On Basing One-way Permutations on NP-hard Problems under Quantum Reductions

Nai-Hui Chia[1], Sean Hallgren[2], and Fang Song[3]

[1]Department of Computer Science, University of Texas at Austin, Austin, TX, 78712, USA.

[2]Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, 16802, USA.

[3]Department of Computer Science, Portland State University, Portland, OR 97201, USA.

A fundamental pursuit in complexity theory concerns reducing worst-case problems to average-case problems. There exist complexity classes such as PSPACE that admit worst-case to average-case reductions. However, for many other classes such as NP, the evidence so far is typically negative, in the sense that the existence of such reductions would cause collapses of the polynomial hierarchy(PH). Basing cryptographic primitives, e.g., the average-case hardness of inverting one-way permutations, on NP-completeness is a particularly intriguing instance. As there is evidence showing that classical reductions from NP-hard problems to breaking these primitives result in PH collapses, it seems unlikely to base cryptographic primitives on NP-hard problems. Nevertheless, these results do not rule out the possibilities of the existence of quantum reductions. In this work, we initiate a study of the quantum analogues of these questions. Aside from formalizing basic notions of quantum reductions and demonstrating powers of quantum reductions by examples of separations, our main result shows that if NP-complete problems reduce to inverting one-way permutations using certain types of quantum reductions, then coNP $\subseteq$ QIP(2).

1 Introduction

A fundamental question in complexity theory is whether or not worst-case problems have reductions to average-case problems. A special case, random-self-reductions, concerns reducing worst-case problems to average-case problems of the same type. Random-self-reductions exist for complete sets of some classes such as PSPACE, EXP and #P. Such reductions are not known to exist for NP-complete problems. Fortnow and Feigenbaum [11] showed that sets which are complete for any level of the polynomial hierarchy are not (non-adaptively) random-self-reducible unless the polynomial hierarchy collapses, giving negative evidence for this possibility.

More broadly, one can ask when the worst-case instances of one problem can be reduced to random instances of a different problem, including basing cryptographic primitives on NP-complete problems. Namely, can we reduce NP-complete problems to breaking the security of cryptosystems? It has been shown that approximating several worst-case lattice problems reduce to average-case lattice problems [2, 23, 24]. These results ignited the booming of lattice cryptography, and breaking these cryptosystems is as hard as solving some worst-case lattice problems [3, 27, 28]. However, the worst-case lattice problems involved are in NP$\cap$ coNP, which are believed not NP-complete.

The pursuit of basing cryptographic primitives on NP-hardness has largely ended up negative. For instance, if one can reduce NP-complete problems to inverting one-way permutations [10], size-verifiable one-way functions [4, 7], single-server single-round private information retrieval [21], or some weak fully homomorphic encryption scheme [8], then the polynomial hierarchy collapses. In this paper we bring this question in the quantum computing paradigm: can cryptographic primitives be based on NP-complete or QMA-complete problems if we allow *quantum* reductions?

Namely, can we establish the security of cryptographic primitives by showing a *quantum* algorithm for an NP-hard (or QMA-hard) problem, whenever there is an attacker breaking the cryptographic primitive?

Is this hopeful at all? First note that previous negative results in [4, 7, 9, 11] would fail when quantum reductions are allowed. Specifically, the hypothetical worst-case to average-case reduction is used to construct a multi-round interactive protocol (IP(k) with $k \geq 3$) for the complement of an NP-complete language. Then we are able to claim containment of coNP in AM (and hence and collapse of the polynomial hierarchy), because of a nice result in complexity theory that IP(k) = AM [14]. A direct translation of the classical argument in a quantum reduction[1], nonetheless, would result in a *quantum interactive proof* protocol with multiple rounds. We would conclude that coNP $\subseteq$ QIP(k). But this is trivially true, since QIP(k)=PSPACE for any $k \geq 3$.

Concrete examples also exist where quantum reductions have proven more powerful than classical counterparts in cryptography. Regev [26] showed that the unique shortest vector problem reduces to random subset sum problems via a quantum reduction. In addition, GapSVP and SIVP reduce to the learning with errors (LWE) problem via quantum reductions [28]. There are no known classical reductions between these problems under the same parameters. In fact, the only worst-case to average-case reduction for the ring variant of LWE (ring-LWE), which is a major competitor in the NIST standardization effort of post-quantum cryptography, still relies on a quantum reduction [22]. Therefore, these are examples where quantum reductions appear to be more powerful than classical reductions, when reducing from worst-case to average-case problems. Kawachi and Yamakami [18] proved several hard-core predicates using quantum reductions, inspired by earlier work on the quantum Goldreich-Levin theorem [1] and the quantum algorithm for the Legendre symbol [32].

As existing negative results fail in the quantum setting and quantum reductions are shown to be more powerful than classical ones, it seems to be a live possibility that we can base cryptographic primitives on NP-hard or even QMA-hard problems via quantum reductions!

Our results. We give a general investigation of using quantum reductions in basing the basic primitive one-way permutation (function) on NP-hardness. Our contributions are summarized below.

We first generalize two central classical notions, *locally random reduction* due to Feigenbaum and Lance Fortnow [11] and *worst-case to average-case reduction* due to Bogdanov and Trevisan [9], into the quantum setting. Locally random reductions are commonplace in reductions between lattice problems in [2, 23, 24], and Regev's reduction for LWE [28] naturally falls in our quantum analogue of locally random reductions. Bogdanov and Trevision's notion is more general, and our quantum formalization also allows to reason about more powerful quantum reductions. We then give some characterizations of the quantum reductions we define. We show that certain restrictions on the quantum reductions will be too week to be interesting. For instance, if a quantum reduction only issues *entangled* queries reminiscent of Bell states, it will not be able to base one-way permutation on a language beyond BQP. On the other hand, we give a couple of examples in the oracle setting that quantum reductions are provably more powerful than their classical counterparts.

Our main result is showing that the existence of some quantum reductions implies unknown consequences in complexity.

Theorem 1.1. *The existence of locally quantum reductions where the queries are non-adaptive and are according to smooth-computable distributions from an* NP-complete *problem (or* QMA-complete *problem) to the task of inverting one-way permutations implies* coNP *(or* coQMA*)* $\subseteq$ *QIP(2).*

A distribution $\mathcal{D}$ is smooth-computable if its maximum and minimum are only polynomially larger and smaller than the average, and given any x, the probability $\Pr_{x \sim \mathcal{D}}[x]$ can be computed efficiently. In particular, this rules out uniform distributions, which are essential in existing worst-case to average-case reductions [2, 3, 11, 23, 24, 27, 28]. We also take an initial step towards the case of one-way *functions*. We show that given *quantum-sampling oracle* of a one-way function, any locally quantum reduction will result in the same negative consequence that coNP $\subseteq$ QIP(2).

---

[1]In some cases, such translation does not exist due to some properties of quantum information

As indicated before, direct translation of the classical proofs will only give quantum interactive proof systems with more than three messages, which will already coincide with PSPACE. We develop a checking technique to mitigate the difficulty and design a two-message protocol. Interestingly, our protocol illustrates a new way of designing QIP(2) than the few existing ones [15, 20, 29].

Admittedly, the containment coNP $\subseteq$ QIP(2) is not as strong as the classical result that the polynomial hierarchy collapses. So far there is very little known about QIP(2) other than the simple fact that QMA$\subseteq$ QIP(2)$\subseteq$ QIP(3)=PSPACE, and there are only a few problems [15, 20, 29] proven to be in QIP(2) that are not known to be in AM or QMA. It is an open question to pin down where QIP(2) stands precisely in the complexity zoo. As a partial progress, we show in Section 6 an oracle problem which is in coNP$^{\mathcal{O}}$ but not in QIP(2)$^{\mathcal{O}}$.

Overview of the proof of our main result. In order to describe the approach, we give more details about the classical approach. The classical proof strategy is to assume that a language L has a random reduction to another problem L', and then construct an interactive proof for $\overline{L}$ (the complement of L) that induces a collapse. For example, if L is NP-complete and has a random reduction to inverting a one-way permutation, then there is a two round protocol for deciding if $x \in \overline{L}$. The verifier runs the generator G to generate the queries for the one-way permutation and sends them to the prover. The prover then sends back the answers. Because the verifier can evaluate the one-way permutation, the prover's answers can be checked, and then R is run to decide if $x \in L$. Finally, the verifier can give the opposite answer. This results in a two round protocol for $\overline{L}$. Therefore if such a reduction exists, then coNP $\subseteq$ AM, giving a collapse. There are much more complicated constructions when other average-case problems are considered, for example, for reducing worst-case NP-complete problems to distributional NP problems. It is more difficult to find an interactive proof in this case because if the prover answers $y \notin L'$, then the verifier has no way to verify this. Nevertheless, with classical non-adaptive reductions it is possible to construct a protocol for $\overline{L}$ [9].

Carrying over the proof strategy to the quantum setting requires resolving several difficulties. We use the unitaries G and R from the reduction to construct a quantum interactive proof for $\overline{L}$. First the unitary G is used to create superposition queries which are sent to the prover. An honest prover will answer the superposition queries for the average-case language and send the states back. The verifier can then use the unitary R to decide whether to accept or reject. The first difficulty that arises in following this approach is that superposition queries are being used, which makes it harder to verify that the prover is not cheating than it is for classical answers. Another limiting factor also immediately arises in the quantum case that does not exist in the classical case. For classical reductions and protocols, it is fine to create a protocol with many (but still constant) rounds of communication, because there is an equivalent two round protocol. This is done in [9] where upper and lower bound protocols are used to bound the sizes of sets. However, in the quantum case, we are limited to finding quantum interactive proofs with only two rounds to begin with, since QIP(m) = QIP(3) = PSPACE. Finding a quantum protocol that is limited even to three rounds would only allow the conclusion that coNP $\subseteq$ QIP(m) = PSPACE, which does not yield a non-trivial result.

The main technical challenge is to ensure that the prover provides the answers honestly in superposition to the average-case problem. A cheating prover would try to return some other state that makes the unitary R answer in the opposite way than it should. Should the prover return such a state, the verifier must be able to detect this. Our approach is to let the verifier create a superposition of two states: the query state that is needed for the reduction, and a trap state with the property that it can be used to detect that the prover is cheating. We show that there is a trap state so that whenever the prover changes the query part of the superposition, then the trap part of the superposition must also change, and that this can be detected by the verifier.

Future directions. There are several open questions. Do adaptive and/or non-smooth-computable quantum reductions from NP-complete problems to inverting one-way permutations exist? Can we generalize the result for permutations to other functions such as 2-to-1 functions or even preimage-size-verifiable functions? We observe that (Section 5.3) if the oracle in the reductions is capable of quantum sampling all solutions, then the existence of such reductions from NP-hard problems to inverting k-to-1 surjective functions also implies coNP $\subseteq$ QIP(2). Moreover, for cryptographic

primitives which have more structures than one-way functions, it is possible that we can construct QIP(2) protocol easily. Hence, we would like to know if we can also show that basing these cryptographic primitives on NP-hard problems via quantum reduction is unlikely. On the other hand, we are also interested to know if we can find cryptographic primitives whose security are not likely to be based on NP-complete problems under classical reductions, but can be if quantum reductions are allowed. In the last, is it possible to rule out a quantum reduction from NP-complete problems to average-case problems in NP? Since we know very little about QIP(2), can we show that QIP(2) $\neq$ QMA, QIP(2) $\neq$ AM, QIP(2) $\neq$ QIP(3), or coNP$\not\subseteq$ QIP(2)?

2 Preliminaries

For a finite set X, $|X|$ denotes the size of X. We use $x \leftarrow X$ to mean that x is drawn uniformly at random from X. poly($\cdot$) denotes an unspecified polynomial, and negl(n) denotes a negligible function in n. A function $\epsilon(n)$ is *negligible* if for all polynomials $p(n)$, $\epsilon(n) < 1/p(n)$ for large enough n. Classical efficient computation is described by probabilistic polynomial time (PPT) algorithms.

We assume basic familiarity with quantum information formalism. In this paper, *quantum register* represents a collection of qubits that we view as a single unit. We typically use capital letters to denote a register and the Hilbert space associated with it. A quantum channel Φ describes any physically admissible transformation of quantum states, which is mathematically a completely positive, trace-preserving linear map.

We recall the definitions of *quantum interactive proofs* (QIP) and *one-way permutations* (OWP).

