The Pennsylvania State University
The Graduate School
College of Engineering

QUANTUM REDUCTIONS FROM HARD PROBLEMS

A Dissertation in
Computer Science and Engineering
by
Nai-Hui Chia

© 2018 Nai-Hui Chia

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

August 2018

The dissertation of Nai-Hui Chia was reviewed and approved* by the following:

Sean Hallgren
Professor of Department of Computer Science and Engineering
Dissertation Advisor, Chair of Committee

Martin Furer
Professor of Department of Computer Science and Engineering

Daniel Kifer
Professor of Department of Computer Science and Engineering

Jason Morton
Professor of Department of Mathematics

Chitaranjan Das
Department Head of Computer Science and Engineering

*Signatures are on file in the Graduate School.

Abstract

Finding reductions between problems is a fundamental way to evaluate hardness of computational tasks. With hypothesis in complexity theory such as $NP \neq P$, finding reductions from hard problems (e.g. SAT) to a task implies the task cannot be accomplished efficiently. For example, if one can find a reduction from SAT to breaking a cryptosystem, then this cryptosystem is computationally secure unless $NP = P$. On the other hand, for some tasks, it can be proven that hard problems cannot reduce to them. For instance, the existence of reductions from SAT to finding Nash equilibrium results in the consequence that polynomial hierarchy collapses. This can view as evidence that finding the Nash equilibrium can not be as hard as NP-hard problems.

There are many similar results studying classical reductions (which are either deterministic or randomized) between hard problems and tasks which have interesting applications. However, for quantum reductions, there are not many known examples. Quantum algorithms are believed to be more powerful than classical algorithms. Therefore, intuitively, we ask: Can we find quantum reductions between problems, where no classical reduction is known? Or, given a task, can we rule out the possibility that there are hard problems reducing to the task via quantum reductions? In this thesis, we study quantum reductions in these two directions.

For the first topic, we study the dihedral hidden subgroup problem by relating its hardness to a well-studied classical problem, the random subset sum problem. The dihedral hidden subgroup is an important open problem in quantum computing and cryptography. It is known that lattice problems reduce to it, and that it reduces to random subset sum with density > 1 and also to quantum sampling subset sum solutions. We examine a decision version of the problem where the question asks whether the hidden subgroup is trivial or order two. The decision problem essentially asks if a given vector is in the span of all coset states. We approach this by first computing an explicit basis for the coset space and the perpendicular space. We then look at the consequences of having efficient unitaries that use this basis. We show that if a unitary maps the basis to the standard basis

in any way, then that unitary can be used to solve random subset sum with constant density > 1. We also show that if a unitary can exactly decide membership in the coset subspace, then the collision problem for subset sum can be solved for density > 1 but approaching 1 as the problem size increases. This strengthens the previous hardness result that implementing the optimal POVM in a specific way is as hard as quantum sampling subset sum solutions.

For the second topic, we consider whether quantum reductions from NP-hard problems to breaking cryptosystem exist. In cryptography, it requires a system to be hard to be broken on average instead of being hard in the worst case. To show the security of a cryptosystem, one ideal approach is reducing a worst-case hard problem to breaking the system on average. Therefore, reducing NP-hard problems to breaking cryptography, e.g., the average-case hardness of inverting one-way permutations is a particularly intriguing instance. We initiate a study of the quantum analogue of these questions and show that if NP-complete problems can be reduced to inverting one-way permutations using certain types of quantum reductions, then coNP $\subseteq$ QIP(2).

Table of Contents

Acknowledgments

First of all, I would like to deeply thank to my advisor, Sean Hallgren, for his individual guidance through out the past six years which leads me toward becoming an independent researcher in quantum computation. He is a very patient advisor and always encourages me to pursue my own research interests. I have learned almost all the basics of doing theoretical research from him which include reading paper, finding problems, presenting research, thinking about research as well as his patience and passion on hard research problems. These greatly fostered me in the past, and will continue to guide me in the future. This thesis could not have been done without his insights throughout this work.

Also, I would like to thank to all the students and faculties in theory group of PSU CSE. The theory seminar organized by Piotr, Martin, Sean, Sofya, and Adam is a great chance for me to meet excellent researchers from different places and in different research areas. From the talks and personal meetings with them, I have broadened my knowledge in theoretical computer science. I enjoyed the time sharing the office with Nithin, Om, Kashap, Eunou, Jalaj, Meiram, Roksana, Ramesh, Jiayu, Raef and Audra. We have lots of good memories from discussions on research to drinking in a gay bar. These memories color my P.h.D. lives with different colors.

For several years, I have had the good fortune to work with Fang Song and Kai-Min Chung. They are good researchers and friends. Fang likes to share his insights in different problems with me and we have many good talks in different cities. The problem of quantum reductions from NP-hard problems to inverting one-way permutations is one of the topic we discussed when I was in my second year. I met Kai-Min in a conference. He is really smart and has deep and broad knowledge in both classical and quantum cryptography. I have learned lots of basics of (quantum) cryptography from our discussion. Also, our discussion pushed me to study topics which are not in this thesis but could be part of my future research interests.

Of course, there are many friends I want to thank to, who are Geng-Yuan,

Wei-Kai, Neil, Yi-Chien, Hsuan-Yi, Yang-Ding, Peter, Pei-Hsuan and so on. I had lots of good memories with them in my leisure time. They taught me things in areas from finance to fitness and help me take care of my cats. These moments and knowledge will definitely support me in the future.

The final thanks is reserved to my parents Chi-Chung Chia and Wei-Hsuan Tseng, sister Nai-Yi Chia and girl friend Jenny Chen, whose unreserved support continues to flow more generously than I deserve.

This dissertation is partially supported by National Science Foundation award CCF-1218721 and CCF-1618287 and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0522 and W911NF-12-1-0541.

Chapter 1
Introduction

This thesis focuses on studying quantum reductions from hard problems to computational tasks with important applications in cryptography. In Chapter 2, we study whether there exists a reduction from random subset sum with the hardest parameter to the dihedral hidden subgroup problem. The dihedral hidden subgroup problem is an important open problem in quantum computing and cryptography. In particular, lattice-based cryptography, which is proposed to be secure against quantum computers is based on problems reducing to the dihedral hidden subgroup problem. In Chapter 3, we explore the possibilities to reduce NP-hard problems to breaking cryptographic primitives under quantum reductions [CHS]. It has been shown that NP-hard problems cannot classically reduce to the task of breaking certain cryptographic primitives unless the polynomial hierarchy collapses. However, it is not known if the existence of quantum reductions from NP-hard problems to these cryptographic primitives implies any nontrivial consequence in complexity theory. In the following, I will elaborate on these two topics.

1.1 The dihedral hidden subgroup problem

The hidden subgroup problem is a successful framework to break cryptographic primitives with quantum computers. By solving abelian hidden subgroup problems in polynomial time, quantum computers break RSA [Sho97], discrete logarithm [Sho97], key exchange based on principle ideal problem [Hal07], the Smart-Vercauteren homomorphic encryption scheme [BS16], and GGH multilinear maps [BS16]. Non-abelian hidden subgroup problems also have important applications in cryptography but only few of them have efficient algorithms. In particular, it has

been shown that the security of lattice-based cryptography reduces to solving the dihedral hidden subgroup problem via the standard approach [Reg04], where the dihedral hidden subgroup problem is still open. Solving the dihedral hidden subgroup problem via the standard approach is defined as the dihedral coset problem (DCP).

In joint work with Hallgren [CH16], we were motivated to understand the hardness of the DCP by relating it to a well-studied classical problem, random subset sum. Random subset sum has a density parameter ρ, which determines its hardness. The DCP reduces to random subset sum with $\rho = 1$ [Reg04], which is known to be the hardest case [IN96]. For the other direction, we would like to show hardness of the DCP based on random subset sum with $\rho = 1$ whose hardness is well studied. However, the only known connection is that random subset sum with $\rho = 1/\log k$ reduces to the DCP by combining the reductions in [IN96, Reg04], where density $1/\log k$ may not be as hard as density 1. Hence, we asked, is the DCP as hard as random subset sum with $\rho = 1$?

Showing hardness would require reducing random subset sum with $\rho = 1$ to the DCP. We were unable to find a reduction, but we proved a weaker relationship in [CH16]. Let $\mathcal{S}$ be the subspace for the order-two coset states, our approach is finding a basis $\mathcal{B} \cup \mathcal{B}^{\perp}$ such that $\mathcal{B}$ spans $\mathcal{S}$ and $\mathcal{B}^{\perp}$ spans its complement. We first showed that measurements which distinguish $\mathcal{B}$ from $\mathcal{B}^{\perp}$ solve the DCP with group size a power of 2. Then we proved that this measurement also solves random subset sum with $\rho = 1 + c$ for c a constant or the collision problem for subset sum with $\rho = 1$. This implies that an efficient implementation of this measurement would solve subset sum with $\rho = 1 + c$ and the collision problem with $\rho = 1$. This also improves the result in [BCvD06] that implementing the optimal POVM for the DCP in a specific way is as hard as worst-case subset sum. It is still open that whether there exist a reduction from random subset sum with hard density to solving the DCP via an arbitrary measurement.

1.2 Quantum reductions from worst-case to average-case problems

Chapter 3 studies how the landscape of complexity theory and cryptography change when quantum reductions are considered. In joint work with Hallgren and Song [CHS], we start our studies from a fundamental question in complexity theory which is when worst-case problems have reductions to average-case problems. Such reductions exist for complete sets of PSPACE, EXP and #P [FF93]. For NP, where this question is open, previous results [FF93, BT06] showed that such non-adaptive reductions do not exist unless the polynomial hierarchy collapses. This question has also been studied in the context of cryptography. For instance, the classical reductions from an NP-hard problem to the task of inverting a one-way permutation do not exist; otherwise, the polynomial hierarchy collapses [Bra79]. These papers only analyzed classical reductions. Quantum reductions appear to be more powerful than classical reductions, when reducing from worst-case to average-case problems. Regev [Reg04, Reg05] showed that some lattice problems reduce to random subset sum or LWE via quantum reductions, while no classical reduction is known. Therefore, we asked the following question: Can we base cryptographic primitives on NP-complete or even QMA-complete problems if we allow quantum reductions?

There are two challenges to show the non-existence of quantum reductions. Previous results showing the non-existence of classical reductions are proven by the following strategy: Suppose there exists a classical reduction from an NP-hard problem L to an average-case problem (e.g., inverting one-way permutations). Then, by simulating the classical reduction, one can build a constant-round interactive proof protocol (IP(c)) for $\overline{L}$. This implies that coNP$\subseteq$ IP(c) = IP(2) and therefore the polynomial hierarchy collapses. The first challenge is that since the messages can be quantum states, the verifier needs to prevent the prover from cheating by entanglement. Second, to show a non-trivial consequence, one needs to construct a QIP(2) protocol for $\overline{L}$ instead of a constant-round protocol since QIP(c) = PSPACE for $c \geq 3$.

In [CHS], we studied the question whether or not the existence of quantum reductions from NP-hard problems to inverting one-way permutations also gives

unlikely consequences in complexity theory. To show the non-existence of reductions, it is important to have general definitions of reductions. There are two types of classical reductions, which are locally random reductions and worst-case to average-case reductions. We showed that the existence of quantum analogue of these two reductions with the restriction that the queries are non-adaptive and uniform superpositions from an NP-complete problems to inverting one-way permutations implies coNP $\subseteq$ QIP(2), where QIP(2) is the two-message quantum interactive proof. Note that the classical result shows that coNP $\subseteq$ AM, which implies the polynomial hierarchy collapses. Though our result does not imply the polynomial hierarchy collapses, it is a non-trivial consequence of the existence of quantum reductions.

Chapter 2
How hard is deciding trivial versus nontrivial in the dihedral coset problem?

2.1 Introduction

The dihedral coset problem is an important open problem in quantum algorithms. It comes from the hidden subgroup problem, which is defined as: given a function on a group G that is constant and distinct on cosets a subgroup H, find H. Here we will focus on the case when G is the dihedral group of order $2N$. It is known that this problem reduces to the case when the subgroup is order two [EH00]. All known approaches for solving the hidden subgroup problem over the dihedral group start by evaluating the function in superposition and measuring the function value. The result is a random coset state $\frac{1}{\sqrt{2}}(|0,x\rangle + |1,x+d\rangle)$, where $d \in \mathbb{Z}_N$ is a fixed label of the subgroup and x is a coset representative uniformly chosen in $\mathbb{Z}_N$. For our purposes, it is more convenient to have the following quantum problem rather than the hidden subgroup problem.

The *dihedral coset problem* [Reg04] is: given a tensor product of k coset states

$$|c^{(d)}_{x_1,x_2,\cdots,x_k}\rangle = \frac{1}{\sqrt{2}}(|0,x_1\rangle + |1,x_1+d\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0,x_k\rangle + |1,x_k+d\rangle),$$

where $x_1,\ldots,x_k$ are randomly chosen in $\mathbb{Z}_N$, compute d. The first register of each state is mod 2, and the second register is mod N.

This is a natural problem to consider after the successes with abelian groups such as $\mathbb{Z}_N$. The dihedral group with $2N$ elements has $\mathbb{Z}_N$ as a normal subgroup. The representations are mostly two dimensional, so it does not have obvious problems like the symmetric group, where we know large entangled measurements are required to get information from the states [HMR$^+$10]. Furthermore, Regev [Reg04] showed that the unique shortest vector problem reduces to the dihedral coset problem, so it could provide a pathway for finding a quantum algorithm for lattice problems.

