, 2, 18, 19, 22–24].

A number of properties of f-measure, f-route, and CDQS have been established in earlier literature. Regarding lower bounds, [19] showed that when $\epsilon = 0$, both f-route and f-measure require resource states with Schmidt rank at least the rank of $f(x,y)$ viewed as a $2^n \times 2^n$ matrix. For both f-route and f-measure, [22] showed that the memory register to complete these tasks for random choices of function f must be linear in n, though the proof left open if this needed to be a quantum memory or if classical memory sufficed. Again for both f-route and f-measure, [18] showed lower bounds on the number of quantum gates needed which are linear in the communication complexity of f. For both f-route and f-measure, [23] showed a parallel repetition property. Some of the lower bounds given in [8] were not known for f-measure (though we know of no attempt to extend them to that case). Thus regarding lower bounds, nearly all properties of f-route and f-measure matched, but were always proven separately and using distinct strategies.

Regarding upper bounds the state of knowledge for f-route and f-measure differed. For instance [13] showed an upper bound on f-route in terms of the minimal size of a span program computing $f(x,y)$; this allows the complexity class $\mathsf{Mod}_k\mathsf{L}$ to be performed with polynomial entanglement.[5] Meanwhile, for f-measure, the best upper bound was $2^{M(f)}$

[4] Notice that compared to the description of f-measure given in the introduction, we now have the referee give Alice and Bob one end of a maximally entangled state and then later measure the reference system. The referee's measurement is chosen such that the post-measurement state is one of the BB84 states, coinciding with the description in the introduction. The two formulations are equivalent.

[5] It was later realized that combining the implications classical CDS $\Rightarrow$ CDQS $\Rightarrow$ f-route from [7] with known upper bounds on classical CDS also yields the same upper bound as was proven in [13].

where $M(f)$ is the memory to compute $f(x,y)$ on a Turing machine [12]; this allowed f-measure instances with $f \in \mathsf{L} \subseteq \mathsf{Mod}_k\mathsf{L}$ to be completed efficiently. For generic functions, [7] employed a result from the CDS literature to show an upper bound of $2^{O(\sqrt{n \log n})}$ for f-route but no such bound was known for f-measure. For f-route, one function (quadratic residuosity) believed to be outside P was known to have an efficient protocol, but no such example was known for f-measure.

3.2 Coherently controlled operations

Next we define our coherently controlled NLQCs, beginning with implementing a coherent phase. This NLQC has been studied previously in [31].

Definition 16 *A **coherent phase** task is defined by a Boolean function, $f : \{0,1\}^{2n} \to \{0,1\}$. System A consisting of n qubits is given to Alice, and system B consisting of n qubits is given to Bob. Alice and Bob's goal is to implement the unitary*

$$C f\text{-PHASE}_{AB} = \sum_{x,y \in \{0,1\}^n} (-1)^{f(x,y)} |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B . \tag{22}$$

in the form of a NLQC, with A starting and ending on Alice's side and B starting and ending on Bob's side. We say they have implemented the coherent phase operation with correctness ϵ if their implementation is ϵ-close to Cf-PHASE in diamond norm distance.

We will be most interested in the case where the phase is -1, but one could define a similar task with other choices of phase. One motivation for considering this NLQC in particular is that these are the NLQCs discussed in [31], for which strong lower bounds can be proven under the assumption of some mathematical conjectures. Any NLQC classes which imply Cf-PHASE also inherit these conditional bounds.

In relating the coherent phase to other NLQC task, it will be helpful to establish some key properties of coherent phase. We give two observations, both proven in Section B.

Theorem 17 *Given a coherent phase protocol for f_1 which uses resource system Ψ_1, and a coherent phase protocol for f_2 using resource system Ψ_2, there is a protocol for $f_1 \oplus f_2$ using resource system $\Psi_1 \otimes \Psi_2$. Furthermore, the construction is an oracle reduction so that an ϵ_1 correct protocol for f_1 and ϵ_2 correct protocol for f_2 leads to a $\epsilon_1 + \epsilon_2$ correct protocol for $f_1 \oplus f_2$.*

Theorem 18 *Suppose we have a coherent phase protocol for $f(x,y)$ using resource system Ψ. Then, there is a coherent phase protocol for $f(x,y) \wedge z$ using $\Psi \otimes \Psi^+$ where Ψ^+ is the maximally entangled state of two qubits. Furthermore, the protocol is an oracle construction and uses a single implementation of $f(x,y)$ so that if the error in the $f(x,y)$ implementation is ϵ, then the error in implementing $f(x,y) \wedge z$ is also ϵ.*

In fact, we extend this to a more general property. To state it, we first need the following definition.

Definition 19 *Consider a function $f : X \times Y \to \{0,1\}$ with $X = \{0,1\}^n$, $Y = \{0,1\}^n$. The **rank** of f is the smallest integer m such that there exist functions $\{h_i(x)\}$, $\{h'_i(y)\}$ satisfying*

$$f(x,y) = \bigoplus_{i=1}^{m} h_i(x) \wedge h'_i(y). \tag{23}$$

With this definition we can state the following theorem.

Theorem 20 *Consider functions f and g, and let the rank of g be denoted m. Then there is a $O(m)$ reduction from a coherent phase protocol for $f \wedge g$ to a coherent phase protocol for f. Furthermore, the construction is an oracle reduction and uses m invocations of the protocol for f, so that the error in implementing $f \wedge g$ is $m \cdot \epsilon$ where ϵ is the error in the protocol for f.*

We give the proof in Section B.

One related class of NLQCs is the following.

Definition 21 *For a unitary $\mathbf{U}_{A'B'}$, a **coherent** $\mathbf{U}$ task is defined by a Boolean function, $f : \{0,1\}^{2n} \to \{0,1\}$. The goal is to implement the unitary*

$$Cf\text{-}\mathbf{U} = \sum_{x,y \in \{0,1\}^n} \mathbf{U}_{A'B'}^{f(x,y)} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \tag{24}$$

in the form of a NLQC, with AA' beginning and ending with Alice and BB' beginning and ending with Bob. We say the implementation is ϵ-correct if it is ϵ-close to the above unitary in diamond norm distance.

Cf-SWAP and Cf-PAULI are special cases of Cf-$\mathbf{U}$, where we choose $\mathbf{U}_{A'B'} = \text{SWAP}_{A'B'}$ and $\mathbf{U}_{A'B'} = \mathbf{Z}_{A'} \otimes \mathcal{I}_{B'}$ respectively.

Remark 22 *A protocol for coherently controlled unitary $\mathbf{U}$ immediately gives a protocol for a classical controlled unitary $\mathbf{U}$, by recording the classical input strings $x, y \in \{0,1\}^n$ as quantum states $|x\rangle_A, |y\rangle_B$ and taking them as input to the coherent protocol. For example, Cf-SWAP implies f-SWAP (and hence f-route by Remark 10).*

Similar to coherent phase, the coherent unitary NLQC also has some nice composition properties. We give the following two properties, both proven in Section C.

Theorem 23 ***Tensor product parallel composition:*** *Suppose we can implement coherently controlled $\mathbf{U}_1$ and $\mathbf{U}_2$, controlled on function f, using resource systems Ψ^1 and Ψ^2 respectively. Then we can apply $\mathbf{U}_1^f \otimes \mathbf{U}_2^f$ coherently using $\Psi^1 \otimes \Psi^2$. Furthermore, the construction isan oracle reduction so that the overall error is the sum of the error for implementing $\mathbf{U}_1$ and $\mathbf{U}_2$.*

Theorem 24 ***Commuting unitaries:*** *Suppose we can implement unitaries $\mathbf{U}_{A'}^1$ and $\mathbf{U}_{A'}^2$ with A' on Alice's side, coherently controlled on function f using resource systems Ψ^1 and Ψ^2 respectively, and that $\mathbf{U}_{A'}^1$ and $\mathbf{U}_{A'}^2$ commute. Then we can apply $\mathbf{U}_{A'}^1\mathbf{U}_{A'}^2$ coherently controlled off of the same function using resource system $\Psi^1 \otimes \Psi^2$. Furthermore, the construction is an oracle reduction so that the overall error is the sum of the errors in the implementations of each of $\mathbf{U}_{A'}^1$ and $\mathbf{U}_{A'}^2$.*

3.3 State and unitary classes

We will also present a preliminary result on NLQC classes not specified by a choice of Boolean function. In particular, inspired by the result of [26], we look for a relationship between the following two classes.

Definition 25 *The **Distinguish** task for two orthogonal states $|\phi_0\rangle_{AB}, |\phi_1\rangle_{AB}$ is defined as follows. System A is given to Alice and system B is given to Bob; system AB is in state $|\phi_0\rangle_{AB}$ with probability $1/2$, or state $|\phi_1\rangle_{AB}$ with probability $1/2$. The goal is to output a bit b labelling whether they were given the state $|\phi_0\rangle$ or $|\phi_1\rangle$. We say Distinguish is implemented ϵ-correctly if the probability or outputting the correct bit b is at least $1-\epsilon$.*

Definition 26 *The **Interchange** task for two orthogonal states $|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}$ is defined as follows. System A is given to Alice and system B is given to Bob; their goal is to map an arbitrary input superposition $\alpha|\psi_0\rangle + \beta|\psi_1\rangle$ to the output superposition $\alpha|\psi_1\rangle + \beta|\psi_0\rangle$ (i.e., interchange $|\psi_0\rangle$ with $|\psi_1\rangle$).*

4 Reductions among NLQCs

4.1 f-route, f-measure, and CDQS

The main result of this section is the following theorem.

Theorem 1: *For any choice of Boolean function family, f-route, CDQS and f-measure are all equivalent under $O(1)$ resource state reductions.*

We will prove this by showing CDQS $\Rightarrow$ f-route $\Rightarrow$ f-measure $\Rightarrow$ CDQS, with each implication given as a separate lemma.

The first lemma is already established in [7].

Lemma 27 *An ϵ-correct and δ-secure CDQS protocol for function f, hiding secret Q, and using resource system Ψ_{LR} implies the existence of a $\max\{\epsilon, 2\sqrt{\delta}\}$-correct f-route protocol that routes system Q using resource system $|\Psi\rangle_{ELR}$ which purifies Ψ_{LR}, with EL held by Alice and R held by Bob.*

Note that this lemma gives an f-route protocol using the purification of the resource system Ψ_{LR} used in the CDQS protocol. Recall that in our definition of a reduction, we always took the resource system to be pure, so that, in our definition, when considering the CDQS protocol we are starting out with a pure state resource and then using the same pure state resource in the f-route protocol. In some contexts it may be important to keep track of the fact that the CDQS protocol potentially can get away with a weaker resource (the unpurified resource system), but our definition of a reduction is too coarse to capture this distinction.

Next, we move on to the implication from f-route to f-measure.