Definition 2.1 (QIP(m)). *A promise problem $A = (A_{yes}, A_{no})$ is in the complexity class QIP(m) if there exists a polynomial-time quantum verifier which exchanges at most m quantum messages of length $O(\text{poly}(|x|))$ with a prover and has the properties:*

- *(Completeness) For $x \in A_{yes}$, there exists a prover who can convince the verifier to accept x with probability at least $2/3$.*

- *(Soundness) For $x \in A_{no}$, no prover can convince the verifier with probability greater than $1/3$.*

Without loss of generality, the prover and the verifier can be described as unitaries. It has been shown that QIP(m)=QIP(3)=PSPACE for $m \geq 3$ [17, 19]. It is known that completeness and soundness can be reduced to negligibly small [16]. In this work, we focus on the class QIP(2).

Definition 2.2 (One-way permutation). *$f : \{0,1\}^* \rightarrow \{0,1\}^*$ is a one-way permutation if*

- *for every n, f is a polynomial-time computable permutation over $\{0,1\}^n$ by either quantum or classical algorithms, and*

- *for every quantum polynomial-time algorithm A, $\Pr_{x \leftarrow \{0,1\}^n}(A(f(x)) = x) = \text{negl}(n)$.*

We denote inverting a one-way permutation as Inv-OWP.

2.1 Formal definitions of classical reductions

We review two defintions of worst-case to average-case reductions that are central in the classical literature. We denote $\mathcal{P}'$ an arbitrary decision, promise or search problem. We will only consider the case where $\mathcal{P}'$ corresponds to inverting one-way permutations. We recall the basic notion of a *distributional* problem.

Definition 2.3 (Distributional problem). *Let $\mathcal{P}'$ be a problem and $\mathcal{D}$ a collection of distributions $\{\mathcal{D}_n\}_{n \in \mathbb{N}}$. The distributional problem $(\mathcal{P}', \mathcal{D})$ is: given an instance x chosen randomly according to $\mathcal{D}_n$, compute $\mathcal{P}'(x)$.*

One important notion of worst-to-average reductions is due to Feigenbaum and Fortnow [11], which we decribe here (with minor adaption).

Definition 2.4 (non-adaptive locally random reduction (G, R)). *Let k and ℓ be variables polynomial in the input length n, and r is a random string chosen uniformly from $\{0,1\}^\ell$. A decision problem $\mathcal{P}$ is non-adaptively locally random reducible to a distributional problem $(\mathcal{P}', \mathcal{D})$ with error ϵ if there are polynomial-time algorithms R and G satisfying two conditions:*

1. *For $n \in \mathbb{N}$ and $x \in \{0,1\}^n$, it holds that $\mathcal{P}(x) = R(x, r, \mathcal{P}'(G(1, x, r)), \ldots, \mathcal{P}'(G(k, x, r)))$ for at least $1 - \epsilon$ fraction of all $r \in \{0,1\}^\ell$.*

2. *For $n \in \mathbb{N}$, $\{x_1, x_2\} \in \{0,1\}^n$, $1 \leq i \leq k$, and y a support of $\mathcal{D}$, it holds that $\Pr_r[G(i, x_1, r) = y] = \Pr_r[G(i, x_2, r) = y] = \Pr[y \sim \mathcal{D}_n]$.*

We note that Definition 2.4 is equivalent to the Definition 2.1 in [11] when $\epsilon = 1/4$. One can let each query be generated according to different fixed distributions in the locally random reduction. However, Definition 2.4 which assumes all queries are drawn from the same distribution is still general. This can be made without loss of generality since one can apply a random permutation to the queries before sending them to the oracle and undo the permutation before applying R. This way, the distributions of each query are the same.

If we only consider $\mathcal{D}$ to be the uniform distribution, then this reduction is a special case considered by Feigenbaum et al. in [12]. One can also define *adaptive* locally random reductions by allowing the algorithm G in Definition 2.4 to generate queries depending on the previous queries and answers.

If $\mathcal{P} = \mathcal{P}'$, then the reduction is also called a random-self reduction [11]. It has been shown that the set of complete problems in PSPACE, EXP and #P are random-self reducible [11]. On the other hand, it has been shown that NP-complete problems are not non-adaptive random-self reducible unless the polynomial hierarchy collapses to the third level [11].

Note that the definition of Feigenbaum and Fortnow [11] assumes a perfect solver for the average-case problem. This restriction is weakened in a later work by Bogdanov and Trevisan [9], which gives another important notion of worst-to-average reductions below. To describe it, we first define δ-close problems.

Definition 2.5. *A problem $\mathcal{P}''$ is δ-close to another problem $\mathcal{P}'$ with respect to $\mathcal{D}$ if for all n, $\Pr_{x \sim \mathcal{D}_n}(\mathcal{P}''(x) \neq \mathcal{P}'(x)) < \delta$.*

Definition 2.6 (non-adaptive worst-case to average-case reduction). *Let k and ℓ be variables polynomial in the input length n, and r is a random string chosen uniformly from $\{0,1\}^\ell$. A decision problem $\mathcal{P}$ is non-adaptive worst-case to average-case reducible to $(\mathcal{P}', \mathcal{D})$ with average hardness δ and error ϵ if there are polynomial-time algorithms R and G satisfying that:*

for any $n \in \mathbb{N}$, and on all inputs $x \in \{0,1\}^n$, let $y_1, \ldots, y_k$ be the outputs of $G(x, r)$. For any $\mathcal{P}''$ which is δ-close to $\mathcal{P}'$ with respect to $\mathcal{D}$,

$$\Pr_r[R(x, r, \mathcal{P}''(y_1), \ldots, \mathcal{P}''(y_k)) = \mathcal{P}(x)] > 1 - \epsilon.$$

Similarly, an adaptive worst-case to average-case reduction is defined by including previous queries and answers to the arguments of G.

It has been shown that NP-complete problems are not non-adaptive worst-case to average-case reducible to themselves, unless the polynomial hierarchy collapses to the third level [9]. In addition, the existence of a non-adaptive worst-case to average-case reduction from NP-hard problem to inverting a one-way function implies that the polynomial hierarchy collapses to the second level [4] and the existence of a worst-case to average-case reduction from an NP-hard problem to inverting a size verifiable one-way function implies that the polynomial hierarchy collapses to the second level [4, 7].

3 Formalizing quantum reductions

In this section we define the quantum analogues of the two classical notions of worst-to-average reductions (Definition 2.4 and 2.6). We then describe some characterizations and examples that illustrates diverse features of quantum reductions.

Definition 3.1 (non-adaptive locally quantum reduction (G, R)). *A decision problem $\mathcal{P}$ is non-adaptive locally quantum reducible to a distributional problem $(\mathcal{P}', \mathcal{D})$ with error ϵ by using k queries if there are two polynomial-time implementable unitaries R and G such that for all n and $x \in \{0,1\}^n$*

- *The generator G creates k superposition queries, with query amplitudes based on the distribution $\mathcal{D}$: $G|0\rangle_{MV}|x\rangle = |Q_{x,1}\rangle \otimes \cdots \otimes |Q_{x,k}\rangle|x\rangle$ where $|Q_{x,i}\rangle = \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, 0\rangle_M |w_{x,i}(q)\rangle_V$ for $i \in [k]$. Note that d_q is the probability that q is drawn from $\mathcal{D}_n$ and the register V for the state $|w_{x,i}\rangle$ is the work register, which could be in arbitrary state.*

- *R takes responses of the queries $|Q_{x,1}^H, \ldots, Q_{x,k}^H\rangle$ and decides whether or not $\mathcal{P}(x)$ is true:*

$$R|Q_{x,1}^H, \ldots, Q_{x,k}^H\rangle = \sqrt{p}|\mathcal{P}(x)\rangle|\psi_x^0\rangle + \sqrt{1-p}|1 - \mathcal{P}(x)\rangle|\psi_x^1\rangle$$

where $p \geq 1 - \epsilon$ and $|Q_{x,i}^H\rangle = \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, \mathcal{P}'(q)\rangle_M |w_{x,i}(q)\rangle_V$, for $i \in [k]$.

Definition 3.2 (non-adaptive quantum worst-case to average-case reduction). *A decision problem $\mathcal{P}$ is non-adaptive quantum worst-case to average-case reducible to $(\mathcal{P}', \mathcal{D})$ with average hardness δ and error ϵ if there are polynomial-time computable unitaries R and G such that for any $n \in \mathbb{N}$ and x*

- *The generator G creates k superposition queries:*

$$G|0\rangle_{MV}|x\rangle = |Q_{x,1}\rangle \otimes \cdots \otimes |Q_{x,k}\rangle|x\rangle, \tag{1}$$

where $|Q_{x,i}\rangle = \sum_{q \in \mathbb{Z}_2^m} c_{x,q,i}|q, 0\rangle_M |w_{x,i}(q)\rangle_V$, for $i \in [k]$. Note that the coefficients $c_{x,q,i}$ for $q \in \mathbb{Z}_2^m$ could be any complex numbers such that the sum of absolute squares is 1.

- *R: for any $\mathcal{P}''$ which is δ-close to $\mathcal{P}$ with respect to $\mathcal{D}$,*

$$R|Q_{x,1}^H, \ldots, Q_{x,k}^H\rangle = \sqrt{p}|\mathcal{P}(x)\rangle|\psi_x^0\rangle + \sqrt{1-p}|1 - \mathcal{P}(x)\rangle|\psi_x^1\rangle, \tag{2}$$

where $p \geq 1 - \epsilon$ and $|Q_{x,i}^H\rangle = \sum_{q \in \mathbb{Z}_2^m} c_{x,q,i}|q, \mathcal{P}''(q)\rangle_M |w_{x,i}(q)\rangle_V$, for $i \in [k]$.

The variables m and k are polynomial in the input length n.

Compared to locally quantum reductions, quantum worst-case to average-case reductions do not require the queries to be drawn from a certain distribution. Instead, we consider an oracle for $\mathcal{P}'$ that can err sometimes, which is captured by δ-close problems $\mathcal{P}''$. $1 - p$ is called the error of the reduction. The choice of $p = 2/3$ is arbitrary, since it can be reduced effectively.

3.1 Separation examples

We give two examples demonstrating the distinct landscapes of classical and quantum worst-case to average-case reductions. Namely, relative to an oracle and under reasonable computational assumptions, there exist a worst-case problem and an average-case problem such that no classical reductions exist whereas they admit an efficient quantum reduction. In fact, the quantum reduction issues non-adaptive *classical* queries only. This makes the separation examples strong.

The idea behind the examples is simple. We design the average-case problem in such a way that to make a meaningful query to a solver for this average-case problem, one has to solve a problem that is (assumed to be) hard for classical algorithms but easy on a quantum computer. Our first example is based on a oracle problem provably hard classically (Simon's Problem), and the quantum reduction needs quantum access to the oracle. The second example needs to assume the existence of problem in BQP that is outside BPP (e.g., factorization). However we remove the need of quantum access to the oracle as a reward. Both constructions rely on the following assumption.

Assumption 1. *There exists language $L \notin$ BQP (hence $L \notin$ BPP too) that admits a random self-reduction $L \leq_{(R,G)} (L, D)$ for some distribution D.*

Accepted in 〈Quantum 2020-08-02, click title to verify. Published under CC-BY 4.0.

6

A candidate is the PSPACE-complete problem True Quantified Boolean Formula (TQBF), which is known to have a *non-adaptive* random self-reduction [11]. Assumption 1 will follow, if BQP $\subsetneq$ PSPACE. Hereafter we treat G as non-adaptive in Assumption 1 for simplicity.

Let $N = 2^n$, and for each $i \in [N]$, let $f_i : \{0,1\}^n \to \{0,1\}^n$ be some function, and $s_i \in \{0,1\}^n$. We define an oracle $O := O_{s_0,\dots,s_{N-1}}$ that generalizes Simon's oracle [31].

$$O : |i, x, y, z\rangle \to |i, x, y \oplus f_i(x), z\rangle ; \quad \text{where } f_i(x) = f_i(x') \text{ iff. } x' = x \oplus s_i .$$

We assume that all $s_i, i \in [N]$ are chose uniformly at random. As an immediate corollary of Simon's result. We have that

Lemma 3.3. *Given O, any classical algorithms needs $\Omega(2^{n/2})$ queries to O to find s_i for some $i \in [N]$. For any $i \in [N]$, there is a quantum algorithm that can find s_i with $O(n^2)$ queries and time.*

Construction 1. We construct our first separation example.