Much is known about the dihedral coset problem, at least compared to most other nonabelian groups (although there are groups with efficient algorithms, e.g. [FIM$^+$14, ISS08, DIK$^+$14]). Ettinger and Hoyer [EH00] showed that a polynomial number of measurements in the Fourier basis has enough classical information to determine d, but the best known algorithm takes exponential time to compute it. Kuperberg found subexponential time algorithms [Kup05, Kup13] for the problem. He also showed that computing one bit of d was sufficient to compute all of d. This algorithm was a big step, although it should be noted that it seems difficult to combine this with Regev's uSVP to dihedral group HSP reduction to get a subexponential time algorithm for the uSVP, partly due to the fact that the coset states created in the reduction have errors with some probability.

The dihedral coset problem also has some connections to the subset sum problem. Bacon, Childs, and van Dam analyzed how well a "pretty good measurement" performs [BCvD06]. This type of measurement maximizes the probability of computing d correctly. It is unknown how to compute the measurement they find without quantum sampling subset sum solutions. A unitary implementing this can be used to solve the worst case subset sum, which is NP-complete. Regev showed how to reduce the dihedral coset problem to the random subset sum problem density $\rho > 1$ where ρ also approaches 1 as the problem size increases. Density 1 is the hardest case for the random subset sum problem as shown in Proposition 1.2 in [IN96]. But is solving the dihedral coset problem as hard as subset sum, and if so, for what parameters? The only connection we are aware of is to compose two known reductions. First, random subset sum with density $\rho = 1/\log k$ reduces to uSVP. Then uSVP reduces to the dihedral coset problem. It is open if an efficient quantum algorithm exists for random subset sum, and density $1/\log k$ may not be as hard to solve as constant density.

2.1.1 New approach

In this paper we focus on distinguishing trivial from order two subgroups. Instead of trying to compute d, we define a problem which asks if the state is an order two coset state, or is the trivial subgroup case. We define this problem as the *dihedral coset space problem (DCSP)*: either an order two coset state is given, or a random standard basis vector is given, decide which. The random standard basis vector corresponds to the trivial subgroup case in the hidden subgroup problem. This problem is a special case of the decision version of the HSP defined by Fenner and Zhou [FZ08] since we are restricting to order two subgroups. In their paper, they found a search to decision reduction when N is a power of two. So it turns out that the problem is not computationally easier in that case.

We start by finding a set of vectors that span C and $C^{\perp}$. Let $\vec{l} \in \mathbb{Z}_N^k$, and $p \in \mathbb{Z}_N$. The vectors have the form

$$|S_{\vec{l},p}^m\rangle = \frac{1}{\sqrt{|T_{\vec{l},p}|}} \sum_{j=0}^{|T_{\vec{l},p}|-1} \omega_{|T_{\vec{l},p}|}^{mj} |\vec{b}_{\vec{l},p}^{(j)}\rangle |\chi_{\vec{l}}\rangle,$$

where $T_{\vec{l},p}$ contains the subset sum solutions for $(\vec{l}, p)$, and the vectors $\vec{b}$ are an ordered set of the subset sum solutions. We call this set of orthonormal vectors the *subset sum* basis. We prove that the $m = 0$ subset of vectors span C and the remaining ones, which have $m \geq 1$, span $C^{\perp}$.

Ideally we would like to reduce subset sum to the DCSP. Since this is still out of reach, we prove a weaker relationship. Instead, we assume there is an algorithm that uses the subset sum basis to solve the DCSP and examine the consequences. Such an algorithm needs to decide if $m = 0$ or $m \geq 1$ to distinguish if the vector is in C or $C^{\perp}$. In this paper we consider two main types of unitaries that use this basis. We show that in one case such a unitary can be used to solve random subset sum and in the other case it can be used to solve the random collision problem. This may indicate that the unitaries are difficult to implement.

The first type of unitary we consider maps the subset sum basis to the standard basis. An example would be one that maps each vector $|S_{\vec{l},p}^m\rangle$ to the corresponding standard basis vector $|m, p, \vec{l}\rangle$, identifying the vector. This unitary can be used to solve a subset sum instance $(\vec{l},\ p)$ by taking $|0, p, \vec{l}\rangle$, applying U^{-1} to get $|S_{\vec{l},p}^0\rangle$ and measuring, since $|S_{\vec{l},p}^0\rangle$ is a uniform superposition of solutions. The ability

to identify the basis vector in this way is very strong because it can solve an NP-complete problem, but we show the connection for a wider range of unitaries. In particular, we show that any unitary that maps the subset sum basis to the standard basis in some way can be used to solve the random subset sum problem in the cryptographic range of constant density $\rho > 1$. This can be view as generalizing the connection to quantum sampling in [BCvD06].

The proof for this case works by showing that such a unitary can be used to solve worst case collision for the subset sum function. That is, given a subset sum instance $(\vec{l}, p)$ and a solution vector $\vec{b}$, the goal is to compute a second solution $\vec{b}'$ if one exists. Then we use the fact that random subset sum reduces to random collision for density a constant greater than one [IN96].

The second type of unitary we consider maps the subset sum basis to vectors where the first bit is zero if the vector is in C, and is one if the vector is from $C^{\perp}$. This type of unitary can be used to solve the DCSP by computing the unitary on the input vector and measuring the first bit. It is a relaxation of the first type of unitary because it could be followed by another unitary mapping to the standard basis. We show that this type of unitary can be used to solve the random collision problem for subset sum with density $\rho = 1 + c \log\log N / \log N$. This collision problem for this density appears to be less well understood than for constant density.

The proof for this case uses the unitary that can solve the DCSP to solve the random collision problem for subset sum. The problem in this case has an arbitrary solution vector $\vec{b}$ fixed, and then a vector $\vec{l}$ is chosen at random. The goal is again to find a second solution $\vec{b}' \neq \vec{b}$ such that $\vec{b}' \cdot \vec{l} = \vec{b} \cdot \vec{l} \bmod N$ on input $\vec{b}$ and $\vec{l}$.

In addition to these two main types of unitaries we show that a small generalization of the form of the subset sum bases has similar results.

The hardness of random subset sum depends on the density and the same is true for the collision problem. But for collision the definition is important also. There are four definitions of finding collisions of hash functions [RS04]. Our definition of random subset sum collision is based on the universal one-way hash-function family. That is, for any point in the domain, given the hash function uniformly at random from the family, the goal is to find another point in the domain having the same hash value. Impagliazzo and Naor have shown that random subset sum collision is at least as hard as the random subset sum problem when the density is

a constant greater than 1 [IN96]. However, the density of the random subset sum collision problem we consider has density $\rho \leq 1+c \log N \log N / \log N$. This density is between the density used for subset sum in [Reg04] and the cryptographic one. The hardness of densities for collision in this range is not known, but it can be contrasted with random subset sum, where the problem gets harder as the density approaches one [IN96].

There are several open questions. Can the second type of unitary above also be used to solve random subset sum? Consider unitaries which decide membership of C with small error, e.g., $1/poly$. Can these unitaries be implemented efficiently or solve some hard problems? Is it possible to implement a unitary efficiently distinguishing C from $C^{\perp}$, with the subset sum basis, or some other basis? If a space has a basis that seems hard to be implemented for some reason, does that mean that no basis for that space is efficient? Is it possible that a larger space C' containing C exists where it is easier to test C' vs. $C'^{\perp}$? Deciding membership in a subspace or its complement is a generalization of classical languages to quantum languages. Are there other examples?

2.2 Background

In this section, we give the background of the dihedral coset problem and the random subset sum problem.

The dihedral coset problem comes from the dihedral hidden subgroup problem which is

Definition 2.2.1 (Dihedral Hidden Subgroup Problem)**.** *Given the dihedral group D_{2N} and a function f that maps D_{2N} to some finite set such that f hides a subgroup H (f takes same value within each coset of H and takes distinct value on different cosets), the problem is to find a set of generators for H.*

Ettinger and Hoyer showed that the problem reduces to the case when the subgroup is order two [EH00]. Hence, we can assume H is an order two subgroup, which can be represented as $\{1, d\}$ for $d \in \mathbb{Z}_N$. All known approaches for solving this problem start by evaluating the function in superposition to get $\sum_{g \in D_{2N}} |g, f(g)\rangle$, and then measuring the function value. This results in an order two coset state $\frac{|0,x\rangle+|1,x+d\rangle}{\sqrt{2}}$, where $x \in \mathbb{Z}_N$ is a random coset representative. Then

the problem becomes to find d when given many random order two coset states. This problem is defined as follows:

Definition 2.2.2 (Dihedral Coset Problem (DCP))**.** *Given a random k-register order two coset state*

$$|c^{(d)}_{x_1,x_2,\ldots,x_k}\rangle = \frac{1}{\sqrt{2}}(|0,x_1\rangle + |1,x_1+d\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0,x_k\rangle + |1,x_k+d\rangle).$$

The problem is to find d.

The hardness of the DCP has been studied by reducing to the random subset sum problem [Reg04] which is defined as follows:

Definition 2.2.3 (Random Subset Sum Problem)**.** *Given a vector of positive integers $\vec{l} = [l_1, l_2, \ldots, l_k]^T$ uniformly distributed in $\mathbb{Z}_N^k$ and $s = \vec{b} \cdot \vec{l} \pmod N$ where $\vec{b} \in \mathbb{Z}_2^k$ is chosen uniformly at random, find a vector $\vec{b}' \in \mathbb{Z}_2^k$ such that $\vec{l} \cdot \vec{b}' = s \pmod N$. The density is defined as $\rho = \frac{k}{\log(N)}$.*

Although the worst-case subset sum problem is NP-hard, the random subset sum problem can be solved in polynomial time when the density is in a certain range. There is no known polynomial-time algorithm for solving the case when ρ is $\Omega(1/k)$ and $O(\frac{k}{\log^2(k)})$. Regev [Reg04] showed that a solution to the random subset sum problem with $\rho > 1$ implies an efficient quantum algorithm for solving the DCP. Moreover, we note that one can reduce the random subset sum problem with $\rho = O(1/\log k)$ to a lattice problem [LO85,CJL+92], and then to the DCP [Reg04]. Since these two ranges are generally believed not equivalent, it is still not clear if the DCP is equivalent to random subset sum with ρ in a hard range.

In the rest of this section, we define one more problem which will be used in the section 2.5.

Definition 2.2.4 (Random Subset Sum Collision Problem)**.** *Let $\vec{b} \in \mathbb{Z}_2^k$ be an arbitrary fixed vector. Given $\vec{b}$, and a vector $\vec{l} \in \mathbb{Z}_N^k$ chosen uniformly at random, the problem is to find a solution $\vec{b}' \in \mathbb{Z}_2^k$ such that $\vec{b} \cdot \vec{l} \equiv \vec{b}' \cdot \vec{l} \pmod N$ and $\vec{b}' \neq \vec{b}$.*

The worst-case version of this problem is to find $\vec{b}'$ for arbitrary $\vec{b}$ and $\vec{l}$ which are given. For simplicity, we will call this problem the random collision problem and the worst-case version as the worst-case collision problem in the rest of the paper.

Impagliazzo and Naor showed a relationship between random collision problem and the random subset sum problem. The input in their notation has n numbers modulo $2^{\ell(n)}$ plus the target value.

Theorem 2.2.5 (Theorem 3.1 in [IN96]). *Let $\ell(n) = (1-c)n$ for $c > 0$. If the subset sum function for length $\ell(n)$ is one-way, then it is also a family of universal one-way hash functions.*

The subset sum function for length $\ell(n)$ can be represented by n integers each of which is $\ell(n)$-bits long. The input is an n-bit binary string $\vec{b}$ which indicates a subset of the n integers and the function outputs an integer s which is the sum of the subsets of integers indexed by $\vec{b}$. A family of universal one-way hash functions is the set of functions $\mathcal{F} = \{f\}$ which satisfies the property that if for all x, when f is chosen randomly from $\mathcal{F}$, then finding a collision (i.e., $y \neq x$ and $f(x) = f(y)$) is hard. Note that the random subset sum problem can be viewed as inverting a random subset sum function and the random collision problem is as finding a collision for a random subset sum function.

In the proof of Theorem 2.2.5 [IN96], Impagliazzo and Naor showed that finding a collision for a random subset sum function is at least as hard as inverting a random subset sum function. Therefore, we can give the following corollary:

Corollary 2.2.6. *The random subset sum problem with N a power of 2 and ρ a constant > 1 reduces to the random collision problem with the same N and ρ.*

This corollary will be used in the section 2.5.

2.3 The Dihedral Coset Space Problem

In this section we set up our approach. We first define the dihedral coset space problem and show how to use it to solve the dihedral coset problem. Then we define the coset space which we wish to understand.

Definition 2.3.1 (Dihedral Coset Space Problem (DCSP)). *Given a state $|\tau\rangle$ which is promised to be a random order-two coset state $|c^{(d)}_{x_1,x_2,\ldots,x_k}\rangle$ or a random standard basis state $|\vec{b}, x\rangle$ where $\vec{b} \in \mathbb{Z}_2^k$ and $x \in \mathbb{Z}_N^k$, the problem is to decide if $|\tau\rangle$ is a k-register order two coset state or not.*

A solution to the DCSP implies a polynomial-time algorithm for solving the DCP with N a power of 2 as shown in [FZ08]. We include a proof of our special case here.

