Detecting mixed-unitary quantum channels is NP-hard

Colin Do-Yan Lee and John Watrous

Institute for Quantum Computing and School of Computer Science

University of Waterloo, Canada

February 8, 2019

A quantum channel is said to be a *mixed-unitary* channel if it can be expressed as a convex combination of unitary channels. We prove that, given the Choi representation of a quantum channel Φ, it is NP-hard with respect to polynomial-time Turing reductions to determine whether or not Φ is a mixed-unitary channel. This hardness result holds even under the assumption that Φ is not within an inverse-polynomial distance (in the dimension of the space upon which Φ acts) of the boundary of the mixed-unitary channels.

1 Introduction

In the theory of quantum information, *quantum channels* represent discrete-time changes in systems that can, in an idealized sense, be realized by physical processes. Mathematically speaking, quantum channels are represented by completely positive and trace-preserving linear maps of the form $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^m)$, where $\mathrm{L}(\mathbb{C}^n)$ is the set of linear maps, or *operators*, from $\mathbb{C}^n$ to itself, and likewise for $\mathrm{L}(\mathbb{C}^m)$. If the state of a system is represented by a density operator $\rho \in \mathrm{L}(\mathbb{C}^n)$ prior to the action represented by the channel Φ, then its state after the channel acts is given by the density operator $\Phi(\rho) \in \mathrm{L}(\mathbb{C}^m)$. This paper focuses on channels for which $n = m$, which represent the common situation in which a discrete-time change preserves the size of a physical system. (The sizes of the input and output systems of a quantum channel are reflected by the dimensions of the underlying spaces $\mathbb{C}^n$ and $\mathbb{C}^m$.)

Unitary channels form one of the simplest categories of quantum channels. A unitary channel is a channel of the form $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ that is given by $\Phi(X) = UXU^*$ for every $X \in \mathrm{L}(\mathbb{C}^n)$, for some fixed choice of a unitary operator $U \in \mathrm{L}(\mathbb{C}^n)$. A *mixed-unitary channel* is one that can be expressed as a convex combination of unitary channels. Equivalently, a channel $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ is mixed-unitary if there exists a positive integer N, a probability vector $(p_1, \ldots, p_N)$, and unitary operators $U_1, \ldots, U_N \in \mathrm{L}(\mathbb{C}^n)$ such that

$$\Phi(X) = \sum_{k=1}^{N} p_k U_k X U_k^* \tag{1}$$

for every operator $X \in \mathrm{L}(\mathbb{C}^n)$. We let $\mathrm{MU}(\mathbb{C}^n)$ denote the set of all such channels.

Mixed-unitary channels are important in quantum information theory for a number of reasons. They provide a rich set of examples of channels, and exhibit many fundamental attributes and properties of general quantum channels [Ros08]. At the same time, their relatively simple form can be beneficial in analyses, as compared with general quantum channels. Mixed-unitary channels arise naturally in both Hermitian operator formulations of majorization [AU82] and in a variety of cryptography situations that concern the encryption of quantum states [AMTdW00, HLSW04, AS04].

Quantum channels can be represented in different ways, but one common representation is the *Choi representation* [Cho75]. The Choi representation of an arbitrary linear map $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$

is defined as

$$J(\Phi) = \sum_{1 \leq i,j \leq n} \Phi(E_{i,j}) \otimes E_{i,j}, \tag{2}$$

where $E_{i,j}$ is the operator mapping the elementary unit vector e_j to e_i and all vectors orthogonal to e_i to 0. (Equivalently, with respect to the standard basis $\{e_1, \ldots, e_n\}$, the operator $E_{i,j}$ is represented by the matrix having a 1 in entry (i, j) and all other entries 0.)

We prove that it is NP-hard, with respect to polynomial-time Turing reductions, to determine whether or not a given quantum channel is mixed-unitary. Specifically, we consider the problem in which the input is the Choi representation $J(\Phi) \in \mathrm{L}(\mathbb{C}^n \otimes \mathbb{C}^n)$ of a quantum channel $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$, along with the unary representation 0^m of a positive integer m, and the task is to determine whether or not Φ is a mixed-unitary channel under the promise that $J(\Phi)$ is not within distance $1/m$ of the boundary of the set of all Choi representations of mixed-unitary channels. That is, the promise guarantees that the decision of whether or not Φ is mixed-unitary is not "artificially hard" due to issues relating to numerical precision. Our proof establishes that this problem is, in fact, *strongly NP-hard*, meaning that it remains NP-hard even when the real and imaginary parts of all of the numbers appearing in the Choi representation of the input channel are expressible as ratios of integers that are bounded in absolute value by a polynomial in the length of the entire input.

The methodology behind our proof is reminiscent of known proofs of the NP-hardness of testing if a given bipartite density operator $\rho \in \mathrm{L}(\mathbb{C}^n \otimes \mathbb{C}^m)$ is *separable* [Gur03, Ioa07, Gha10, Yu16], meaning that it can be represented as a convex combination of *product states*, which represent independence between the two individual systems that define the bipartition in question. In particular, following the strong NP-hardness proof of separability testing due to Gharibian [Gha10], we make use of a theorem due to Liu [Liu07] that establishes the existence of a polynomial-time Turing reduction from the *weak optimization* problem to the *weak membership* problem in certain families of convex sets. We note that our main result can, in fact, be closely linked with the problem of separability testing, in the sense that testing if a channel is mixed-unitary may alternatively be formulated as a problem concerning the expression of a bipartite density operator in a certain way. More specifically, the set of all Choi representations of mixed-unitary channels, when normalized, is equivalent to the set of bipartite quantum states that can be written as convex combinations of *maximally entangled* states.

The remainder of this paper is organized as follows. Section 2 summarized preliminary material on computational complexity and quantum information theory that is required to understand this paper, and formally defines the *mixed-unitary detection* problem described above along with a different problem, called *unitary quadratic minimization*, that plays an important role in the proof of our main result. In Section 3 we prove that the NP-complete *graph 3-coloring* problem (3COL) reduces to *unitary quadratic minimization* (UQM) through a polynomial-time mapping reduction, and in Section 4 we prove that *unitary quadratic minimization* reduces to *mixed-unitary detection* (MUD) through a polynomial-time Turing reduction. In symbols, these two sections establish the relations

$$\mathrm{3COL} \leq_m^p \mathrm{UQM} \leq_T^p \mathrm{MUD}, \tag{3}$$

which implies the NP-hardness of testing if a channel is mixed-unitary. The paper concludes with Section 5, which mentions a few open problems that relate to the main results of the paper.

2 Preliminaries

The main purpose of this section is to clarify some of the notation and conventions we use throughout the paper, and to define two decision problems: one is the *mixed-unitary detection* problem, whose hardness is the primary focus of this paper, and the second is the *unitary quadratic minimization* problem, which serves as an intermediate problem through which an NP-complete problem (the *graph 3-coloring* problem) is reduced to the *mixed-unitary detection* problem.

2.1 Computational complexity

We assume the reader is familiar with basic notions of computational complexity, such as polynomial-time mapping reductions, polynomial-time Turing reductions, the concept of NP-completeness, and the fact that the *graph 3-coloring* problem is NP-complete. This material is covered in several textbooks on computational complexity, such as the book of Arora and Barak [AB09]. When we speak of *polynomials* in this paper, we are referring only to resource bounds—so it should be understood that we are referring more precisely to nonzero univariate polynomials having non-negative integer coefficients.

The decision problems we consider involve approximations of real number values and/or guarantees on distances between real or complex vectors, and for this reason they are naturally stated as *promise problems* [ESY84]. Formally speaking, a promise problem is a pair $A = (A_{\text{yes}}, A_{\text{no}})$ of disjoint sets $A_{\text{yes}}, A_{\text{no}} \subseteq \Sigma^*$ of strings over an alphabet Σ. A hypothetical algorithm or protocol for A is required to output "yes" (or 1) on input strings in A_{yes} (which are called *yes-inputs* or *yes-instances*) and output "no" (or 0) on input strings in A_{no} (which are called *no-inputs* or *no-instances*). No constraints are placed on an algorithm or protocol for A on strings outside of the set $A_{\text{yes}} \cup A_{\text{no}}$. In the promise problem statements found below and later in the paper, we first list general assumptions on the form of the input, which is understood to be a string encoding of one or more mathematical objects, followed by a specification of which of these inputs are to be considered yes-instances and which are to be considered no-instances.