- $L_1 = \text{TQBF} = \{\phi = \phi(v_1, \dots, v_n)\}$ containing satisfiable quantified n-variable formulae in 3-CNF. Let L_1^O be the language L_1 relative to oracle O, which simply ignores O.

- $\hat{L}_1^O := \{x = (i, s, \phi) : s = s_i \text{ and } \phi \text{ is true}\}$. We associate $\hat{L}_1^O$ a distribution $\hat{D}_1$, which is uniform on $N \times \{0,1\}^n$ and samples a formula according to D (the distribution in Assumption 1).

Theorem 3.4. *Under Assumption 1, there does not exist a PPT reduction from L_1^O to $(\hat{L}_1^O, \hat{D}_1)$. In contrast, there is a quantum poly-time non-adaptive reduction $L_1^O \leq_{R_1^Q, G_1^Q} (\hat{L}_1^O, \hat{D}_1)$.*

Proof. Let A be an algorithm that solves the average-case problem $(\hat{L}_1^O, \hat{D}_1)$. For simplicity, we assume that A is a perfect decider, i.e., for a random input $x = (i, s, \phi) \leftarrow \hat{D}_1$, $A(i, s, \phi) = 1$ iff. $s = s_i$ and $\phi = 1$. Any classical reduction is unable to find s_i in polynomial time, hence the solver A is useless. Formally speaking, if there were such a reduction $L_1^O \leq (\hat{L}_1^O, \hat{D}_1)$, one can turn it into an efficient solver for Simon's problem or an efficient decider for L. This violates Lemma 3.3 or Assumption 1.

For the second part, we construct a quantum reduction (R_1^Q, G_1^Q) as follows. Recall that there is a random self-reduction $L \leq_{(R,G)} (L, D)$. Given a worst-case input ϕ, $G_1^Q(\phi)$ runs $G(\phi)$ to get random $\{\phi_j\}_{j=1}^k$. Then for $j = 1, \dots k$, G_1^Q generates random $i_j \leftarrow [N]$, and runs Simon's algorithm to find s_{i_j} efficiently. Then the queries to A are $\{i_j, s_{i_j}, \phi_j\}_{j=1}^k$, which are correctly distributed according to $\hat{D}_1$. Therefore A will respond correctly with $\{\phi_j \overset{?}{=} 1\}$. Then R_1^Q runs the decision procedure R, which correctly decides ϕ. $\qed$

Remark 1. *We have designed O to encode exponentially many instances of Simon's problem for the technicality of non-uniform reductions. Because otherwise, a classical reduction could hardwire the solution s and make use of an average-case solver.*

Construction 2. We give another separation example. It is still in the oracle setting, and we need to make an additional assumption. What we gain is that the quantum reduction does not need quantum access to the oracle, as opposed to Example 1 where we need to run Simon's algorithm with quantum access to the oracle.

Assumption 2. *There exists a classically secure one-way function $f : X \to Y$, which is invertible by an efficient quantum algorithm.*

A natural candidate would be adaption of FACTORIZATION. Let $(p, q) \leftarrow \mathsf{Gen}(1^n)$ be an efficient algorithm that generates two large primes at random, and define $f(p, q) = pq$. Then it is reasonable to assume that there exists a Gen algorithm relative to which f is hard to invert. In fact this is necessary for the RSA assumption, which is the basis of modern public-key cryptography. This assumption is hence likely to be true given the current state of art.

Given a function f as in Assumption 2, we define an oracle $H : i \mapsto y_i$ for $i \in [N]$. Here we sample $z_i \leftarrow X$ randomly and set $y_i := f(z_i)$.

- $L_2 = \mathrm{TQBF} = \{\phi = \phi(v_1, \ldots, v_n)\}$ containing satisfiable quantified n-variable formulae in 3-CNF. Let L_2^O be the language L relative to oracle H, which ignores H.

- $\hat{L}_2^H := \{x = (i, z, \phi) : f(z) = y_i$ and ϕ is true$\}$. We associate $\hat{L}_2^H$ a distribution $\hat{D}_2$, which is uniform on $[N] \times X$ and samples a formula according to D (the distribution in Assumption 1).

Remark 2. *For the same reason as above, we introduce the oracle H to encode superpolynomial-many instances of inverting f to avoid a non-uniform classical reduction that can hardwire solutions to (at most poly-many) inversion instances.*

Following similar arguments to Theorem 3.4, we can prove the theorem below. The only change is that in the quantum reduction, we query *classically* a random index i_j to H, and obtain y_{i_j}. Then we run Shor's algorithm to find $z_{i_j} := f^{-1}(y_{i_j})$, and then form correct queries to the solver of $(\hat{L}_2^H, \hat{D}_2)$.

Theorem 3.5. *Under Assumption 1 and 2, there does not exist a classical reduction from L_2^H to $(\hat{L}_2^H, \hat{D}_2)$. In contrast, there is a quantum poly-time non-adaptive reduction $L_2^H \leq_{R_2^Q, G_2^Q} (\hat{L}_2^H, \hat{D}_2)$.*

3.2 Discussion of the definitions: special cases

3.2.1 Classical queries.

If G outputs classical queries, then we can immediately derive a negative result, analogous to a classical result by Brassard [10]. In the following, $L <_{R,G} \mathcal{P}'$ denotes a non-adaptive quantum reduction from L to $\mathcal{P}'$, where G generates oracle queries and R decides L according to the oracle's responses. We will add more constraints to the reductions accordingly in this section.

Theorem 3.6. *If there is a non-adaptive quantum reduction $L \leq_{R,G}$ Inv-OWP where G only issues classical queries, then $L \in$ QIP(2) with classical interactions.*

Proof. The protocol is as follows: The verifier first applies G to generate queries and sends these queries to the prover. Then, the prover simulates the oracle for Inv-OWP and sends the responses back. Finally, the verifier checks if the responses are correct by computing the permutation. If the prover is not cheating, the verifier applies R and accepts if the reduction accepts. Otherwise, the verifier rejects. Note that the prover can only give the correct answer for Inv-OWP. Otherwise, the verifier rejects. $\qquad\square$

3.2.2 EPR queries.

As another special case, we consider that $w_{x,i}(q)$ is the identity function in Definition 3.1. Namely G generates k identical copies of $|\Psi\rangle^{\otimes m} = \sum_q |q\rangle|q\rangle$, where $\Psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an EPR-pair. Then half of the EPR-pairs are submitted as queries to the solver of the average-case problem. Note the reduced density of each query is totally mixed, and this looks a natural generalization of classical uniform queries. Nonetheless, we show that this is too strong a constraint that trivializes the study of worst-to-average reductions, as far as OWP is concerned.

Proposition 3.7. *If there is a reduction $L \leq_{R,G}$ Inv-OWP where G issues EPR-queries, then $L \in$ BQP.*

Proof. Observe that a uniform superposition over a set is *invariant* under an arbitrary permutation. This means that a quantum reduction could create the correct state that otherwise would require invoking an inverting oracle I of the OWP f. Namely applying I on an EPR query gives us

$$\sum_q |q, q\rangle \overset{I}{\mapsto} \sum_q |q, q, f^{-1}(q)\rangle .$$

This can be created without help of I as follows:

$$|0,0,0\rangle \mapsto \sum_q |q,0,0\rangle \overset{f}{\mapsto} \sum_q |q,f(q),f(q)\rangle = \sum_{q'} |f^{-1}(q'),q',q'\rangle$$

$$\overset{\text{SWAP}_{1,3}}{\mapsto} \sum_{q'} |q',q',f^{-1}(q')\rangle.$$

□

Remark 3. *Consequently, it is* necessary *that the query states maintain more sophisticated correlations between the query register and the work register of the reduction. We note the same phenomenon also occur classically. Namely, although the marginal distribution of each query is uniformly* random, *it is important that the internal state of the reduction should not be independent of the queries. Otherwise, existence of such a reduction will trivialize the language under consideration to fall in BPP.*

4 On uniform locally quantum reductions

We prove our main result in this section. We first consider quantum reductions that make *one-query* only. It demonstrates the main idea of our general result with a cleaner analysis. Section 4.2 will handle multiple non-adaptive queries.

4.1 Uniform one-query locally quantum reductions

Let f be a one-way permutation on $\{0,1\}^n$, and let $U_f : |x,y\rangle \mapsto |x,y \oplus f(x)\rangle$ be a unitary quantum circuit computing it. Note that $U_f|f^{-1}(x),0\rangle = |f^{-1}(x),x\rangle$. A uniform one-query locally quantum reduction for L works as follows:

$$|x,0\rangle|0\rangle \quad \overset{G}{\longrightarrow} \quad \frac{1}{\sqrt{2^m}} \sum_{q \in \mathbb{Z}_2^m} |q,0\rangle|w_x(q)\rangle \tag{3}$$

$$\overset{O_{f^{-1}}}{\longrightarrow} \quad \frac{1}{\sqrt{2^m}} \sum_{q \in \mathbb{Z}_2^m} |q,f^{-1}(q)\rangle|w_x(q)\rangle \overset{R}{\longrightarrow} a_0|0\rangle|\psi_{x,0}\rangle + a_1|1\rangle|\psi_{x,1}\rangle, \tag{4}$$

where $|a_1|^2 \geq 1 - \epsilon$ if $x \in L$ and $|a_1|^2 \leq \epsilon$ if $x \notin L$ is the accepting probability of the reduction.

Theorem 4.1. *Suppose there exists a one-query uniform locally quantum reduction with exponentially small error ϵ from a worst-case decision problem L to the task of inverting a polynomial-time computable permutation. Then there exists a $QIP(2)$ protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\overline{L}$*

4.1.1 The protocol for $\overline{L}$.

We are given the uniform one-query locally quantum reduction (G, R). We enlarge the size of register V and define a unitary C which performs a CNOT on the first register of M into the second register of V: $|q,x\rangle_M|y,z\rangle_V \overset{C}{\longrightarrow} |q,x\rangle_M|y,z \oplus q\rangle_V$. The whole protocol takes place in the space $\mathcal{H}_P \otimes \mathcal{H}_M \otimes \mathcal{H}_V \otimes \mathcal{H}_\Pi$ where P is the private register of the prover, M is the register exchanged between the prover and the verifier, V and Π are registers which are private to the verifier.

We describe some states that are crucial in the protocol.

- The verifier prepares the state $|S\rangle_{MV\Pi} = \frac{1}{\sqrt{2}}(|Q\rangle_{MV}|0\rangle_\Pi + |T\rangle_{MV}|1\rangle_\Pi)$, where

$$|Q\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q,0\rangle_M|w_x(q),q\rangle_V \tag{5}$$

without the extra copy of q in the register V is the query state generated from G as in Equation 3, and

$$|T\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, 0\rangle_M |0, q\rangle_V \tag{6}$$

is the trap state, which will be used to catch a cheating prover.

- The honest prover replies $|S^H\rangle_{MV\Pi} = \frac{1}{\sqrt{2}}(|Q^H\rangle_{MV}|0\rangle_\Pi + |T^H\rangle_{MV}|1\rangle_\Pi)$, where

$$|Q^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |w_x(q), q\rangle_V \tag{7}$$

$$|T^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |0, q\rangle_V. \tag{8}$$

The state $|Q^H\rangle$ without the extra copy of q in register V is the state the actual reduction R gets after querying the oracle as in Equation 4. The state $|T^H\rangle$ can be mapped to $|0\rangle_{MV}$ efficiently as shown below. This gives the verifier an efficient way to check if $|T^H\rangle$ is changed significantly.

We do the following to map $|T^H\rangle_{MV}$ back to $|0\rangle_{MV}$ efficiently

$$\sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |0, q\rangle_V \xrightarrow{C} \sum_q |q, f^{-1}(q)\rangle_M |0, q \oplus q\rangle_V$$

$$\xrightarrow{U_f} \sum_q |q \oplus f(f^{-1}(q)), f^{-1}(q)\rangle_M |0, 0\rangle_V \xrightarrow{F} |0, 0\rangle_M |0, 0\rangle_V.$$

Here U_f is applied from the second register of M into the first, and f is applied to the second register of M. The last two steps use the property that f can be evaluated efficiently and f is a permutation.

Given the reduction (G, R), we can get a $\mathsf{QIP}(2)$ protocol for L by answering the same as R and a protocol for $\overline{L}$ by flipping R's answer. The $\mathsf{QIP}(2)$ protocol for $\overline{L}$ is described in Protocol 1.