Claim 2.3.2. *The dihedral coset problem (DCP) with N a power of 2 reduces to the dihedral coset space problem (DCSP).*

Proof. Suppose we are given the input of the DCP with subgroup d, we first show how to get the least significant bit of d.

Since N is a power of 2, the least significant bit of x and $x + d \pmod N$ are equal for $x \in \mathbb{Z}_N$ if and only if d is even. Therefore by measuring the least significant bit of the state $\frac{|0,x\rangle+|1,x+d\rangle}{\sqrt{2}}$, we get the same state if d is even and get either $|0, x\rangle$ or $|1, x + d\rangle$ (which are standard-basis states) otherwise.

According to the observation above, the least significant bit of d can be computed by the following algorithm. First, we measure the least significant bit of each register. Then all the registers do not change or collapse to a standard-basis state. Finally, apply the algorithm for the DCSP. If the result is an order-two coset state, the least significant bit is 0; otherwise, the least significant bit is 1.

To get bit $(i + 1)$, one subtracts d by the least significant i bits computed and measure the $I + 1$-th least significant bit of the state. Repeat the process above until all bits of d are known. □

It is worth noting that this fact also implies that the lattice problem can be reduced to the DCSP due to the known reduction from the lattice problem to the DCP with N a power of 2 [Reg04].

The main objects we want to understand are the coset space and its complement.

Definition 2.3.3. *The coset space $C = \mathrm{span}(\{|c^{(d)}_{x_1,\ldots,x_k}\rangle : d, x_1, \ldots, x_k \in \mathbb{Z}_N\})$ and the orthogonal complement of C is $C^\perp$.*

Note that a test for a vector being in C or $C^\perp$ is sufficient to solve the DCSP if k is big enough. This follows from counting the number of k-register order two coset states. There are at most N subgroups, and at most N^k coset representatives, so the number of k-register order two coset states is at most $N(N)^k$. The dimension of the whole space is $(2N)^k$. Hence, the subspace spanned by k-register order-two coset states is at most $1/2$ of the whole space when $k \geq \log 2N$.

Claim 2.3.4. *Let $k = \log 2N + k'$. Let Π_C be a projector onto C and $\Pi_{C^\perp}$ be a projector onto $C^\perp$. If the input is an order two coset state, the measurement $\{\Pi_C, \Pi_{C^\perp}\}$ outputs C always. Otherwise, if the input is a random standard basis state, then this measurement outputs $C^\perp$ with probability at least $1 - 1/2^{k'+1}$.*

2.4 The Subset Sum Basis

In this section, we start by finding an orthonormal basis for C and one for $C^\perp$. Note that if we can give a unitary which distinguishes which of the two subspaces we are in (C or $C^\perp$) efficiently, we can solve the DCSP efficiently as in Claim 2.3.4.

In order to make the basis easier to understand, we permute the subsystems so that the first bit of all registers are on the left, and the integers mod N are on the right. That is, write the original basis state $|b_1, x_1, b_2, x_2, \ldots, b_k, x_k\rangle$ as $|b_1, b_2, \cdots, b_k, x_1, x_2, \cdots, x_k\rangle$. In this notation the coset state is written as

$$|c^{(d)}_{x_1,x_2,\ldots,x_k}\rangle = \frac{1}{2^{k/2}} \sum_{b_1,\ldots,b_k=0}^{1} |b_1, \ldots, b_k, x_1+b_1 d, \ldots, x_k+b_k d\rangle = \frac{1}{2^{k/2}} \sum_{\vec{b}\in\{0,1\}^k} |\vec{b}, \vec{x}+\vec{b}d\rangle.$$

The subset sum basis is defined as follows:

Definition 2.4.1 (The Subset Sum Basis)**.** *Let $\vec{l} = (l_1, l_2, \cdots, l_k)^T \in \mathbb{Z}_N^k$, and $p \in \mathbb{Z}_N$. Let $T_{\vec{l},p} = \{\vec{b} : \vec{b}\cdot\vec{l} = p, \vec{b} \in \mathbb{Z}_2^k\}$ contain subset sum solutions for input $\vec{l}$, p. If $|T_{\vec{l},p}| = 0$ then define $|S^m_{\vec{l},p}\rangle = 0$. If $|T_{\vec{l},p}| \geq 1$, then let $m \in \{0, \ldots, |T_{\vec{l},p}| - 1\}$ and pick an ordering $\{\vec{b}^{(j)}_{\vec{l},p}\}$ of the solutions in $T_{\vec{l},p}$. Define the vector*

$$|S^m_{\vec{l},p}\rangle = \tfrac{1}{\sqrt{|T_{\vec{l},p}|}} \sum_{j=0}^{|T_{\vec{l},p}|-1} \omega^{mj}_{|T_{\vec{l},p}|} |\vec{b}^{(j)}_{\vec{l},p}\rangle. \tag{2.1}$$

For $N, k \in \mathbb{Z}$, define two sets

$$\mathcal{B}^\perp = \mathcal{B}^\perp_{k,N} = \{|S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle : \vec{l} \in \mathbb{Z}_N^k,\ p \in \mathbb{Z}_N,\ m \in \{1, \ldots, |T_{\vec{l},p}|-1\},\ |T_{\vec{l},p}| \geq 2\} \tag{2.2}$$

and

$$\mathcal{B}^0 = \mathcal{B}^0_{k,N} = \{|S^m_{l,p}\rangle|\chi_{\vec{l}}\rangle : \vec{l} \in \mathbb{Z}_N^k,\ p \in \mathbb{Z}_N,\ m = 0,\ |T_{\vec{l},p}| \geq 1\}. \tag{2.3}$$

The set $\mathcal{B} = \mathcal{B}^0 \bigcup \mathcal{B}^\perp$ is called the subset sum basis *of $\mathbb{C}^{(2N)^k}$.*

In this definition, $|\chi_j\rangle$ is the Fourier basis state $|\chi_j\rangle = \frac{1}{\sqrt{N}} \sum_i \omega_N^{ij} |i\rangle$, and $|\chi_{\vec{l}}\rangle = |\chi_{l_1}\rangle \cdots |\chi_{l_k}\rangle$. Note that $\mathcal{B}^0 \cup \mathcal{B}^\perp$ is an orthonormal basis for the whole space and the two sets are disjoint. The vector $|S^m_{\vec{l},p}\rangle$ is a superposition of solution vectors $\vec{b}$ to the equation $\vec{l} \cdot \vec{b} = p$. If no such $\vec{b}$ exists then there is no corresponding $|S^m_{\vec{l},p}\rangle$. If at least one solution $\vec{b}$ exists then $|S^0_{\vec{l},p}\rangle$ is in $\mathcal{B}^0$. If at least two solutions $\vec{b}$ exist then vectors appear in $\mathcal{B}^\perp$. Varying m gives orthogonal superpositions of the solutions. Ranging over all $\vec{l} \in \mathbb{Z}_N^k$ and $p \in \mathbb{Z}$ covers all possible bit vectors. Furthermore, these vectors are tensored with every possible Fourier basis state over $\mathbb{Z}_N$.

Next we show that $\mathcal{B}^\perp$ forms an orthonormal basis for $C^\perp$.

Claim 2.4.2. *The vectors in the set $\mathcal{B}^\perp$ form an orthonormal basis of a space that is orthogonal to the k-register order two coset space.*

Proof. As noted, the vectors form an orthonormal basis of the whole space. We will show that an arbitrary state in $\mathcal{B}^\perp$ is orthogonal to all k-register order two coset states. Fix $\vec{l}$ and p, and let

$$|\psi\rangle = |S^m_{\vec{l},p}\rangle |\chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}} \sum_{j=0}^{|T|-1} \omega_{|T|}^{mj} |\vec{b}^{(j)}\rangle |\chi_{\vec{l}}\rangle$$

be a state in $\mathcal{B}^\perp$ where $T = T_{\vec{l},p}$ and $\vec{b}^{(j)} = \vec{b}^{(j)}_{\vec{l},p}$ to simplify notation. Then for an arbitrary order-two coset state $|c^d_{x_1,x_2,\cdots,x_k}\rangle$, the inner product $\langle c^{(d)}_{x_1,x_2,\cdots,x_k} | \psi \rangle$ is

$$\begin{aligned}
\frac{1}{\sqrt{2^k|T|}} \sum_{\vec{b} \in \{0,1\}^k} \langle \vec{b} | \langle \vec{x} + \vec{b}d | \sum_{j=0}^{|T|-1} \omega_{|T|}^{mj} |\vec{b}^{(j)}\rangle |\chi_{\vec{l}}\rangle &= \frac{1}{\sqrt{2^k N^k |T|}} \sum_{j=0}^{|T|-1} \omega_{|T|}^{mj} \omega_N^{\vec{l} \cdot (\vec{x} + d\vec{b}^{(j)})} \\
&= \frac{\omega_N^{\vec{l} \cdot \vec{x}}}{\sqrt{2^k N^k |T|}} \sum_{j=0}^{|T|-1} \omega_{|T|}^{mj} \omega_N^{dp} \qquad (2.4) \\
&= \frac{\omega_N^{\vec{l} \cdot \vec{x} + dp}}{\sqrt{2^k N^k |T|}} \sum_{j=0}^{|T|-1} \omega_{|T|}^{mj} = 0. \qquad (2.5)
\end{aligned}$$

Eq. 2.4 is true because $\vec{b}^{(j)} \cdot \vec{l} = p$ iff $\vec{b}^{(j)} \in T$ by the definition of T. Then since $m \geq 1$ and $|T| \geq 2$ by the definition of $\mathcal{B}^\perp_{k,N}$, Eq. 2.5 is true. □

According to Claim 2.4.2, $\text{span}(\mathcal{B}^\perp) \subseteq C^\perp$. Next we show that $\mathcal{B}^0$ exactly spans the subspace C (and thus $\text{span}(\mathcal{B}^\perp) = C^\perp$).

Lemma 2.4.3. *The set $\mathcal{B}^0$ is an orthonormal basis for the subspace spanned by the order-two coset states.*

Proof. Because C is orthogonal to $\text{span}(\mathcal{B}^\perp)$ by Claim 2.4.2, $C \subseteq \text{span}(\mathcal{B}^0)$. We want to show equality. Suppose for contradiction that $C \subset \text{span}(\mathcal{B}^0)$. Then there is a vector $|\alpha\rangle \in C^\perp$ that is orthogonal to $\text{span}(\mathcal{B}^\perp)$, so $|\alpha\rangle \in C^\perp \cap \text{span}(\mathcal{B}^0)$. We show that there is no non-zero linear combination of states in $\mathcal{B}^0$ whose inner product with all order-two coset states is zero.

Suppose the state

$$|\alpha\rangle = \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} |S^0_{\vec{l},p}\rangle |\chi_{l_1}, \ldots, \chi_{l_k}\rangle$$

is orthogonal to all order-two coset states, i.e., $\langle c^{(d)}_{x_1,x_2,\ldots,x_k}|\alpha\rangle = 0$ for $x_1, \ldots, x_k, d \in \mathbb{Z}_N$, for some nonzero vector $|\alpha\rangle \in \text{span}(B^0)$. This inner product is

$$\begin{aligned}
& \frac{1}{\sqrt{2^k}} \sum_{\vec{b}\in\{0,1\}^k} \langle \vec{b}, \vec{x} + \vec{b}d | \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} |S^0_{\vec{l},p}\rangle |\chi_{l_1}, \ldots, \chi_{l_k}\rangle \\
= & \frac{1}{\sqrt{2^k}} \sum_{\vec{b}\in\{0,1\}^k} \langle \vec{b}, \vec{x} + \vec{b}d | \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} \frac{1}{\sqrt{|T_{\vec{l},p}|}} \sum_{j=0}^{|T_{\vec{l},p}|-1} |\vec{b}^{(j)}_{\vec{l},p}\rangle |\chi_{l_1}, \ldots, \chi_{l_k}\rangle \\
= & \frac{1}{\sqrt{2^k N^k}} \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} \frac{1}{\sqrt{|T_{\vec{l},p}|}} \sum_{\vec{b}\in\{0,1\}^k} \sum_{j=0}^{|T_{\vec{l},p}|-1} \langle \vec{b} | b^{(j)}_{\vec{l},p}\rangle \omega_N^{\vec{l}\cdot(\vec{x}+\vec{b}d)} \\
= & \frac{1}{\sqrt{2^k N^k}} \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} \frac{\omega_N^{\vec{l}\cdot\vec{x}+pd}}{\sqrt{|T_{\vec{l},p}|}} \sum_{\vec{b}:\vec{b}\cdot\vec{l}=p} \sum_{j=0}^{|T_{\vec{l},p}|-1} \langle \vec{b} | b^{(j)}_{\vec{l},p}\rangle \\
= & \frac{1}{\sqrt{2^k N^k}} \sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \alpha_{\vec{l},p} \omega_N^{\vec{l}\cdot\vec{x}+pd} \sqrt{|T_{\vec{l},p}|}.
\end{aligned}$$

Then we have the following equations:

$$\sum_{\vec{l}\in\mathbb{Z}_N^k, p\in\mathbb{Z}_N} \sqrt{\frac{|T_{\vec{l},p}|}{2^k N^k}} \alpha_{\vec{l},p} \cdot \omega_N^{x_1\cdot l_1 + \cdots + x_k \cdot l_k + d\cdot p} = 0, \, \forall x_1, \ldots, x_k, d \in \mathbb{Z}_N.$$

Define $\vec{v}$ as an $N^{k+1} \times 1$ vector such that $(\vec{v})_{\vec{l},p} = \sqrt{\frac{|T_{\vec{l},p}|}{2^k N^k}} \alpha_{\vec{l},p}$. The sums above

can be represented as follows:

$$A^{\otimes(k+1)} \cdot \vec{v} = \vec{0}, \tag{2.6}$$

where A is an $N \times N$ Fourier matrices with the (i,j)-th entry as $A_{i,j} = \omega_N^{ij}$ and $\vec{0}$ is an $N^{k+1} \times 1$ vector with all entries as 0. Note that the column of $A^{\otimes(k+1)}$ is indexed by $\vec{l}$ and p and the the row is indexed by $\vec{x}$ and d.