Lemma 28 ***f-route $\Rightarrow$ f-measure:*** *An ϵ-correct f-route protocol for function f using resource system Ψ implies the existence of a 2ϵ-correct f-measure protocol for the same function using resource system $\Psi^{\otimes 2}$.*

Proof. We first describe the proof when the f-route protocol is perfectly correct; we then comment on the $\epsilon > 0$ case.

In the f-measure protocol, we are given input $x \in \{0,1\}^n$, $H^{f(x,y)}|b\rangle_A$ on Alice's side, $y \in \{0,1\}^n$ on Bob's side. Alice's protocol begins by copying system A in the computational basis into a register C, then copying A in the Hadamard basis into B, and C in the Hadamard basis into D. Thus for example when $f(x,y) = 0, b = 0$, system A is in state $|0\rangle$ and this procedure is

$$\begin{aligned}
|0\rangle_A \overset{\text{copy}}{\to} |00\rangle_{AC} &= (|+\rangle_A + |-\rangle_A)(|+\rangle_C + |-\rangle_C) \\
&= |++\rangle_{AC} + |+-\rangle_{AC} + |-+\rangle_{AC} + |--\rangle_{AC} \\
&\overset{\text{copy}\,H}{\to} |++++\rangle_{ABCD} + |++--\rangle_{ABCD} + |--++\rangle_{ABCD} + |----\rangle_{ABCD} \\
&= |0000\rangle_{ABCD} + |0011\rangle_{ABCD} + |1100\rangle_{ABCD} + |1111\rangle_{ABCD}\,,
\end{aligned}$$

where we haven't kept track of normalization. Repeating this for all four input states, we find

$$\begin{aligned}
|\Psi_{f=0,b=0}\rangle_{ABCD} &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right), \\
|\Psi_{f=0,b=1}\rangle_{ABCD} &= \frac{1}{2}\left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle\right), \\
|\Psi_{f=1,b=0}\rangle_{ABCD} &= \frac{1}{\sqrt{2}}\left(|++++\rangle + |----\rangle\right), \\
|\Psi_{f=1,b=1}\rangle_{ABCD} &= \frac{1}{\sqrt{2}}\left(|++--\rangle + |--++\rangle\right). \qquad (25)
\end{aligned}$$

Alice and Bob perform f-route on the B system, and $\neg f$-route on the C system. This uses two copies of the resource system for f-route.[6] Alice always sends D to Bob. Afterwards, Alice labels the two systems she holds (which may be AB if $f(x,y)=0$ or AC if $f(x,y)=1$) as AB, and Bob labels the two systems he holds (CD if $f(x,y)=0$ or BD if $f(x,y)=1$) as CD. This produces the four states

$$\begin{aligned}
|\Psi_{f=0,b=0}\rangle_{ABCD} &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right), \\
|\Psi_{f=0,b=1}\rangle_{ABCD} &= \frac{1}{2}\left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle\right), \\
|\Psi_{f=1,b=0}\rangle_{ABCD} &= \frac{1}{\sqrt{2}}\left(|++{+}{+}\rangle + |--{-}{-}\rangle\right), \\
|\Psi_{f=1,b=1}\rangle_{ABCD} &= \frac{1}{\sqrt{2}}\left(|+-{+}{-}\rangle + |-+{-}{+}\rangle\right).
\end{aligned} \tag{26}$$

In the second round, Alice and Bob know x, y and hence know $f(x,y)$. Then, Alice measures AB and Bob measures CD; they measure each qubit in the computational basis if $f(x,y)=0$ and in the Hadamard basis if $f(x,y)=1$. Doing so, we see by inspection of the above states that Alice's two measurement outcomes will have even parity if $b=0$, and odd parity if $b=1$. The same is true of Bob's two measurement outcomes. Thus Alice and Bob both output the parity of their measurement outcomes, and this will correctly complete the f-measure task.

Since the protocol uses oracle instances of protocols for f-route and $\neg f$-route, and the $\neg f$-route protocol is ϵ correct when the f-route protocol is, the overall protocol will be 2ϵ correct by Remark 8. ■

The final lemma needed is the implication from f-measure to CDQS'. For this result, we need to introduce some machinery developed in earlier analyses of f-measure [18, 22]. We follow the notation of [18]. We begin with the following definition.

Definition 29 *For $\epsilon \in [0,1]$, let S_C^ϵ be the set of states $|\phi\rangle_{PMM'}$ such that there exists a measurement on subsystem M and a measurement on subsystem M' that each determine the outcome of a measurement in the computational basis on P with probability at least $1-\epsilon$. Similarly, let S_H^ϵ be the set of states $|\phi\rangle_{PMM'}$ such that there exists a measurement on subsystem M and a measurement on subsystem M' that allows us to guess the outcome of a measurement in the Hadamard basis on P with probability at least $1-\epsilon$.*

Next we record the following lemma, proven in [18].

Lemma 30 *Let $h(x) = -x\log x - (1-x)\log(1-x)$ be the binary entropy function. Suppose $\left|\psi^C\right\rangle_{PMM'} \in S_C^\epsilon$, and $\rho^C_{ZMM'}$ is obtained by measuring P in the computational basis and recording the outcome in system Z. Then*

$$S(Z|M')_{\rho^C_{ZMM'}} \leq h(\epsilon).$$

Now we are ready to prove that f-measure implies CDQS. To show this, we actually first show f-measure implies CDQS' (where the secret is taken to be classical). The intuition for the reduction is that an f-measure protocol has the effect of copying the input in the computational basis when $f(x,y)=0$, and in the Hadamard basis when $f(x,y)=1$. We exploit this functionality by preparing $H|s\rangle_Q$ and taking Q as the quantum input to the f-measure protocol, so that the secret is copied correctly (and sent to the referee) when $f(x,y)=1$, but not when $f(x,y)=0$. Finally, Theorem 40 (proven in Section A) shows that CDQS' implies CDQS, completing the chain of equivalences.

[6] Note that f-route and $\neg f$-route can be performed using the same resource system. This is because Alice and Bob can run the f-route protocol, then swap the message systems sent left and right to negate the function.

Lemma 31 ***f*-measure ⇒ CDQS':** *Given a protocol for f-measure for function f using resource system Ψ, there is a protocol for CDQS' for the same function using the same resource system. Further, as the error in the f-measure protocol goes to zero the correctness and security errors in the CDQS' protocol goes to zero.*

Proof. Beginning with the f-measure protocol, take the input system Q to be in the state $H|r\rangle_Q$, with $r \in \{0,1\}$ chosen uniformly at random. The f-measure protocol produces system M' which ends up on Alice's side after the communication round, and system M which ends up on Bob's side. In the CDQS' protocol, Alice and Bob run the same operations but then throw away M' and send M to the referee. Alice additionally sends the bit $s \oplus r$ for s the secret input to the CDQS. We claim this defines a CDQS' protocol which hides s and is both correct and secure.

Notice that the protocol involves running the first round operations of the f-measure protocol once, so uses one copy of the resource system Ψ. We give the proof below assuming a single bit secret, but it extends easily to any $O(1)$ size secret.

Correctness: By ϵ-correctness of the f-measure protocol, when $f(x,y) = 1$ Alice and Bob in the f-measure protocol can obtain r with probability at least $1-\epsilon$. Since here the referee in the CDQS receives the systems Bob would have received, he can also determine r with at least probability $1-\epsilon$, and hence recover s from $s \oplus r$ and r with the same probability. This means the CDQS' protocol is also ϵ-correct.

Security: In the case where $f(x,y) = 0$, the intuition is that correctness of the f-measure protocol means a state in the computational basis inserted into the protocol would allow r to be determined. However, since we have recorded r in the Hadamard basis, we expect r (and hence s) cannot be determined perfectly. To make this precise, we imagine preparing the system Q in the state $H|r\rangle_Q$ by first preparing the maximally entangled state on PQ, then measuring P in the Hadamard basis. This measurement on P commutes with the actions of Alice and Bob in the f-measure protocol, so we can first analyze that protocol as if PQ were maximally entangled. Recalling Definition 29, we have by ϵ-correctness of the f-measure protocol that

$$\rho_{PMM'} \in S_C^\epsilon. \tag{27}$$

Then, from Lemma 30, we have that

$$S(Z|M')_{\rho^C_{ZMM'}} \leq h(\epsilon). \tag{28}$$

Then applying CIT we have that

$$S(Z|M)_{\rho^H_{ZMM'}} \geq 1 - S(Z|M')_{\rho^C_{ZMM'}} \geq 1 - h(\epsilon), \tag{29}$$

which says that, from the referee's perspective, Z (which determines r) is high entropy, suggesting the referee cannot learn s.

To prove security of the CDQS' protocol formally, we need that the state the referee sees is close to one that doesn't depend on s. We will first show that a protocol where Alice and Bob only send M is secure (in the sense that ρ_M is independent of r). To show this, note that the general form of ρ^H_{ZM} is

$$\rho^H_{ZM}(r,x,y) = \frac{1}{2}\sum_r |r\rangle\langle r|_Z \otimes \rho'_M(r,x,y). \tag{30}$$

We now use

$$I(Z:M)_{\rho^H} = S(Z)_{\rho^H} - S(Z|M)_{\rho^H} \tag{31}$$

and the lower bound above on $S(Z|M)_{\rho^H}$ to bound

$$I(Z:M)_{\rho^H} \leq h(\epsilon). \tag{32}$$

Next use $I(A:B)_\rho = D(\rho_{AB}\|\rho_A \otimes \rho_B)$ and Pinsker's inequality (10) to obtain

$$\left\| \frac{1}{2}\sum_r |r\rangle\langle r| \otimes \rho_M^H(x,y) - \frac{1}{2}\sum_r |r\rangle\langle r|_Z \otimes \rho'_M(r,x,y) \right\|_1 \leq \sqrt{(2\ln 2)h(\epsilon)}, \tag{33}$$

where ρ_M^H is formed by tracing out Z from ρ_{ZM}^H, and is from Equation (30)

$$\rho_M^H(x,y) = \frac{1}{2}\sum_r \rho'_M(r,x,y). \tag{34}$$

Then, pulling the sum out of the trace distance in Equation (33), we obtain

$$\frac{1}{2}\sum_r \left\| \rho_M^H(x,y) - \rho'_M(r,x,y) \right\|_1 \leq \sqrt{(2\ln 2)h(\epsilon)}. \tag{35}$$

From this we have that, for all r, we must have

$$\left\| \rho_M^H(x,y) - \rho'_M(r,x,y) \right\|_1 \leq 2\sqrt{(2\ln 2)h(\epsilon)}. \tag{36}$$

Comparing to the security Definition 13 we see that at small enough ϵ, the CDQS' protocol becomes arbitrarily secure (where the secret is r), as needed. ■

Remark 32 ***f*-measure ⇒ CDQS:** *By Theorem 40 along with Lemma 31 we have that we can construct a CDQS protocol using $O(1)$ copies of the f-measure resource state Ψ.*

4.2 Coherent unitary and coherent phase

In this section we prove the implications Cf-SWAP ⇒ Cf-PHASE ⇒ Cf-PAULI.