In the problems considered in this paper, every complex number is assumed to be encoded as a triple (x, y, z) that represents the number $(x + iy)/z$, where x and y are integers represented in signed binary notation and z is a positive integer represented in binary notation. Real numbers are encoded similarly, but where the imaginary part represented by y is omitted. One exception is when positive integers are explicitly stated to be represented in unary notation, which means that each positive integer m is encoded as the string 0^m. Real or complex vectors and matrices are encoded as complete lists of their real or complex number entries (as opposed to compact representations of sparse matrices, for instance).

For a given polynomial p, we may say that an instance of any of the problems discussed in this paper is *p-bounded* if, for every real or complex number appearing in that problem instance (and encoded as described above), the values x, y, and z are bounded in absolute value by $p(n)$, for n being the length of the entire instance being considered. A polynomial-time mapping reduction $A \leq_m^p B$ between promise problems A and B will be called *strong* if, for every polynomial p there exists a polynomial q such that this property holds: for every p-bounded instance of A_{yes} or A_{no}, the reduction produces a q-bounded instance of B_{yes} or B_{no}, respectively. Along similar lines, a polynomial-time Turing reduction $A \leq_T^p B$ is *strong* if, for every polynomial p there exists a polynomial q such that, on every p-bounded instance of A_{yes} or A_{no}, the reduction only queries q-bounded instances of B, and accepts or rejects accordingly. Finally, a problem is *strongly NP-hard* (with respect to either polynomial-time mapping or Turing reductions) if it remains NP-hard even under the additional promise that every yes- or no-instance is p-bounded, for some choice of a polynomial p.

2.2 Linear algebra and quantum information

Similar to computational complexity, we assume that the reader is familiar with basic notions of linear algebra and quantum information. There is, in fact, little in the way of quantum information theory that is required for an understanding of this paper, aside from the definition of quantum channels and their Choi representations (which are described in Chapter 2 of [Wat18], for instance).

For n a positive integer, the vector space $\mathbb{C}^n$ is defined in the usual way, an inner product on this space is defined as

$$\langle u, v \rangle = \sum_{k=1}^{n} \overline{u(k)} v(k) \tag{4}$$

(conjugate linear in the first argument), and the *Euclidean norm* is given by

$$\|u\| = \sqrt{\langle u, u \rangle}. \tag{5}$$

The *standard basis* of $\mathbb{C}^n$ is the basis $\{e_1, \ldots, e_n\}$ of elementary unit vectors.

We write $\mathrm{L}(\mathbb{C}^n)$ to denote the set of linear operators (or mappings) from $\mathbb{C}^n$ to itself, and associate this set with the set of all $n \times n$ complex matrices, where the understanding is that the matrix is a representation of the operator with respect to the standard basis. We already introduced the notation $E_{i,j}$ in the previous section; the operator $E_{i,j}$ is the operator whose matrix representation has a 1 in entry (i, j) and 0 in all other entries. The inner product of two operators $A, B \in \mathrm{L}(\mathbb{C}^n)$ is defined as $\langle A, B \rangle = \mathrm{Tr}(A^* B)$, where A^* is the *adjoint* of A (which, in terms of matrix representations, is equivalent to the *conjugate transpose* of A). An operator $A \in \mathrm{L}(\mathbb{C}^n)$ is *Hermitian* if $A = A^*$, and is *unitary* if $A^* A = \mathbb{1}_n$, where $\mathbb{1}_n \in \mathrm{L}(\mathbb{C}^n)$ is the identity operator acting on $\mathbb{C}^n$. The notations $\mathrm{Herm}(\mathbb{C}^n)$ and $\mathrm{U}(\mathbb{C}^n)$ refer to the sets of all Hermitian and unitary operators in $\mathrm{L}(\mathbb{C}^n)$, respectively.

We refer to three different norms of operators. The *spectral norm* of A is defined as

$$\|A\| = \max\bigl\{\|Au\| \,:\, u \in \mathbb{C}^n,\ \|u\| \leq 1\bigr\}, \tag{6}$$

the *2-norm* (or *Frobenius norm*) of A is defined as

$$\|A\|_2 = \sqrt{\langle A, A \rangle}, \tag{7}$$

and the *trace norm* is defined as

$$\|A\|_1 = \mathrm{Tr}\Bigl(\sqrt{A^* A}\Bigr), \tag{8}$$

where $\sqrt{A^* A}$ is the unique positive semidefinite operator whose square is $A^* A$. These norms satisfy $\|A\| \leq \|A\|_2 \leq \|A\|_1$ for every $A \in \mathrm{L}(\mathbb{C}^n)$.

The notion of quantum channels was also already introduced in the previous section. For the purposes of this paper, it suffices to note that the property of *complete positivity* of a linear map $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ is equivalent to its Choi representation

$$J(\Phi) = \sum_{1 \leq i,j \leq n} \Phi(E_{i,j}) \otimes E_{i,j} \tag{9}$$

being positive semidefinite. Similarly, the property that Φ is *Hermitian-preserving* (which means that $\Phi(X) \in \mathrm{Herm}(\mathbb{C}^n)$ for every $X \in \mathrm{Herm}(\mathbb{C}^n)$) is equivalent to $J(\Phi)$ being Hermitian. The property that Φ *preserves trace* is equivalent to

$$\bigl(\mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathbb{C}^n)}\bigr)(J(\Phi)) = \mathbb{1}_n, \tag{10}$$

and the property that Φ is *unital* (which means that $\Phi(\mathbb{1}_n) = \mathbb{1}_n$) is equivalent to

$$\bigl(\mathbb{1}_{\mathrm{L}(\mathbb{C}^n)} \otimes \mathrm{Tr}\bigr)(J(\Phi)) = \mathbb{1}_n, \tag{11}$$

where $\mathbb{1}_{\mathrm{L}(\mathbb{C}^n)}$ refers to the identity mapping from $\mathrm{L}(\mathbb{C}^n)$ to itself.

2.3 Problem statements

Finally, we formally define the decision problems (stated as promise problems) that were referred to in the introduction.

Definition 1. The *unitary quadratic minimization* (UQM) promise problem is as follows.

Input: Operators $A_1, \ldots, A_k \in \mathrm{L}(\mathbb{C}^n)$ with $\|A_j\|_2 \leq 1$ for each $j \in \{1, \ldots, k\}$, a real number α, and the unary representation 0^m of a positive integer m.

Yes: There exists a unitary operator $U \in \mathrm{U}(\mathbb{C}^n)$ such that

$$\sum_{j=1}^{k} |\langle A_j, U \rangle|^2 \leq \alpha. \tag{12}$$

No: For every unitary operator $U \in \mathrm{U}(\mathbb{C}^n)$ it is the case that

$$\sum_{j=1}^{k} |\langle A_j, U \rangle|^2 \geq \alpha + \frac{1}{m}. \tag{13}$$

Definition 2. The *mixed-unitary detection* (MUD) promise problem is as follows.

Input: The Choi representation $J(\Phi) \in \mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n)$ of a trace-preserving, unital, and Hermitian-preserving map $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ along with the unary representation 0^m of a positive integer m.

Yes: Every trace-preserving, unital, Hermitian-preserving map $\Psi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ that satisfies

$$\big\| J(\Psi) - J(\Phi) \big\|_2 \leq \frac{1}{m} \tag{14}$$

is a mixed-unitary channel.

No: Every trace-preserving, unital, Hermitian-preserving map $\Psi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ that satisfies

$$\big\| J(\Psi) - J(\Phi) \big\|_2 \leq \frac{1}{m} \tag{15}$$

it not a mixed-unitary channel.

Two brief remarks about the previous two definitions are in order. First, the fact that both problems expect a *unary* representation of a positive integer m (as opposed to a binary representation, say) is a standard mechanism in computational complexity that forces the value of m to be polynomially related to its input size. If the integer m were instead to be input in binary notation, the value of m would be exponential in its input length, and as a result the problems themselves would become harder in a computational sense. As our main result is a hardness result, it is therefore a stronger result given the assumption that m is input in unary notation.

Second, we note that in Definition 2 specifically, the maps Φ and Ψ are assumed to range over all trace-preserving, unital, and Hermitian-preserving maps rather than over all unital channels. We have defined the mixed-unitary detection problem in this way so that it has a form that is standard within the study of computational geometric problems [GLS88]: the input is a vector in a real vector space, and the task is to determine if a ball of a certain radius either lies entirely within or is disjoint from a set of interest. The computational difficulty of the problem would not change in a fundamental way if Φ were assumed to be a channel, given that this property can be tested efficiently. We do, however, require that Ψ ranges over all trace-preserving, unital, and Hermitian-preserving maps in the yes case, so as to properly reflect the property that every map in a ball of radius $1/m$ around Φ is a mixed-unitary channel.