4.1.2 Proof of Theorem 4.1.

We first prove a few useful lemmas. Lemma 4.2 is an immediate consequence of the fact two purifications of the same state are related by an isometry. In fact, this exactly explains why the entanglement fidelity is well defined [30].

Lemma 4.2. *Let ρ_A be a state in some Hilbert space. Let $|\phi\rangle_{AB}$ and $|\psi\rangle_{AB}$ be two purifications of ρ_A, i.e., $\mathrm{Tr}_B(|\phi\rangle\langle\phi|_{AB}) = \mathrm{Tr}_B(|\psi\rangle\langle\psi|_{AB}) = \rho_A$. Let $\Psi_A : \mathcal{H}_A \to \mathcal{H}_A$ be a quantum channel. Let $\rho_{AB} := (\Psi_A \otimes I_B)(|\phi\rangle\langle\phi|_{AB})$ and $\sigma_{AB} := (\Psi_A \otimes I_B)(|\psi\rangle\langle\psi|_{AB})$, where the notation $\Psi_A \otimes I_B$ means that the channel is only applied on the space $\mathcal{H}_A$ and space $\mathcal{H}_B$ is not changed. Then $\langle\phi|\rho_{AB}|\phi\rangle = \langle\psi|\sigma_{AB}|\psi\rangle$.*

Proof. Observe that (e.g., by Schmidt decomposition) there is a unitary U_B operating only on B such that $I_A \otimes U_B|\psi\rangle_{AB} = |\phi\rangle_{AB}$. Then

$$\langle\phi|\rho_{AB}|\phi\rangle = \langle\phi|(\Psi_A \otimes I_B)((|\phi\rangle\langle\phi|)_{AB})|\phi\rangle$$

$$= \langle\psi|(I_A \otimes U_B^\dagger)(\Psi_A \otimes I_B)(I_A \otimes U_B(|\psi\rangle\langle\psi|)_{AB} I_A \otimes U_B^\dagger)(I_A \otimes U_B)|\psi\rangle$$

$$= \sum_\ell \langle\psi|(I_A \otimes U_B^\dagger)(E_A^\ell \otimes I_B)(I_A \otimes U_B(|\psi\rangle\langle\psi|)_{AB} I_A \otimes U_B^\dagger)$$

$$(E_A^{\ell\dagger} \otimes I_B)(I_A \otimes U_B)|\psi\rangle \tag{9}$$

$$= \sum_\ell \langle\psi|(E_A^\ell \otimes I_B)((|\psi\rangle\langle\psi|)_{AB})(E_A^{\ell\dagger} \otimes I_B)|\psi\rangle \tag{10}$$

$$= \langle\psi|(\Psi_A \otimes I_B)((|\psi\rangle\langle\psi|)_{AB})|\psi\rangle = \langle\psi|\sigma_{AB}|\psi\rangle.$$

Protocol 1 QIP(2) protocol for $\overline{L}$ using a one-query locally quantum reduction.

The protocol takes place in the space $\mathcal{H}_P \otimes \mathcal{H}_M \otimes \mathcal{H}_V \otimes \mathcal{H}_\Pi$ where P is the private register of the prover, M is the register exchanged between the prover and the verifier, and V and Π are registers which are private to the verifier.

1. *The verifier's query.* The verifier prepares $|S\rangle_{MV\Pi} := \frac{1}{\sqrt{2}}(|Q\rangle_{MV}|0\rangle_\Pi + |T\rangle_{MV}|1\rangle_\Pi)$.

   The message register M is sent to the prover, and the verifier keeps V and Π. This is generated by conditioning on the register Π, which is initialized in $|+\rangle$. If $\Pi = 0$, G is applied and then q is copied to the second part of the verifier's internal register V, which produces $|Q\rangle_{MV}$. If $\Pi = 1$, compute the Fourier transform followed by CNOT to create $|T\rangle_{MV}$, a trap state we use to catch a cheating prover.

2. *The prover's response.* The prover applies some unitary U_{PM} on register M and its private register P and sends the message register back to the verifier.

3. *The verifier's verification.* The verifier applies C to erase q in V. The verifier then measures Π to obtain $b \in \{0, 1\}$, and does the following:

   - (Computation verification) If $b = 0$, apply R on MV and measure the output qubit. Accept if the outcome is 0.
   - (Trap verification) If $b = 1$, apply V_T on MV and measure MV. Accept if the outcome is all 0, (i.e., if the reduction rejects).

The operators $\{E_A^\ell\}$ in Equation 9 are the operation elements of the channel Ψ_A, where $(\Psi_A \otimes I_B)((|\phi\rangle\langle\phi|)_{AB}) = \sum_\ell (E_A^\ell \otimes I_B)((|\phi\rangle\langle\phi|)_{AB})(E_A^{\ell\dagger} \otimes I_B)$ and $(\Psi_A \otimes I_B)((|\psi\rangle\langle\psi|)_{AB}) = \sum_\ell (E_A^\ell \otimes I_B)((|\psi\rangle\langle\psi|)_{AB})(E_A^{\ell\dagger} \otimes I_B)$. Equation 10 is correct due to the property that $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$. □

Without loss of generality, we can always represent the prover's operator U_{PM} as $U'_{PM}O_{f^{-1}}$ where U'_{PM} is an arbitrary unitary the cheating prover may apply. Let

$$\sigma_Q^{U'} = \mathrm{Tr}_P(U'_{PM} \otimes I_V(|0\rangle\langle0| \otimes |Q^H\rangle\langle Q^H|)U'^\dagger_{PM} \otimes I_V), \text{ and}$$
$$\sigma_T^{U'} = \mathrm{Tr}_P(U'_{PM} \otimes I_V(|0\rangle\langle0| \otimes |T^H\rangle\langle T^H|)U'^\dagger_{PM} \otimes I_V).$$

The following claim shows that for any unitaries the prover applies, the change on $|T^H\rangle$ is as much as the change on $|Q^H\rangle$.

Lemma 4.3. *For an arbitrary U'_{PM}, let $|Q^H\rangle_{MV}$ and $|T^H\rangle_{MV}$ be as defined in Equation 7 and Equation 8, and let $\sigma_Q^{U'}$ and $\sigma_T^{U'}$ be as above. Then $\langle Q^H|\sigma_Q^{U'}|Q^H\rangle = \langle T^H|\sigma_T^{U'}|T^H\rangle$.*

Proof. We represent the prover's behavior U'_{PM} on the state $|Q^H\rangle$ and $|T^H\rangle$ as a noisy channel $\Psi_M^{U'}$ operating on register M, which is formally defined as follows:

For all $\rho \in \mathcal{H}_P \otimes \mathcal{H}_M \otimes \mathcal{H}_V$, $(\Psi_M^{U'} \otimes I_V)(\rho) := \mathrm{Tr}_P((U'_{PM} \otimes I_V)\rho(U'^\dagger_{PM} \otimes I_V))$.

Therefore,

$$(\Psi_M^{U'} \otimes I_V)(|Q^H\rangle\langle Q^H|) = \sigma_Q^{U'} \qquad\qquad (\Psi_M^{U'} \otimes I_V)(|T^H\rangle\langle T^H|) = \sigma_T^{U'}.$$

$|T^H\rangle$ and $|Q^H\rangle$ are actually two purifications of a mixed state on register M since $\mathrm{Tr}_V(|Q^H\rangle\langle Q^H|) = \mathrm{Tr}_V(|T^H\rangle\langle T^H|)$, and by Lemma 4.2, we can conclude that

$$\langle Q^H|\sigma_Q^{U'}|Q^H\rangle = \langle T^H|\sigma_T^{U'}|T^H\rangle.$$

□

Given a state $|\phi\rangle$ and a projector Π_S, Lemma 4.4 shows that the state ρ which maximizes the quantity $\text{Tr}(\Pi_S\rho) + \langle\phi|\rho|\phi\rangle$ is the bisector of $|\phi\rangle$ and its projection on Π_S.

Lemma 4.4. *Let $S \subseteq \mathcal{H}$ be a subspace and Π_S be the projection operator on S. Let $|\phi\rangle$ be a state such that $\langle\phi|\Pi_S|\phi\rangle = \sin^2\theta$, for some $\theta \in [0, \pi/2]$. Then for any density operator $\rho \in D(\mathcal{H})$, $\text{Tr}(\Pi_S\rho) + \langle\phi|\rho|\phi\rangle \leq 1 + \sin\theta$.*

Proof. We first prove this lemma for any pure state $\rho = |\psi\rangle\langle\psi|$. Let $\dim(S) = k$. Let $|v_0\rangle := \frac{\Pi_S|\phi\rangle}{\|\Pi_S|\phi\rangle\|}$ and $|v_k\rangle := \frac{|\phi\rangle - |v_0\rangle}{\||\phi\rangle - |v_0\rangle\|}$. Clearly, $|v_k\rangle \perp |v_0\rangle$, and $|\phi\rangle = \sin\theta|v_0\rangle + \cos\theta|v_k\rangle$. Then we pick $\{|v_1\rangle, \ldots, |v_{k-1}\rangle\}$ in S such that $\{|v_0\rangle, \ldots, |v_{k-1}\rangle\}$ form an orthonormal basis for S. As a result, $\{|v_0\rangle, \ldots, |v_k\rangle\}$ will be an orthonormal basis for $\tilde{S} := \text{span}(S \cup |\phi\rangle)$. Consider any $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \tilde{S}$. Then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=0}^{k} \alpha_i|v_i\rangle, \quad \sum_i |\alpha_i|^2 = 1. \tag{11}$$

We have that

$$\begin{aligned}
\langle\phi|(|\psi\rangle\langle\psi|)|\phi\rangle &= |\alpha_0\sin\theta + \alpha_k\cos\theta|^2 = |\alpha_0|^2\sin^2\theta + |\alpha_k|^2\cos^2\theta \\
&\quad + \sin\theta\cos\theta(\alpha_0\alpha_k^* + \alpha_0^*\alpha_k); \\
\text{Tr}(\Pi_S|\psi\rangle\langle\psi|) &= \sum_{i=0}^{k-1}|\alpha_i|^2 = 1 - |\alpha_k|^2.
\end{aligned}$$

Therefore

$$\begin{aligned}
&\text{Tr}(\Pi_S|\psi\rangle\langle\psi|) + \langle\phi|(|\psi\rangle\langle\psi|)|\phi\rangle \tag{12} \\
=\; & 1 + \sin^2\theta|\alpha_0|^2 + (\cos^2\theta - 1)|\alpha_k|^2 + \sin\theta\cos\theta(\alpha_0\alpha_k^* + \alpha_0^*\alpha_k) \\
=\; & 1 + \sin\theta\cdot\left(\sin\theta(|\alpha_0|^2 - |\alpha_k|^2) + \cos\theta(\alpha_0\alpha_k^* + \alpha_0^*\alpha_k)\right) \\
\leq\; & 1 + \sin\theta\cdot(\sin\theta(|\alpha_0|^2 - |\alpha_k|^2) + 2\cos\theta(|\alpha_0||\alpha_k|)). \tag{13}
\end{aligned}$$

Since the expression in Equation 13 is strictly increasing with $|\alpha_0|$ and independent to $|\alpha_1|, \ldots |\alpha_{k-1}|$, we can suppose the optimal $|\psi\rangle$ for Equation 12 is on the subspace spanned by $|v_0\rangle$ and $|v_k\rangle$ without loss of generality. Thus we let $|\alpha_0| = \cos\theta_0$ and $|\alpha_k| = \sin\theta_0$ and the upper bound for Equation 13 as below

$$\begin{aligned}
&1 + \sin\theta\cdot(\sin\theta(|\alpha_0|^2 - |\alpha_k|^2) + 2\cos\theta(|\alpha_0||\alpha_k|)) \\
=\; & 1 + \sin\theta(\sin\theta(\cos^2\theta_0 - \sin^2\theta_0) + 2\cos\theta\cos\theta_0\sin\theta_0) \\
=\; & 1 + \sin\theta(\sin\theta\cos 2\theta_0 + \cos\theta\sin 2\theta_0) \\
=\; & 1 + \sin\theta(\sin(\theta + 2\theta_0)) \leq 1 + \sin\theta.
\end{aligned}$$

The maximum is achieved when $\theta_0 = \frac{1}{2}(\pi/2 - \theta)$, i.e., when $|\psi\rangle$ bisects $|\phi\rangle$ and $|v_0\rangle$.