The determinant of $A^{\otimes(k+1)}$ is not zero, so the only vector $\vec{v}$ satisfying Equation 2.6 is $\vec{v} = \vec{0}$. When $|T_{\vec{l},p}| \geq 1$ this forces $\alpha_{\vec{l},p} = 0$ for every coefficient used in $|\alpha\rangle$. When $|T_{\vec{l},p}| = 0$, $\alpha_{\vec{l},p}$ is not used in the sum because $|S^m_{\vec{l},p}\rangle = 0$. Therefore, these facts contradict the hypothesis that there exists a nonzero vector $|\alpha\rangle \in \text{span}(\mathcal{B}^0)$ which is orthogonal to all order-two coset states. □

Now, it is easy to see that a unitary which can efficiently distinguish $\text{span}(\mathcal{B}^0)$ from $\text{span}(\mathcal{B}^\perp)$ also distinguishes C from $C^\perp$ by Claim 2.3.4 and Lemma 2.4.3. The next question we address is whether any unitaries that use this basis can be implemented efficiently or not.

2.5 The hardness results

In general we would like to understand unitaries that can be used to decide if a state is in the coset space C or in $C^\perp$. In this section we look at two types of unitaries using the subset sum basis, plus an extension of each one:

1. A unitary U_S that maps every basis vector $|S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle$ to a standard basis state. Note that if these standard basis states specify p and $\vec{l}$, then this can be used to solve the worst case subset sum, but we are allowing a more general type of unitary here.

2. A unitary U_C that maps every basis vector $|S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle$ to $|m = 0?\rangle|\phi^m_{\vec{l},p}\rangle$, indicating whether or not the state is in the coset space.

3. A unitary $U = \tilde{U}_S$ that satisfies condition (1) or $U = \tilde{U}_C$ that satisfies (2), but U uses a slightly more general basis, where any basis can be chosen for each $(\vec{l},p)$ subspace $\text{span}\{|S^m_{\vec{l},p},\chi_{\vec{l}}\rangle : m \geq 1\}$.

For the last type we use any basis satisfying the following definition.

Definition 2.5.1. *Let* $\tilde{\mathcal{B}}^0 = \mathcal{B}^0 = \{|S^0_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle : \vec{l} \in \mathbb{Z}_N^k, p \in \mathbb{Z}_N, m = 0, |T_{\vec{l},p}| \geq 1\}$ *be as in Definition 2.4.1, and let* $\tilde{\mathcal{B}}^\perp = \{|\tilde{S}^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle : \vec{l} \in \mathbb{Z}_N^k, p \in \mathbb{Z}_N, m \in \{1, \ldots, |T_{\vec{l},p}| - 1\}, |T_{\vec{l},p}| \geq 2\}$ *be an orthogonal basis such that* $\mathrm{span}(\{|\tilde{S}^m_{\vec{l},p}\rangle : m \in \{1, \ldots, |T_{\vec{l},p}| - 1\}\}) = \mathrm{span}(\{|S^m_{\vec{l},p}\rangle : m \in \{1, \ldots, |T_{\vec{l},p}| - 1\}\})$ *for all* $\vec{l}, p$.

We show that unitaries of type 1 above can be used to solve random subset sum for the cryptographic density ρ a constant greater than 1, indicating that such a unitary may be hard to implement. This strengthens the result in [BCvD06] which is a special case where the unitary must perform quantum sampling, i.e., map an input $|\vec{l}, p\rangle$ to a superposition of solutions $|\vec{l}, S^0_{\vec{l},p}\rangle$. Such a unitary implementing quantum sampling can used to solve worst-case subset sum by taking an input $|0, p, \vec{l}\rangle$, applying U inverse to get $|S^0_{\vec{l},p}\rangle|\vec{l}\rangle$ and measuring, since this is a uniform superposition of solutions.

An algorithm that uses the subset sum basis to solve the DCSP needs to decide if $m = 0$ (for C), or $m > 0$ (for $C^\perp$). The second type of unitary above allows an arbitrary unitary that writes the answer in the first bit. We show that such a unitary can solve random collision for density $\rho = 1 + c \log\log N / \log N$. This may indicate that no such unitary can be efficiently implemented, although we are less clear on the difficulty of the random collision problem.

The third type of unitary allows an arbitrary basis within each subspace of solutions, but does not mix solutions of different inputs $\vec{l}, p$. Note that $|S^0_{\vec{l},p}\rangle$ cannot change in this case, since it is one dimension in $\mathcal{B}^0$. Let $\tilde{\mathcal{B}} = \tilde{\mathcal{B}}^0 \cup \tilde{\mathcal{B}}^\perp$ be the basis used by the unitary.

The proofs work by using U_S to solve the worst-case collision problem, or U_C, $\tilde{U}_S$, or $\tilde{U}_C$ to solve the random collision problem.

2.5.1 Unitary mapping to a standard basis

First we give an algorithm that finds a solution to the worst-case collision problem when given a unitary U_S that maps the subset sum basis $\mathcal{B}$ to the standard basis in an arbitrary way. Given $\vec{b}$ and $\vec{l}$ where $\vec{b} \in \mathbb{Z}_2^k$ and $\vec{l} \in \mathbb{Z}_N^k$, the task in the worst-case collision problem is to find $\vec{b}' \neq \vec{b}$ such that $\vec{b}' \cdot \vec{l} = \vec{b} \cdot \vec{l}$.

Here QFT_N^k is the quantum Fourier transform over $\mathbb{Z}_N^k$.

Theorem 2.5.2. *If there exists an efficient unitary operator* U_S*, where* U_S *is a bijection between the subset sum basis and the standard basis, then the worst-*

On input $\vec{l} \in \mathbb{Z}_N^k$ and $\vec{b} \in \mathbb{Z}_2^k$:

1. Prepare the quantum state $|\vec{b}, \vec{l}\rangle$.
2. Apply QFT_N^k on $\vec{l}$, then the state becomes $|\vec{b}\rangle|\chi_{\vec{l}}\rangle$.
3. Apply U_S to $|\vec{b}\rangle|\chi_{\vec{l}}\rangle$.
4. Measure $U_S(|\vec{b}\rangle|\chi_{\vec{l}}\rangle)$ in the standard basis.
5. Apply $U_S^\dagger$.
6. Measure value $\vec{b'}$ in the first register.

case collision problem can be solved efficiently by a quantum algorithm. Therefore random subset sum with density a constant greater than 1 can also be solved.

Proof. Given $\vec{l}$ and $\vec{b}$ as input, let $p = \vec{l} \cdot \vec{b}$ and $T = T_{\vec{l},p}$. For $\vec{b} = \vec{b}^{(j_0)} \in T$, after computing the Fourier transform of the second register, the resulting state $|\vec{b}^{(j_0)}, \chi_{\vec{l}}\rangle$ can be wrtten in the subset sum basis as

$$|\vec{b}^{(j_0)}, \chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}} \sum_{m=0}^{|T|-1} \omega^{-j_0 m} |S_{\vec{l},p}^m\rangle|\chi_{\vec{l}}\rangle.$$

Applying U_S to this state gives the state

$$\frac{1}{\sqrt{|T|}} \sum_{m=0}^{|T|-1} \omega^{-j_0 m} |D_{\vec{l},p}^m\rangle, \tag{2.7}$$

where $|D_{\vec{l},p}^m\rangle := U_S(|S_{\vec{l},p}^m\rangle|\chi_{\vec{l}}\rangle)$ is a standard basis vector by assumption on U_S. Measuring the state in Equation (2.7) in the standard basis gives $|D_{\vec{l},p}^m\rangle$ for some $m \in [0 : |T| - 1]$. Applying $U_S^\dagger$ to $|D_{\vec{l},p}^m\rangle$ gives $|S_{\vec{l},p}^m\rangle|\chi_{\vec{l}}\rangle$, where the first register is $|S_{\vec{l},p}^m\rangle = \frac{1}{\sqrt{|T|}} \sum_{j=0}^{|T|-1} \omega^{jm} |\vec{b}^{(j)}\rangle$ in the standard basis. Measuring this gives a vector $\vec{b'} \neq \vec{b}$ with probability $\frac{|T|-1}{|T|}$.

Theorem 2.2.5 reduces random subset sum to solving the random collision problem for constant density greater than one, so random subset sum also reduces to the worst case collision problem. □

The proof that Algorithm 2.5.1 works used a special property of the subset

sum basis, which is that every basis vector $|S^m_{\vec{l},p}\rangle$ spreads the solutions with equal magnitude. When this is not the case then the algorithm does not work for the worst case collision problem. However, we will later show that it solves the random collision problem, as long as the number of solutions is not too large.

First we describe an example basis where the algorithm fails. The idea is that the unitary can map a solution vector $|\vec{b}, \chi_\ell\rangle$ to a vector that is very close to itself. In that case the algorithm will measure the same value $\vec{b}$ that it started with and not solve the collision problem, which can be seen as follows. Let $\vec{b} = \vec{b}^{(0)}$, let

$$|\hat{S}^1\rangle|\chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} |S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle,$$

and pick arbitrary orthonormal vectors $|\hat{S}^2\rangle, \ldots, |\hat{S}^{|T|-1}\rangle$ to form a basis for the subspace $\text{span}(\{|S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle : m \in [1 : |T|-1]\})$. Note that $|\langle\vec{b}, \chi_{\vec{l}}|\hat{S}^1, \chi_{\vec{l}}\rangle|^2 = \frac{|T|-1}{|T|}$, which implies that one gets $U_S(|\hat{S}^1\rangle|\chi_{\vec{l}}\rangle)$ with probability $\frac{|T|-1}{|T|}$ after applying U_S and measuring in the standard basis. In that case, applying $U_S^\dagger$ results in the input vector $\vec{b}$. Therefore, given a unitary mapping this new basis $\{|S^0, \chi_{\vec{l}}\rangle, |\hat{S}^1, \chi_{\vec{l}}\rangle, \ldots, |\hat{S}^{|T|-1}, \chi_{\vec{l}}\rangle\}$ to standard basis, the algorithm returns an answer $\vec{b}' \neq \vec{b}$ happens with probability $1/|T|$. The number of solutions $|T|$ can be very large for larger densities.

Next we show that if we limit the size of T, then random collision can be solved.

Corollary 2.5.3. *Suppose Algorithm 2.5.1 is run with $\tilde{U}_S$. If $\tilde{U}_S$ is an efficient unitary operator which maps every state in $\tilde{\mathcal{B}}$ to an arbitrary state in the standard basis, then on input $\vec{l}, \vec{b}$, the algorithm solves the collision problem with probability at least $\frac{1}{|T_{\vec{l},p}|}(1 - \frac{1}{|T_{\vec{l},p}|})$, where $p = \vec{l} \cdot \vec{b}$. In particular, when $k \leq \log N + c \log\log N$, the random collision problem can be solved in quantum polynomial time.*

Proof. Similar to the proof for Theorem 2.5.2, first represent $|\vec{b}, \chi_{\vec{l}}\rangle$ as a linear combination of states in $\tilde{\mathcal{B}}$ as follows:

$$|\vec{b}, \chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}}|S^0\rangle|\chi_{\vec{l}}\rangle + \sqrt{\frac{|T|-1}{|T|}}\Big(\sum_{m=1}^{|T|-1} c_m|\tilde{S}^m\rangle\Big)|\chi_{\vec{l}}\rangle,$$

where $T = T_{\vec{l},p}$ and $\tilde{S}^m = \tilde{S}^m_{\vec{l},p}$.

After applying the unitary $\tilde{U}_S$, the state is

$$\tilde{U}_S|\vec{b},\chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}}|D^0\rangle + \sqrt{\frac{|T|-1}{|T|}}(\sum_{m=1}^{|T|-1} c_m|D^m\rangle), \tag{2.8}$$

where D^m for $m \in [0 : |T| - 1]$ are arbitrary distinct states in the standard basis. By measuring the state in the Equation (2.8) in the standard basis, $|D^0\rangle$ is measured with probability $1/|T|$. Then applying $\tilde{U}_S^\dagger$ and measuring the output state in the standard basis gives $\vec{b}' \neq \vec{b}$ with probability $\frac{|T|-1}{|T|}$. Based on the Claim 2.6.1, $|T| = poly(k)$ with high probability. Thus, given a random input $\vec{b}$ and $\vec{l}$, the probability to get $\vec{b}' \neq \vec{b}$ using $\tilde{U}_S$ in Algorithm 2.5.1 is at least $\frac{|T|-1}{|T|^2} = 1/poly(k)$. □

2.5.2 Deciding membership in C

The unitary U_S illustrated how our algorithm works and used the subset sum basis, but U_S may not be useful for distinguishing C from $C^\perp$ in general. Next we consider a unitary U_C that can distinguish C from $C^\perp$. Suppose U_C works on a larger Hilbert space to have work space and exactly distinguishes $\mathcal{B}^0$ from $\mathcal{B}^\perp$ in the first qubit as follows:

Definition 2.5.4. *Let U_C be a unitary operator such that*

$$U_C(|S^m_{\vec{l},p}\rangle|\chi_{\vec{l}}\rangle|0\rangle) = \begin{cases} |0\rangle|\psi_{\vec{l},p,0}\rangle & \text{if } m = 0 \\ |1\rangle|\psi_{\vec{l},p,m}\rangle & \text{otherwise} \end{cases}$$

where $\{|\psi_{\vec{l},p,m}\rangle : \vec{l} \in \mathbb{Z}_N^k, p \in \mathbb{Z}_N, m \in [0 : |T_{\vec{l},p}| - 1]\}$ are states resulting from applying U_C and the third register is a workspace initialized to $|0\rangle$.