The coherently controlled SWAP NLQC asks us to implement the unitary

$$Cf\text{-SWAP}_{AA'BB'} = \sum_{x,y} \text{SWAP}_{A'B'}^{f(x,y)} \otimes |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \ . \tag{37}$$

We can see that a protocol for Cf-SWAP implies a protocol for Cf-PHASE, which recall asks us to implement the unitary

$$Cf\text{-PHASE}_{AB} = \sum_{x,y} (-1)^{f(x,y)} |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B \, . \tag{38}$$

We state this implication as the next lemma.

Lemma 33 *For every family of Boolean functions, there is a $O(1)$ implication from Cf-SWAP to Cf-PHASE.*

Proof. First consider the case where we have access to an exactly correct Cf-SWAP protocol. Alice and Bob hold one extra EPR pair, which we take to be on the $A'B'$ systems, $\Psi^+_{A'B'}$. Have Alice apply $\mathbf{Z}_{A'}\mathbf{X}_{A'}$ operator to put the $A'B'$ systems in the state

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{39}$$

Then, run the Cf-SWAP protocol with this state as the input on $A'B'$, and then trace out $A'B'$ at the end, which will implement the operation

$$\begin{aligned}\left|\Phi^-\right\rangle_{A'B'}|x\rangle_A|y\rangle_B &\overset{Cf\text{-SWAP}}{\to} \text{SWAP}^{f(x,y)}_{A'B'}\left|\Phi^-\right\rangle_{A'B'}|x\rangle_A|y\rangle_B \\ &= (-1)^{f(x,y)}\left|\Phi^-\right\rangle_{A'B'}|x\rangle_A|y\rangle_B \\ &\overset{\text{tr}_{A'B'}}{\to} (-1)^{f(x,y)}|x\rangle_A|y\rangle_B\,. \end{aligned} \tag{40}$$

This is exactly the action of the Cf-PHASE operator on a basis, as needed.

Observe that this protocol uses the Cf-SWAP protocol as an oracle, so Remark 8 implies that Cf-SWAP protocol with error ϵ gives a Cf-PHASE protocol with error at most ϵ. ■

Note that we have not been able to show an implication from Cf-PHASE to Cf-SWAP, but we do not have any formal evidence this is not possible.

Continuing, we can find an implication from Cf-PHASE to Cf-PAULI, which choosing the Pauli to be $\mathbf{Z}$ is the unitary

$$Cf\text{-}\mathbf{Z}_{A'AB} = \sum_{x,y}\mathbf{Z}^{f(x,y)}_{A'}\otimes|x\rangle\langle x|_A\otimes|y\rangle\langle y|_B\,. \tag{41}$$

We can now state the following theorem.

Theorem 34 *For every family of Boolean functions, there is a $O(1)$ implication from Cf-PHASE to Cf-PAULI and from Cf-PAULI to Cf-PHASE.*

Proof. Consider the action of Cf-$\mathbf{Z}$ on an arbitrary basis state, $|z\rangle_{A'}|x\rangle_A|y\rangle_B$,

$$Cf\text{-}\mathbf{Z}_{A'AB}|z\rangle_{A'}|x\rangle_A|y\rangle_B = \mathbf{Z}^{f(x,y)}_{A'}|z\rangle_{A'}|x\rangle_A|y\rangle_B = (-1)^{f(x,y)\wedge z}|z\rangle_{A'}|x\rangle_A|y\rangle_B\,. \tag{42}$$

Thus, a Cf-PHASE protocol for the function $f(x,y)\wedge z$ is exactly a Cf-$\mathbf{Z}$ protocol, where the input qubit for the Cf-PHASE that holds z is treated as the target qubit in the Cf-$\mathbf{Z}$ protocol. Let the resource system used in the Cf-PHASE protocol for function f be Ψ. Using Theorem 18, we know the Cf-PHASE protocol for $f(x,y)\wedge z$ can be implemented using $\Psi\otimes\Psi^+$, and so Cf-$\mathbf{Z}$ can be as well.

To obtain Cf-PHASE from Cf-PAULI, we choose A' to be in the state $|1\rangle_{A'}$ and run the Cf-PAULI protocol.

To handle the approximate case, we again observe that because the above reductions are oracle reduction we can employ Remark 8. ■

Cf-PHASE can also be used to implement other coherently controlled unitaries. In particular any unitaries that act on qubits held entirely by Alice (or entirely by Bob) and have ±1 eigenvalues can be implemented via a similar strategy to the one used to implement Cf-$\mathbf{Z}$. To implement $\mathbf{U}_{A'}$ Alice should first apply a unitary $\mathbf{V}_{A'}$ to map the inputs from the eigenbasis of $\mathbf{U}_{A'}$ to the computational basis, implement a controlled phase as needed, then apply $\mathbf{V}^\dagger$. For instance, a CZ gate can be implemented in this way with $\mathbf{V}_{A'}=\mathcal{I}_{A'}$ and using the controlled phase operation $f(x,y)\wedge z_1\wedge z_2$. Similarly, $\text{SWAP}_{A'_1A'2}$ can be implemented by choosing $\mathbf{V}_{A'_1A'_2}$ to map from the Bell basis to the computational basis and a controlled phase with function $f(x,y)\wedge z_1\wedge z_2$ again.[7] Similar strategies to those described here also relate controlled phase operations with other choices of phase $\omega\neq\pm1$ and unitaries with eigenvalues $1,\omega$.

[7]Note that while coherently controlled $\text{SWAP}_{A'_1A'_2}$ follows from Cf-PHASE, this does not imply that controlled $\text{SWAP}_{A'B'}$ can, where in the later case the two qubits being swapped are separately on Alice and Bob's side. In this article when we refer to Cf-SWAP we mean implementing $\text{SWAP}_{A'B'}$.

4.3 Coherent Pauli to CDQS

Previously, we noted that Cf-SWAP $\Rightarrow$ f-route, and hence Cf-SWAP also implies the other classically controlled protocols we study. Here, we show that in fact the potentially weaker coherent primitive of Cf-PAULI already suffices to obtain the classically controlled classes.

Theorem 35 *For every family of Boolean functions, there is a $O(1)$ implication from Cf-PAULI to CDQS.*

Proof. We use the Cf-PAULI protocol to implement a CDQS' protocol. Theorem 40 then gives us the CDQS protocol. We use the following procedure.

1. From their classical inputs Alice prepares quantum systems $|s\rangle_{A'}|x\rangle_A$; Bob prepares $|0\rangle_{B'}|y\rangle_B$.
2. Alice and Bob execute the first round operations of a protocol for Cf-$\mathbf{X}_{B'}$ with choice of function $f(x,y) \wedge s$.
3. The systems that would be sent to Bob (call them system M) in the second round are sent to the referee in the CDQS protocol. The remaining degrees of freedom which would be sent to Alice (call them system M') are traced out.

Using Theorem 18 and the equivalence of Cf-PAULI and Cf-PHASE, we have that this uses one copy of the resource system for a Cf-$\mathbf{X}$ protocol for function f, plus $O(1)$ additional EPR pairs.

Correctness: We have that $f(x,y) = 1$. Let the action of (both rounds of) the Cf-$\mathbf{X}$ protocol be described by a channel $\boldsymbol{\mathcal{N}}$. Then, perfect correctness of the Cf-$\mathbf{X}$ protocol would give that

$$\begin{aligned}\boldsymbol{\mathcal{N}}\left(|s,x\rangle\langle s,x|_{A'A} \otimes |0,y\rangle\langle 0,y|_{B'B}\right) &= |s,x\rangle\langle s,x|_{A'A} \otimes |f(x,y)\wedge s, y\rangle\langle f(x,y)\wedge s, y|_{B'B} \\ &= |s,x\rangle\langle s,x|_{A'A} \otimes |s,y\rangle\langle s,y|_{B'B}\,,\end{aligned}$$

where in the second line we used that $f(x,y) = 1$. Since the referee in the CDQS gets the same systems as Bob obtains in the Cf-$\mathbf{X}$, the referee can apply the same local channel as Bob and hence recover the $B'B$ portion of the above density matrix. Thus the referee in the perfectly correct case can measure B' and learn $f(x,y) \wedge s = s$.

To obtain approximate correctness when the Cf-$\mathbf{X}$ protocol is approximately correct, we note that the CDQS protocol we implement produces the same state on $B'B$ as if we implemented the Cf-$\mathbf{X}$ protocol as an oracle, and then traced out the system on the left. Because of this, Remark 8 implies the protocol here is ϵ-correct if the Cf-$\mathbf{X}$ protocol is ϵ correct.

Security: Let $\mathbf{V}_{SAB'B\to MM'}$ be an isometric extension of Alice and Bob's first round operations in the $Cf-\mathbf{X}$ protocol. Let $\mathbf{W}^L_{M'\to SAl}$ and $\mathbf{W}^R_{M\to B'Br}$ to be isometric extensions of the second round operations, with l and r the purifying systems. Define channels

$$\begin{aligned}\boldsymbol{\mathcal{V}}_{SAB'B\to MM'} &= \mathbf{V}_{SAB'B\to MM'}(\cdot)\mathbf{V}^\dagger_{SAB'B\to MM'} \\ \boldsymbol{\mathcal{W}}^L_{M'\to A'Al} &= \mathbf{W}^L_{M'\to A'Al}(\cdot)(\mathbf{W}^L_{M'\to A'Al})^\dagger \\ \boldsymbol{\mathcal{W}}^R_{M'\to A'Ar} &= \mathbf{W}^R_{M\to B'Br}(\cdot)(\mathbf{W}^R_{M\to B'Br})^\dagger. \end{aligned} \tag{43}$$

Then the action of the Cf-$\mathbf{X}$ protocol, in $f(x,y) = 0$ instances and assuming perfect correctness of the Cf-$\mathbf{X}$, is

$$\begin{aligned}&|s,x\rangle\langle s,x|_{A'A} \otimes |0,y\rangle\langle 0,y|_{B'B} \\ &\qquad = \mathrm{tr}_{lr}(\boldsymbol{\mathcal{W}}^L_{M'\to A'Al} \otimes \boldsymbol{\mathcal{W}}^R_{M\to B'Br}) \circ \boldsymbol{\mathcal{V}}_{A'AB'B\to M'M}(|s,x\rangle\langle s,x|_{A'} \otimes |0,y\rangle\langle 0,y|_{B'}).\end{aligned}$$