3 Reduction from graph 3-coloring to unitary quadratic optimization

In this section we prove that the *unitary quadratic minimization* problem is NP-hard, via a polynomial-time mapping reduction from the *graph 3-coloring* problem. Our reduction establishes that this problem is, in fact, strongly NP-hard, as the operators $A_1, \ldots, A_k$ that are produced by our reduction from any instance of *graph 3-coloring* have entries restricted to the set $\{0, 1/2, 1\}$.

3.1 The reduction

Let $G = (V, E)$ be a graph with n vertices $V = \{1, \ldots, n\}$ and m edges

$$E = \big\{\{a_1, b_1\}, \ldots, \{a_m, b_m\}\big\}, \tag{16}$$

where $1 \leq a_j < b_j \leq n$ for every $j \in \{1, \ldots, m\}$. Let $N = n + m$ and consider the following two collections of operators drawn from $\mathrm{L}(\mathbb{C}^N)$:

1. $E_{i,j}$ for every choice of $i, j \in \{1, \ldots, N\}$ with $i \neq j$.
2. $\big(E_{a_j,a_j} + E_{b_j,b_j} + E_{n+j,n+j}\big)/2$ for every $j \in \{1, \ldots, m\}$.

(The factor of $1/2$ in the second type of operator guarantees that each of the operators produced by the reduction has 2-norm at most 1.) The total number of operators in these two collections is

$$k = (N^2 - N) + m = (n + m)^2 - n. \tag{17}$$

Let $A_1, \ldots, A_k$ denote these operators taken in any reasonable ordering that allows for the computation of these operators in polynomial time given the graph G. The instance of UQM produced by the reduction is

$$\Big(A_1, \ldots, A_k, 0, 0^{526n^2}\Big) \tag{18}$$

3.2 Analysis: yes-instances map to yes-instances

Assume first that G is 3-colorable, so that there exists a function $\varphi : \{1, \ldots, n\} \to \{0, 1, 2\}$ with the property that $\varphi(a) \neq \varphi(b)$ whenever $\{a, b\} \in E$. One may obtain a unitary operator $U \in \mathrm{U}(\mathbb{C}^N)$ such that

$$\sum_{j=1}^{k} |\langle A_j, U\rangle|^2 = 0 \tag{19}$$

by taking U to be the diagonal operator whose diagonal entries are third-roots of unity as follows (assuming $\omega = \exp(2\pi i/3)$):

1. For each $a \in \{1, \ldots, n\}$, let $U(a, a) = \omega^{\varphi(a)}$.
2. For each $j \in \{1, \ldots, m\}$, let $U(n + j, n + j) = \omega^{c_j}$ for $c_j \in \{0, 1, 2\}$ being the unique color such that $c_j \notin \{\varphi(a_j), \varphi(b_j)\}$.

As U is diagonal, it is the case that $\big\langle E_{i,j}, U\big\rangle = 0$ whenever $i \neq j$. For the j-th edge $\{a_j, b_j\}$, it is the case that

$$\Big\langle \big(E_{a_j,a_j} + E_{b_j,b_j} + E_{n+j,n+j}\big)/2, U\Big\rangle = \frac{1}{2}\big(U(a_j, a_j) + U(b_j, b_j) + U(n + j, n + j)\big), \tag{20}$$

which is zero because it is proportional to the sum of the three roots of unity $1 = \omega^0$, ω^1, and ω^2.

3.3 Analysis: no-instances map to no-instances

It remains to prove that if G is not 3-colorable, then for every unitary operator U one has

$$\sum_{j=1}^{k} |\langle A_j, U \rangle|^2 \geq \frac{1}{526n^2}. \tag{21}$$

This statement will be proved in the contrapositive form. To this end, assume hereafter that U is a unitary operator, and for the operators $A_1, \ldots, A_k$ produced from a given graph G by the reduction described previously it is the case that

$$\sum_{j=1}^{k} |\langle A_j, U \rangle|^2 < \eta = \frac{1}{526n^2}. \tag{22}$$

From this assumption we will recover a 3-coloring of the graph G. We will make use of the following lemma, which is proved at the end of the present subsection, to do this.

Lemma 3. *Suppose $\varepsilon \in [0, 1/6]$ and $\alpha, \beta, \gamma \in \mathbb{C}$ satisfy the following conditions:*

1. $|\alpha|, |\beta|, |\gamma| \in [1 - \varepsilon, 1]$.
2. $|\alpha + \beta + \gamma| \leq \varepsilon$.

For each angle $\theta \in \{\arg(\alpha) - \arg(\beta), \arg(\beta) - \arg(\gamma), \arg(\gamma) - \arg(\alpha)\}$, interpreted as an element of the set $[0, 2\pi)$, it is the case that

$$\left|\theta - \frac{2\pi}{3}\right| \leq 6\varepsilon \quad \text{or} \quad \left|\theta - \frac{4\pi}{3}\right| \leq 6\varepsilon. \tag{23}$$

We begin by observing that the diagonal entries of U must be close to 1 in absolute value. Specifically, for every $j \in \{1, \ldots, N\}$ it is the case that

$$\sum_{i \neq j} |U(i,j)|^2 = \sum_{i \neq j} |\langle E_{i,j}, U \rangle|^2 \leq \sum_{i=1}^{k} |\langle A_i, U \rangle|^2 < \eta, \tag{24}$$

and therefore

$$|U(j,j)| > \sqrt{1 - \eta} \geq 1 - \sqrt{\eta}, \tag{25}$$

as every column of U has unit norm. Next, observe that

$$\begin{aligned} &\frac{1}{2} |U(a_j, a_j) + U(b_j, b_j) + U(n+j, n+j)| \\ &\quad = \frac{1}{2} \left|\left\langle E_{a_j,a_j} + E_{b_j,b_j} + E_{n+j,n+j}, U \right\rangle\right| \leq \left(\sum_{i=1}^{k} |\langle A_i, U \rangle|^2 \right)^{\frac{1}{2}} \leq \sqrt{\eta} \end{aligned} \tag{26}$$

for every $j \in \{1, \ldots, m\}$. By Lemma 3, we conclude that for any two adjacent vertices $a, b \in \{1, \ldots, n\}$ of G, the angle

$$\theta_{a,b} = \arg(U(a,a)) - \arg(U(b,b)) \tag{27}$$

satisfies

$$\left|\theta_{a,b} - \frac{2\pi}{3}\right| \leq 12\sqrt{\eta} \quad \text{or} \quad \left|\theta_{a,b} - \frac{4\pi}{3}\right| \leq 12\sqrt{\eta}. \tag{28}$$

Define sets S_0, S_1, and S_2 as

$$S_0 = \left[\frac{11\pi}{6}, 2\pi\right) \cup \left[0, \frac{\pi}{6}\right], \quad S_1 = \left[\frac{\pi}{2}, \frac{5\pi}{6}\right], \quad \text{and} \quad S_2 = \left[\frac{7\pi}{6}, \frac{3\pi}{2}\right]. \tag{29}$$

Because

$$12n\sqrt{\eta} < \frac{\pi}{6}, \tag{30}$$

it follows from an iterative application of the argument above that, for any two *connected* (but not necessarily adjacent) vertices $a, b \in \{1, \ldots, n\}$ of G, exactly one of the following three inclusions holds:

$$\begin{aligned} \theta_{a,b} &\in \left[2\pi - 12n\sqrt{\eta}, 2\pi\right) \cup \left[0, 12n\sqrt{\eta}\right] \subseteq S_0, \\ \theta_{a,b} &\in \left[\frac{2\pi}{3} - 12n\sqrt{\eta}, \frac{2\pi}{3} + 12n\sqrt{\eta}\right] \subseteq S_1, \\ \theta_{a,b} &\in \left[\frac{4\pi}{3} - 12n\sqrt{\eta}, \frac{4\pi}{3} + 12n\sqrt{\eta}\right] \subseteq S_2. \end{aligned} \tag{31}$$

A 3-coloring of G may therefore be obtained by repeating the following procedure for each connected component H of G:

1. Choose an arbitrary vertex $a \in \{1, \ldots, n\}$ of H (or, for concreteness, the lowest-numbered vertex of H), and assign this vertex the color 0 (i.e., set $\varphi(a) = 0$).
2. For each vertex $b \in \{1, \ldots, n\}$ of H, assign b a color as follows:
   (a) If $\theta_{a,b} \in S_0$, then set $\varphi(b) = 0$.
   (b) If $\theta_{a,b} \in S_1$, then set $\varphi(b) = 1$.
   (c) If $\theta_{a,b} \in S_2$, then set $\varphi(b) = 2$.