We modify Algorithm 2.5.1 so that only the first bit is measured in step four, and U_C is used instead of U_S.

Theorem 2.5.5. *If U_C can be implemented efficiently, then Algorithm 2.5.2 solves the collision problem on input $\vec{l}, \vec{b}$ with probability $\frac{2}{|T_{\vec{l},p}|}(1 - \frac{1}{|T_{\vec{l},p}|})$, where $p = \vec{l} \cdot \vec{b}$. In particular, when $k \leq \log N + c \log\log N$ the random collision problem can be solved in quantum polynomial time.*

On input $\vec{l} \in \mathbb{Z}_N^k$ and $\vec{b} \in \mathbb{Z}_2^k$:

1. Prepare the quantum state $|\vec{b}, \vec{l}\rangle$.
2. Apply QFT_N^k on $\vec{l}$, then the state becomes $|\vec{b}\rangle|\chi_{\vec{l}}\rangle$.
3. Apply U_C to $|\vec{b}\rangle|\chi_{\vec{l}}\rangle$.
4. Measure the first qubit of $U_C(|\vec{b}\rangle|\chi_{\vec{l}}\rangle)$ in the standard basis.
5. Apply $U_C^\dagger$.
6. Measure the first register in the standard basis.

Proof. Given $\vec{l}$ and $\vec{b}$ as input, let $p = \vec{l} \cdot \vec{b}$ and $T = T_{\vec{l},p}$. For $\vec{b} = \vec{b}^{(j_0)} \in T$, after computing the Fourier transform of the second register, we can write the resulting state $|\vec{b}^{(j_0)}, \chi_{\vec{l}}\rangle$ in the subset sum basis as follows:

$$|\vec{b}^{(j_0)}, \chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}} \sum_{m=0}^{|T|-1} \omega^{-j_0 m} |S_{\vec{l},p}^m\rangle|\chi_{\vec{l}}\rangle.$$

Applying U_C to this state plus a work register results in

$$\frac{1}{\sqrt{|T|}}(|0\rangle|\psi_{\vec{l},p,0}\rangle + \sum_{m=1}^{|T|-1} \omega^{-j_0 m}|1\rangle|\psi_{\vec{l},p,m}\rangle). \tag{2.9}$$

Measuring the first qubit of the state in Equation (2.9) gives $|0\rangle|\psi_{\vec{l},p,m}\rangle$ with probability $1/|T|$ and $\frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m}|1\rangle|\psi_{\vec{l},p,m}\rangle$ with probability $1 - 1/|T|$.

Applying $U_C^\dagger$ to the result gives $|S_{\vec{l},p}^0\rangle|\chi_{\vec{l}}\rangle$ in the first case and

$$\frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m}|S_{\vec{l},p}^m\rangle|\chi_{\vec{l}}\rangle$$

in the second case.

Finally, the state is measured in the standard basis. In the first case, when a zero is measured in the first bit, which happens with probability $1/|T|$, a vector $\vec{b}' \neq \vec{b}$ is measured with probability $1 - 1/|T|$ in the last step. In the second case

when a one is measured the amplitude of $|\vec{b}^{(j_0)}, \chi_{\vec{l}}\rangle$ in $\frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m} |S^m_{\vec{l},p}\rangle |\chi_{\vec{l}}\rangle$ is

$$\frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m} \langle \vec{b}^{(j_0)}, \chi_{\vec{l}} | S^m_{\vec{l},p}\rangle |\chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|-1}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m} \langle \vec{b}^{(j_0)} | S^m_{\vec{l},p}\rangle$$

$$= \frac{1}{\sqrt{(|T|-1)|T|}} \sum_{m=1}^{|T|-1} \omega^{-j_0 m} \omega^{j_0 m} = \frac{|T|-1}{\sqrt{(|T|-1)|T|}}.$$

Thus, the probability that the measurement gives $\vec{b}' \neq \vec{b}$ is $1 - \frac{(|T|-1)^2}{(|T|-1)|T|} = 1/|T|$. Therefore, the probability the algorithm returns $\vec{b}' \neq \vec{b}$ is $\frac{2}{|T|}(1 - \frac{1}{|T|})$.

By Claim 2.6.1 the probability that a randomly chosen $\vec{l}$ satisfies $|T_{\vec{l},p}| \leq poly(k)$ is at least $1/poly(k)$ when $k = \log N + c \log\log N$. Thus, the random collision problem can be solved by repeating the algorithm $poly(k)$ times. □

Now we consider the case where an arbitrary basis can be used within each subspace spanned by solutions of a given subset sum instance $\vec{l}$, p as in Definition 2.5.1. Let $\tilde{U}_C$ be a unitary that maps every state in $\tilde{\mathcal{B}}$ to quantum state whose first qubit indicates if the state is in $\tilde{\mathcal{B}}^0$ or $\tilde{\mathcal{B}}^\perp$

Corollary 2.5.6. *If Algorithm 2.5.2 is run with $\tilde{U}_C$ on input $\vec{l}, \vec{b}$, then it solves the collision problem with probability at least $\frac{1}{|T_{\vec{l},p}|}(1 - \frac{1}{|T_{\vec{l},p}|})$, where $p = \vec{l} \cdot \vec{b}$. In particular, if $k \leq \log N + c \log\log N$ then it solves the random collision problem in quantum polynomial time.*

Proof. Suppose $\tilde{U}_C$ maps $|S^0_{\vec{l},p}\rangle$ to a state $|0\rangle|\psi_{\vec{l},p,0}\rangle$ and maps $|\tilde{S}^m_{\vec{l},p}\rangle$ to $|1\rangle|\psi_{\vec{l},p,m}\rangle$ for $m \in [1 : |T|-1]$, where the set of vectors $\{|\psi_{\vec{l},p,m}\rangle : m \in [1 : |T|-1]\}$ are an arbitrary orthonormal set of quantum states. The analysis is similar to the proof above, but we only consider the case when the state collapses to $m = 0$. Specifically, after applying $\tilde{U}_C$ to $|\vec{b}, \chi_{\vec{l}}\rangle$, the state is

$$\tilde{U}_C |\vec{b}, \chi_{\vec{l}}\rangle = \frac{1}{\sqrt{|T|}} |0\rangle|\psi_{\vec{l},p,0}\rangle + \sqrt{\frac{|T|-1}{|T|}} \Big(\sum_{m=1}^{|T|-1} c_m |1\rangle|\psi_{\vec{l},p,m}\rangle \Big). \tag{2.10}$$

The probability the state collapses to $|0\rangle|\psi_{\vec{l},p,0}\rangle$ after measuring the first qubit is $1/|T|$. After applying $\tilde{U}_C^\dagger$ and measuring the state a vector $\vec{b}' \neq \vec{b}$ is measured with probability $1 - 1/|T|$. In total the probability of success is at least $\frac{|T|-1}{|T|^2}$.

For the choice of k given, this is at least $1/poly(k)$ with probability $1/poly(k)$ by Claim 2.6.1. □

2.6 Appendix

Claim 2.6.1. *Let $\vec{b} \in \mathbb{Z}_2^k$ be an arbitrary fixed vector with $k = \log N + c \log\log N$ for some constant c. Then over random choices of $\vec{l} \in \mathbb{Z}_N^k$, the probability that $|T_{\vec{l},\vec{b}\cdot\vec{l}}| \leq poly(k)$ is at least $\frac{1}{poly(k)}$.*

Proof. Fix $\vec{b} \in \mathbb{Z}_2^k$ and let $X_{\vec{b'}}$ be a random variable over $\vec{l}$ such that $X_{\vec{b'}} = 1$ if $\vec{b'} \cdot \vec{l} = \vec{b} \cdot \vec{l}$ and $X_{\vec{b'}} = 0$ otherwise. Then $|T_{\vec{l},\vec{l}\cdot\vec{b}}| = \sum_{\vec{b'} \in \mathbb{Z}_2^k} X_{\vec{b'}} = \sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} X_{\vec{b'}} + 1$.

For $\vec{b'} \neq \vec{b}$, the expected value of $X_{\vec{b'}}$ is $\mathrm{E}[X_{\vec{b'}}] = \mathrm{Prob}_{\vec{l}}(X_{\vec{b'}} = 1) = \mathrm{Prob}_{\vec{l}}(\vec{l} \cdot \vec{b'} = \vec{l} \cdot \vec{b}) = \frac{1}{N}$. The last equality can be seen by choosing i such that $b'_i = 1$ and $b_i = 0$ without loss generality ($\vec{b}$ and $\vec{b'}$ can be swapped if needed). Then by fixing l_j for $j \neq i$, and choosing l_i uniformly, $\vec{b} \cdot \vec{l}$ is fixed while $\vec{b'} \cdot \vec{l}$ is uniformly distributed. The variance of $X_{\vec{b'}}$ is $\mathrm{Var}(X_{\vec{b'}}) = \frac{1}{N} - \frac{1}{N^2}$.

Therefore, the expected value of $|T_{\vec{l},\vec{l}\cdot\vec{b}}| - 1$ is

$$\mathrm{E}[\sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} X_{\vec{b'}}] = \sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} \mathrm{E}[X_{\vec{b'}}] = \frac{2^k - 1}{N},$$

and the variance of $|T_{\vec{l},\vec{l}\cdot\vec{b}}| - 1$ is

$$\begin{aligned} \mathrm{Var}(\sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} X_{\vec{b'}}) &= \sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} \mathrm{Var}(X_{\vec{b'}}) + \sum_{\vec{b'} \neq \vec{b''}, \vec{b'}, \vec{b''} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} \mathrm{Cov}(X_{\vec{b'}}, X_{\vec{b''}}) \\ &\leq \frac{2^k - 1}{N} + \sum_{\vec{b''} \neq \vec{b'}, \vec{b'}, \vec{b''} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} \mathrm{Cov}(X_{\vec{b'}}, X_{\vec{b''}}). \end{aligned} \tag{2.11}$$

This results in $\mathrm{Var}(\sum_{\vec{b'} \in \mathbb{Z}_2^k \setminus \{\vec{b}\}} X_{\vec{b'}}) \leq \frac{2^k - 1}{N}$ provided that the covariences are all zero, which we show below. First we finish proving the claim by applying Chebyshev's inequality to get

$$\mathrm{Prob}(|T_{\vec{l},\vec{b}\cdot\vec{l}}| \geq poly(k)) \leq \frac{2^k - 1}{N} \frac{1}{poly(k)} = \frac{1}{poly(k)},$$

when $k \leq \log N + c \log\log N$.

In the following, we show that $X_{\vec{b}'}$ and $X_{\vec{b}''}$ are independent when $\vec{b}$, $\vec{b}'$, and $\vec{b}''$ are all different values, which implies $\mathrm{Cov}(X_{\vec{b}'}, X_{\vec{b}''}) = 0$. To see this let 1 be a coordinate such that $b'_1 = 1$ and $b''_1 = 0$ without loss of generality (b'_j and b''_j can be swapped). If $b_1 = 0$, then

$$\begin{aligned}
& \mathrm{Prob}_{\vec{l}}(X_{\vec{b}'} = 1, X_{\vec{b}''} = 1) \\
= & \sum_{l_2,\ldots,l_k=0:}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}'} = 1, X_{\vec{b}''} = 1 | l_2, \ldots, l_k) \cdot \mathrm{Prob}(l_2, \ldots, l_k) \\
= & \frac{1}{N^{k-1}} \sum_{l_2,\ldots,l_k=0}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}'} = 1 | l_2, \ldots, l_k) \cdot \mathrm{Prob}_{l_1}(X_{\vec{b}''} = 1 | l_2, \ldots, l_k) \quad (2.12) \\
= & \frac{1}{N} \cdot \frac{1}{N^{k-1}} \sum_{l_2,\ldots,l_k=0}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}''} = 1 | l_2, \ldots, l_k) \\
= & \frac{1}{N} \cdot \frac{1}{N^{k-1}} \cdot N^{k-2} = \frac{1}{N^2}. \quad (2.13)
\end{aligned}$$

Equation 2.12 is true because $X_{b''}$ is fixed after fixing $l_2, \ldots, l_k$. For Equation 2.13 note that $\vec{b}$ and $\vec{b}''$ differ in at least one bit besides position $i = 1$. Therefore a $1/N$ fraction of the N^{k-1} choices for $l_2, \ldots, l_k$ satisfy $\vec{l} \cdot \vec{b} = \vec{l} \cdot \vec{b}''$.