For an arbitrary mixed state $\rho := \sum_i p_i|\psi_i\rangle\langle\psi_i|$ with $\sum_i p_i = 1$, $p_i \geq 0$.

$$\text{Tr}(\Pi_S\rho) + \langle\phi|\rho|\phi\rangle = \sum_i p_i\left(\text{Tr}(\Pi_S|\psi_i\rangle\langle\psi_i|) + \langle\phi|(|\psi_i\rangle\langle\psi_i|)|\phi\rangle\right) \leq 1 + \sin\theta.$$

$\square$

Proof of Theorem 4.1. The intuition behind the soundness proof is that the two branches (conditioning on register Π) of verifier's verification are competing and the prover cannot cheat one without also changing the other. When the input $x \notin L$, a cheating prover must apply an operation far from $O_{f^{-1}}$ on $|Q\rangle$ to make R accept. We will show that when it applies such an operation, it must move the trap state $|T\rangle$ far from the correct state $|T^H\rangle$ which will be detected by the verifier. Now, we can finish the proof by showing the completeness and soundness.

We introduce some notation first. Let the state of the entire system after the prover's action be $\frac{1}{\sqrt{2}}(|\psi_0\rangle_{PMV}|0\rangle_B + |\psi_1\rangle_{PMV}|1\rangle_B)$.

If the prover is honest, then $|\psi_0\rangle = |0\rangle_P |Q^H\rangle$, $\quad |\psi_1\rangle = |0\rangle_P |T^H\rangle$.

If the prover is dishonest, we can always assume that $O_{f^{-1}}$ is applied honestly, followed by an arbitrary unitary $\tilde{U}$ on its work register P and message register M. In this case

$$|\psi_0\rangle = \tilde{U} \otimes I_V (|0\rangle_P |Q^H\rangle_{MV}), \quad |\psi_1\rangle = \tilde{U} \otimes I_V (|0\rangle_P |T^H\rangle_{MV}).$$

For ease of notation, define $\rho_0 := \mathrm{Tr}_P(|\psi_0\rangle\langle\psi_0|_{PMV})$ and $\rho_1 := \mathrm{Tr}_P(|\psi_1\rangle\langle\psi_1|_{PMV})$.

Let Π_R be the projection to the acceptance subspace $S_{\mathrm{acc}} \subseteq \mathcal{H}_M \otimes \mathcal{H}_V$ induced by R. Observe that the verifier accepts with probability

$$p_{\mathrm{succ}} := \frac{1}{2}(p_0 + p_1), \quad \text{where } p_0 = \mathrm{Tr}(\Pi_R \rho_0), \quad p_1 = \langle T^H | \rho_1 | T^H \rangle.$$

Completeness. If $x \in \bar{L}$, then $\rho_0 = |Q^H\rangle\langle Q^H|$ and $\rho_1 = |T^H\rangle\langle T^H|$. Therefore, $p_0 = \mathrm{Tr}(\Pi_R \rho_0) \geq 1 - \varepsilon$ by our hypothesis on the reduction. Meanwhile $p_1 = \langle T^H | \rho_1 | T^H \rangle = 1$. Therefore $p_{\mathrm{succ}} = \frac{1}{2}(p_0 + p_1) \geq 1 - \varepsilon/2$.

Soundness. Suppose that $x \notin \bar{L}$. By Lemma 4.3, we have that $p_1 = \langle T^H | \rho_1 | T^H \rangle = \langle Q^H | \rho_0 | Q^H \rangle$. Therefore $p_{\mathrm{succ}} = \frac{1}{2}(p_0 + p_1) = \frac{1}{2}(\mathrm{Tr}(\Pi_R \rho_0) + \langle Q^H | \rho_0 | Q^H \rangle)$. Since $x \notin \bar{L}$, we know that $RC|Q^H\rangle = \sqrt{\delta}|0\rangle|\phi_{x,0}\rangle + \sqrt{1-\delta}|1\rangle|\phi_{x,1}\rangle$ with $\delta \leq \varepsilon$. Therefore, $\langle Q^H | \Pi_R | Q^H \rangle \leq \varepsilon$, i.e., $|Q^H\rangle$ is almost orthogonal to the acceptance subspace S_{acc}. Then from the prover's perspective, to maximize the verifier's accepting probability, it needs to find a state whose projection on $|Q^H\rangle$ and S_{acc} combined is maximized. By Lemma 4.4, the maximum is achieved by a state bisecting $|Q^H\rangle$ and its projection on S_{acc}, and we conclude that $p_{\mathrm{succ}} = \frac{1}{2}(\mathrm{Tr}(\Pi_R \rho_0) + \langle Q^H | \rho_0 | Q^H \rangle) \leq \frac{1}{2}(1 + \sqrt{\varepsilon})$. $\qquad\square$

Let L be a hard problem in NP or QMA, we derive the following corollaries from Theorem 4.1.

Corollary 4.5. *If there exists a uniform one-query locally quantum reduction from a worst-case NP-hard decision problem to inverting a one-way permutation, then $\mathsf{coNP} \subseteq \mathsf{QIP}(2)$.*

Proof. Suppose L is NP-hard, and it reduces to Inv-OWP via a uniform one-query quantum locally random reduction. By Theorem 4.1, $\bar{L} \in \mathsf{QIP}(2)$, hence $coNP \subseteq \mathsf{QIP}(2)$. $\qquad\square$

Corollary 4.6. *If there exists a uniform one-query locally quantum reduction from a worst-case promise problem which is QMA-hard to inverting a one-way permutation, then $\mathsf{coQMA} \subseteq \mathsf{QIP}(2)$*

Proof. Suppose L is QMA-hard and there exists a uniform one-query quantum locally random reduction from L to Inv-OWP. By Theorem 4.1, $\bar{L} \in \mathsf{QIP}(2)$. This implies $coQMA \subseteq \mathsf{QIP}(2)$. $\qquad\square$

4.2 Uniform non-adaptive locally quantum reductions

In this section, we are going to generalize Theorem 4.1 such that the existence of a *multi-query* uniform non-adaptive locally quantum reduction with constant error implies coNP$\subseteq$QIP(2).

Let f be a one-way permutation, and let U_f be a circuit computing it. A uniform non-adaptive locally quantum reduction (G, R) from a decision problem to the task of inverting f is defined as:

$$|x, 0\rangle \xrightarrow{G} \frac{1}{\sqrt{2^{mk}}} \sum_{q_1,\dots,q_k \in \mathbb{Z}_2^m} |q_1, 0, w_{x,1}(q_1)\rangle \otimes \cdots \otimes |q_k, 0, w_{x,k}(q_k)\rangle$$

$$\xrightarrow{O_{f^{-1}}} \frac{1}{\sqrt{2^{mk}}} \sum_{q_1,\dots,q_k \in \mathbb{Z}_2^m} |q_1, f^{-1}(q_1), w_{x,1}(q_1)\rangle \otimes \cdots \otimes |q_k, f^{-1}(q_k), w_{x,k}(q_k)\rangle$$

$$\xrightarrow{R} a_0 |0\rangle |\psi_{x,0}\rangle + a_1 |1\rangle |\psi_{x,1}\rangle,$$

where $|a_1|^2 \geq 2/3$ if $x \in L$ and $|a_1|^2 \leq 1/3$ if $x \notin L$ is the probability the reduction accepts.

Theorem 4.7. *Suppose there exists a uniform non-adaptive locally quantum reduction (G, R) from a worst-case decision problem L to Inv-OWP. Then, there exists a $\mathsf{QIP}(2)$ protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\bar{L}$, where ϵ is negligible.*

Before giving the main theorem, we first show that the error of locally quantum reductions and quantum worst-case to average-case reductions can be reduced by parallel repetition.

Lemma 4.8 (Error reduction). *The error of locally quantum reductions and quantum worst-case to average-case reductions can be reduced to an exponential small parameter ϵ in polynomial time and polynomial number of queries.*

Proof. The error of both reductions can be reduced by parallel repetition. The new reduction (R', G') is described as follows:

1. G' operates G t times to generate t copies of $|Q_{x,1}\rangle \otimes \cdots \otimes |Q_{x,k}\rangle$ and send all copies to the oracle in parallel, where t is polynomial in the input length n.

2. After getting all t responses $|Q_{x,1}^H, \ldots, Q_{x,k}^H\rangle$ from the oracle, R' operates R t times and make the majority vote. If more than $t/2$ copies are accepted, R' accepts; otherwise, R' rejects.

For completeness, the probability that (G', R') rejects is $\sum_{u < \frac{t}{2}} \binom{t}{u} \frac{2}{3}^u (1 - \frac{2}{3})^{t-u}$. For soundness, the probability that (G', R') accepts is $\sum_{u > \frac{t}{2}} \binom{t}{u} \frac{1}{3}^u (1 - \frac{1}{3})^{t-u}$. Both are negligible. This completes the proof. $\qquad\square$

Then we will show that such reduction does not exist unless $\mathsf{coNP} \subseteq \mathsf{QIP}(2)$.

Proof of Theorem 4.7. The error can be reduced to an exponentially small parameter ϵ by applying Lemma 4.8. The idea of the protocol for multiple queries is the same as the protocol in Protocol 1 for one query. The verifier generates a superposition of the query state and the trap state and sends part of the state to the prover. In the following, we will give a $\mathsf{QIP}(2)$ protocol which is similar to the protocol in Protocol 1 for $\overline{L}$.

By Lemma 4.8, the error of a quantum locally random (G, R) can be reduced to an exponentially small parameter ϵ by parallel repetition, where we suppose G is operated t times and each time it generates k queries. We denote the new reduction as (G', R').

We now introduce the query state and the trap state the verifier generates. By applying G' and C, the verifier generates $|Q_{1,1}\rangle|Q_{1,2}\rangle \otimes \cdots \otimes |Q_{t,k}\rangle$, where

$$|Q_{i,j}\rangle = \frac{1}{\sqrt{2^m}} \sum_{q \in \mathbb{Z}_2^m} |q, 0\rangle |w_{x,j}(q), q\rangle \text{ for } 1 \le i \le t, 1 \le j \le k.$$

Note that i indicates the i-th copy generated from the parallel repetition in Lemma 4.8. Also, the verifier generates $|T\rangle^{\otimes tk}$, where $|T\rangle$ is defined in Equation 6.

Then, we rearrange the qubits such that the first two registers of all $|Q_{i,j}\rangle$ and $|T\rangle$ are moved to the beginning in sequence as follows:

$$|Q_{1,1}, \ldots, Q_{t,k}\rangle \rightarrow |\hat{Q}\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, 0\rangle_M |w_x(\hat{q}), \hat{q}\rangle_V \tag{14}$$

$$|T\rangle^{\otimes k} \rightarrow |\hat{T}\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, 0\rangle_M |0, \hat{q}\rangle_V. \tag{15}$$

where $\hat{q} = [q_{1,1}, \ldots, q_{1,k}, \ldots, q_{t,1}, \ldots, q_{t,k}]$ and $w_x(\hat{q}) = [w_{x,1}(q_{1,1}), \ldots, w_{x,k}(q_{t,k})]$. For example, given a state of two queries $\sum_{q,q'} |q, 0\rangle|w_{x,1}(q), q\rangle|q', 0\rangle|w_{x,2}(q), q'\rangle$, following the rearrangement, we represent it as $\sum_{q,q'} |qq', 0\rangle|w_{x,1}(q)w_{x,2}(q'), qq'\rangle$.

Similarly, we define

$$|\hat{Q}^H\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, f^{-1}(\hat{q})\rangle_M |w_x(\hat{q}), \hat{q}\rangle_V$$

$$|\hat{T}^H\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, f^{-1}(\hat{q})\rangle_M |0, \hat{q}\rangle_V,$$

where $f^{-1}(\hat{q}) = (f^{-1}(q_{1,1}), \ldots, f^{-1}(q_{t,k}))$.

Protocol 2 QIP(2) protocol for $\overline{L}$ using a non-adaptive locally quantum reduction.

The protocol takes place in the space $\mathcal{H}_P \otimes \mathcal{H}_M \otimes \mathcal{H}_V \otimes \mathcal{H}_\Pi$ where P is the private register of the prover, M is the register exchanged between the prover and the verifier, and V and Π are registers which are private to the verifier.

