Testing non-isometry is QMA-complete

Bill Rosgen

bill.rosgen@nus.edu.sg
Centre for Quantum Technologies, National University of Singapore

Abstract. Determining the worst-case uncertainty added by a quantum circuit is shown to be computationally intractable. This is equivalent to detecting when a quantum channel given as a circuit is approximately invertible, or close to a linear isometry, and it is shown to be complete for the complexity class QMA of verifiable quantum computation.

1 Introduction

A fundamental problem in quantum computing is to characterise the behaviour of a physical system that is to be used for computation or communication. Unfortunately, this type of problem becomes intractable for large systems as the dimension of the underlying Hilbert space often grows exponentially with the size of the system being considered. In this talk we consider a simpler problem. Instead of obtaining a complete understanding of a system, we ask only the question: is a given physical process reversible? This is equivalent to detecting when a quantum operation is an isometry on the set of density matrices.

The main result of this talk is that this apparently simpler task is also intractable. This is done by demonstrating that, when formalised properly, it is complete for the class QMA of problems that can be efficiently verified on a quantum computer. The model used is the unitary circuit model with the addition of two operations: the introduction of ancillary qubits in a known pure state and the partial trace. From this result follows the hardness of non-isometry testing in any other model of quantum computing that can approximately simulate this model.

2 Background

The complexity class QMA is the class of all computational problems that can be verified using a quantum proof. For any language L in QMA there is an associated verifier V. This verifier generates from the input string x a unitary quantum circuit V_x. This circuit that takes as input a quantum proof state ρ and some ancillary qubits in the $|0\rangle$ state. To determine whether or not the computation accepts, the circuit V_x is run on this input and one of the output qubits is measured. When $x \in L$, we are promised that there exists a state ρ that will cause this measurement to succeed with probability $1 - \varepsilon$. On the other hand, if $x \notin L$, then no state ρ will cause the verifier to accept with probability more than ε. The exact value of the constant ε is not significant: it can be made arbitrarily small by repeating the protocol in parallel.

The class QMA has complete (promise) problems, which are problems in QMA that are computationally at least as hard as any other problem in the class. This implies that an efficient algorithm for any of these complete problems can be used to find an efficient algorithm for any problem in QMA. The simplest of these complete problems is the 2-local Hamiltonian problem, which is informally the quantum version of the circuit satisfiability problem for unitary circuits with gates of constant size [1]. Several other complete problems for QMA are known, such as the problem of testing whether unitary circuits are close to the identity [2].

This paper adds a new complete problem to this list: the problem of determining if a quantum circuit implements an operation that is close to being reversible. This is shown to be equivalent to the problem of determining if there is an input pure state on which the output of a certain channel is highly mixed, or if the channel always maps pure states to nearly pure states.

3 Non-isometry testing

A map is an isometry if it preserves the inner product $\mathrm{tr}(\rho\sigma)$ of any two density matrices ρ and σ. Equivalently, any linear isometry is given by some unitary operator on a larger Hilbert space. In quantum information terms, a channel is an isometry if and only if it can be implemented as a unitary circuit with access to ancillary qubits in a known pure state.

An important property of the linear isometries is that they do not increase rank. This property does not characterise the isometries. Consider the channel $\Phi(\rho) = |0\rangle\langle 0|$. This channel is not an isometry, but it is also rank non-increasing.

This property can be used to characterise the isometries if we make a small adjustment. The channels that are rank non-increasing when joined with an auxiliary space of arbitrary dimension are exactly the isometries. We call channels satisfying this condition *completely* rank non-increasing. The channel $\Phi(\rho) = |0\rangle\langle 0|$ fails to be completely rank non-increasing. Consider applying this channel to half of the maximally entangled state $|\phi^+\rangle \in \mathcal{H} \otimes \mathcal{H}$. The resulting state is $|0\rangle\langle 0| \otimes \mathbb{1}_{\mathcal{H}}$, which has rank $\dim \mathcal{H}$.

In order to show that non-isometry detection is QMA-complete we consider an approximate version of the problem. This is due to the fact that a protocol for a QMA language is permitted to fail with probability ε. We call a channel Φ taking input density operators on $\mathcal{H}$ an approximate-isometry if $\Phi \otimes I_{\mathcal{H}}$ always maps pure states to states that are within trace distance ε of a pure state. Using this notion, we state the computational problem:

Problem (Non-isometry). For $0 \leq \varepsilon < 1/2$, and a channel $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ given as a mixed-state quantum circuit, the promise problem is to decide between:

Yes: There exists an input pure state $|\psi\rangle \in \mathcal{H}^{\otimes 2}$ such that $(\Phi \otimes I_{\mathcal{H}})(|\psi\rangle\langle\psi|)$ has trace distance at least $2 - \varepsilon$ from any pure state.

No: For all pure states $|\psi\rangle \in \mathcal{H}^{\otimes 2}$, $(\Phi \otimes I_{\mathcal{H}})(|\psi\rangle\langle\psi|)$ is within trace distance ε of a pure state.

The main result is that Non-isometry is QMA complete for $\varepsilon < 1/19$. To show this we prove two things: first, that the problem is as hard as any problem in QMA, and second that the problem is in QMA.

Proving the hardness of this problem is relatively straightforward, as a simple modification of the verifier's circuit in a QMA protocol reduces the question of whether the verifier can be made to accept to the problem of determining if a circuit can be made to output a mixed state.

Placing Non-isometry into QMA is more difficult. The straightforward technique does not work, but a modified version of it involving the swap test to estimate the purity of a state can be made to work. This modified protocol is simple and intuitive. That this protocol works in the exact case (i.e. $\varepsilon = 0$) is easy to see and is presented in the talk. The argument to show that the prover cannot cheat when ε is permitted to grow becomes more technical.

References

[1] Kempe, J., Kitaev, A., Regev, O.: The complexity of the local Hamiltonian problem. SIAM Journal on Computing **35**(5) (2006) 1070–1097

[2] Janzing, D., Wocjan, P., Beth, T.: "Non-identity-check" is QMA-complete. International Journal of Quantum Information **3**(3) (2005) 463–473