As the angle $\theta_{b,c} = \arg(U(b,b)) - \arg(U(c,c))$ must exceed the width $\pi/3$ of each set S_0, S_1, and S_2, adjacent vertices cannot be assigned the same color, and therefore φ is a valid 3-coloring of G. This completes the proof of the reduction from 3-coloring to UQM, aside from the proof of Lemma 3, which follows.

Proof of Lemma 3. It suffices to prove the lemma for $\theta = \arg(\alpha) - \arg(\beta)$, as the bound follows for the other two angles by symmetry.

Observe first that the triangle inequality implies

$$\big||\alpha + \beta| - |\gamma|\big| \leq \varepsilon, \tag{32}$$

and therefore

$$1 - 2\varepsilon \leq |\alpha + \beta| \leq 1 + \varepsilon. \tag{33}$$

It is the case that

$$|\alpha + \beta|^2 = |\alpha|^2 + |\beta|^2 + 2|\alpha||\beta|\cos(\theta), \tag{34}$$

and therefore

$$\cos(\theta) = \frac{|\alpha + \beta|^2 - |\alpha|^2 - |\beta|^2}{2|\alpha||\beta|}. \tag{35}$$

A lower bound on $\cos(\theta)$ may be obtained as follows:

$$\cos(\theta) = \frac{|\alpha + \beta|^2}{2|\alpha||\beta|} - \frac{1}{2}\left(\frac{|\alpha|}{|\beta|} + \frac{|\beta|}{|\alpha|}\right) \geq \frac{(1 - 2\varepsilon)^2}{2} - \frac{2 + \varepsilon}{2} \geq -\frac{1}{2} - \frac{5\varepsilon}{2}. \tag{36}$$

Here we have used the observation that $|\alpha|, |\beta| \in [1 - \varepsilon, 1]$ implies

$$\frac{|\alpha|}{|\beta|} + \frac{|\beta|}{|\alpha|} \leq (1 - \varepsilon) + \frac{1}{1 - \varepsilon} \leq 2 + \varepsilon. \tag{37}$$

An upper bound on $\cos(\theta)$ is given by

$$\cos(\theta) = \frac{|\alpha+\beta|^2 - |\alpha|^2 - |\beta|^2}{2|\alpha||\beta|} \leq \frac{(1+\varepsilon)^2 - 2(1-\varepsilon)^2}{2} \leq -\frac{1}{2} + 3\varepsilon. \tag{38}$$

(Note that the numerator $|\alpha+\beta|^2 - |\alpha|^2 - |\beta|^2$ of the first fraction in (38) is necessarily non-positive, which explains why the denominator of the second fraction is 2 and not $2(1-\varepsilon)^2$.)

Now, because $\cos(\theta)$ is non-positive, it cannot be that $\theta \in [0, \pi/2) \cup (3\pi/2, 2\pi)$. It therefore suffices to consider the case that $\theta \in [\pi/2, 3\pi/2]$. We will split this case into two sub-cases, $\theta \in [\pi/2, \pi]$ and $\theta \in [\pi, 3\pi/2]$, which can be handled by symmetric arguments.

With this in mind, suppose that $\theta \in [\pi/2, \pi]$, and observe that the cosine function is convex on the interval $[\pi/2, \pi]$. On this interval, the graph of the cosine function therefore lies above the tangent line passing through the point $(2\pi/3, -1/2)$, which implies

$$\cos(\theta) \geq -\frac{1}{2} + \frac{\sqrt{3}}{2}\left(\frac{2\pi}{3} - \theta\right). \tag{39}$$

Combining this inequality with (38) yields

$$\frac{2\pi}{3} - \theta \leq \frac{6\varepsilon}{\sqrt{3}} \leq 4\varepsilon. \tag{40}$$

Again using convexity, the graph of the cosine function on the interval $[2\pi/3, \pi]$ lies below the line segment whose endpoints are $(2\pi/3, -1/2)$ and $(\pi, -1)$. If $\theta \in [2\pi/3, \pi]$, then it follows that

$$\cos(\theta) \leq -\frac{1}{2} - \frac{3}{2\pi}\left(\theta - \frac{2\pi}{3}\right), \tag{41}$$

and therefore by (36) we have

$$\theta - \frac{2\pi}{3} \leq \frac{5\pi\varepsilon}{3} \leq 6\varepsilon. \tag{42}$$

The same bound is, of course, trivial when $\theta \in [\pi/2, 2\pi/3]$. It is therefore the case that

$$\left|\theta - \frac{2\pi}{3}\right| \leq 6\varepsilon. \tag{43}$$

A similar argument implies that if $\theta \in [\pi, 3\pi/2]$, then

$$\left|\theta - \frac{4\pi}{3}\right| \leq 6\varepsilon. \tag{44}$$

which completes the proof. □

4 Reduction from unitary quadratic optimization to mixed-unitary detection

In this section we prove that there exists a polynomial-time Turing reduction from the *unitary quadratic minimization* problem to the *mixed-unitary detection* problem:

$$\text{UQM} \leq_T^p \text{MUD}. \tag{45}$$

At the heart of this reduction is a general result due to Liu [Liu07] that establishes that there exists a polynomial-time Turing reduction from the *weak optimization* problem to the *weak membership* problem for certain convex sets and problem parameterizations. These problems and Liu's reduction (but not the specifics of the reduction itself or the proof that it is correct) are described in the first subsection that follows, and the subsequent subsections connect these problems and Liu's reduction to the reduction (45).

4.1 Weak optimization, weak membership, and Liu's reduction

In order to define the *weak optimization* and *weak membership* problems, and to explain Liu's reduction from *weak optimization* to *weak membership*, a couple of definitions will be required. The first definition simply establishes some convenient notation.

Definition 4. Let N be a positive integer and let $\delta \geq 0$ be a non-negative real number. For every vector $x \in \mathbb{R}^N$, the (closed) ball of radius δ around x is defined as

$$\mathcal{B}_N(x, \delta) = \big\{ y \in \mathbb{R}^N \,:\, \|y - x\| \leq \delta \big\}, \tag{46}$$

and for every set $\mathcal{A} \subset \mathbb{R}^N$, one defines

$$\mathcal{B}_N(\mathcal{A}, \delta) = \bigcup_{x \in \mathcal{A}} \mathcal{B}_N(x, \delta). \tag{47}$$

The second definition is one for a *polynomially bounded* sequence of convex sets. Intuitively speaking, one should view the sets in such a sequence as corresponding in some way to possible input lengths in a computational problem. The term *polynomially bounded* refers to both a polynomial upper-bound on the norm of every element in each set and to an inverse polynomial lower bound on the size of a ball around 0 that is fully contained within each set.

Definition 5. Let $\mathcal{K}_N \subset \mathbb{R}^N$ be a compact, convex set for each positive integer N. The collection $\{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$ is *polynomially bounded* if there exists a polynomial p with the property that

$$\mathcal{B}_N(0, 1/p(N)) \subseteq \mathcal{K}_N \quad \text{and} \quad \mathcal{K}_N \subseteq \mathcal{B}_N(0, p(N)) \tag{48}$$

for every positive integer N.

Remark 6. It is common that a somewhat more general definition is used in place of the one just given, where the smaller ball that is contained in each $\mathcal{K}_N$ need not be centered around 0, and where it is only the ratio of the radii of the two balls that needs to be polynomially bounded—but because the simpler definition above is sufficient for our needs, we adopt it rather than the more general definition.

We are now ready to define the *weak optimization* and *weak membership* problems, which are variants of standard problems in the analysis of geometric algorithms [GLS88]. Both are defined with respect to a collection $\{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$ of compact, convex sets of the sort considered in the previous definition. (The problem definitions themselves do not require these collections to be polynomially bounded, but Liu's result will require this assumption.)

Definition 7 (Weak membership and weak optimization)**.** Let $\mathcal{K}_N \subset \mathbb{R}^N$ be a compact, convex set for each positive integer N and let $\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$.