Removing the trace, we have

$$\begin{aligned}
&|s,x\rangle_{A'A} \otimes |0,y\rangle_{B'B} \otimes |\Psi(s,x,y)\rangle_{lr} \\
&\qquad = (\mathbf{W}^L_{M'\to A'Al} \otimes \mathbf{W}^R_{M\to B'Br}) \circ \mathbf{V}_{A'AB'B\to M'M} \, |s,x\rangle_{A'} \otimes |0,y\rangle_{B'}) \\
&\qquad = \mathbf{M}_{A'AB'B\to A'AB'Blr} \, |s,x,y\rangle \, ,
\end{aligned} \tag{44}$$

where the last line defines $\mathbf{M}$. We can actually simplify the above by noting that the state on lr must be independent of s, x, y. To see why, suppose we had inserted a superposition of $|s,x,y\rangle$ basis states, producing

$$\sum_{s,x,y} c_{s,x,y} \, |s,x,0,y\rangle \to \sum_{s,x,y} c_{s,x,y} \mathbf{M} \, |s,x,0,y\rangle = \sum_{s,x,y} c_{s,x,y} \, |s,x,0,y\rangle_{AA'BB'} \, |\Psi(s,x,y)\rangle_{lr} \, . \tag{45}$$

But now tracing out lr we obtain

$$\sum_{s,x,y} c_{s,x,y} \bar{c}_{s',x',y'} \, \langle \Psi(s,x,y) | \Psi(s',x',y') \rangle \, |s,x,0,y\rangle\langle s',x',0,y'|_{A'AB'B} \, . \tag{46}$$

By correctness, this must equal the output of the correct protocol, so that

$$\begin{aligned}
&\sum_{s,x,y} c_{s,x,y} \bar{c}_{s',x',y'} \, |s,x,0,y\rangle\langle s',x',0,y'|_{A'AB'B} \\
&\qquad = \sum_{s,x,y} c_{s,x,y} \bar{c}_{s',x',y'} \, \langle \Psi(s,x,y) | \Psi(s',x',y') \rangle \, |s,x,0,y\rangle\langle s',x',0,y'|_{A'AB'B} \, .
\end{aligned}$$

This gives that $\langle \Psi(s,x,y) | \Psi(s',x',y') \rangle = 1$, so that $|\Psi(s,x,y\rangle$ must not depend on s, x, y. Using this, we can simplify Equation (44) to take Ψ_{lr} to be independent of s, x, y, so that

$$\begin{aligned}
&(|s,x\rangle\langle s,x|_{A'} \otimes |0,y\rangle\langle 0,y|_{B'B} \otimes \Psi_{lr}) \\
&\qquad = (\boldsymbol{\mathcal{W}}^L_{M'\to A'A} \otimes \boldsymbol{\mathcal{W}}^R_{M\to B'B}) \circ \boldsymbol{\mathcal{V}}_{A'AB'B\to M'M}(|s,x\rangle\langle s,x|_{A'} \otimes |0,y\rangle\langle 0,y|_{B'}).
\end{aligned}$$

Next act with $(\boldsymbol{\mathcal{W}}^L_{M'\to A'Al} \otimes \boldsymbol{\mathcal{W}}^R_{M\to B'Br})^\dagger$ to produce

$$\begin{aligned}
(\boldsymbol{\mathcal{W}}^L_{M'\to A'A})^\dagger \otimes (\boldsymbol{\mathcal{W}}^R_{M\to B'B})^\dagger(|s,x\rangle\langle s,x|_{A'} \otimes |0,y\rangle\langle 0,y|_{B'B} \otimes \Psi_{lr}) \\
= \boldsymbol{\mathcal{V}}_{A'AB'B\to M'M}(|s,x\rangle\langle s,x|_{A'} \otimes |0,y\rangle\langle 0,y|_{B'}) \\
= \rho_{M'M}(x,y,s).
\end{aligned} \tag{47}$$

Tracing out M' to find the density matrix that describes M, we see that the system the referee obtains is

$$\begin{aligned}
\rho_M(x,y,s) &= \mathrm{tr}_{M'}(\boldsymbol{\mathcal{W}}^L_{M'\to A'Al})^\dagger \otimes (\boldsymbol{\mathcal{W}}^R_{M\to B'Br})^\dagger(|s,x\rangle\langle s,x|_{A'A} \otimes |0,y\rangle\langle 0,y|_{B'B} \otimes \Psi_{lr}) \\
&= \mathrm{tr}_{A'Al}(\boldsymbol{\mathcal{W}}^R_{M\to B'Br})^\dagger(|s,x\rangle\langle s,x|_{A'Al} \otimes |0,y\rangle\langle 0,y|_{B'Br} \otimes \Psi_{lr}) \\
&= (\boldsymbol{\mathcal{W}}^R_{M\to B'Br})^\dagger(|0,y\rangle\langle 0,y|_{B'Br} \otimes \Psi_r) \\
&=: \sigma_M(y).
\end{aligned} \tag{48}$$

Since this state does not depend on s, the CDQS protocol is perfectly secure.

To establish approximate security in the case where Cf-$\mathbf{X}$ is approximately correct, we again note that the state produced on the referee's side is the same one as if we had made an oracle invocation of the Cf-$\mathbf{X}$ protocol. Thus the state produced must be ϵ-close to $\sigma(y)$, which is exactly ϵ security of the CDQS protocol. ■

4.4 Interchange implies Distinguish

In this section we give a different type of reduction, this one between two NLQC tasks that aren't characterized in terms of a Boolean function. These tasks are Interchange (i.e., coherently transform a state $|\psi_0\rangle$ to an orthogonal state $|\psi_1\rangle$ and vice versa), and Distinguish (i.e., distinguish between two orthogonal states $|\phi_0\rangle, |\phi_1\rangle$). See Section 3.3 for formal definitions of these tasks. At a high level, we show that an efficient NLQC protocol for Interchange with states $|\psi_0\rangle, |\psi_1\rangle$ implies an efficient NLQC protocol for Distinguish with the "Fourier" states $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle \pm |\psi_1\rangle)$.

Our result is inspired by the equivalence of these tasks in the standard model of quantum circuits: it is known [26] that an efficient algorithm for Interchange with $|\psi_0\rangle, |\psi_1\rangle$ implies an efficient algorithm for Distinguish $|\phi_\pm\rangle$, *and vice versa*. Note that in this setting we are considering global operations, with no division of the inputs between players. This equivalence, though simple, has had important applications in quantum cryptography [32–34] in recent years.

While we found a reduction in one direction (Interchange implies Distinguish) in the NLQC setting, we weren't able to find the other direction. It is an interesting open question of whether this other direction is possible.

Before describing our reduction more precisely, we first define the notion of a **catalytic** NLQC protocol. Intuitively, it is one where the resource state is used as part of the protocol, and then returned to its original state at the end.

Definition 36 (Catalytic NLQC protocol) *Let $\mathbf{U}_{AB\to AB}$ denote a unitary $2\to 2$ task. We say that a NLQC $\boldsymbol{\mathcal{N}}_{AB\to AB}$ for $\mathbf{U}$ is **catalytic** if the isometric extensions V, W of the first and second round operations and the resource state Ψ_{LR} satisfy the following: for all input states $|\phi\rangle_{AB}$,*

$$\mathbf{WV}\,|\phi\rangle_{AB} \otimes |\Psi\rangle_{LR} = (\mathbf{U}\,|\phi\rangle_{AB}) \otimes |\Psi\rangle_{LR}\ .$$

In other words, the resource state $|\Psi\rangle_{LR}$ serves as a catalyst *for the nonlocal computation.*

We now argue that any NLQC for a unitary task can be made *approximately* catalytic, with only a linear factor overhead in the size of the resource state.

Lemma 37 *Let $\mathbf{U}$ denote a unitary $2\to 2$ task. Suppose that $\boldsymbol{\mathcal{N}}_{AB\to AB}$ is a δ-correct NLQC for $\mathbf{U}$ (not necessarily catalytic) with an m-qubit resource state. Then for all $\epsilon > 0$, there exists an $(\epsilon + \sqrt{\delta})$-approximately catalytic NLQC $\hat{\boldsymbol{\mathcal{N}}}_{AB\to AB}$ for $\mathbf{U}$ using a $O(m/\epsilon^2)$-qubit resource state $\Xi_{L'R'}$, in the sense that for all input states $|\phi\rangle_{AB}$,*

$$\|\hat{\mathbf{W}}\hat{\mathbf{V}}(|\phi\rangle_{AB} \otimes |\Xi\rangle_{L'R'}) - (\mathbf{U}\,|\phi\rangle_{AB}) \otimes |\Xi\rangle_{L'R'}\,\|_2 \leq \epsilon + \sqrt{\delta}$$

where $\hat{\mathbf{V}}, \hat{\mathbf{W}}$ are the isometric extensions of the first and second round operations, respectively, of the NLQC $\hat{\boldsymbol{\mathcal{N}}}$.

Proof. This proof relies on the idea of *entanglement embezzlement states* [35]; these are a family of bipartite states $\{|\Xi_n\rangle_{LR}\}$ where $|\Xi_n\rangle$ is on n-qubits, such that for all bipartite pure states $|\psi\rangle_{AB}$ on m qubits, there exists local isometries $\mathbf{S}_{L\to LA}, \mathbf{T}_{R\to RB}$ such that

$$\|\mathbf{S}_{L\to LA} \otimes \mathbf{T}_{R\to RB}\,|\Xi_n\rangle_{LR} - |\Xi_n\rangle_{LR} \otimes |\psi\rangle_{AB}\,\|_2^2 \leq \frac{2m}{n}\ . \tag{49}$$

In other words, using only local operations, the entanglement $|\psi\rangle$ has been *embezzled* from the state $|\Xi_n\rangle$, and this is not very noticeable (provided that $n \gg m$).

From δ-correctness of $\boldsymbol{\mathcal{N}}_{AB\to AB}$, we have that for an arbitrary input state $|\psi\rangle_{AB}$

$$\|\boldsymbol{\mathcal{N}}_{AB\to AB}(|\psi\rangle\langle\psi|_{AB}) - \mathbf{U}_{AB}\,|\psi\rangle\langle\psi|\,\mathbf{U}_{AB}^\dagger\|_1 \leq \delta. \tag{50}$$

Let $\mathbf{V}, \mathbf{W}$ be isometric extensions of the first- and second-round operations of $\boldsymbol{\mathcal{N}}$, respectively. Let $|\Psi\rangle_{LR}$ denote the resource state, and $\tilde{L}\tilde{R}$ the Hilbert space of the purifying system at the end of the protocol. Then the above gives that

$$\| \operatorname{tr}_{\tilde{L}\tilde{R}}(\mathbf{WV}(|\psi\rangle\langle\psi| \otimes |\Psi\rangle\langle\Psi|)\mathbf{V}^\dagger\mathbf{W}^\dagger) - \mathbf{U}\,|\psi\rangle\langle\psi|\,\mathbf{U}^\dagger\|_1 \leq \delta. \tag{51}$$

Converting this to a fidelity using the Fuchs van de Graff inequalities, applying Uhlmann's theorem to express the fidelity in terms of purified states, and converting back to a trace distance we obtain that there exists a state $|\Theta\rangle_{\tilde{L}\tilde{R}}$ such that

$$\|\mathbf{WV}(|\psi\rangle\langle\psi| \otimes |\Psi\rangle\langle\Psi|)\mathbf{V}^\dagger\mathbf{W}^\dagger - \mathbf{U}\,|\psi\rangle\langle\psi|\,\mathbf{U}^\dagger \otimes |\Theta\rangle\langle\Theta|\,\|_1 \leq \sqrt{2\delta}\,. \tag{52}$$

Using that $\|\,|u\rangle\langle u| - |v\rangle\langle v|\,\|_1 = 2\sqrt{1 - |\,\langle u|v\rangle\,|^2} \geq 2\sqrt{1 - |\,\langle u|v\rangle\,|}$ and the fact that we are free to choose the phase of $|\Theta\rangle$ such that the inner product of the vectors in (52) is positive, we can also infer that

$$\|\mathbf{WV}(|\psi\rangle \otimes |\Psi\rangle) - \mathbf{U}\,|\psi\rangle \otimes |\Theta\rangle\,\|_2 \leq \sqrt{\delta}\,. \tag{53}$$

In other words, in the process of transforming $|\phi\rangle$ to $\mathbf{U}\,|\phi\rangle$, the resource state $|\Psi\rangle$ has been transformed to another resource state $|\Theta\rangle$. This is not a catalytic protocol when $|\Psi\rangle$ is far from $|\Theta\rangle$.