1. *The verifier's query.* The verifier prepares the state below. The message register M is sent to the prover.

$$|\hat{S}\rangle_{MV\Pi} := \frac{1}{\sqrt{2}}(|\hat{Q}\rangle_{MV}|0\rangle_\Pi + |\hat{T}\rangle_{MV}|1\rangle_\Pi).$$

2. *The prover's response.* The prover applies some unitary U_{PM} on register M and its private register P and sends the message register back to the verifier.

3. *The verifier's verification.* The verifier applies C to erase $\hat{q}$ in V. The verifier then measures Π to obtain $b \in \{0, 1\}$, and does the following:

   - (Computation verification) If $b = 0$, apply R' on MV and measure the output qubit. Accept if the outcome is 0.

   - (Trap verification) If $b = 1$, apply V_T on each $|T\rangle$ in MV and measure MV. Accept if the outcome is the all 0 string.

The QIP(2) protocol for $\overline{L}$ is shown in Protocol 2. Note that the prover's behavior U_{PM} can be represented as $U'_{PM}O_{f^{-1}}$ where U'_{PM} is an arbitrary unitary a cheating prover may apply. In the following, we show that the protocol in Protocol 2 is a QIP(2) protocol for $\overline{L}$.

For the completeness condition, when $x \in \overline{L}$, the verifier accepts with probability $\geq 1 - \epsilon/2$ via the same calculation in Section 4.1.

For the soundness condition, assume $x \notin \overline{L}$. Let

$$\hat{\sigma}_Q^{U'} = \mathrm{Tr}_P(U'_{PM} \otimes I_V(|0\rangle\langle 0| \otimes |\hat{Q}^H\rangle\langle\hat{Q}^H|)U'^\dagger_{PM} \otimes I_V)$$

$$\hat{\sigma}_T^{U'} = \mathrm{Tr}_P(U'_{PM} \otimes I_V(|0\rangle\langle 0| \otimes |\hat{T}^H\rangle\langle\hat{T}^H|)U'^\dagger_{PM} \otimes I_V).$$

Since $|\hat{T}^H\rangle$ and $|\hat{Q}^H\rangle$ are two purifications of the mixed state $\mathrm{Tr}_V(|\hat{Q}^H\rangle\langle\hat{Q}^H|)$ on register M,

$$\langle\hat{Q}^H|\hat{\sigma}_Q^{U'}|\hat{Q}^H\rangle = \langle\hat{T}^H|\hat{\sigma}_T^{U'}|\hat{T}^H\rangle \tag{16}$$

by Lemma 4.2. Then, we do a similar calculation as in the proof of soundness for Theorem 4.1, which gives an upper bound $1/2 + \sqrt{\epsilon}$ on the probability that the verifier accepts. $\qquad\square$

The following two corollaries follow from Theorem 4.7, which proofs are the same as the proof for Corollary 4.5 and Corollary 4.6.

Corollary 4.9. *If there exists a uniform non-adaptive quantum locally random reduction from a worst-case decision problem which is NP-hard to the task of inverting a one-way permutation, then coNP $\subseteq$ QIP(2).*

Corollary 4.10. *If there exists a uniform non-adaptive quantum locally random reduction from a worst-case promise problem which is QMA-hard to the task of inverting a one-way permutation, then coQMA $\subseteq$ QIP(2).*

5 Generalizations

In this section, we will show that we can generalize our techniques to other settings. We will first see that we can deal with distributions which are not uniform but close to uniform. Then, we

will show that in addition to locally quantum reduction, we can also handle the case of quantum worst-case to average-case reduction when the queries are "smooth". Finally, we will consider the task of inverting a regular one-way function and will show that when the oracle can do a quantum sampling of the preimages, then the same theorem for Inv-OWP also holds for Inv-OWF.

5.1 Smooth locally quantum reductions to Inv-OWP

We first show that when the distribution is not far from uniform distribution, we can still construct a QIP(2) protocol given the non-adaptive quantum locally reduction. Therefore, the existence of such reduction also imply coNP $\subseteq$ QIP(2).

The difficulty to apply Protocol 1 and Protocol 2 to non-uniform distributions is that we do not know how to construct a trap state that can be mapped to $|0\rangle$ efficiently and has the state in the message register be indistinguishable from the actual query state. Here we show that if the distribution is smooth-computable, then the verifier can use the same trap state by applying quantum rejection sampling [25] to prevent the prover from cheating.

Definition 5.1 (Smooth-computable distributions). *A distribution $\mathcal{D} = \{\mathcal{D}_n : n \in \mathbb{N}\}$ is said to be smooth-computable if it satisfies the following properties. Let $d_q = \Pr[q \sim \mathcal{D}_n]$, $d_{min,n} = \min_{q \in \{0,1\}^n} d_q$ and $d_{max,n} = max_{q \in \{0,1\}^n} d_q$.*

1. For $n \in \mathbb{N}$, for all q where $|q| = n$, the function $f_n : f_n(q) = d_q$ is polynomial-time computable.

2. For $n \in \mathbb{N}$, $2^n d_{min,n} \geq \frac{1}{poly(n)}$ and $2^n d_{max,n} \leq poly(n)$.

Loosely speaking, smooth-computable distributions are point-wise close to the uniform distribution. It is worth noting that Protocol 2 can handle those that have negligible statistical distance to the uniform distribution. However, there exists some smooth-computable distribution that has inverse-polynomial distance from the uniform distribution. In such cases, it is unclear if soundness still holds in Protocol 2.

Again, we start with the special case of *one-query* reductions with negligible error. Generalizing to multiple non-adaptive queries is similar to the case of uniform distributions.

Let f be a one-way permutation on $\{0,1\}^n$, and let U_f be a quantum circuit computing it. A smooth one-query locally quantum reduction according to a smooth-computable distribution $\mathcal{D} = \{\mathcal{D}_n : n \in \mathbb{N}\}$ proceeds as follows:

$$|x,0\rangle|0\rangle \quad \xrightarrow{G} \quad \frac{1}{\sqrt{2^m}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q,0\rangle|w_x(q)\rangle \tag{17}$$

$$\xrightarrow{O_{f^{-1}}} \quad \frac{1}{\sqrt{2^m}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q,f^{-1}(q)\rangle|w_x(q)\rangle \tag{18}$$

$$\xrightarrow{R} \quad a_0|0\rangle|\psi_{x,0}\rangle + a_1|1\rangle|\psi_{x,1}\rangle, \tag{19}$$

where $|a_1|^2 \geq 1 - \epsilon$ if $x \in L$ and $|a_1|^2 \leq \epsilon$ if $x \notin L$ is the probability the reduction accepts and d_q is the probability q is drawn from $\mathcal{D}_n$ for $n = |q|$.

Theorem 5.2. *Suppose there exists a one-query smooth locally quantum reduction with exponentially small error ϵ from a worst-case decision problem L to the task of inverting a polynomial-time computable permutation. Then there exists a QIP(2) protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\overline{L}$*

The proof of Theorem 5.2 relies on the quantum rejection sampling technique in [25]. We give the definition of the quantum rejection sampling problem and we adapt their tools in the Lemma 5.4.

Definition 5.3 (Quantum rejection sampling problem $QRSP(\mathcal{D}, \mathcal{D}', n)$). *Given an oracle $O_\mathcal{D} : |0\rangle \rightarrow \sum_{x=1}^{2^n} \sqrt{d_x}|\xi_x\rangle|x\rangle$ as a unitary, where $d_x \sim \mathcal{D}_n$ and $|\xi_x\rangle$ are some unknown fixed states. The Quantum rejection sampling problem is to prepare the state $\sum_{x=1}^{2^n} \sqrt{d'_x}|\xi_x\rangle|x\rangle$ for $d'_x \sim \mathcal{D}'_n$.*

Lemma 5.4. *Let $\mathcal{D} = \{\mathcal{D}_n : n \in \mathbb{N}\}$ be a smooth-computable distribution and $\mathcal{U}$ be the uniform distribution. There exists a quantum polynomial-time algorithm $QRSampling(\mathcal{D} \to \mathcal{U})$ that takes $\gamma = (\lceil \frac{1}{2^n d_{min,n}} \rceil)^2$ copies of $\sum_{x=1}^{2^n} \sqrt{d_x}|\xi_x\rangle|x\rangle$ and outputs a state that has negligible trace distance δ to $\sum_{x=1}^{2^n} \sqrt{\frac{1}{2^n}}|\xi_x\rangle|x\rangle$. Similarly $QRSampling(\mathcal{U} \to \mathcal{D})$ takes $\gamma' = (\lceil 2^n d_{max,n} \rceil)^2$ copies of $\sum_{x=1}^{2^n} \sqrt{\frac{1}{2^n}}|\xi_x\rangle|x\rangle$ and outputs a state that has negligible trace distance δ' to $\sum_{x=1}^{2^n} \sqrt{d_x}|\xi_x\rangle|x\rangle$.*

Note that γ and γ' are polynomial in n when $\mathcal{D}$ is smooth according to Definition 5.1.

Proof. We first show the sample complexity. It has been shown in [25] that Algorithm 3 can solve the $QRSP(\mathcal{D}, \mathcal{D}', k)$ exactly with $1 - e^{-\beta}$ with β^2 samples generated from $O_\mathcal{D}$ for $\frac{1}{\beta} = min_x d_x/d'_x$. In case $\mathcal{D} = \mathcal{U}$, we have $\frac{1}{\beta} = min_x \frac{1}{2^n d_x} = \frac{1}{2^n d_{max,n}}$. In case $\mathcal{D}' = \mathcal{U}$, we have $\frac{1}{\beta} = 2^n d_{min,n}$.

Algorithm 3 can also be done in polynomial time. Consider the case where $\mathcal{D}' = \mathcal{U}$. The Step 2 in Algorithm 3 can be viewed as a control rotation on the first and the third register.

$$S = \sum_{i=1}^{2^n} \frac{1}{d_i} \begin{bmatrix} \sqrt{d_i - \frac{1}{2^n \gamma}} & -\sqrt{\frac{1}{2^n \gamma}} \\ \sqrt{\frac{1}{2^n \gamma}} & \sqrt{d_i - \frac{1}{2^n \gamma}} \end{bmatrix} \otimes I \otimes |i\rangle\langle i|$$

By Solovay-Kitaev theorem, any known one-qubit unitary V can be approximated by V' which is implemented by polynomial number of gates from a finite universal gate set with an exponentially small error $\delta = max_{|\psi\rangle} \|(V - V')|\psi\rangle\|$. Since $\mathcal{D}$ and $\mathcal{U}$ are polynomial-time computable as in Definition 5.1, we can approximate S in polynomial time. This completes the proof. The analysis for the case where $\mathcal{D} = \mathcal{U}$ is the same.

Algorithm 3 $QRSampling(\mathcal{D} \to \mathcal{D}')$

1: Let $\frac{1}{\beta} = min_x \frac{d_x}{d'_x}$.
2: Apply $O_\mathcal{D}$ to generate $\sum_{x=1}^{2^n} \sqrt{d_i}|\xi_i\rangle|i\rangle$.
3: Pick $\vec{\alpha} \in \mathbb{R}_+^{2^n}$ where $\alpha_i = \frac{d'_i}{\beta}$ and rotate the state in the first register by S

$$S : |0\rangle(\sum_{x=1}^{2^n} \sqrt{d_i}|\xi_i\rangle|i\rangle) \to \sum_{x=1}^{2^n} (\sqrt{d_i - \alpha_i}|0\rangle + \sqrt{\alpha_i}|1\rangle)|\xi_i\rangle|i\rangle.$$

4: Measure the first qubit, which gives $\sum_{i=1}^{2^n} \sqrt{d'_i}|\xi_i\rangle|i\rangle$ with probability $\frac{1}{\beta}$.
5: By repeating steps 2 to 4 $\Theta(\beta^2)$ times, one can prepare the state $\sum_{i=1}^{2^n} \sqrt{d'_i}|\xi_i\rangle|i\rangle$ with probability $1 - e^{-\beta}$.

□

In the following, we first give a new protocol Protocol 4 in Section 5.1.1 and then prove that the protocol is a $\mathsf{QIP}(2)$ protocol.