1. The *weak membership* promise problem WMEM($\mathcal{K}$) for $\mathcal{K}$ is as follows:

Input:	A vector $x \in \mathbb{R}^N$ and the unary representation 0^m of a positive integer m.
Yes:	$\mathcal{B}_N(x, 1/m) \subseteq \mathcal{K}_N$.
No:	$\mathcal{B}_N(x, 1/m) \cap \mathcal{K}_N = \varnothing$.

2. The *weak optimization* promise problem WOPT($\mathcal{K}$) for $\mathcal{K}$ is as follows:

Input:	A vector $u \in \mathbb{R}^N$ with $\|u\| \leq 1$, a real number β, and the unary representation 0^m of a positive integer m.
Yes:	There exists a vector $x \in \mathbb{R}^N$ such that $\mathcal{B}_N(x, 1/m) \subseteq \mathcal{K}_N$ and $\langle u, x \rangle \leq \beta$.
No:	For every vector $x \in \mathcal{B}_N(\mathcal{K}_N, 1/m)$ it is the case that $\langle u, x \rangle \geq \beta + 1/m$.

These problems are referred to as *weak* versions of membership testing and optimization because the promises effectively make the problems easier than they might otherwise be. That is, in the case of weak membership testing, any point within a distance $1/m$ of the boundary of the corresponding convex set is viewed as a "don't care" input, as is any input to the *weak optimization* problem for which the objective value β is (informally speaking) neither "easily achievable" or "far from achievable." Variants of these problems in which m is input in binary rather than unary notation are also commonly referred to as *weak membership testing* and *weak optimization*, but the inverse polynomial bound obtained by taking m to be input in unary is an essential feature of Liu's result and is required for our purposes.

Finally, we may now state the result due to Liu that forms the heart of the reduction from *unitary quadratic minimization* to *mixed-unitary detection*.

Theorem 8 (Liu)**.** *For every polynomially bounded collection $\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$ of compact, convex sets, it is the case that*

$$\mathrm{WOPT}(\mathcal{K}) \leq_T^p \mathrm{WMEM}(\mathcal{K}). \tag{49}$$

Moreover, there exists a strong polynomial-time Turing reduction that establishes this relation.

Remark 9. Liu actually proved this theorem for a slightly more restricted version of WOPT($\mathcal{K}$) in which the vector u must satisfy $\|u\| = 1$ rather than $\|u\| \leq 1$. The benefit of adopting the definition with the inequality $\|u\| \leq 1$ rather than the equality $\|u\| = 1$ is that it allows us to largely circumvent precision issues that arise when taking square roots of rational numbers. Fortunately, Liu's theorem still holds for the less restricted variant of WOPT($\mathcal{K}$), as it has been defined above, as there exists a strong polynomial-time mapping reduction from this problem to its more restricted variant, under the assumption that there exists a polynomial p for which $\mathcal{K}_N \subseteq \mathcal{B}_N(0, p(N))$ for every positive integer N (which, of course, is the case when $\mathcal{K}$ is polynomially bounded).

We will now argue that this is so. Consider a reduction that transforms a given instance $(u, \gamma, 0^m)$ of WOPT($\mathcal{K}$), where $u \in \mathbb{R}^N$ satisfies $\|u\| \leq 1$, to an instance $(v, \delta, 0^{4m})$ of the equality-restricted variant of WOPT($\mathcal{K}$), where v and δ are as follows:

1. The vector $v \in \mathbb{R}^N$ is a unit vector satisfying

$$\left\| v - \frac{u}{\|u\|} \right\| \leq \frac{1}{4m(p(N)+1)}. \tag{50}$$

2. The number δ satisfies

$$\frac{\gamma}{\|u\|} + \frac{1}{4m} \leq \delta \leq \frac{\gamma}{\|u\|} + \frac{1}{2m}. \tag{51}$$

In the case that $(u, \gamma, 0^m)$ is a yes-instance of WOPT($\mathcal{K}$), one has that there exists a vector $x \in \mathbb{R}^N$ such that $\mathcal{B}_N(x, 1/m) \subseteq \mathcal{K}_N$ and $\langle u, x \rangle \leq \gamma$. The same vector x trivially satisfies $\mathcal{B}_N(x, 1/(4m)) \subseteq \mathcal{K}_N$, as well as

$$\langle v, x \rangle = \left\langle \frac{u}{\|u\|}, x \right\rangle + \left\langle v - \frac{u}{\|u\|}, x \right\rangle \leq \frac{\gamma}{\|u\|} + \frac{\|x\|}{4m(p(N)+1)} \leq \delta. \tag{52}$$

The instance $(v, \delta, 0^{4m})$ is therefore a yes-instance of the equality-restricted variant of WOPT($\mathcal{K}$).

In the case that $(u, \gamma, 0^m)$ is a no-instance of WOPT($\mathcal{K}$), every vector $x \in \mathcal{B}_N(\mathcal{K}_N, 1/m)$ satisfies $\langle u, x \rangle \geq \gamma + 1/m$, and therefore also satisfies

$$\begin{aligned} \langle v, x \rangle &= \left\langle \frac{u}{\|u\|}, x \right\rangle + \left\langle v - \frac{u}{\|u\|}, x \right\rangle \\ &\geq \frac{\gamma}{\|u\|} + \frac{1}{m\|u\|} - \frac{\|x\|}{4m(p(N)+1)} \geq \frac{\gamma}{\|u\|} + \frac{3}{4m} \geq \delta + \frac{1}{4m}. \end{aligned} \tag{53}$$

Of course this is therefore true for all $x \in \mathcal{B}_N(\mathcal{K}_N, 1/(4m))$, so $(v, \delta, 0^{4m})$ is a no-instance of the equality-restricted variant of WOPT($\mathcal{K}$).

Given $(u, \gamma, 0^m)$, one can compute $(v, \delta, 0^{4m})$ in polynomial time by performing the required arithmetic computations to inverse-polynomial accuracy. If it is the case that γ and the entries of u are given by ratios of integers that are bounded in absolute value by some polynomial in N, then the numerators and denominators of δ and the entries of v will also be polynomially bounded in absolute value, and therefore this is a strong polynomial-time mapping reduction.

4.2 Full-dimensional real convex sets for mixed-unitary optimization

The *weak optimization* and *weak membership* problems are concerned with convex subsets of $\mathbb{R}^N$, for different choices of N, and the assumption that $\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$ is a polynomially bounded collection of compact, convex sets implies that these sets are full-dimensional. On the other hand, the *unitary quadratic minimization* and *mixed-unitary detection* problems are concerned with complex operators, and moreover (as will shortly become clear), these problems are most naturally connected with affine subspaces of vector spaces that do not have full dimension. In this section we consider a particular family $\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$ that will allow for a translation from *unitary quadratic minimization* to *weak optimization* and from *weak membership* to *mixed-unitary detection*. It is also proved that $\mathcal{K}$ is polynomially bounded, so that Liu's reduction holds for this choice of $\mathcal{K}$.

To begin, for a given positive integer $n \geq 2$, consider the space of all $n \times n$ traceless Hermitian operators, which is a real vector space of dimension $n^2 - 1$. We will require an orthogonal basis for this space, and one reasonable choice for such a basis is given by the generalized Gell Mann operators. Specifically, let $G_1, \ldots, G_{n^2-1}$ denote the elements of $\mathrm{Herm}(\mathbb{C}^n)$ obtained by taking the natural ordering suggested by the following list:

1. The first $\binom{n}{2}$ of these operators are $E_{j,k} + E_{k,j}$ for $1 \leq j < k \leq n$.
2. The next $\binom{n}{2}$ of these operators are $iE_{j,k} - iE_{k,j}$ for $1 \leq j < k \leq n$.
3. The last $n - 1$ of these operators are

$$\sum_{j=1}^{k} E_{j,j} - kE_{k+1,k+1} \tag{54}$$

   for $k = 1, \ldots, n-1$.

It will be convenient later to make use of the observation that $1 \leq \|G_j\|_2 \leq n$ for all $j \in \{1, \ldots, n^2-1\}$.