In the case where $b_1 = 1$ the properties of $X_{\vec{b}'}$ and $X_{\vec{b}''}$ are reversed:

$$\begin{aligned}
& \mathrm{Prob}_{\vec{l}}(X_{\vec{b}'} = 1, X_{\vec{b}''} = 1) \\
= & \sum_{l_2,\ldots,l_k=0}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}'} = 1, X_{\vec{b}''} = 1 | l_2, \ldots, l_k) \cdot \mathrm{Prob}(l_2, \ldots, l_k) \\
= & \frac{1}{N^{k-1}} \sum_{l_2,\ldots,l_k=0}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}'} = 1 | l_2, \ldots, l_k) \cdot \mathrm{Prob}_{l_1}(X_{\vec{b}''} = 1 | l_2, \ldots, l_k) \quad (2.14) \\
= & \frac{1}{N} \frac{1}{N^{k-1}} \sum_{l_2,\ldots,l_k=0}^{N-1} \mathrm{Prob}_{l_1}(X_{\vec{b}'} = 1 | l_2, \ldots, l_k) \\
= & \frac{1}{N} \cdot \frac{1}{N^{k-1}} \cdot N^{k-2} = \frac{1}{N^2}. \quad (2.15)
\end{aligned}$$

Equation 2.14 is true because $X_{\vec{b}'}$ is fixed to 0 or 1 for all l_1. Equation 2.15 is true because $\vec{b}$ and $\vec{b}'$ differ in at least one bit besides $i = 1$.

Therefore, the covariance of $X_{\vec{b}'}$ and $X_{\vec{b}''}$ is 0.

□

Chapter 3
On basing one-way permutations on NP-hard problems under quantum reductions

3.1 Introduction

A fundamental question in complexity theory is whether or not worst-case problems have reductions to average-case problems. When reducing worst-case problems to average-case problems of the same type, these are called random-self-reductions. These have many applications (see [FF93]), including the question of whether or not cryptographic primitives can be based on NP-complete problems. Random-self-reductions exist for complete sets of some classes such as PSPACE, EXP and #P. It is unknown if such reductions exist for NP-complete problems. Fortnow and Feigenbaum [FF93] 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. Basing cryptography on NP-hardness is by reducing NP-complete problems to breaking average-case security of cryptosystems. However, the pursuit along this line has largely ended up negative. For instance, if one can reduce NP-complete problems to inverting

one-way permutations [Bra79], size-verifiable one-way functions [AGGM06, BB15], single-server single-round private information retrieval [LV15], or weak fully homomorphic evaluation of sensitive collection of functions [BL13], 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?

Quantum reductions have been shown to be useful in cryptography. In [Reg04], Regev showed that the unique shortest vector problem reduces to random subset sum problems via a quantum reduction. In addition, gapSVP and SIVP reduce to LWE via quantum reductions [Reg05]. There are no known classical reductions between these problems under the same parameters. 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 [KY10] proved several hard-core predicates using quantum reductions, inspired by earlier work on the quantum Goldreich-Levin theorem [AC02] and the quantum algorithm for the Legendre symbol [VDHI06].

In order to draw conclusions based on the existence of reductions, it is important to define a general model that captures a wide range of reduction types. Classically there are two types of reductions which we will consider. The first is called a *locally random reduction* [FF93]. In this model, there are two classical algorithms G and R, where the first algorithm G generates queries to the oracle for the average-case problem according to a given distribution, and the second algorithm R uses the answers to solve the worst-case problem.

The second type of reduction is called a *worst-case to average-case reduction*, defined by Bogdanov and Trevisan [BT06]. In this model there are also two classical algorithms G and R, one to generate queries and the other to use the answers and solve the problem. However, in this model, G can generate queries in an arbitrary way, but the oracle is allowed to answer incorrectly on some predefined set of queries.

In this work, we give two examples where quantum reductions from worst-case to average-case reduction exist but classical reductions do not. The main contribution, however, is showing that the existence of some quantum reductions implies unknown consequences in complexity. We consider the quantum analogues of locally random reductions and worst-case to average-case reductions. We define

locally quantum reductions to consist of two quantum circuits G and R. The unitary G generates superposition queries for the oracle of the average-case problem with the restriction that the coefficients of those queries match a given distribution. The unitary R solves the problem based on the answers from the oracle. We define *quantum worst-case to average-case reductions* to also be described by two quantum circuits G and R. The unitary G generates arbitrary superposition queries for the average-case problem. The unitary R uses the results of the queries to solve the worst-case problem. As in the classical case, this oracle may answer incorrectly on some predefined set of queries. Both locally random reductions and worst-case to average-case reductions are special cases of their quantum analogues. We describe our main theorems informally:

Theorem 3.1.1. *The existence of locally quantum reductions or worst-case to average-case reductions with the restriction that the queries are non-adaptive and are according to known smooth-computable distributions from NP-complete problems (or QMA-complete problems) to the task of inverting one-way permutations implies coNP $\subseteq$ QIP(2) (or coQMA $\subseteq$ QIP(2)).*

A distribution is smooth-computable if its maximum and minimum are only polynomially larger and smaller than the average. In particular, this handles uniform distributions.

The containment coNP $\subseteq$ QIP(2) is not as strong as the classical result that the polynomial hierarchy collapses. However, we note that so far only a few problems are known to be in QIP(2) that are not known to be in AM or QMA. Hence, if coNP is not contained in AM and QMA, then it also appears unlikely to be in QIP(2).

In order to describe the approach, we first describe the classical approach. The classical proof strategy is to assume that a language L has a random reduction to some problem L', and then construct an interactive proof for $\overline{L}$ that creates 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 $\overline{L}$. Then one can conclude that if such a reduction exists, then coNP $\subseteq$ AM, giving a collapse. There are much more complicated constructions, for example, for reducing to NP-complete 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 reductions it is possible to construct a protocol for $\overline{L}$.

In order to follow the same proof strategy as the classical case, we use the unitaries G and R from the reduction to create 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 difficultly 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 [BT06] 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 problem we must solve is how to ensure that the prover provides the answers 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. We must show that if the prover returns such a state, then the verifier has some way to detect this. In order to do this, we show it is possible to send 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.

One interesting aspect of this work is that it provides an example of a QIP(2)

protocol. Compared to QIP(3) = PSPACE and QIP(1) = QMA, less is known about the power of QIP(2). Rosgen defined a complete problem for QIP(2), called the close image problem. This problem resembles the acceptance condition for the verifier in a quantum interactive proof system [Ros09]. There are two QIP(2) protocols for other problems. The first is for testing the separability of a bipartite state generated by a quantum circuit [HMW14]. The second studies a generalized version of public coins to the quantum setting, where instead of coins, EPR pairs are used [KLGN15]. Both of these protocols have a definition which lends itself to QIP(2). The problems in [HMW14, KLGN15] are defined in a way that is close to the statement of Ulhmann's theorem, which makes it possible to apply Uhlmann's theorem to construct a QIP(2) protocol for these problems.

There are several open questions. Do adaptive and/or non-smooth-computable quantum reductions from NP-complete problems to inverting one-way permutations exist? For cryptographic primitives which security are not based on NP-complete problems under classical reductions, can NP-complete problems reduce to them if quantum reductions are allowed? Is it possible to rule out a non-adaptive reduction from NP-hard problems to average-case problems in NP, as in [BT06]? Since we know very little about QIP(2), can we show that QIP(2) $\neq$ QMA, QIP(2) $\neq$ AM, or coNP$\not\subseteq$ QIP(2)?

3.2 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 captial 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 per-*

mutations.

Definition 3.2.1 (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 quantum messages 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 $2/3$ by exchanging at most m messages.*
- *(Soundness) For $x \in A_{no}$, no prover can convince the verifier with probability greater than $1/3$ by exchanging at most m messages.*

The length of the messages exchanged between the verifier and the prover can be bounded by $O(\mathrm{poly}(|x|))$.

Without loss of generality, the behaviors of the prover and the verifier can always be described as unitaries. It has been shown that QIP(m)=QIP(3)=PSPACE for $m > 3$ [KW00,JJUW11]. In this work, we focus on the class QIP(2). It is known that completeness and soundness can be reduced to negligibly small [JUW09].

Definition 3.2.2 (One-way permutation)**.** *$f : \{0,1\}^* \to \{0,1\}^*$ 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,* $\Pr_{x \leftarrow \{0,1\}^n}(A(f(x)) = x) = \mathrm{negl}(n)$.

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

3.2.1 Locally random reductions and worst-case to average-case reductions

We review classical definitions of worst-case to average-case reductions. The basic notion is a *distributional* problem. We denote $\mathcal{P}'$ an arbitrary decision problem, search problem or promise problem. We will only consider the case where $\mathcal{P}'$ corresponds to inverting one-way permutations.

Definition 3.2.3. *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 $\mathcal{P}'(x)$.*

We first adapt a notion of Feigenbaum and Fortnow [FF93].

Definition 3.2.4 (non-adaptive locally random reduction (G, R))**.** *Let k and ℓ be variables polynomial in the input length n and let $r \leftarrow \{0,1\}^\ell$. A decision problem $\mathcal{P}$ is* non-adaptively locally random reducible *to a distributional problem $(\mathcal{P}', \mathcal{D})$ if there are polynomial-time algorithms R and G satisfying:*

- *For all n and $x \in \{0,1\}^n$, $\mathcal{P}(x) = R(x, r, \mathcal{P}'(G(1, x, r)), \ldots, \mathcal{P}'(G(k, x, r)))$ for at least $3/4$ of all $r \in \{0,1\}^\ell$.*
- *For $1 \leq i \leq k$, if $x_1 \neq x_2$ and $|x_1| = |x_2|$ then $\Pr_r[G(i, x_1, r) = y] = \Pr_r[G(i, x_2, r) = y] = \Pr[y \sim \mathcal{D}_{|x_1|}]$.*

We note that Definition 3.2.4 is equivalent to the Definition 2.1 in [FF93]. In Definition 3.2.4, we assume that all queries are drawn from the same distribution instead of different distributions. However, the assumption 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 [FKN90]. One can also define *adaptive* locally random reductions by allowing the algorithm G in Definition 3.2.4 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 [FF93]. It has been shown that the set of complete problems in PSPACE, EXP and #P are random-self reducible [FF93]. 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 [FF93].

The definition of Feigenbaum and Fortnow assumes a perfect solver for the average-case problem [FF93]. This restriction is weakened in a later work by Bogdanov and Trevisan [BT06].

Definition 3.2.5 (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 at random 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 *if there are polynomial-time algorithms* R *and* G *satisfying the properties that: For any* $n \in \mathbb{N}$

- *On all inputs* $x \in \{0,1\}^n$, $G(x,r)$ *outputs* $y_1, \ldots, y_k$.
- *For any* $\mathcal{P}''$ *which is* δ*-close to* $\mathcal{P}'$ *with respect to* $\mathcal{D}$,

$$\Pr_r[R(x, r, \mathcal{P}''(y_1), \ldots, \mathcal{P}''(y_k)) = \mathcal{P}(x)] > 2/3.$$

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 [BT06]. 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 [AGGM06] 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 [AGGM06, BB15].

3.3 Locally quantum reductions and quantum worst-case to average-case reductions

In this section we define the quantum analogues of non-adaptive locally random reductions given in Definition 3.2.4 and non-adaptive worst-case to average-case reductions given in Definition 3.2.5, which are introduced in Section 3.2.1.

Definition 3.3.1 (non-adaptive locally quantum reduction (G, R))**.** *A decision problem* $\mathcal{P}$ *is* non-adaptive locally quantum reducible *to a distributional problem* $(\mathcal{P}', \mathcal{D})$ *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* $i \in [k]$ *and* d_q *is the probability that* q *is drawn from* $\mathcal{D}_n$

- R *takes responses of the queries and decides whether or not* $\mathcal{P}(x)$ *is true:*

$$R|Q^H_{x,1},\ldots,Q^H_{x,k}\rangle = \sqrt{p}|\mathcal{P}(x)\rangle|\psi^0_x\rangle + \sqrt{1-p}|1-\mathcal{P}(x)\rangle|\psi^1_x\rangle$$

where $p \geq 2/3$ *and* $|Q^H_{x,i}\rangle = \sum_{q\in\mathbb{Z}_2^m} \sqrt{d_q}|q,\mathcal{P}'(q)\rangle_M|w_{x,i}(q)\rangle_V$*, for* $i \in [k]$*.*

We introduce δ-close problems to defint the generalized notion of worst-case to average-case reduction.

Definition 3.3.2. *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 3.3.3 (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 *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:*

$$G|0\rangle_{MV}|x\rangle = |Q_{x,1}\rangle \otimes \cdots \otimes |Q_{x,k}\rangle|x\rangle, \tag{3.1}$$

where $|Q_{x,i}\rangle = \sum_{q\in\mathbb{Z}_2^m} c_{x,q,i}|q,0\rangle_M|w_{x,i}(q)\rangle_V, \quad$ *for* $i \in [k]$*.*

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

$$R|Q^H_{x,1},\ldots,Q^H_{x,k}\rangle = \sqrt{p}|\mathcal{P}(x)\rangle|\psi^0_x\rangle + \sqrt{1-p}|1-\mathcal{P}(x)\rangle|\psi^1_x\rangle, \tag{3.2}$$

where $p \geq 2/3$ *and* $|Q^H_{x,i}\rangle = \sum_{q\in\mathbb{Z}_2^m} c_{x,q,i}|q,\mathcal{P}''(q)\rangle_M|w_{x,i}(q)\rangle_V$*, 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.

3.3.1 Discussion of the definitions: special cases

Classical queries. If G outputs classical queries, then we can already derive a negative result, analogous to a classical result by Brassard [Bra79].