5.1.1 The new protocol for $\overline{L}$ using quantum rejection sampling.

We first describe some states which are used in the protocol.

$$|Q_\mathcal{D}\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, 0\rangle_M |w_x(q), q\rangle_V, \tag{20}$$

where $|Q_\mathcal{D}\rangle_{MV}$ without the copy of q in V is the query state generated from G as in Equation 17.

$$|Q_\mathcal{D}^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, f^{-1}(q)\rangle_M |w_x(q), q\rangle_V, \tag{21}$$

where $|Q_{\mathcal{D}}^H\rangle$ without the extra copy q in register V is the state the actual reduction R gets after querying the oracle as in Equation 19.

By applying $QRSampling(\mathcal{D} \to \mathcal{U})$, one can prepare the state $|\tilde{Q}\rangle$ from $|Q_{\mathcal{D}}\rangle_{MV}$ such that $D(|\tilde{Q}\rangle, |Q\rangle) \le \delta$, where δ is an exponentially small error. We also define $|\tilde{Q}^H\rangle := O_{f^{-1}}|\tilde{Q}\rangle$. Similarly, one can prepare the state $|\tilde{Q}_{\mathcal{D}}^H\rangle$ from $|\tilde{Q}^H\rangle$ by $QRSampling(\mathcal{U} \to \mathcal{D})$ such that $D(|\tilde{Q}_{\mathcal{D}}^H\rangle, |Q_{\mathcal{D}}^H\rangle) \le \delta'$, where δ' is exponentially small.

We give Protocol 4 for $\bar{L}$ with non-adaptive smooth locally quantum reductions and proves Theorem 5.2.

Proof of Theorem 5.2. Let the state of the entire system after the prover's action be

$$\frac{1}{\sqrt{2}}\left(|\tilde{\psi}\rangle_{PM_1\ldots M_{\gamma'}V_1\ldots V_{\gamma'}}|0\rangle_B + |\phi\rangle_{PM_1\ldots M_{\gamma'}V_1\ldots V_{\gamma'}}|1\rangle_B\right).$$

To simplify the notation, we let $M = M_1M_2\ldots M_{\gamma'}$ and $V = V_1V_2\ldots V_{\gamma'}$. If the prover is honest, then

$$|\tilde{\psi}\rangle = |0\rangle_P|\tilde{Q}^H\rangle \otimes \cdots \otimes |\tilde{Q}^H\rangle, \quad |\phi\rangle = |0\rangle_P|T^H\rangle \otimes \cdots \otimes |T^H\rangle,$$

where $F(|\tilde{Q}^H\rangle, |Q^H\rangle) \ge 1 - \delta$ according to Lemma 5.4. If the prover is dishonest, we can always assume that the prover first applies $O_{f^{-1}}$ honestly and then applies an arbitrary unitary $\tilde{U}$ on its work register P and message register M. In this case

$$|\tilde{\psi}\rangle = \tilde{U}_{PM} \otimes I_V(|0\rangle_P|\tilde{Q}^H\rangle \otimes \cdots \otimes |\tilde{Q}^H\rangle), \quad |\phi\rangle = \tilde{U}_{PM} \otimes I_V(|T^H\rangle \otimes \cdots \otimes |T^H\rangle).$$

For ease of notation, we define

$$\tilde{\rho}_0 := \text{Tr}_P(|\tilde{\psi}\rangle\langle\tilde{\psi}|); \quad \rho_1 := \text{Tr}_P(|\phi\rangle\langle\phi|).$$

Let Π_R be the projection to the acceptance subspace $S_{\text{acc}} \subseteq \mathcal{H}_M \otimes \mathcal{H}_V$ induced by the verifier's verification. Observe that the verifier accepts with probability

$$p_{\text{succ}} := \frac{1}{2}(p_0 + p_1), \quad \text{where } p_0 = \text{Tr}(\Pi_R\tilde{\rho}_0), \quad p_1 = \langle T^H|^{\otimes\gamma'}\rho_1|T^H\rangle^{\otimes\gamma'}.$$

Completeness. If $x \in \bar{L}$, then $\tilde{\rho}_0 = |\tilde{Q}^H\rangle\langle\tilde{Q}^H|$ and $\rho_1 = |T^H\rangle\langle T^H|$. Therefore, $p_0 = \text{Tr}(\Pi_R\tilde{\rho}_0) \ge 1 - \varepsilon - 2\delta$ where ϵ is from our hypothesis on the reduction and δ is the error from the quantum rejection sampling. Meanwhile $p_1 = \langle T^H|\rho_1|T^H\rangle = 1$. Therefore $p_{\text{succ}} = \frac{1}{2}(p_0 + p_1) \ge 1 - (\varepsilon + 2\delta)/2$.

Soundness. Suppose that $x \notin \bar{L}$. Let $|\psi\rangle = \tilde{U}_{PM} \otimes I_V(|0\rangle_P|Q^H\rangle \otimes \cdots \otimes |Q^H\rangle)$ and $\rho_0 := \text{Tr}_P(|\psi\rangle\langle\psi|)$. By Lemma 4.3, we have that

$$\langle T^H|^{\otimes\gamma'}\rho_1|T^H\rangle^{\otimes\gamma'} = \langle Q^H|^{\otimes\gamma'}\rho_0|Q^H\rangle^{\otimes\gamma'},$$

and then we are going to show that $\langle T^H|^{\otimes\gamma'}\rho_1|T^H\rangle^{\otimes\gamma'}$ is close to $\langle Q^H|^{\otimes\gamma'}\tilde{\rho}_0|Q^H\rangle^{\otimes\gamma'}$ except for a exponentially small error.

First, by monotonicity of the fidelity, $F(\rho_0, \tilde{\rho}_0) \ge F(|Q^H\rangle, |\tilde{Q}^H\rangle) \ge 1 - \delta$. Then we define the angles between states $|Q^H\rangle^{\otimes\gamma'}$, ρ_0 and $\tilde{\rho}_0$ as

$$A(|Q^H\rangle^{\otimes\gamma'}, \rho_0) = \arccos F(|Q^H\rangle^{\otimes\gamma'}, \rho_0), \quad A(\tilde{\rho}_0, \rho_0) = \arccos F(\tilde{\rho}_0, \rho_0), \text{ and}$$

$$A(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0) = \arccos F(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0).$$

By the triangular inequality,

$$A(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0) \le A(|Q^H\rangle^{\otimes\gamma'}, \rho_0) + A(\tilde{\rho}_0, \rho_0).$$

This gives

$$\begin{aligned}
F(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0) &\ge \cos\left(A(|Q^H\rangle^{\otimes\gamma'}, \rho_0) + A(\tilde{\rho}_0, \rho_0)\right) \\
&= F(|Q^H\rangle^{\otimes\gamma'}, \rho_0)F(\tilde{\rho}_0, \rho_0) - \sqrt{1 - F(|Q^H\rangle^{\otimes\gamma'}, \rho_0)}\sqrt{1 - F(\tilde{\rho}_0, \rho_0)} \\
&\ge F(|Q^H\rangle^{\otimes\gamma'}, \rho_0) - 2\sqrt{\delta}.
\end{aligned}$$

We can also get an upper bound on $F(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0)$ as follows: By triangular inequality,

$$A(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0) \geq A(|Q^H\rangle^{\otimes\gamma'}, \rho_0) - A(\tilde{\rho}_0, \rho_0),$$

which implies

$$
\begin{aligned}
F(|Q^H\rangle^{\otimes\gamma'}, \tilde{\rho}_0) &\leq \cos\left(A(|Q^H\rangle^{\otimes\gamma'}, \rho_0) - A(\tilde{\rho}_0, \rho_0)\right) \\
&= F(|Q^H\rangle^{\otimes\gamma'}, \rho_0)F(\tilde{\rho}_0, \rho_0) + \sqrt{1 - F(|Q^H\rangle^{\otimes\gamma'}, \rho_0)}\sqrt{1 - F(\tilde{\rho}_0, \rho_0)} \\
&\leq F(|Q^H\rangle^{\otimes\gamma'}, \rho_0) + \sqrt{\delta}.
\end{aligned}
$$

We can conclude that

$$\langle Q^H|^{\otimes\gamma'}\tilde{\rho}_0|Q^H\rangle^{\otimes\gamma'} = \langle Q^H|^{\otimes\gamma'}\rho_1|Q^H\rangle^{\otimes\gamma'} + c\sqrt{\delta} = \langle T^H|^{\otimes\gamma'}\rho_1|T^H\rangle^{\otimes\gamma'} + c\sqrt{\delta}$$

for c a small constant. Therefore

$$p_{\text{succ}} = \frac{1}{2}(p_0 + p_1) = \frac{1}{2}\left(\text{Tr}(\Pi_R\tilde{\rho}_0) + \langle Q^H|^{\otimes\gamma'}\tilde{\rho}_0|Q^H\rangle^{\otimes\gamma'} + c\sqrt{\delta}\right).$$

By Lemma 4.4, we can give an upper bound on p_{succ} as follows.

$$p_{\text{succ}} = \frac{1}{2}(\text{Tr}(\Pi_R\rho_0) + \langle Q^H|\rho_0|Q^H\rangle) \leq \frac{1}{2}(1 + \sqrt{\varepsilon} + c\sqrt{\delta}).$$

$\square$

Protocol 4 QIP(2) protocol for $\overline{L}$ with non-adaptive smooth locally quantum reductions.

Let $\gamma = (\lceil\frac{1}{2^n d_{min}}\rceil)^2$ and $\gamma' = (\lceil 2^n d_{max}\rceil)^2$, where $d_{min} = \min_{q\in\{0,1\}^n}\Pr[q \sim \mathcal{D}_n]$ and $d_{max} = max_{q\in\{0,1\}^n}\Pr[q \sim \mathcal{D}_n]$.

1. *The verifier's query.* The verifier prepares the state

$$|S\rangle_{MV\Pi} := \frac{1}{\sqrt{2}}(|\tilde{Q}\rangle_{M_1 V_1} \otimes \cdots \otimes |\tilde{Q}\rangle_{M_{\gamma'} V_{\gamma'}}|0\rangle_\Pi + |T\rangle_{M_1 V_1} \otimes \cdots \otimes |T\rangle_{M_{\gamma'} V_{\gamma'}}|1\rangle_\Pi).$$

The message registers $M_1, \ldots, M_{\gamma'}$ are sent to the prover, and the verifier keeps $V_1, \ldots, V_{\gamma'}$ and Π. $|\tilde{Q}\rangle$ can be prepared from γ copies of $|Q_\mathcal{D}\rangle$ by applying $QRSampling(\mathcal{D} \to \mathcal{U})$.

2. *The prover's response.* The prover applies some unitary $U_{PM_1\ldots M_{\gamma'}}$ on registers $M_1 \ldots M_{\gamma'}$ and its private register P and sends the message registers back to the verifier.

3. *The verifier's verification.* The verifier applies C to erase q in $V_1 \ldots V_{\gamma'}$. The verifier then measures Π to obtain $b \in \{0, 1\}$, and does the following:

   - (Computation verification) If $b = 0$, apply $QRSampling(\mathcal{U} \to \mathcal{D})$ to get a state $|\tilde{Q}_\mathcal{D}^H\rangle$, apply R on $|\tilde{Q}_\mathcal{D}^H\rangle$ and measure the output qubit. Accept if the outcome is 0.
   - (Trap verification) If $b = 1$, apply V_T on $M_i V_i$ for $i \in [\gamma']$ and measure. Accept if the outcome is all 0.

By the same proof as in Section 4.2, we generalize Theorem 5.2 to Theorem 5.5.