Let us now define $N = (n^2-1)^2$, which is to be viewed hereafter as a function of whatever value of $n \geq 2$ is under consideration. Let $H_1, \ldots, H_N \in \mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n)$ be the operators obtained by tensoring together the operators $G_1, \ldots, G_{n^2-1}$ in all possible pairs:

$$H_1 = G_1 \otimes G_1, \quad H_2 = G_1 \otimes G_2, \quad \ldots, \quad H_N = G_{n^2-1} \otimes G_{n^2-1}. \tag{55}$$

The operators $H_1, \ldots, H_N$ represent an orthogonal basis for the real vector space

$$\mathcal{V}_n = \big\{X \in \mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n) \,:\, \big(\mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathbb{C}^n)}\big)(X) = 0,\ \big(\mathbb{1}_{\mathrm{L}(\mathbb{C}^n)} \otimes \mathrm{Tr}\big)(X) = 0\big\}. \tag{56}$$

The relevance of this space is that the smallest real affine subspace of $\mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n)$ that contains $J(\Phi)$ for every mixed-unitary channel of the form $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ is equal to

$$\mathcal{V}_n + \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n}. \tag{57}$$

Note that $1 \leq \|H_j\|_2 \leq n^2 < N$ for every $j \in \{1, \ldots, N\}$.

Next, consider the affine linear mapping $\varphi_n : \mathbb{R}^N \to \mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n)$ given by

$$\varphi_n(x) = x(1)H_1 + \cdots + x(N)H_N + \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n}. \tag{58}$$

This function is one-to-one, and as $x \in \mathbb{R}^N$ ranges over all vectors, $\varphi_n(x)$ ranges over the Choi representations of all trace-preserving, unital, and Hermitian-preserving maps.

Finally, define

$$\mathcal{K}_N = \big\{x \in \mathbb{R}^N \,:\, \varphi_n(x) = J(\Phi) \text{ for } \Phi \in \mathrm{C}(\mathbb{C}^n) \text{ mixed-unitary}\big\}, \tag{59}$$

define $\mathcal{K}_k = \mathcal{B}_k(0,1)$ for each positive integer k that does not take the form $(n^2-1)^2$ for an integer $n \geq 2$, and let $\mathcal{K} = \{\mathcal{K}_1, \mathcal{K}_2, \ldots\}$. The particular choice $\mathcal{K}_k = \mathcal{B}_k(0,1)$ when $k \neq (n^2-1)^2$ for any integer $n \geq 2$ is not really important—it is just a trivial choice of a set for each such dimension that will allow the reduction to work. Each $\mathcal{K}_N$ is the preimage of the compact and convex set of mixed-unitary channels under an affine linear map, from which it follows that $\mathcal{K}_N$ is also compact and convex. Of course $\mathcal{K}_k$ is trivially compact and convex when $k \neq (n^2-1)^2$ for every integer $n \geq 2$.

To prove that $\mathcal{K}$ is polynomially bounded, suppose first that $x \in \mathcal{K}_N$ for $N = (n^2-1)^2$, so that $\varphi_n(x) = J(\Phi)$ for $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ a mixed-unitary channel. Because Φ is a channel, it is the case that

$$\|J(\Phi)\|_2 \leq \|J(\Phi)\|_1 = \mathrm{Tr}(J(\Phi)) = n; \tag{60}$$

the inequality follows from the fact that $\|X\|_2 \leq \|X\|_1$ for all operators, the first equality follows from the fact that $J(\Phi)$ is positive semidefinite whenever Φ is a channel, and the second equality follows from the fact that Φ must preserve trace. Because the operators $H_1, \ldots, H_N$ are orthogonal and traceless (and therefore orthogonal to $\mathbb{1}_n \otimes \mathbb{1}_n$), we conclude that

$$\|J(\Phi)\|_2^2 = \sum_{j=1}^{N} x(j)^2 \|H_j\|_2^2 + \left\| \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\|_2^2 = \sum_{j=1}^{N} x(j)^2 \|H_j\|_2^2 + 1. \tag{61}$$

As $\|H_j\|_2 \geq 1$ for every $j \in \{1, \ldots, N\}$, it follows that

$$\|x\|^2 \leq \sum_{j=1}^{N} x(j)^2 \|H_j\|_2^2 = \|J(\Phi)\|_2^2 - 1 \leq n^2 - 1, \tag{62}$$

and therefore $\|x\| < n$. It has therefore been proved that $\mathcal{K}_N \subseteq \mathcal{B}_N(0,n)$. Of course, when $k \neq (n^2-1)^2$ for every integer $n \geq 2$, it trivially holds that $\mathcal{K}_N \subseteq \mathcal{B}_N(0,1)$.

To prove that there exists a ball with inverse polynomial radius within each set $\mathcal{K}_N$, we will make use of the following theorem, which was proved in [Wat09].

Theorem 10. *Let n be a positive integer and let $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ be a trace-preserving, unital, and Hermitian-preserving map. If it is the case that*

$$\left\| J(\Phi) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\| \leq \frac{1}{n(n^2-1)}, \tag{63}$$

then Φ is a mixed-unitary channel.

For an arbitrary choice of $x \in \mathbb{R}^N$, the mapping Φ given by $J(\Phi) = \varphi_n(x)$ satisfies

$$\begin{aligned} \left\| J(\Phi) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\|^2 &\leq \left\| J(\Phi) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\|_2^2 \\ &= \sum_{j=1}^{N} x(j)^2 \|H_j\|_2^2 \leq n^4 \sum_{j=1}^{N} x(j)^2 = n^4 \|x\|^2. \end{aligned} \tag{64}$$

Therefore, if

$$\|x\| \leq \frac{1}{n^3(n^2-1)}, \tag{65}$$

then

$$\left\| J(\Phi) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\| \leq \frac{1}{n(n^2-1)}, \tag{66}$$

so Φ is mixed-unitary by Theorem 10. As $N^2 > n^3(n^2-1)$, we conclude that

$$\mathcal{B}_N(0, 1/N^2) \subseteq \mathcal{K}_N. \tag{67}$$

When $k \neq (n^2-1)^2$ for every integer $n \geq 2$, it trivially holds that $\mathcal{B}_N(0,1) \subseteq \mathcal{K}_N$.

In conclusion, for all positive integers k, it is the case that

$$\mathcal{B}_k(0, 1/k^2) \subseteq \mathcal{K}_k \subseteq \mathcal{B}_k(0, k^2), \tag{68}$$

and therefore $\mathcal{K}$ is polynomially bounded. By Theorem 8 it therefore follows that

$$\mathrm{WOPT}(\mathcal{K}) \leq_T^p \mathrm{WMEM}(\mathcal{K}) \tag{69}$$

for this choice of $\mathcal{K}$.

4.3 From unitary quadratic minimization to weak optimization

In order to prove that UQM $\leq_T^p$ MUD, we will establish the following chain of reductions:

$$\mathrm{UQM} \leq_m^p \mathrm{WOPT}(\mathcal{K}) \leq_T^p \mathrm{WMEM}(\mathcal{K}) \leq_m^p \mathrm{MUD}. \tag{70}$$

The Turing reduction has already been established in the previous subsection, and in the current subsection we will prove that the first mapping reduction holds.

To this end, consider an arbitrary instance

$$(A_1, \ldots, A_k, \alpha, 0^m) \tag{71}$$

of UQM. We will first describe the instance of $\mathrm{WOPT}(\mathcal{K})$ to which each such instance of UQM maps, and then we will argue the correctness of the reduction.

1. Define an operator $P \in \mathrm{Herm}(\mathbb{C}^n \otimes \mathbb{C}^n)$, vectors $w, v \in \mathbb{R}^N$, and a real number $\gamma \in \mathbb{R}$ as follows:

$$\begin{aligned} P &= \sum_{j=1}^{k} \mathrm{vec}(A_j)\,\mathrm{vec}(A_j)^*, \\ w &= \big(\langle P, H_1\rangle, \ldots, \langle P, H_N\rangle\big), \\ v &= \frac{w}{kN^2}, \\ \gamma &= \alpha - \frac{\mathrm{Tr}(P)}{knN^2} + \frac{1}{2kmN^2}. \end{aligned} \tag{72}$$

   (The vec mapping refers to the vectorization of an operator $A \in \mathrm{L}(\mathbb{C}^n)$:

$$\mathrm{vec}(A) = \sum_{1 \leq i,j \leq n} A(i,j) e_i \otimes e_j, \tag{73}$$

   which is equivalent to taking the rows of the matrix representation of A, transposing them to obtain column vectors, and then stacking these column vectors on top of one another to form a single vector.)