We now adapt this to be a catalytic NLQC. Consider the following NLQC. Set $n = 8m/\epsilon^2$, and consider the n-qubit embezzlement state $|\Xi_n\rangle_{L'R'}$. By the above there exist unitary operations $\mathbf{S}_{L'L\to L'L}, \mathbf{T}_{R'R\to R'R}$ such that $\mathbf{S}\otimes\mathbf{T}$, acting on $|\Xi_n\rangle \otimes |0\rangle^{\otimes m}$, is $\epsilon/2$-close to $|\Xi_n\rangle_{L'R'} \otimes |\Psi\rangle_{LR}$. First, apply these local operations. Then, apply the original isometries $\mathbf{V}, \mathbf{W}$ with the resource state $|\Psi\rangle$ as in $\boldsymbol{\mathcal{N}}$, and finally apply the inverse of a pair of local unitaries $\mathbf{S}'\otimes\mathbf{T}'$ that "reverse" the embezzlement, which satisfy

$$\|\mathbf{S}'\otimes\mathbf{T}'\,|\Xi_n\rangle \otimes |0\cdots 0\rangle - |\Xi_n\rangle \otimes |\Theta\rangle\,\|_2 \leq \epsilon/2\ . \tag{54}$$

Define the isometric extensions $\hat{\mathbf{V}} = \mathbf{V}(\mathbf{S}\otimes\mathbf{T})$ and $\hat{\mathbf{W}} = ((\mathbf{S}')^\dagger \otimes (\mathbf{T}')^\dagger)\mathbf{W}$. Since $\mathbf{V}, \mathbf{W}$ factor into local operations (i.e., $\mathbf{V} = \mathbf{V}_{AL}\otimes\mathbf{V}_{BR}$ and $\mathbf{W} = \mathbf{W}_{AL}\otimes\mathbf{W}_{BR}$) these isometries $\hat{\mathbf{V}}, \hat{\mathbf{W}}$ yield a NLQC. By the triangle inequality this NLQC for $\mathbf{U}$ is $(\epsilon+\sqrt{\delta})$-approximately catalytic. ■

Finally, we now show that any efficient, catalytic, Interchange protocol (for which Lemma 37 shows the catalytic property is without loss of generality) implies an efficient Distinguish protocol for a related pair of states.

Theorem 38 *Suppose there is an ϵ-correct catalytic NLQC for Interchange between two orthogonal states $|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}$ using an m-qubit resource state. Then there exists a ϵ correct NLQC for Distinguish between the "Fourier" states $|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle \pm |\psi_1\rangle)$ that uses the same m-qubit resource state, with two extra EPR pairs.*

Proof. Label an isometric extension of the first round operations in the catalytic Interchange protocol $\mathbf{V}$, and an isometric extension of the second round operations $\mathbf{W}$. Let the catalytic resource state used by the Interchange protocol be $|\Phi\rangle_{LR}$. Define states

$$\begin{aligned} |\phi_0\rangle &= \mathbf{V}\,|\psi_0\rangle\,|\Phi\rangle \\ |\phi_1\rangle &= \mathbf{V}\,|\psi_1\rangle\,|\Phi\rangle \end{aligned} \tag{55}$$

and notice that since by correctness $\|\,|\psi_1\rangle\,|\Phi\rangle - \mathbf{WV}\,|\psi_0\rangle\,|\Phi\rangle\,\|_1 \leq \epsilon$ and $\|\,|\psi_0\rangle\,|\Phi\rangle - \mathbf{WV}\,|\psi_1\rangle\,|\Phi\rangle\,\|_1 \leq \epsilon$, we have also

$$\begin{aligned} \|\,|\psi_1\rangle\,|\Phi\rangle - \mathbf{W}\,|\phi_0\rangle\,\|_1 &\leq \epsilon, \\ \|\,|\psi_0\rangle\,|\Phi\rangle - \mathbf{W}\,|\phi_1\rangle\,\|_1 &\leq \epsilon. \end{aligned} \tag{56}$$

Now consider the following protocol for Distinguish. Distribute one extra EPR pair, so that Alice and Bob hold

$$\frac{1}{2}\left(|\psi_0\rangle_{AB} + (-1)^b |\psi_1\rangle_{AB}\right)\left(|00\rangle_{A_0B_0} + |11\rangle_{A_0B_0}\right)|\Phi\rangle_{LR} \ . \tag{57}$$

Then, we have Alice and Bob do the following: controlled on A_0, Alice implements her operations from $\mathbf{V}$ if A_0 is in state $|0\rangle$, and her operations from $\mathbf{W}^\dagger$ if it is in state $|1\rangle$. Similarly, Bob does his operations from $\mathbf{V}$ or $\mathbf{W}^\dagger$ controlled on B_0. This brings the state to one ϵ-close in trace distance to

$$\frac{1}{2}\left(|\phi_0\rangle_{AB} + (-1)^b |\phi_1\rangle_{AB}\right)|00\rangle_{A_0B_0} + \frac{1}{2}\left(|\phi_1\rangle_{AB} + (-1)^b |\phi_0\rangle_{AB}\right)|11\rangle_{A_0B_0}$$
$$= \frac{1}{2}\left(|\phi_0\rangle_{AB} + (-1)^b |\phi_1\rangle_{AB}\right)\left(|00\rangle_{A_0B_0} + (-1)^b |11\rangle_{A_0B_0}\right) .$$

Next, Alice and Bob throw away the AB systems. This leaves the A_0B_0 systems in a state ϵ-close to $\frac{1}{\sqrt{2}}\left(|00\rangle_{A_0B_0} + (-1)^b |11\rangle_{A_0B_0}\right)$ and run Distinguish on the inputs $|00\rangle, |11\rangle$. This can be implemented using one EPR pair, and will be ϵ correct. Along with the EPR pair used above, this implements Distinguish on the inputs $|\psi_0\rangle, |\psi_1\rangle$ with two extra EPR pairs compared to the catalytic Interchange protocol. ■

5 Implications and simplifications

Because f-route and f-measure are well studied in the literature, our proof that they are equivalent leads to a large number of simplifications. In particular, the papers [18, 19, 22, 23] each contain repeated proofs, once for f-measure and once for f-route, which can now become one proof for either measure or routing, and then Theorem 1 ensures the other NLQC inherits the same property. Notably, the proofs in these papers often used different techniques for each protocol; our reduction lets either one suffice for both.

As an additional simplification, we can also notice that both of the results in [36] now follow immediately from earlier literature combined with our reductions. In particular, in [37] security was shown for the f-measure protocol in the *random oracle model*: the success probability for an f-measure protocol is small unless many oracle calls to f are made by Alice and Bob. Separately, security for f-route in the random oracle model was shown in [36] using different techniques. Now, only one of these two proofs is needed, along with the observation that from our implication from f-route to f-measure, the oracle calls needed for f-route upper bound those for f-measure. In [36] the authors also show strong parallel repetition of f-route in the no pre-shared entanglement model. Again, this property was known for f-measure [15], and is also carried over by our reductions.

Beyond simplifying the literature, we also obtain a number of new properties of f-route and f-measure via our reductions. Regarding lower bounds, [8] proved lower bounds on CDQS (equivalently, f-route) on communication and the dimension of the shared resource state in terms of various measures of communication complexity. For instance, among other bounds, they proved a lower bound on communication in CDQS for a function f in terms of the communication cost of two-round quantum interactive proof for the same function. An alternative lower bound in terms of a public coin quantum interactive proof, again with two rounds but now with two provers, was proven in [9]. Both of these are now inherited by f-measure.

Regarding upper bounds, more was previously known about f-route than about f-measure. In particular [13] gave an upper bound from span program size for f-route; f-measure now inherits this bound. Via the connection to classical CDS, [7] gave upper bounds on f-route for all functions of $2^{O(\sqrt{n \log n})}$, which is also now inherited by f-

measure.[8] Finally [7] gave an efficient f-route protocol for quadratic residuosity, which we now obtain for f-measure.

On a more negative side, proving linear lower bounds on CDQS or f-route was known to face a 'CDS barrier': placing such a lower bound on entanglement in CDQS also puts the same lower bound on randomness in classical CDS, which is a long standing open problem in the classical literature. Now, we see that placing such lower bounds on f-measure also faces the same barrier.

6 Discussion

Taking a comparative approach opens many new directions towards understanding NLQC and the subjects it is related to. Perhaps most clearly, future explorations of further NLQC classes and their relationships may yield more insight into entanglement cost in NLQC. For instance, inspired by our observation here that many superficially distinct classically controlled NLQC classes are equivalent, it is natural to ask if *all* NLQC classes involving controlling an $O(1)$ size, non-trivial, quantum operation off of classical inputs could be equivalent.

A direction we have not explored here is to prove that some instances of NLQC *cannot* be reduced to one another. For instance, it seems plausible that coherent protocols cannot be reduced to classically controlled ones. In fact, Cf-PHASE and hence Cf-SWAP are subject to the conditional exponential lower bounds from [31], while CDQS has a sub-exponential upper bound [7]. Assuming the conjectures needed for the exponential lower bound hold then, there can be no efficient implication from CDQS to Cf-SWAP. More generally, one could look for general properties that imply one NLQC cannot be reduced to another. Doing so would identify those properties as key to the "hardness" of a NLQC.

One of the key open questions in NLQC is to prove a linear lower bound on a classically controlled function class. For instance, to prove a linear bound against f-route while allowing correctness errors. This would be highly desirable from the perspective of QPV. At the same time, such a bound would also imply a highly sought after lower bound for CDS, where a key goal is to show a linear lower bound on communication in the setting with correctness and privacy errors allowed. Our approach suggests a starting point to proving such lower bounds: pick a harder but related NLQC and try to lower bound it first. For instance, since Cf-PAULI implies f-route, placing a linear, robust, lower bound on Cf-PAULI is an easier but related problem to proving a robust lower bound on f-route and CDS.