Theorem 5.5. *Suppose there exists a one-query smooth locally quantum reduction with constant error from a worst-case decision problem L to Inv-OWP. Then there exists a QIP(2) protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\overline{L}$, where ϵ is negligible.*

5.2 Non-adaptive quantum worst-case to average-case reductions

The same idea above actually also works for the non-adaptive quantum worst-case to average-case reduction defined in Definition 3.2. We show that if the queries are generated arbitrarily according to known smooth-computable distributions, i.e., the distributions of each query can be different but are smooth-computable and known, then the existence of such reductions also implies coNP⊆ QIP(2). We call this reduction *known smooth non-adaptive quantum worst-case to average-case reduction.*

Theorem 5.6. *Suppose there exists a known smooth non-adaptive quantum worst-case to average-case reduction with average hardness δ (G, R) from a worst-case decision problem L to Inv-OWP. Then, there exists a QIP(2) protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\overline{L}$*

Proof. Suppose (G, R) is the reduction and G generates k uniform queries. Given any function g which is δ-close to f^{-1} as Definition 2.5. Then, the smooth non-adaptive worst-case to average-case reduction is as follows:

$$
\begin{aligned}
|x, 0\rangle \quad &\xrightarrow{G} \quad (\sum_q \sqrt{d_{1,q}}|q, 0, w_x(q)\rangle) \otimes \cdots \otimes (\sum_q \sqrt{d_{k,q}}|q, 0, w_x(q)\rangle) \\
&\xrightarrow{O_g} \quad (\sum_q \sqrt{d_{1,q}}|q, f^{-1}(q), w_x(q)\rangle) \otimes \cdots \otimes (\sum_q \sqrt{d_{k,q}}|q, f^{-1}(q), w_x(q)\rangle) \\
&\xrightarrow{R} \quad \sqrt{p}|L(x)\rangle|\psi_{x,0}\rangle + \sqrt{1-p}|1 - L(x)\rangle|\psi_{x,1}\rangle,
\end{aligned}
$$

where $p \geq 2/3$ and $d_{i,q}$ are the probability that q is drawn from a smooth-computable distribution $\mathcal{D}_{|q|}^{(i)}$. Note that $\mathcal{D}_{|q|}^{(i)}$ can be difference from $\mathcal{D}_{|q|}^{(j)}$ for $i \neq j$. The error of the reduction can be reduced to an exponentially small parameter ϵ by Lemma 4.8.

Given such a reduction from L to Inv-OWP, Protocol 4 decides $\overline{L}$. It is worth noting that since the distribution of each query is known and smooth-computable, one can apply quantum resampling for uniform distribution as in Protocol 4. For completeness, the honest prover always simulates $O_{f^{-1}}$, which is the same honest prover considered in Theorem 5.2. Hence, the verifier accepts with probability at least $1 - \frac{\epsilon}{2}$. For soundness, if the prover's operation is δ-close to $O_{f^{-1}}$, then the verifier accepts with probability $\leq (1 + \epsilon)/2$. Else if it chooses an operation U'_{PM} which is not close to any δ-close oracle for $O_{f^{-1}}$, then the modified trap state must be far from the original trap state. By the calculation in Section 5.1, we get the same upper bound on the soundness. $\square$

The following two corollaries follow from Theorem 5.6.

Corollary 5.7. *If there exists a known smooth non-adaptive quantum worst-case to average-case reduction from a worst-case decision problem which is NP-hard to Inv-OWP, then coNP $\subseteq$ QIP(2)*

Corollary 5.8. *If there exists a known smooth non-adaptive quantum worst-case to average-case reduction from a worst-case promise problem which is QMA-hard to Inv-OWP, then coQMA $\subseteq$ QIP(2)*

5.3 Fixed-preimage-sized functions and quantum-sampling oracles

One interesting question to address is whether the protocol we give in Section 4.1 can be used for more general functions. We observe that it indeed extends to functions which have fixed preimage size and surjective (onto), e.g., k-to-1 functions, if the oracle in the reduction is capable of quantum sampling from all k preimages. To be more specific, this reduction follows Definition 3.1 except that the response of each query changes to

$$
|Q^H\rangle = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} (|q\rangle \frac{1}{\sqrt{|f^{-1}(q)|}} \sum_{z \in f^{-1}(q)} |z\rangle)|w_x(q), q\rangle,
$$

where the oracle gives a uniform superposition of all solutions to q. We call such reductions a *locally quantum reduction with a quantum-sampling oracle.* This kind of oracle has been considered in cryptography. For instance, Bacon et al. [5] showed that the dihedral hidden subgroup

problem reduces to quantum sampling subset sum solutions. Our result naturally generalizes when considering this kind of reductions.

Corollary 5.9. *If there exists a uniform one-query **locally quantum reduction with a quantum-sampling oracle** from a worst-case NP-hard decision problem L to inverting a one-way function which is fixed-preimage-sized and surjective, then $\overline{L} \in \mathsf{QIP}(2)$.*

Proof. This can be done by forcing the prover to give a superposition of all preimages. Suppose the function is k-to-1 and onto, we use the same protocol in Section 4.1 except that the honest prover replies

$$|Q^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} (|q\rangle \frac{1}{\sqrt{|f^{-1}(q)|}} \sum_{z \in f^{-1}(q)} |z\rangle)_M |w_x(q), q\rangle_V \tag{22}$$

$$|T^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} (|q\rangle \frac{1}{\sqrt{|f^{-1}(q)|}} \sum_{z \in f^{-1}(q)} |z\rangle)_M |0, q\rangle_V. \tag{23}$$

It is not hard to see that $|T^H\rangle_{MV}$ can be mapped to all-zero state by the same unitary in the protocol of Section 4.1. Furthermore, since $|Q^H\rangle$ and $|T^H\rangle$ have the same reduced density matrix in M, Lemma 4.3 and Lemma 4.4 can be applied. $\qquad\square$

We can extend Corollary 5.9 to locally quantum reductions with a quantum-sampling oracle, multiple non-adaptive queries, and smooth-computable distributions.

6 Oracle separation between coNP and QIP

In this section, we show an oracle A such that $\mathsf{coNP}^A \not\subseteq \mathsf{QIP}(2)^A$.

Theorem 6.1. *There exists an oracle A and a language $L(A) \in \mathsf{coNP}^A$ such that $L(A) \notin \mathsf{QIP}(2)^A$.*

Proof. We first define the language $L(A)$ on any oracle A. For any oracle A, let

$$L(A) = \{1^n : A \text{ contains all strings of length n}\}.$$

It is not hard to see that $L(A) \in \mathsf{coNP}$. Specifically, if 1^n is not in $L(A)$, then there exists an n-bit string a which is not in A, and thus a can be a certificate.

To show there exists an oracle A such that $L(A) \notin \mathsf{QIP}(2)^A$, we create the oracle A in stages as in [13] via the diagonization technique. We enumerate all possible quantum verifiers in the manner such that V_i is bounded in time by n^i, where n is the input size. Then, every verifier V_i will fail to recognize 1^{N_i} for some N_i large enough. The main challenge in adapting to the quantum setting is to program the oracle without changing an algorithm's output by too much, even if it can query the oracle in quantum superposition.

Consider V_i, we pick N_i large enough such that $2^{N_i} > 12(N_i)^{2i}$ and no oracle queries of length N_i has been made by verifier $V_1, \ldots, V_{i-1}$. Note that V_i can only make queries with length at most $(N_i)^i$ and at most $(N_i)^i$ queries since the running time is bounded by $(N_i)^i$. Now, every time V_i makes queries which have not been queried before, we let the oracle A output 1. If there is no prover can convince V_i that 1^{N_i} is in $L(A)$ with probability at least $2/3$, then we let A contains all strings with length N_i. Otherwise, if there exists a prover which can convince V_i that $1^{N_i} \in L(A)$ with probability at least $2/3$, then there must exist an N_i-bit string x such that the sum of its query amplitude is at most $\frac{(N_i)^i}{2^{N_i/2}}$. Finally, we use the hybrid argument as in [6]. Let V_i be $U_{(N_i)^i+1} A U_{(N_i)^i} A \cdots A U_1$. Let $A' = A$ except that $A'(x) = 0$. Then, for any initial state $|\psi\rangle$

$$\|U_{(N_i)^i+1} A U_{(N_i)^i} A \cdots A U_1 |\psi\rangle - U_{(N_i)^i+1} A' U_{(N_i)^i} A' \cdots A' U_1 |\psi\rangle\| \leq \frac{2(N_i)^i}{2^{N_i/2}}.$$

This implies that the probability that the probability that the same prover convinces V_i with oracle A' is $\frac{2}{3} - \frac{4(N_i)^{2i}}{2^{N_i}} \geq \frac{1}{3}$. This contradicts the hypothesis that there is no prover can convince V_i to accept 1^{N_i} with probability at most $1/3$.

$\qquad\square$

References

[1] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science*, volume 2285, pages 323–334. Springer, 2002. DOI: 10.1007/3-540-45841-7"26.

[2] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC 96, pages 99–108, 1996. DOI: 10.1145/237814.237838.

[3] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 284–293, 1997. DOI: 10.1145/258533.258604.

[4] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. On basing one-way functions on np-hardness. In *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing*, STOC '06, pages 701–710, 2006. DOI: 10.1145/1132516.1132614.

[5] Dave Bacon, Andrew M. Childs, and Wim van Dam. Optimal measurements for the dihedral hidden subgroup problem. *Chicago J. Theor. Comput. Sci.*, 2006, 2006.

[6] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. DOI: 10.1137/S0097539796300933.

[7] Andrej Bogdanov and Christina Brzuska. On basing size-verifiable one-way functions on np-hardness. In *Theory of Cryptography Conference*, pages 1–6. Springer, 2015. DOI: 10.1007/978-3-662-46494-6"1.

[8] Andrej Bogdanov and Chin Ho Lee. *Limits of Provable Security for Homomorphic Encryption*, pages 111–128. Springer Berlin Heidelberg, 2013. DOI: 10.1007/978-3-642-40041-4"7.

[9] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. *SIAM Journal on Computing*, 36(4):1119–1159, 2006. DOI: 10.1137/S0097539705446974.

[10] Gilles Brassard. Relativized cryptography. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, (undefined):383–391, 1979. ISSN 0272-5428. DOI: 10.1109/TIT.1983.1056754.

[11] Joan Feigenbaum and Lance Fortnow. Random-self-reducibility of complete sets. *SIAM Journal on Computing*, 22(5):994–1005, 1993. DOI: 10.1137/0222061.

[12] Joan Feigenbaum, Sampath Kannan, and Noam Nisan. Lower bounds on random-self-reducibility. In *Proceedings of Fifth Annual Structure in Complexity Theory Conference*, pages 100–109. IEEE, 1990. DOI: 10.1109/SCT.1990.113959.

[13] Lance Fortnow and Michael Sipser. Are there interactive protocols for co-np languages? *Information Processing Letters*, 28:249–251, 1988. DOI: 10.1016/0020-0190(88)90199-8.

[14] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 59–68. ACM, 1986. DOI: 10.1145/12130.12137.

[15] Patrick M. Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Inf. Comput.*, 14(5-6):384–416, 2014.

[16] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, pages 534–543, 2009. DOI: 10.1109/FOCS.2009.30.

[17] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP= PSPACE. *Journal of the ACM (JACM)*, 58(6):30, 2011. DOI: 10.1145/2049697.2049704.

[18] Akinori Kawachi and Tomoyuki Yamakami. Quantum hardcore functions by complexity-theoretical quantum list decoding. *SIAM Journal on Computing*, 39(7):2941–2969, 2010. DOI: 10.1137/080716840.

[19] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 608–617, 2000. DOI: 10.1145/335305.335387.

[20] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Generalized quantum arthur-merlin games. In *Proceedings of the 30th Conference on Computational Complexity*, pages 488–511, 2015. DOI: 10.4230/LIPIcs.CCC.2015.488.

[21] Tianren Liu and Vinod Vaikuntanathan. On basing private information retrieval on np-hardness. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A*, volume 9562 of *Lecture Notes in Computer Science*, pages 372–386. Springer, 2016. DOI: 10.1007/978-3-662-49096-9``16.

[22] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, 60(6):43, 2013. DOI: 10.1145/2535925.

[23] Daniele Micciancio. Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. *SIAM Journal on Computing*, 34(1):118–169, 2004. DOI: 10.1137/S0097539703433511. Preliminary version in STOC 2002.

[24] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. ISSN 0097-5397. DOI: 10.1137/S0097539705447360.

[25] Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. *ACM Trans. Comput. Theory*, 5(3):11:1–11:33, August 2013. ISSN 1942-3454. DOI: 10.1145/2493252.2493256.

[26] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004. DOI: 10.1137/S0097539703440678.

[27] Oded Regev. New lattice-based cryptographic constructions. *J. ACM*, 51(6):899–942, 2004. ISSN 0004-5411. DOI: 10.1145/1039488.1039490.

[28] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93. ACM, 2005. DOI: 10.1145/1060590.1060603.

[29] Bill Rosgen. Computational distinguishability of degradable and antidegradable channels. *Quantum Inf. Comput.*, 10(9&10):735–746, 2010.

[30] Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54(4):2614, 1996. DOI: 10.1103/PhysRevA.54.2614.

[31] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5): 1474–1483, 1997. DOI: 10.1137/S0097539796298637.

[32] Wim Van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*, 36(3):763–778, 2006. DOI: 10.1137/S009753970343141X.