2. Define $u \in \mathbb{R}^N$ as

$$u(j) = \frac{\operatorname{trunc}\big(8kmnN^3 v(j)\big)}{8kmnN^3} \tag{74}$$

for each $j \in \{1, \ldots, N\}$ and define

$$\beta = \frac{\operatorname{trunc}(8kmN^2\gamma)}{8kmN^2}. \tag{75}$$

(The truncation function is defined as $\operatorname{trunc}(\theta) = \lfloor \theta \rfloor$ and $\operatorname{trunc}(-\theta) = -\lfloor \theta \rfloor$ for $\theta \geq 0$, so that it always rounds toward zero.)

3. The output of the reduction is $(u, \beta, 0^r)$ for $r = 8kmn^4N^3$.

It is evident that $(u, \beta, 0^r)$ is polynomial-time computable from $(A_1, \ldots, A_k, \alpha, 0^m)$. Moreover, under the assumption that α is upper-bounded by a polynomial, the number β and the entries of u can be expressed as ratios of polynomially bounded integers. The reduction is therefore a strong polynomial-time mapping reduction.

It remains to argue that if $(A_1, \ldots, A_k, \alpha, 0^m)$ is a yes-instance of UQM then $(u, \beta, 0^r)$ is a yes-instance of WOPT($\mathcal{K}$), and if $(A_1, \ldots, A_k, \alpha, 0^m)$ is a no-instance of UQM then $(u, \beta, 0^r)$ is a no-instance of WOPT($\mathcal{K}$). First we note, by the assumption that $\|A_j\|_2 \leq 1$ for each $j \in \{1, \ldots, k\}$, that $\operatorname{Tr}(P) \leq k$. The norm of w may therefore be upper-bounded,

$$\|w\| = \left(\sum_{j=1}^{N} |\langle P, H_j \rangle|^2\right)^{\frac{1}{2}} \leq \left(\sum_{j=1}^{N} \|P\|_1^2 \|H_j\|^2\right)^{\frac{1}{2}} \leq \sqrt{k^2 N^3} < kN^2, \tag{76}$$

which implies $\|v\| \leq 1$. As the entries of u are obtained from v by truncations, it is therefore clear that $\|u\| \leq 1$.

Next, observe that

$$\big\langle P, \operatorname{vec}(U) \operatorname{vec}(U)^* \big\rangle = \sum_{j=1}^{k} \big|\big\langle A_j, U \big\rangle\big|^2 \tag{77}$$

for every unitary operator $U \in \mathrm{U}(\mathbb{C}^n)$. It is evident that

$$\min_{\Phi \in \mathrm{MU}(\mathbb{C}^n)} \big\langle P, J(\Phi) \big\rangle = \min_{U \in \mathrm{U}(\mathbb{C}^n)} \big\langle P, \operatorname{vec}(U) \operatorname{vec}(U)^* \big\rangle, \tag{78}$$

by virtue of the fact that the function $J(\Phi) \mapsto \langle P, J(\Phi) \rangle$ is linear, the unitary channels are the extreme points of the set of mixed-unitary channels, and the Choi representation of a unitary channel $\Phi(X) = UXU^*$ is

$$J(\Phi) = \operatorname{vec}(U) \operatorname{vec}(U)^*. \tag{79}$$

It is also the case that

$$\min_{x \in \mathcal{K}_N} \big\langle P, \varphi_n(x) \big\rangle = \min_{\Phi \in \mathrm{MU}(\mathbb{C}^n)} \big\langle P, J(\Phi) \big\rangle \tag{80}$$

because $\varphi_n(x)$ ranges over the set $\mathrm{MU}(\mathbb{C}^n)$ as x ranges over $\mathcal{K}_N$. Finally, for any choice of a vector $x \in \mathbb{R}^N$, it is the case that

$$\big\langle P, \varphi_n(x) \big\rangle = x(1)\langle P, H_1 \rangle + \cdots + x(N)\langle P, H_N \rangle + \frac{\operatorname{Tr}(P)}{n} = \langle w, x \rangle + \frac{\operatorname{Tr}(P)}{n}. \tag{81}$$

Altogether, this implies that

$$\min_{x \in \mathcal{K}_N} \langle v, x \rangle = \frac{1}{kN^2} \min_{U \in \mathrm{U}(\mathbb{C}^n)} \sum_{j=1}^{k} \big|\big\langle A_j, U \big\rangle\big|^2 - \frac{\operatorname{Tr}(P)}{knN^2}. \tag{82}$$

If $(A_1, \ldots, A_k, \alpha, 0^m)$ is a yes-instance of UQM, then it follows that

$$\min_{x \in \mathcal{K}_N} \langle v, x \rangle \leq \frac{\alpha}{kN^2} - \frac{\mathrm{Tr}(P)}{knN^2} = \gamma - \frac{1}{2kmN^2}, \tag{83}$$

while if $(A_1, \ldots, A_k, \alpha, 0^m)$ is a no-instance of UQM, then

$$\min_{x \in \mathcal{K}_N} \langle v, x \rangle \geq \frac{\alpha}{kN^2} - \frac{\mathrm{Tr}(P)}{knN^2} + \frac{1}{kmN^2} = \gamma + \frac{1}{2kmN^2}. \tag{84}$$

We now turn to the vector u and the real number β, which may be viewed as approximations of v and γ, respectively. In particular,

$$\|u - v\| \leq \|u - v\|_1 \leq \frac{1}{8kmnN^2} \tag{85}$$

and

$$|\beta - \gamma| \leq \frac{1}{8kmN^2}. \tag{86}$$

We have already proved that $\|x\| \leq n$ for every $x \in \mathcal{K}_N$, and this implies that

$$\big|\langle u, x \rangle - \langle v, x \rangle\big| \leq \frac{1}{8kmN^2} \tag{87}$$

for all $x \in \mathcal{K}_N$. We conclude that

$$\min_{x \in \mathcal{K}_N} \langle u, x \rangle \leq \beta - \frac{1}{4kmN^2} \quad \text{or} \quad \min_{x \in \mathcal{K}_N} \langle u, x \rangle \geq \beta + \frac{1}{4kmN^2}, \tag{88}$$

depending on whether $(A_1, \ldots, A_k, \alpha, 0^m)$ is a yes- or no-instance of UQM, respectively.

Now, observe that for every $x \in \mathcal{K}_N$ and $\varepsilon \in [0, 1]$, it is the case that

$$\mathcal{B}_N\left((1-\varepsilon)x, \frac{\varepsilon}{n(n^2-1)N}\right) \subseteq \mathcal{K}_N. \tag{89}$$

This is a consequence of Theorem 10, for if $z \in \mathbb{R}^N$ satisfies

$$\|z\| \leq \frac{1}{n(n^2-1)N}, \tag{90}$$

then

$$\left\| \varphi_n(z) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\| \leq \left\| \varphi_n(z) - \frac{\mathbb{1}_n \otimes \mathbb{1}_n}{n} \right\|_2 \leq N \|z\| \leq \frac{1}{n(n^2-1)}, \tag{91}$$

so that $\varphi_n(z) \in \mathrm{MU}(\mathbb{C}^n)$, and therefore $(1-\varepsilon)\varphi_n(x) + \varepsilon\varphi_n(z)$ is a convex combination of mixed-unitary channels. In particular, for

$$\varepsilon = \frac{1}{8kmnN^2} \tag{92}$$

we have that

$$\mathcal{B}_N\left((1-\varepsilon)x, \frac{1}{r}\right) \subseteq \mathcal{K}_N \tag{93}$$

for every $x \in \mathcal{K}_N$. If $(A_1, \ldots, A_k, \alpha, 0^m)$ is a yes-instance of UQM, then there must exist $x \in \mathcal{K}_N$ so that

$$\langle u, x \rangle \leq \beta - \frac{1}{4kmN^2}. \tag{94}$$

As

$$\big|\langle u, x \rangle - \langle u, (1-\varepsilon)x \rangle\big| = \varepsilon |\langle u, x \rangle| < \varepsilon n \tag{95}$$

it is the case that

$$\langle u, (1-\varepsilon)x\rangle \leq \beta - \frac{1}{8kmN^2}. \tag{96}$$

This implies that $(u, \beta, 0^r)$ is a yes-instance of WOPT($\mathcal{K}$).

Finally, if $(A_1, \ldots, A_k, \alpha, 0^m)$ is a no-instance of UQM, then

$$\langle u, x\rangle \geq \beta + \frac{1}{4kmN^2} \tag{97}$$

for every $x \in \mathcal{K}_N$. For every $x \in \mathcal{B}_N(\mathcal{K}_N, 1/r)$ we therefore have

$$\langle u, x\rangle \geq \beta + \frac{1}{4kmN^2} - \frac{1}{r} \geq \beta + \frac{1}{8kmN^2}, \tag{98}$$

where the first inequality makes use of the fact that $\|u\| \leq 1$. This implies that $(u, \beta, 0^r)$ is a no-instance of WOPT($\mathcal{K}$), and therefore completes the proof that UQM $\leq_m^p$ WOPT($\mathcal{K}$).