We can also hope that new reductions will lead to new connections among the many areas tied to NLQC. For instance, information-theoretic cryptography and in particular CDS is related to f-route, while f-measure seems to be related to uncloneable cryptography. In particular parallel repetition for f-measure is proven using the same key results on monogamy of entanglement games as appear in uncloneable cryptography [15]. It would be interesting to further explore this connection, or other ways in which bridges among NLQCs can relate apparently distinct areas in quantum cryptography and information theory.

Finally, as a speculative comment, we can ask if the connections between NLQC and complexity theory highlighted here can give insight into complexity theory, for instance by providing a route to new lower bounds on complexity measures. It is interesting to note here a comparison to communication complexity: in communication complexity it is possible to obtain good lower bounds on the needed non-local resource (communication),

[8] Note that as of this writing, all classically controlled function NLQCs use sub-exponential entanglement even in the worst case. It would be interesting to understand if this is always the case.

but the applications of this to complexity theory are restricted by the fact that communication never needs to be larger than linear. In NLQC, we again have some non-local resource we can hope to bound (correlation or entanglement), but now we can hope for super-linear lower bounds. Since entanglement in many NLQC classes is upper bounded by complexity measures, entanglement lower bounds in NLQC provide complexity lower bounds. This was already observed in earlier works, for instance in the context of f-routing [12, 13], but we hope that finding new complexity based upper bounds on further NLQC classes and exploring the relationships among classes can lead to interesting complexity lower bounds.

Acknowledgements

AB was supported by the ANR project PraQPV, grant number ANR-24-CE47-3023. AM and MS acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC); this work was supported by an NSERC Discovery grant (RGPIN-2025-03966) and NSERC-UKRI Alliance grant (ALLRP 597823-24). Research at the Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Industry Canada and by the Province of Ontario through the Ministry of Colleges and Universities. PVL is supported by France 2030 under the French National Research Agency award number ANR-22-PETQ-0007. HY is supported by AFOSR award FA9550-23-1-0363, NSF CAREER award CCF-2144219, and the Sloan Foundation. SH acknowledges that: This work was supported by the MSCA cofund QuanG [grant number : 101081458] Funded by the European Union

A Properties of CDQS

Theorem 39 *A CDQS protocol using resource system Ψ implies a CDQS' protocol for the same function using the same resource system.*

Proof. Take the classical secret $s \in S$ for the CDQS' protocol and record it as a computational basis state $|s\rangle_Q$, which serves as the secret for the CDQS protocol. The referee runs the decoder for the CDQS protocol and then measures the outcome in the computational basis, and takes the output as his guess for the value of S.

Correctness: We have that $f(x, y) = 1$. By correctness of the CDQS protocol we have

$$\left\| \boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_Q \right\|_\diamond \leq \epsilon. \tag{58}$$

Evaluating these channels on the input state $|s\rangle_Q$, we obtain

$$\left\| \boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(|s\rangle\langle s|_Q) - |s\rangle\langle s|_Q \right\|_1 \leq \epsilon\,. \tag{59}$$

To obtain a classical outcome for the CDQS protocol, the referee then measures the output of the decoder in the computational basis. Label the outcome of this measurement as s'. Their probability of a correct outcome is then

$$\Pr[s' = s] = \langle s|\, \boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(|s\rangle\langle s|_Q)\, |s\rangle = F(|s\rangle\langle s|\,, \boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(|s\rangle\langle s|_Q)). \tag{60}$$

Using the Fuchs Van de Graaf inequalities (4) and the bound (59) on the trace distance, we obtain

$$\begin{aligned} \Pr[s' = s] &= F(|s\rangle\langle s|\,, \boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(|s\rangle\langle s|_Q)) \\ &\geq (1 - \epsilon/2)^2\,, \end{aligned} \tag{61}$$

so that we obtain a perfectly correct CDQS' protocol as the CDQS protocol becomes perfectly correct, as needed.

Security: We have that $f(x,y) = 0$. From the definition of security in the CDQS protocol, we have that there exists a simulator channel $\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M}$ such that

$$\|\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q - \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}\|_\diamond \leq \delta. \tag{62}$$

Consider taking as input the state $|s\rangle_Q$, as we do in the CDQS' protocol. This gives

$$\|\sigma_M(x,y) - \rho_M(s,x,y)\|_1 \leq \delta, \tag{63}$$

where $\sigma_M(x,y) = \boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q(|s\rangle\langle s|_Q)$. Taking these $\sigma_M(x,y)$ as our simulator distribution, this is exactly δ security of the CDQS' protocol. ■

Theorem 40 *A CDQS' protocol using resource system Ψ implies a CDQS protocol for the same function using resource system $\Psi^{\otimes 2}$.*

Proof. Alice takes the quantum system Q input to the CDQS protocol and applies the one-time pad, using $2\log d_Q$ bits of classical key, which we call s. We use two instances of the CDQS' protocol, each of which hide $\log d_Q$ bits of secret, to hide the $2\log d_Q$ bits of key for the one-time pad. A lemma in [7] shows the correctness and security errors of the CDQS' protocol are at most twice that of the original CDQS' protocol. The encoded system Q is sent to the referee, along with the message systems for the CDQS' protocol. The channel applied by Alice and Bob's combined actions is then

$$\boldsymbol{\mathcal{N}}^{x,y}_{Q\to QM}(\cdot) = \frac{1}{2^{|s|}} \sum_{m,s} P^s_Q(\cdot) P^s_Q \otimes \rho_M(s,x,y), \tag{64}$$

where M is the message system for (both instances of) the CDQS' protocol.

Correctness: We have that $f(x,y) = 1$. Correctness of the CDQS' states that there exists a decoder $\boldsymbol{\mathcal{D}}'^{x,y}_{M\to S}$ such that

$$\forall s \in S,\ \ \Pr\left[\boldsymbol{\mathcal{D}}'^{x,y}_{M\to S}(\rho_M(x,y,s)) = s\right] \geq 1 - 2\epsilon. \tag{65}$$

The 2ϵ rather than ϵ is because we need to use two instances of the CDQS' protocol, as mentioned. We can also frame this condition in terms of the conditional probabilities,

$$p_{s'|s} = \Pr\left[s' = \boldsymbol{\mathcal{D}}'^{x,y}_{M\to S}(\rho_M(x,y,s))\right]. \tag{66}$$

In particular Equation (65) is the statement that $p_{s'=s|s} \geq 1 - 2\epsilon$ for all s. This also means that $\sum_{s'\neq s} p_{s'|s} \leq 2\epsilon$, so that

$$\frac{1}{2^{|s|}} \sum_{s',s} |\delta_{s's} - p_{s'|s}| = \frac{1}{2^{|s|}} \sum_s \left(\sum_{s'=s} |1 - p_{s|s}| + \sum_{s'\neq s} p_{s'|s} \right) \leq \frac{1}{2^{|s|}} \sum_s 4\epsilon = 4\epsilon. \tag{67}$$

To recover the secret, the referee applies $\boldsymbol{\mathcal{D}}'^{x,y}_{M\to S}$ to the message system he receives, producing a variable s', and then applies $P^{s'}_Q$, then finally traces out M. Let the combined action of these steps be denoted by the channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to S}$. This produces

$$\boldsymbol{\mathcal{D}}^{x,y}_{QM\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to QM}(\cdot) = \frac{1}{2^{|s|}} \sum_{s',s} p_{s'|s} P^{s-s'}_Q(\cdot) P^{s-s'}_Q. \tag{68}$$

We need to show this is close to the identity channel, which we do in the following calculation

$$\begin{aligned}
\left\| \frac{1}{2^{|s|}} \sum_{s',s} p_{s'|s} P_Q^{s-s'}(\cdot) P_Q^{s-s'} - \boldsymbol{\mathcal{I}}_Q \right\|_\diamond &= \left\| \frac{1}{2^{|s|}} \sum_{s',s} p_{s'|s} P_Q^{s-s'}(\cdot) P_Q^{s-s'} - \frac{1}{2^{|s|}} \sum_{s',s} \delta_{s's} P_Q^{s-s'}(\cdot) P_Q^{s-s'} \right\|_\diamond \\
&= \sup_d \max_{\Psi_{R_dQ}} \frac{1}{2^{|s|}} \left\| \sum_{s',s} \left(p_{s'|s} P_Q^{s-s'} \Psi_{R_dQ} P_Q^{s-s'} - \delta_{s's} P_Q^{s-s'} \Psi_{R_dQ} P_Q^{s-s'} \right) \right\|_1 \\
&\leq \sup_d \max_{\Psi_{R_dQ}} \frac{1}{2^{|s|}} \sum_{s',s} \left\| \left(p_{s'|s} - \delta_{s's} \right) P_Q^{s-s'} \Psi_{R_dQ} P_Q^{s-s'} \right\|_1 \\
&\leq \left(\frac{1}{2^{|s|}} \sum_{s',s} |p_{s'|s} - \delta_{s's}| \right) \sup_d \max_{\Psi_{R_dQ},s,s'} \left\| P_Q^{s-s'} \Psi_{R_dQ} P_Q^{s'-s} \right\|_1 \\
&= 4\epsilon. \qquad (69)
\end{aligned}$$

We used sub-additivity in the first inequality. The second inequality follows by bringing the $p_{s'|s} - \delta_{s's}$ factor out using absolute homogeneity, and then moving the sup and max through the sum by adding the maximization over s, s'. Finally we use Equation (67) to obtain the last line. This is 4ϵ-correctness of the CDQS protocol.