Theorem 3.3.4. *If there is a non-adaptive quantum reduction $L \leq_{R,G}$ Inv-OWP where G produces* 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 R accepts. Otherwise, the verifier rejects. Note that the prover can only give the correct answer for Inv-OWP. Otherwise, the verifier rejects. □

The proof for Theorem 3.3.4 above is similar to the proof in [Bra79] except that the verifier who applies quantum reduction needs to send the queries by itself. The reason is that the randomness of a quantum circuit is from the nature of quantum mechanism. So, the verifier cannot make its randomness to be public. In addition, we do not know if the theorem above is correct when the quantum reduction is adaptive.

EPR queries. As another special case, we consider that $w_{x,i}(q)$ is the identity function in Definition 3.3.1. 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 3.3.5. *If there is a reduction $L \leq_{R,G}$ Inv-OWP where G issues EPR-queries, then $L \in BQP$.*

Proof. The key (and simple) observation is 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:

$$\begin{aligned} |0,0,0\rangle &\mapsto \sum_q |q,0,0\rangle \\ &\overset{f}{\mapsto} \sum_q |q,f(q),f(q)\rangle = \sum_{q'} |f^{-1}(q'),q',q'\rangle \\ &\overset{\mathrm{SWAP}_{1,3}}{\mapsto} \sum_{q'} |q',q',f^{-1}(q')\rangle\,. \end{aligned}$$

□

Remark 1. *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.*

3.4 Uniform one-query locally quantum reduction to Inv-OWP

In this section we consider quantum reductions that make *one-query* only. It demonstrates the main idea of our general result with a cleaner analysis. Section 3.5 will handle multiple non-adaptive queries. Let f be a one-way permutation on $\{0,1\}^n$, and let U_f be a unitary quantum circuit computing it. That is, $U_f|x,0\rangle = |x,f(x)\rangle$. 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:

$$|x,0\rangle|0\rangle \xrightarrow{G} \frac{1}{\sqrt{2^m}} \sum_{q\in\mathbb{Z}_2^m} |q,0\rangle|w_x(q)\rangle \tag{3.3}$$

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

$$\xrightarrow{R} a_0|0\rangle|\psi_{x,0}\rangle + a_1|1\rangle|\psi_{x,1}\rangle, \tag{3.4}$$

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.

The main theorem we are going to prove in this section is

Theorem 3.4.1. *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 $\overline{L}$*

To prove Theorem 3.4.1, we are going to give a QIP(2) protocol for $\overline{L}$ by using the reduction.

3.4.1 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: $|q,x\rangle_M|y,z\rangle_V \xrightarrow{C} |q,x\rangle_M|y,z\oplus q\rangle_V$. 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

$$|Q\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q\in\mathbb{Z}_2^m} |q,0\rangle_M|w_x(q),q\rangle_V \tag{3.5}$$

  without the extra copy of q in the register V is the query state generated

from G as in Equation 3.3, and

$$|T\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, 0\rangle_M |0, q\rangle_V \tag{3.6}$$

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

$$|Q^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |w_x(q), q\rangle_V \tag{3.7}$$

$$|T^H\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |0, q\rangle_V. \tag{3.8}$$

  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 3.4. 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 $|T^H\rangle$ has been changed a lot.

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

$$\begin{aligned}
\sum_{q \in \mathbb{Z}_2^m} |q, f^{-1}(q)\rangle_M |0, q\rangle_V &\xrightarrow{C} \sum_q |q, f^{-1}(q)\rangle_M |0, q \oplus q\rangle_V \\
&\xrightarrow{U_f} \sum_q |q \oplus f(f^{-1}(q)), f^{-1}(q)\rangle_M |0, 0\rangle_V \\
&\xrightarrow{F} |0, 0\rangle_M |0, 0\rangle_V.
\end{aligned}$$

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 QIP(2) protocol for L by answering the same as R and a protocol for $\overline{L}$ by flipping R's answer. The QIP(2) protocol for $\overline{L}$ is described in Protocol 1.

3.4.2 Lemmas for proving Theorem 3.4.1

In this section, we prove Lemma 3.4.2, Lemma 3.4.4 and Claim 3.4.3, which we use to prove Theorem 3.4.1.

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).

Lemma 3.4.2 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 [Sch96].

Lemma 3.4.2. *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 oper-

ating only on B such that $I_A \otimes U_B|\psi\rangle_{AB} = |\phi\rangle_{AB}$. Then

$$\begin{aligned}
& \langle\phi|\rho_{AB}|\phi\rangle \\
= \; & \langle\phi|(\Psi_A \otimes I_B)((|\phi\rangle\langle\phi|)_{AB})|\phi\rangle \\
= \; & \langle\psi|(I_A \otimes U_B^\dagger)(\Psi_A \otimes I_B)(I_A \otimes U_B(|\psi\rangle\langle\psi|)_{AB} I_A \otimes U_B^\dagger)(I_A \otimes U_B)|\psi\rangle \\
= \; & \sum_\ell \langle\psi|(I_A \otimes U_B^\dagger)(E_A^\ell \otimes I_B)(I_A \otimes U_B(|\psi\rangle\langle\psi|)_{AB} I_A \otimes U_B^\dagger) \\
& (E_A^{\ell\dagger} \otimes I_B)(I_A \otimes U_B)|\psi\rangle \qquad (3.9) \\
= \; & \sum_\ell \langle\psi|(E_A^\ell \otimes I_B)((|\psi\rangle\langle\psi|)_{AB})(E_A^{\ell\dagger} \otimes I_B)|\psi\rangle \qquad (3.10) \\
= \; & \langle\psi|(\Psi_A \otimes I_B)((|\psi\rangle\langle\psi|)_{AB})|\psi\rangle \\
= \; & \langle\psi|\sigma_{AB}|\psi\rangle.
\end{aligned}$$

The operators $\{E_A^\ell\}$ in Equation 3.9 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 3.10 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

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

and

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

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

Claim 3.4.3. *For an arbitrary U'_{PM}, let $|Q^H\rangle_{MV}$ and $|T^H\rangle_{MV}$ be as defined in Equation 3.7 and Equation 3.8, 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,

$$(\Psi_M^{U'} \otimes I_V)(|Q^H\rangle\langle Q^H|) = \sigma_Q^{U'}$$

and

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

$|T^H\rangle$ 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 3.4.2, 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 3.4.4 is shows that the state ρ which maximizes the quantity $\mathrm{Tr}(\Pi_S\rho) + \langle\phi|\rho|\phi\rangle$ is the bijection of $|\phi\rangle$ and its projection on Π_S.

Lemma 3.4.4. *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 $\rho \in D(\mathcal{H})$, $\mathrm{Tr}(\Pi_S\rho) + \langle\phi|\rho|\phi\rangle \leq 1 + \sin\theta$.*

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 $\tilde{S} := \mathrm{span}(S \cup |\phi\rangle)$. Consider any $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \tilde{S}$. Then $|\psi\rangle$ can be writen as

$$|\psi\rangle = \sum_{i=0}^{k} \alpha_i|v_i\rangle, \quad \sum_i |\alpha_i|^2 = 1\,. \tag{3.11}$$

We have that

$$\begin{aligned}\langle\phi|(|\psi\rangle\langle\psi|)|\phi\rangle &= |\alpha_0\sin\theta + \alpha_k\cos\theta|^2 \\ &= |\alpha_0|^2\sin^2\theta + |\alpha_k|^2\cos^2\theta + \sin\theta\cos\theta(\alpha_0\alpha_k^* + \alpha_0^*\alpha_k)\,;\end{aligned}$$

$$\mathrm{Tr}(\Pi_S|\psi\rangle\langle\psi|) \;=\; \sum_{i=0}^{k-1}|\alpha_i|^2 = 1-|\alpha_k|^2\,.$$

Therefore

$$\begin{aligned}
&\mathrm{Tr}(\Pi_S|\psi\rangle\langle\psi|) + \langle\phi|(|\psi\rangle\langle\psi|)|\phi\rangle && (3.12)\\
&= 1+\sin^2\theta|\alpha_0|^2 + (\cos^2\theta-1)|\alpha_k|^2 + \sin\theta\cos\theta(\alpha_0\alpha_k^* + \alpha_0^*\alpha_k)\\
&= 1+\sin\theta\cdot\Big(\sin\theta(|\alpha_0|^2-|\alpha_k|^2) + \cos\theta(\alpha_0\alpha_k^*+\alpha_0^*\alpha_k)\Big)\\
&\le 1+\sin\theta\cdot(\sin\theta(|\alpha_0|^2-|\alpha_k|^2) + 2\cos\theta(|\alpha_0||\alpha_k|)). && (3.13)
\end{aligned}$$

Since the expression in Equation 3.13 is strictly increasing with $|\alpha_0|$ and independent to $|\alpha_1|,\ldots|\alpha_{k-1}|$, we can suppose the optimal $|\psi\rangle$ for Equation 3.12 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 3.13 as below

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

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 $\sum_i p_i = 1$, $p_i \ge 0$.

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

□

3.4.3 Proof of Theorem 3.4.1

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 of the protocol.

Proof of Theorem 3.4.1. 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 Claim 3.4.3, 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 3.4.4, the maximum is achieved by a state bisecting $|Q^H\rangle$ and its projection on S_{acc}, and we conclude that $p_{\text{succ}} = \frac{1}{2}(\text{Tr}(\Pi_R\rho_0) + \langle Q^H|\rho_0|Q^H\rangle) \leq \frac{1}{2}(1+\sqrt{\varepsilon})$.

□

Corollary 3.4.5. *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 coNP* $\subseteq$ *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 3.4.1, $\overline{L} \in QIP(2)$, hence $coNP \subseteq QIP(2)$. □

Corollary 3.4.6. *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 coQMA* $\subseteq$ *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 3.4.1, $\overline{L} \in QIP(2)$. This implies $coQMA \subseteq QIP(2)$. □

3.5 Uniform non-adaptive locally quantum reduction to Inv-OWP

In Section 3.4, we concern the special case of locally quantum reduction with only one query and negligible error. In this section, we are going to generalize Theorem 3.4.1 such that the existence of a uniform non-adaptive (multiple-queries) locally quantum reduction with constant error implies coNP⊆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:

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

$$\begin{aligned}
&\xrightarrow{O_{f^{-1}}} \quad \frac{1}{\sqrt{2^{mk}}} \sum_{q_1,\ldots,q_k \in \mathbb{Z}_2^m} |q_1, f^{-1}(q_1), w_{x,1}(q_1)\rangle \otimes \cdots \otimes |q_k, f^{-1}(q_k), w_{x,k}(q_k)\rangle \\
&\xrightarrow{R} \quad a_0|0\rangle|\psi_{x,0}\rangle + a_1|1\rangle|\psi_{x,1}\rangle,
\end{aligned}$$

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 3.5.1. *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 $QIP(2)$ protocol with completeness $1 - \epsilon/2$ and soundness $1/2 + 2\sqrt{\epsilon}$ for $\overline{L}$, where ϵ is negligible.*

3.5.1 Main theorem

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 3.5.2 (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 $|Q^H_{x,1}, \ldots, Q^H_{x,k}\rangle$ 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. □

We are going to show that such reduction does not exist unless coNP $\subseteq$ QIP(2).

Proof. The error can be reduced to an exponentially small parameter ϵ by applying Lemma 3.5.2. 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 QIP(2) protocol which is similar to the protocol in Protocol 1 for $\overline{L}$.

By Lemma 3.5.2, 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').

Now, we introduce the new 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

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

Note that i indicates the i-th copy which is generated from the parallel repetition in Lemma 3.5.2. Also, the verifier generates $|T\rangle^{\otimes tk}$, where $|T\rangle$ is defined in Equation 3.6.

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:

$$|Q_{1,1}, \ldots, Q_{t,k}\rangle \;\; \rightarrow \;\; |\hat{Q}\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, 0\rangle_M |w_x(\hat{q}), \hat{q}\rangle_V \tag{3.14}$$

and

$$|T\rangle^{\otimes k} \;\; \rightarrow \;\; |\hat{T}\rangle_{MV} = \frac{1}{2^{mkt/2}} \sum_{\hat{q} \in \mathbb{Z}_2^{mkt}} |\hat{q}, 0\rangle_M |0, \hat{q}\rangle_V. \tag{3.15}$$

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

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

and

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

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 3.4.

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

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

and

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

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,

$$\langle\hat{Q}^H|\hat{\sigma}_Q^{U'}|\hat{Q}^H\rangle = \langle\hat{T}^H|\hat{\sigma}_T^{U'}|\hat{T}^H\rangle \tag{3.16}$$

by Lemma 3.4.2. Then, we do a similar calculation as in the proof of soundness for Theorem 3.4.1, which gives an upper bound $1/2 + \sqrt{\epsilon}$ on the probability that the verifier accepts. □

The following two corollaries follow from Theorem 3.5.1, which proofs are the same as the proof for Corollary 3.4.5 and Corollary 3.4.6.

Corollary 3.5.3. *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 3.5.4. *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).

3.6 Smooth locally quantum reductions to Inv-OWP

In this section, we study non-adaptive quantum reductions which generate queries according to smooth-computable distributions. We show that the existence of such reductions 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 [ORR13] to prevent the prover from cheating.

Definition 3.6.1 (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-computatble 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 before.