4.4 From weak membership to mixed-unitary detection

The remaining reduction in the chain (70) is the reduction WMEM($\mathcal{K}$) $\leq_m^p$ MUD, which we prove in this subsection.

Before describing the reduction, it will be helpful to observe the following fact: if $N = (n^2-1)^2$ for some integer $n \geq 2$, and $y, z \in \mathbb{R}^N$ are arbitrary vectors, then for the mappings Ψ and Ξ defined by $J(\Psi) = \varphi_n(y)$ and $J(\Xi) = \varphi_n(z)$, it is the case that

$$\|J(\Psi) - J(\Xi)\|_2^2 = \sum_{j=1}^{N} (y(j) - z(j))^2 \|H_j\|_2^2 \geq \|y - z\|^2, \tag{99}$$

by virtue of the fact that $\|H_j\|_2 \geq 1$ for every $j \in \{1, \ldots, N\}$.

Now consider an arbitrary instance $(x, 0^m)$ of WMEM($\mathcal{K}$). There are two cases to be considered, the first of which is that $x \in \mathbb{R}^N$ for $N = (n^2-1)^2$, where $n \geq 2$ is an integer. In this case, the first step of the reduction is to compute a vector $z \in \mathbb{R}^N$ as follows:

$$z(j) = \frac{\operatorname{trunc}\big(2mNx(j)\big)}{2mN}. \tag{100}$$

The vector z satisfies $\|x - z\| \leq 1/(2m)$, and is such that every entry shares the same denominator $2mN$. (This property will be needed to guarantee that the reduction is strong, and specifically to avoid a situation in which a polynomial number of rational numbers, each of which has a polynomially bounded denominator, have an exponentially large least common denominator.) The second and final step of the reduction is to output the instance

$$\big(\varphi_n(z), 0^{2m}\big) \tag{101}$$

of MUD.

To prove that this reduction operates correctly for the case being considered, let Φ and Ξ be the maps defined by $J(\Phi) = \varphi_n(x)$ and $J(\Xi) = \varphi_n(z)$, let Ψ be any unital, trace-preserving, and Hermitian-preserving map that satisfies

$$\|J(\Psi) - J(\Xi)\|_2 \leq \frac{1}{2m}, \tag{102}$$

and let $y \in \mathbb{R}^N$ be the unique vector satisfying $J(\Psi) = \varphi_n(y)$. By (99) we have $\|y - z\| \leq 1/(2m)$, and therefore $\|x - y\| \leq 1/m$. If $(x, 0^m)$ is a yes-instance of WMEM($\mathcal{K}$), we therefore have that $y \in \mathcal{K}_N$, which implies that Ψ is a mixed-unitary channel, and hence $(J(\Xi), 0^{2m}) = (\varphi_n(z), 0^{2m})$ is a

yes-instance of MUD. Similarly, if $(x, 0^m)$ is a no-instance of WMEM($\mathcal{K}$), we have that $y \notin \mathcal{K}_N$, which implies that Ψ is not mixed-unitary, and hence $(J(\Xi), 0^{2m}) = (\varphi_n(z), 0^{2m})$ is a no-instance of MUD.

In the case that $(x, 0^m)$ is an instance of WMEM($\mathcal{K}$) for which $x \in \mathbb{R}^k$ for k a positive integer that is not of the form $(n^2-1)^2$ for some choice of an integer $n \geq 2$, it is straightforward to decide whether $(x, 0^m)$ is a yes-input or no-input by simply computing the norm of x numerically to additive error strictly less than $1/m$, then comparing the result to 1. In case $(x, 0^m)$ is a yes-instance of WMEM($\mathcal{K}$), the reduction may output any fixed yes-instance of MUD, and if $(x, 0^m)$ is a no-instance of WMEM($\mathcal{K}$), then the reduction may output any fixed no-instance of MUD. It has therefore been been proved that WMEM($\mathcal{K}$) $\leq_m^p$ MUD, which completes the proof that UQM $\leq_T^p$ MUD.

5 Conclusion

We have proved that it is strongly NP-hard, with respect to polynomial-time Turing reductions, to determine if a given quantum channel is mixed-unitary, promised that the given channel is not within an inverse-polynomial distance to the boundary of the set of mixed-unitary channels. We conclude with a couple of open problems relating to this result.

1. What is the computational difficulty of deciding if a given channel is mixed-unitary, given stronger promises on the channel's distance from the boundary of the set of mixed-unitary channels? For example, one may consider the problem in which a given channel is promised either to be mixed-unitary or to be at an inverse logarithmic (or even constant) distance from the boundary of the mixed-unitary channels.

   We note that these two examples are likely to be more sensitive to the specific choice of a distance measure from the boundary of the mixed-unitary channels, in comparison to the inverse polynomial distance case we have considered in this paper. A variety of distance measures between channels, including the trace-norm, 2-norm, and spectral-norm distances between their Choi representations, as well as the completely bounded trace norm (or diamond norm) distance between channels, are all equivalent to one another within a polynomial factor, but not within a logarithmic or constant factor.

2. As was suggested in the introduction, an operator $X \in \mathrm{L}(\mathbb{C}^n \otimes \mathbb{C}^n)$ satisfies $X = J(\Phi)$ for a mixed-unitary channel $\Phi : \mathrm{L}(\mathbb{C}^n) \to \mathrm{L}(\mathbb{C}^n)$ if and only if $X = n\rho$ for ρ being a bipartite quantum state of two n-dimensional systems that can be expressed as a convex combination of maximally entangled pure states:

   $$\rho = \sum_{k=1}^{N} p_k u_k u_k^*, \tag{103}$$

   where $u_1, \ldots, u_N \in \mathbb{C}^n \otimes \mathbb{C}^n$ satisfy

   $$\big(\mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathbb{C}^n)}\big)(u_k u_k^*) = \mathbb{1}_n \tag{104}$$

   for each $k \in \{1, \ldots, N\}$. Our main result therefore establishes that it is NP-hard to determine whether or not a given bipartite quantum state can be expressed as a convex combination of maximally entangled pure states.

   It is also NP-hard to determine whether or not a given bipartite quantum state can be expressed as a convex combination of unentangled pure states (i.e., is a separable state) [Gur03, Ioa07, Gha10, Yu16], and it is interesting that these two extremes represent NP-hard decision problems. The computational hardness of detecting membership in a variety of other convex sets of bipartite (or multipartite) quantum states may also be considered.

3. Is the *mixed-unitary detection* problem NP-hard with respect to polynomial-time mapping reductions? We note that the analogous problem for separable states is also open.

Acknowledgments

This research was supported by Canada's NSERC and the Canadian Institute for Advanced Research.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[AS04] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *Proceedings of the 8th International Workshop on Randomization and Computation*, volume 3122 of *Lecture Notes in Computer Science*, pages 249–260, 2004.

[AU82] Peter Alberti and Armin Uhlmann. *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing*, volume 9 of *Mathematics and Its Applications*. D. Reidel Publishing Company, 1982.

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(3):285–290, 1975.

[ESY84] Shimon Even, Alan Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information & Computation*, 10(3):343–360, 2010.

[GLS88] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer–Verlag, 1988.

[Gur03] Leonid Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, pages 10–19. ACM, 2003.

[HLSW04] Patrick Hayden, Debbie Leung, Peter Shor, and Andreas Winter. Randomizing quantum states: constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[Ioa07] Lawrence Ioannou. Computational complexity of the quantum separability problem. *Quantum Information & Computation*, 7(4):335–370, 2007.

[Liu07] Yi-Kai Liu. *The Complexity of the Consistency and N-Representability Problems for Quantum States*. PhD thesis, University of California, San Diego, 2007.

[Ros08] Bill Rosgen. Additivity and distinguishability of random unitary channels. *Journal of Mathematical Physics*, 49(10):102107, 2008.

[Wat09] John Watrous. Mixing doubly stochastic quantum channels with the completely depolarizing channel. *Quantum Information & Computation*, 9(5):406–413, 2009.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[Yu16] Nengkun Yu. Separability of a mixture of Dicke states. *Physical Review A*, 94(6):060101, 2016.