Security: We have now $f(x, y) = 0$. We choose the simulator channel

$$\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing \to MQ} = \frac{\mathcal{I}_Q}{d_Q} \otimes \sigma_M(x, y), \qquad (70)$$

where $\sigma_M(x, y)$ is the family of channels appearing in the security definition for the CDQS' protocol, which recall states that

$$\forall s \in S, \ \ \|\sigma_M(x, y) - \rho_M(s, x, y)\|_1 \leq \delta. \qquad (71)$$

We need to bound the following diamond norm,

$$\begin{aligned}
&\|\boldsymbol{\mathcal{S}}^{xy}_{\varnothing \to MQ} \circ \mathrm{tr}_Q - \boldsymbol{\mathcal{N}}_{Q \to QM}\|_\diamond \\
&\quad = \sup_n \max_{\Psi_{R_nQ}} \left\| \boldsymbol{\mathcal{S}}^{xy}_{\varnothing \to MQ} \circ \mathrm{tr}_Q(\Psi_{R_nQ}) - \boldsymbol{\mathcal{N}}^{xy}_{Q \to QM}(\Psi_{R_nQ}) \right\|_1 \\
&\quad = \sup_n \max_{\Psi_{R_nQ}} \left\| \Psi_{R_n} \otimes \frac{\mathcal{I}_Q}{d_Q} \otimes \sigma_M(x, y) - \frac{1}{2^{|s|}} \sum_s P_Q^s \Psi_{R_nQ} P_Q^s \otimes \rho_M(s, x, y) \right\|_1 \\
&\quad = \sup_n \max_{\Psi_{R_nQ}} \left\| \frac{1}{2^{|s|}} \sum_s P_Q^s \Psi_{R_nQ} P_Q^s \otimes \sigma_M(x, y) - \frac{1}{2^{|s|}} \sum_s P_Q^s \Psi_{R_nQ} P_Q^s \otimes \rho_M(s, x, y) \right\|_1 \\
&\quad \leq \|\sigma_M(x, y) - \rho_M(s, x, y)\|_1 \sup_n \max_{\Psi_{R_nQ}} \left\| \frac{1}{2^{|s|}} \sum_s P_Q^s \Psi_{R_nQ} P_Q^s \right\|_1 \\
&\quad \leq 2\delta. \qquad (72)
\end{aligned}$$

We used sub-multiplicativity of the one-norm in the first inequality, and the security statement (71) along with normalization of the state Ψ_{R_dQ} in the second inequality. The above is exactly 2δ security of the CDQS protocol.[9] ■

Theorem 41 *Suppose we have a CDQS' protocol which hides a uniformly random classical secret r. Then, at the cost of $|r|$ bits of communication, we can build a protocol that hides a secret s with $|s| = |r|$ with an arbitrary distribution.*

[9]Note 2δ is appearing again rather than δ because we use two instances of the CDQS' protocol.

Proof. Run the CDQS' protocol on secret r, and additionally have Alice send $s' = s \oplus r$.

Correctness: To decode, the referee recovers r' from the CDQS' protocol, which will equal the input r with probability at least $1 - \epsilon$. They then compute $s' \oplus r'$ as output. Since $s' = s \oplus r$, this will be correct whenever $r' = r$, so with probability at least $1 - \epsilon$. Thus the protocol storing s is $1 - \epsilon$ correct.

Security: Security of the CDQS' protocol storing r implies that

$$\forall (x, y) \in X \times Y \;\; s.t.\; f(x, y) = 0, \;\; \forall s \in S, \;\; \|\sigma_M(x, y) - \rho_M(s, x, y)\|_1 \leq \delta. \tag{73}$$

For the CDQS' protocol storing s, we take

$$\tilde{\sigma}_{SM}(x, y) = \pi_{A'} \otimes \sigma_M(x, y) = \frac{1}{2^{|r|}} \sum_r |s \oplus r\rangle\langle s \oplus r| \otimes \sigma_M(x, y), \tag{74}$$

where $\pi_{A'}$ is the maximally mixed state on S. Then by the triangle inequality,

$$\begin{aligned}
\left\| \tilde{\sigma}_{SM}(x, y) - \frac{1}{2^{|r|}} \sum_r |s \oplus r\rangle\langle s \oplus r|_{A'} \otimes \rho_M(r, x, y) \right\|_1 &= \left\| \frac{1}{2^{|r|}} \sum_r |s \oplus r\rangle\langle s \oplus r|_{A'} \otimes \sigma_M(x, y) \right. \\
&\quad \left. - \frac{1}{2^{|r|}} \sum_r |s \oplus r\rangle\langle s \oplus r|_{A'} \otimes \rho_M(r, x, y) \right\|_1 \\
&= \|\sigma_M(x, y) - \rho_M(r, x, y)\|_1 \\
&\leq \delta
\end{aligned}$$

so that the protocol hiding s is also δ secure. ■

B Properties of Cf-PHASE

Theorem 17 *Given a coherent phase protocol for f_1 which uses resource system Ψ_1, and a coherent phase protocol for f_2 using resource system Ψ_2, there is a protocol for $f_1 \oplus f_2$ using resource system $\Psi_1 \otimes \Psi_2$. Furthermore, the construction is an oracle reduction so that an ϵ_1 correct protocol for f_1 and ϵ_2 correct protocol for f_2 leads to a $\epsilon_1 + \epsilon_2$ correct protocol for $f_1 \oplus f_2$.*

Proof. The protocol proceeds by

1. In the first round operations, copying the inputs in the computational basis.
2. Executing the protocol for f_1 on the first copy and the protocol for f_2 on the second
3. Inverting the copying procedure to reset the ancillas in the second round operations.

Following these steps, let us first evaluate the action of the protocol in the case where $\epsilon_1 = \epsilon_2 = 0$ on a basis element $|x\rangle_A |y\rangle_B$,

$$\begin{aligned}
|x\rangle_A |y\rangle_B |0\rangle_{\bar{A}} |0\rangle_{\bar{B}} &\xrightarrow{1)} |x\rangle_A |y\rangle_B |x\rangle_{\bar{A}} |y\rangle_{\bar{B}} \\
&\xrightarrow{2)} ((-1)^{f_1(x,y)} |x\rangle_A |y\rangle_B)((-1)^{f_2(x,y)} |x\rangle_{\bar{A}} |y\rangle_{\bar{B}}) \\
&= (-1)^{f_1(x,y) \oplus f_2(x,y)} |x\rangle_A |y\rangle_B |x\rangle_{\bar{A}} |y\rangle_{\bar{B}} \\
&\xrightarrow{3)} (-1)^{f_1(x,y) \oplus f_2(x,y)} |x\rangle_A |y\rangle_B |0\rangle_{\bar{A}} |0\rangle_{\bar{B}} \; .
\end{aligned} \tag{75}$$

We see that this is an exactly correct protocol for $f_1 \oplus f_2$ whenever the protocols for f_1 and f_2 are exactly correct.

It is clear that the reduction is an oracle reduction, so Remark 8 leads to the additive error property. ■

Next consider Theorem 18, which deals with taking the AND of $f(x, y)$ with a single bit z.

Theorem 18 *Suppose we have a coherent phase protocol for $f(x,y)$ using resource system Ψ. Then, there is a coherent phase protocol for $f(x,y) \wedge z$ using $\Psi \otimes \Psi^+$ where Ψ^+ is the maximally entangled state of two qubits. Furthermore, the protocol is an oracle construction and uses a single implementation of $f(x,y)$ so that if the error in the $f(x,y)$ implementation is ϵ, then the error in implementing $f(x,y) \wedge z$ is also ϵ.*

Proof. Consider the function

$$f(x, y \wedge Z) \equiv f(x_1, ..., x_n, y_1 \wedge z, ..., y_n \wedge z). \tag{76}$$

This can be implemented by having Bob, who holds $|y\rangle$ and $|z\rangle$, compute the AND locally and input $|y \wedge Z\rangle$ into the phase protocol for $f(x,y)$. Then when $z = 1$, this implements the original function $f(x,y)$, while if $z = 0$ this implements $f(x,0)$. This is not quite performing $f(x,y) \wedge z$, but is performing something close: it only differs in $z = 0$ cases, and in that case differs by a function computed only from x (in particular $f(x,0)$ is applied, rather than applying no phase).

To correct this, it suffices to have Alice and Bob implement using Theorem 17 the two functions $f_1(x,y,z) = f(x,0) \wedge (z \oplus 1)$, and $f_2(x,y,z) = f(x, y \wedge Z)$. Then using that

$$f(x,y) \wedge z = [f(x,0) \wedge (z \oplus 1)] \oplus [f(x, y \wedge Z)] \tag{77}$$

this will correctly implement $f(x,y) \wedge z$ as needed. We noted above how to implement $f(x, y \wedge Z)$ using a single instance of the protocol for $f(x,y)$. It remains to see that we can implement $f(x,0) \wedge (z \oplus 1)$ with a single EPR pair Ψ^+.

To do this, Alice locally computes $f(x,0)$ coherently from $|x\rangle$ and stores it in a register A_0. Meanwhile, Bob computes $z \oplus 1$ coherently and stores it in a register B_0. Then, they execute a coherent phase protocol on A_0 and B_0 for the AND function; this amounts to implementing a $CZ_{A_0B_0}$ gate which can be done with one EPR pair by a standard teleportation strategy. Alice and Bob then uncompute $f(x,0)$ and $z \oplus 1$ in their second round operations to reset the A_0 and B_0 registers to 0.

Using Remark 8 and the fact that we use a single invocation of the protocol for $f(x,y)$ (along with an exact protocol for a single AND function) the overall error is the same as the error in the protocol for $f(x,y)$. ■

Next, we will develop the proof of the more general Theorem 20, which replaces z with an arbitrary function. We restate the theorem before giving the proof.

Theorem 20 *Consider functions f and g, and let the rank of g be denoted m. Then there is a $O(m)$ reduction from a coherent phase protocol for $f \wedge g$ to a coherent phase protocol for f. Furthermore, the construction is an oracle reduction and uses m invocations of the protocol for f, so that the error in implementing $f \wedge g$ is $m \cdot \epsilon$ where ϵ is the error in the protocol for f.*

Proof. Write $g(k,\ell)$ in its rank decomposition,

$$\begin{aligned} f(x,y) \wedge g(k,\ell) &= f(x,y) \wedge \bigoplus_{i=1}^{m} h_i(k) \wedge h'_i(\ell) \\ &= \bigoplus_{i=1}^{m} f(x,y) \wedge h_i(k) \wedge h'_i(\ell). \end{aligned} \tag{78}$$

In the second line we distributed the first AND operator over the sum. Next, use that from Theorem 17 we can implement the XOR of a collection of functions by implementing each function in parallel, so it suffices to implement each of the functions $f(x,y) \wedge h_i(k) \wedge h'_i(\ell)$. To do this, we apply Theorem 18 twice: by one invocation of the theorem a protocol for

$f(x,y)$ allows us to implement $f(x,y) \wedge h_i(k)$ by adding one EPR pair to the resource system, and then by a second invocation the resulting protocol for $f(x,y) \wedge h_i(k)$ plus one further EPR pair gives an implementation of $f(x,y) \wedge h_i(k) \wedge h'_i(\ell)$. Thus, if Ψ is the resource system for $f(x,y)$ we can implement $f(x,y) \wedge h_i(k) \wedge h(\ell)$ using $\Psi \otimes (\Psi^+)^{\otimes 2}$. Repeating this for each of the m terms in the above decomposition, we find that $f(x,y) \wedge g(k,\ell)$ can be implemented using the resource system $\Psi^{\otimes m} \otimes (\Psi^+)^{\otimes 2m}$.

Noting that we use the protocol for $f(x,y)$ a total of m times and using Remark 8 we have that the overall error is $\epsilon \cdot m$, where ϵ is the error in the coherent phase protocol for $f(x,y)$. ■

C Properties of Cf-$\mathbf{U}$

We record the proofs of the composition properties given for the coherent unitary NLQC.