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:

$$
\begin{aligned}
|x,0\rangle|0\rangle &\xrightarrow{G} \frac{1}{\sqrt{2^m}} \sum_{q\in\mathbb{Z}_2^m} \sqrt{d_q}|q,0\rangle|w_x(q)\rangle && (3.17)\\
&\xrightarrow{O_{f^{-1}}} \frac{1}{\sqrt{2^m}} \sum_{q\in\mathbb{Z}_2^m} \sqrt{d_q}|q,f^{-1}(q)\rangle|w_x(q)\rangle \\
&\xrightarrow{R} a_0|0\rangle|\psi_{x,0}\rangle + a_1|1\rangle|\psi_{x,1}\rangle, && (3.18)
\end{aligned}
$$

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 that q is drawn from $\mathcal{D}_n$ for $n = |q|$. We can show the following theorem.

Theorem 3.6.2. *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 $\overline{L}$*

3.6.1 Quantum Rejection Sampling

The proof of Theorem 3.6.2 relies on the quantum rejection sampling technique in [ORR13]. We give the definition of the quantum rejection sampling problem and we adapt their tool in the Lemma 3.6.4.

Definition 3.6.3 (Quantum rejection sampling problem $QRSP(\mathcal{D}, \mathcal{D}', n)$)**.** *Given an oracle $O_{\mathcal{D}} : |0\rangle \to \sum_{x=1}^{2^n} \sqrt{d_x}|\xi_x\rangle|x\rangle$ 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 3.6.4. *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 poly-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 3.6.1.

Proof. We first show the sample complexity. It has been shown in [ORR13] 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 3.6.1, 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 $1 - e^{-\beta}$.

□

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

Here we describe some states which are used in the protocol.

$$|Q_{\mathcal{D}}\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, 0\rangle_M |w_x(q), q\rangle_V, \tag{3.19}$$

where $|Q_{\mathcal{D}}\rangle_{MV}$ without the copy of q in V is the query state generated from G as in Equation 3.17.

$$|Q^H_{\mathcal{D}}\rangle_{MV} = \frac{1}{\sqrt{2^n}} \sum_{q \in \mathbb{Z}_2^m} \sqrt{d_q}|q, f^{-1}(q)\rangle_M |w_x(q), q\rangle_V, \tag{3.20}$$

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 3.18.

By applying $QRSampling(\mathcal{D} \to \mathcal{U})$, one can prepare the state $|\tilde{Q}\rangle$ from $|Q_{\mathcal{D}}\rangle_{MV}$ such that $D(|\tilde{Q}\rangle, |Q\rangle) \leq \delta$, 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 $D(|\tilde{Q}_{\mathcal{D}}^H\rangle, |Q_{\mathcal{D}}^H\rangle) \leq \delta'$, where δ' is exponentially small.

We give Protocol 4 for $\overline{L}$ with non-adaptive smooth locally quantum reductions. Its analysis and proof of Theorem 3.6.2 are deferred in Section 3.6.3.

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

$$|S\rangle_{MV\Pi} := \frac{1}{\sqrt{2}}(|\tilde{Q}\rangle_{M_1V_1} \otimes \cdots \otimes |\tilde{Q}\rangle_{M_{\gamma'}V_{\gamma'}}|0\rangle_\Pi + |T\rangle_{M_1V_1} \otimes \cdots \otimes |T\rangle_{M_{\gamma'}V_{\gamma'}}|1\rangle_\Pi).$$

   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_iV_i for $i \in [\gamma']$ and measure. Accept if the outcome is all 0.

3.6.3 Proof of Theorem 3.6.2

Proof of Theorem 3.6.2. Let the state of the entire system after the prover's action be

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

To simplify the notation, we let $M = M_1M_2\dots M_{\gamma'}$ and $V = V_1V_2\dots V_{\gamma'}$. 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 $F(|\tilde{Q}^H\rangle, |Q^H\rangle) \geq 1-\delta$ according to Lemma 3.6.4. If the prover is dishonest, we can always assume that the 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

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

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

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

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, $p_0 = \mathrm{Tr}(\Pi_R\tilde{\rho}_0) \geq 1-\varepsilon-2\delta$ 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 $p_{\mathrm{succ}} = \frac{1}{2}(p_0 + p_1) \geq 1 - (\varepsilon + 2\delta)/2$.

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 $\rho_0 := \mathrm{Tr}_P(|\psi\rangle\langle\psi|)$. By Claim 3.4.3, 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, $F(\rho_0,\tilde{\rho}_0) \geq F(|Q^H\rangle,|\tilde{Q}^H\rangle) \geq 1-\delta$. 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,

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

This gives

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

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

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

By Lemma 3.4.4, we can give an upper bound on p_{succ} as follows.

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

□

By the same proof as in Section 3.5, we can generalize Theorem 3.6.2 to Theorem 3.6.5.

Theorem 3.6.5. *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.*

3.7 Quantum worst-case to average-case reduction to Inv-OWP

Here, we consider the non-adaptive quantum worst-case to average-case reduction defined in Definition 3.3.3. We show that if the queries are generated arbitrarily according to smooth-computable distributions, i.e., the distributions of each query can be different but are smooth-computable, then the existence of such reductions also implies coNP$\subseteq$ QIP(2). We call this reduction *smooth non-adaptive quantum worst-case to average-case reduction*.

Theorem 3.7.1. *Suppose there exists a 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 3.3.2. Then, the smooth non-adaptive worst-case to average-case reduction is as follows:

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

$$\xrightarrow{R} \quad \sqrt{p}|L(x)\rangle|\psi_{x,0}\rangle + \sqrt{1-p}|1-L(x)\rangle|\psi_{x,1}\rangle,$$

where $p \geq 2/3$ and $d_{i,q}$ are the probability that q is drawn from a smooth-computable distribution $\mathcal{D}^{(i)}_{|q|}$. Note that $\mathcal{D}^{(i)}_{|q|}$ can be difference from $\mathcal{D}^{(j)}_{|q|}$ for $i \neq j$. The error of the reduction can be reduced to an exponentially small parameter ϵ by Lemma 3.5.2.

It is not hard to show that given such a reduction from L to Inv-OWP, Protocol 4 decides $\overline{L}$. For completeness, the honest prover always simulates $O_{f^{-1}}$, which is the same honest prover considered in Theorem 3.6.2. 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 oroacle for $O_{f^{-1}}$, then the modified trap state must be far from the original trap state. By the calculation in Section 3.6, we get the same upper bound on the soundness. □

The following two corollaries follow from Theorem 3.7.1.

Corollary 3.7.2. *If there exists a 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 3.7.3. *If there exists a 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)

3.8 Separation examples

We give two examples demonstrating the distinct landscapes of classical and quantum worst-case to average-case reductions. Namely, relative to some oracle and under reasonable computational assumptions, there exist problems (a worst-case problem and an average-case problem) where there are no classical reductions, but 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). In return, we remove the need of quantum access to the oracle.

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.*

A candidate is the PSPACE-complete problem TQBF, which is known to have a *non-adaptive* random self-reduction [FF93]. Assumption 1 will follow, if BQP $\subsetneq$ PSPACE holds. 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 $O := O_{s_0,\ldots,s_{N-1}}$ that generalizes Simon's oracle [Sim97].

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

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 3.8.1. *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.

- $L_1 = \text{TQBF} = \{\phi = \phi(v_1, \ldots, v_n)\}$ 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 3.8.2. *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 3.8.1 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 $j = 1, \ldots k$, 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 $\{\phi_j \stackrel{?}{=} 1\}$. Then R_1^Q runs the decision procedure R, which correctly decides ϕ. □

Remark 2. *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 $y_i := f(z_i)$.

- $L_2 = \text{TQBF} = \{\phi = \phi(v_1, \ldots, v_n)\}$ containing satisfiable quantified n-variable formulae in 3-CNF. Let L_2^O be the language L relative to oracle H, which ignores H.
- $\hat{L}_2^H := \{x = (i, z, \phi) : f(z) = y_i \text{ and } \phi \text{ is true}\}$. 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 3. *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 3.8.2, 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 quantum factorization 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 3.8.3. *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 $L_2^H \leq_{R_2^Q, G_2^Q} (\hat{L}_2^H, \hat{D}_2)$.*

Bibliography

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 323–334. Springer, 2002.

[AGGM06] 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.

[BB15] 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.

[BCvD06] D. Bacon, A. M. Childs, and Wim van Dam. Optimal measurements for the dihedral hidden subgroup problem. *Chicago J. Theor. Comput. Sci.*, 2006.

[BL13] Andrej Bogdanov and Chin Ho Lee. *Limits of Provable Security for Homomorphic Encryption*, pages 111–128. Springer Berlin Heidelberg, 2013.

[Bra79] Gilles Brassard. Relativized cryptography. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 00(undefined):383–391, 1979.

[BS16] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '16, pages 893–902, 2016.

[BT06] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. *SIAM Journal on Computing*, 36(4):1119–1159, 2006.

[CH16] Nai-Hui Chia and Sean Hallgren. How hard is deciding trivial versus nontrivial in the dihedral coset problem? In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2016, September 27-29, 2016, Berlin, Germany*, pages 6:1–6:16, 2016.

[CHS] Nai-Hui Chia, Sean Hallgren, and Fang Song. Basing one-way permutation on np-hard problems under quantum reductions. *submitted to QIP2018*.

[CJL+92] Matthijs J. Coster, Antoine Joux, Brian A. LaMacchia, Andrew M. Odlyzko, Claus-Peter Schnorr, and Jacques Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2(2):111–128, 1992.

[DIK+14] Thomas Decker, Gábor Ivanyos, Raghav Kulkarni, Youming Qiao, and Miklos Santha. *An Efficient Quantum Algorithm for Finding Hidden Parabolic Subgroups in the General Linear Group*, pages 226–238. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[EH00] Mark Ettinger and Peter Høyer. On quantum algorithms for noncommutative hidden subgroups. *Advances in Applied Mathematics*, 25(3):239 – 251, 2000.

[FF93] Joan Feigenbaum and Lance Fortnow. Random-self-reducibility of complete sets. *SIAM Journal on Computing*, 22(5):994–1005, 1993. `https://doi.org/10.1137/0222061`.

[FIM+14] Katalin Friedl, Gábor Ivanyos, Frédéric Magniez, Miklos Santha, and Pranab Sen. Hidden translation and translating coset in quantum computing. *SIAM J. Comput.*, 43(1):1–24, 2014.

[FKN90] 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. `https://doi.org/10.1109/SCT.1990.113959`.

[FZ08] Stephen Fenner and Yong Zhang. *Theory and Applications of Models of Computation: 5th International Conference, TAMC 2008, Xi'an, China, April 25-29, 2008. Proceedings*, chapter On the Complexity of the Hidden Subgroup Problem, pages 70–81. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[Hal07] Sean Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. *J. ACM*, 54(1):4:1–4:19, March 2007.

[HMR+10] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. *J. ACM*, 57:34:1–34:33, November 2010.

[HMW14] Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Info. Comput.*, 14(5&6):384–416, April 2014.

[IN96] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology*, 9:236–241, 1996.

[ISS08] Gábor Ivanyos, Luc Sanselme, and Miklos Santha. *An Efficient Quantum Algorithm for the Hidden Subgroup Problem in Nil-2 Groups*, pages 759–771. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. Qip= pspace. *Journal of the ACM (JACM)*, 58(6):30, 2011. Preliminary version in STOC 2010.

[JUW09] 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.

[KLGN15] 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. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[Kup13] Greg Kuperberg. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, May 21-23, 2013, Guelph, Canada*, pages 20–34, 2013.

[KW00] 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.

[KY10] Akinori Kawachi and Tomoyuki Yamakami. Quantum hardcore functions by complexity-theoretical quantum list decoding. *SIAM Journal on Computing*, 39(7):2941–2969, 2010.

[LO85] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *Journal of the Association for Computing Machinery*, 32(1):229–246, 1985.

[LV15] Tianren Liu and Vinod Vaikuntanathan. On basing private information retrieval on np-hardness. Cryptology ePrint Archive, Report 2015/1061, 2015. `http://eprint.iacr.org/2015/1061`.

[ORR13] Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. *ACM Trans. Comput. Theory*, 5(3):11:1–11:33, August 2013.

[Reg04] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.

[Reg05] 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, New York, NY, USA, 2005. ACM.

[Ros09] Bill Rosgen. Computational distinguishability of quantum channels, 2009.

[RS04] Phillip Rogaway and Thomas Shrimpton. *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance*, pages 371–388. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[Sch96] Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54(4):2614, 1996.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997. `https://doi.org/10.1137/S0097539796298637`. Preliminary version in FOCS 1994.

[VDHI06] Wim Van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*, 36(3):763–778, 2006.

Vita

Nai-Hui Chia

Contact

Email: nxc233@psu.edu
Homepage: www.cse.psu.edu/∼nxc233
Address: W342 Westgate building, The Pennsylvania State University, University Park, PA, 16802

Research interests

- Quantum algorithms, computational complexity (quantum interactive proof in particular), quantum cryptography, quantum machine learning.

Education

- **The Pennsylvania State University, University Park**
  Ph.D., Computer Science and Engineering
  August 2012 - present.
  Adviser: Sean Hallgren
  Fields: Quantum Algorithms/Complexity/Quantum Cryptography
- **National Taiwan University**
  Bachelor, Computer Science and Information Technology
  August 2006 - May 2010.

Employment

- Research Assistant: August 2013 - present
  Department of Computer Science and Engineering,
  The Pennsylvania State University, University Park
- Teaching Assistant: August 2012 - December 2012 and August 2016 - December 2016
  Department of Computer Science and Engineering,
  The Pennsylvania State University, University Park