Theorem 23 ***Tensor product parallel composition:*** *Suppose we can implement coherently controlled $\mathbf{U}_1$ and $\mathbf{U}_2$, controlled on function f, using resource systems Ψ^1 and Ψ^2 respectively. Then we can apply $\mathbf{U}_1^f \otimes \mathbf{U}_2^f$ coherently using $\Psi^1 \otimes \Psi^2$. Furthermore, the construction isan oracle reduction so that the overall error is the sum of the error for implementing $\mathbf{U}_1$ and $\mathbf{U}_2$.*

Proof. The protocol for the tensor product unitary is

1. Initialize the ancilla systems $\bar{A}$ and $\bar{B}$ on the respective sides in state $|0\rangle$.
2. Apply CNOTs to $A\bar{A}$ and $B\bar{B}$ locally to copy A and B in the computational basis.
3. Implement coherent $\mathbf{U}_1$ on $A'AB$ and $\mathbf{U}_2$ on $B'\bar{A}\bar{B}$.
4. Locally uncompute $\bar{A}$ and $\bar{B}$ using again the same CNOTs.

To see that this succeeds explicitly, we can track the state through the steps in the protocol,

$$|\Psi\rangle_{A'B'AB} \otimes |0\rangle_{\bar{A}} |0\rangle_{\bar{B}} = \sum_{abxy} c_{abxy} |a\rangle_{A'} |b\rangle_{B'} |x\rangle_A |y\rangle_B \otimes |0\rangle_{\bar{A}} |0\rangle_{\bar{B}} \tag{79}$$

$$\overset{CNOT_{A\bar{A}} \otimes CNOT_{B\bar{B}}}{\rightarrow} \quad \sum_{abxy} c_{abxy} |a\rangle_{A'} |b\rangle_{B'} |x\rangle_A |y\rangle_B \otimes |x\rangle_{\bar{A}} |y\rangle_{\bar{B}}$$

$$\overset{(\mathbf{U}_1^f)_{A'AB} \otimes (\mathbf{U}_2^f)_{B'\bar{A}\bar{B}}}{\rightarrow} \quad \sum_{abxy} c_{abxy} \mathbf{U}_1^{f(x,y)} |a\rangle_{A'} \mathbf{U}_2^{f(x,y)} |b\rangle_{B'} |x\rangle_A |y\rangle_B \otimes |x\rangle_{\bar{A}} |y\rangle_{\bar{B}}$$

$$\overset{CNOT_{A\bar{A}} \otimes CNOT_{B\bar{B}}}{\rightarrow} \quad \sum_{abxy} c_{abxy} \mathbf{U}_1^{f(x,y)} |a\rangle_{A'} \mathbf{U}_2^{f(x,y)} |b\rangle_{B'} |x\rangle_A |y\rangle_B \otimes |0\rangle_{\bar{A}} |0\rangle_{\bar{B}} . \tag{80}$$

Tracing out the ancillas yields the desired output.

Notice that the construction is an oracle reduction, so has an additive error by Remark 8. ■

Theorem 24 ***Commuting unitaries:*** *Suppose we can implement unitaries $\mathbf{U}^1_{A'}$ and $\mathbf{U}^2_{A'}$ with A' on Alice's side, coherently controlled on function f using resource systems Ψ^1 and Ψ^2 respectively, and that $\mathbf{U}^1_{A'}$ and $\mathbf{U}^2_{A'}$ commute. Then we can apply $\mathbf{U}^1_{A'}\mathbf{U}^2_{A'}$ coherently controlled off of the same function using resource system $\Psi^1 \otimes \Psi^2$. Furthermore, the construction is an oracle reduction so that the overall error is the sum of the errors in the implementations of each of $\mathbf{U}^1_{A'}$ and $\mathbf{U}^2_{A'}$.*

Proof. Since $\mathbf{U}^1_{A'}$ and $\mathbf{U}^2_{A'}$ commute, they must share an eigenbasis, which we label $\{|u_k\rangle\}_k$. Label the eigenvalues of $\mathbf{U}^1_{A'}$ as $\{\mu_i\}_i$ and the eigenvalues of $\mathbf{U}^2_{A'}$ as $\{\nu_i\}_i$. Alice and Bob execute the following protocol.

1. Alice copies system A' in the eigenbasis $|u_k\rangle$, producing systems A'_1 and A'_2.
2. Alice and Bob run a NLQC protocol for $\mathbf{U}^1_{A'_1} \otimes \mathbf{U}^2_{A'_2}$.
3. Alice undoes the copying operation, leaving only output system $A'_1 = A'$.

To see the effect of this protocol, consider an arbitrary basis state $|u_i\rangle_{A'} |x\rangle_A |y\rangle_B$. Then the steps above produce

$$\begin{aligned} |u_i\rangle_{A'} |x\rangle_A |y\rangle_B &\xrightarrow{1} |u_i\rangle_{A'_1} |u_i\rangle_{A'_2} |x\rangle_A |y\rangle_B \\ &\xrightarrow{2} (\mu_i |u_i\rangle_{A'_1})(\nu_i |u_i\rangle_{A'_2}) |x\rangle_A |y\rangle_B \\ &\xrightarrow{3} (\mu_i \nu_i) |u_i\rangle_{A'} |x\rangle_A |y\rangle_B \\ &= \mathbf{U}^1_{A'} \mathbf{U}^2_{A'} |u_i\rangle_{A'} |x\rangle_A |y\rangle_B \ . \end{aligned} \tag{81}$$

Since this holds for a basis, it also holds for an arbitrary input state. Notice that the construction is an oracle reduction, so has an additive error by Remark 8. ■

References

[1] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A—Atomic, Molecular, and Optical Physics*, 84(1):012326, 2011. doi:https://doi.org/10.1103/PhysRevA.84.012326.

[2] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014. doi:https://doi.org/10.1137/130913687.

[3] Alex May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10): 1–39, 2019. doi:https://doi.org/10.1007/JHEP10(2019)233.

[4] Alex May, Geoff Penington, and Jonathan Sorce. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics*, 2020(8):1–34, 2020. doi:https://doi.org/10.1007/JHEP08(2020)132.

[5] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, 2022. doi:https://doi.org/10.22331/q-2022-11-28-864.

[6] Aleksander M Kubicki, Alex May, and David Pérez-Garcia. Constraints on physical computers in holographic spacetimes. *SciPost Physics*, 16(1):024, 2024. doi:doi:10.21468/SciPostPhys.16.1.024.

[7] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024. doi:https://doi.org/10.22331/q-2024-06-27-1387.

[8] Vahid R Asadi, Kohdai Kuroiwa, Debbie Leung, Alex May, Sabrina Pasterski, and Chris Waddell. Conditional disclosure of secrets with quantum resources. *arXiv preprint arXiv:2404.14491*, 2024. doi:https://doi.org/10.22331/q-2025-10-16-1885.

[9] Uma Girish, Alex May, Leo Orshansky, and Chris Waddell. Comparing classical and quantum conditional disclosure of secrets. *Quantum*, 10:2049, April 2026. ISSN 2521-327X. doi:10.22331/q-2026-04-01-2049. URL `https://doi.org/10.22331/q-2026-04-01-2049`.

[10] Prabhanjan Ananth, Vipul Goyal, Jiahui Liu, and Qipeng Liu. Unclonable secret sharing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 129–157. Springer, 2025. doi:https://doi.org/10.1007/978-981-96-0947-5_5.

[11] Harriet Apel, Toby Cubitt, Patrick Hayden, Tamara Kohler, and David Pérez-García. Security of position-based quantum cryptography limits Hamiltonian simulation via holography. *arXiv preprint arXiv:2401.09058*, 2024. doi:https://doi.org/10.1007/JHEP08(2024)152.

[12] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013. doi:https://doi.org/10.1145/2422436.2422455.

[13] Joy Cree and Alex May. Code-routing: a new attack on position verification. *Quantum*, 7:1079, 2023. doi:https://doi.org/10.22331/q-2023-08-09-1079.

[14] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. doi:10.1088/1367-2630/13/9/093036.

[15] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.

[16] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, pages 1–4, 2022. doi:https://doi.org/10.1038/s41567-022-01577-0.

[17] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2019. doi:10.1109/TIT.2019.2950190.

[18] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification. *Quantum*, 9:1604, 2025. doi:https://doi.org/10.22331/q-2025-01-21-1604.

[19] Vahid R. Asadi, Eric Culf, and Alex May. Rank Lower Bounds on Non-Local Quantum Computation. In Raghu Meka, editor, *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-361-4. doi:10.4230/LIPIcs.ITCS.2025.11. URL `https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2025.11`.

[20] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 151–160, 1998. doi:10.1006/jcss.1999.1689.

[21] Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems*, pages 174–183. IEEE, 1997. doi:10.1109/ISTCS.1997.595170.

[22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18 (6):623–626, 2022. doi:https://doi.org/10.1038/s41567-022-01577-0.

[23] Llorenç Escolà-Farràs and Florian Speelman. Quantum position verification in one shot: parallel repetition of the f-BB84 and f-routing protocols. *arXiv preprint arXiv:2503.09544*, 2025. doi:https://doi.org/10.48550/arXiv.2503.09544.

[24] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *Physical Review Letters*, 135(26):260801, 2025. doi:https://doi.org/10.1103/szwj-s7r6.

[25] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Re-*

view A—Atomic, Molecular, and Optical Physics, 83(1):012322, 2011. doi:https://doi.org/10.1103/PhysRevA.83.012322.

[26] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions. *arXiv preprint arXiv:2009.07450*, 2020. doi:https://doi.org/10.48550/arXiv.2009.07450.

[27] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002. doi:http://doi.org/10.1090/gsm/047.

[28] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013. doi:http://doi.org/10.1017/9781316809976.

[29] Joseph M Renes and Jean-Christian Boileau. Conjectured strong complementary information tradeoff. *Physical Review Letters*, 103(2):020402, 2009. doi:https://doi.org/10.1103/PhysRevLett.103.020402.

[30] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010. doi:https://doi.org/10.1038/nphys1734.

[31] Marius Junge, Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of Banach spaces: a new route towards position based cryptography. *Communications in Mathematical Physics*, 394(2):625–678, 2022. doi:https://doi.org/10.1007/s00220-022-04407-9.

[32] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary Complexity and the Uhlmann Transformation Problem. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:17, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-410-9. doi:10.4230/LIPIcs.ITCS.2026.24. URL `https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2026.24`.

[33] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 639–667. Springer, 2023. doi:https://doi.org/10.1007/978-3-031-30545-0_22.

[34] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. Quantum unpredictability. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–32. Springer, 2025. doi:https://doi.org/10.1007/978-981-96-0947-5_1.

[35] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003. doi:https://doi.org/10.1103/PhysRevA.67.060302.

[36] Léo Colisson Palais, Llorenç Escolà-Farràs, and Florian Speelman. A quantum cloning game with applications to quantum position verification. In *20th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2025. doi:https://doi.org/10.4230/LIPIcs.TQC.2025.2.

[37] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II 34*, pages 1–18. Springer, 2014. doi:https://doi.org/10.1007/978-3-662-44381-1_1.