Testing quantum circuits and detecting insecure encryption

Bill Rosgen

Centre for Quantum Technologies, National University of Singapore

arXiv:1108.1052

Centre for Quantum Technologies
National University of Singapore

Overview

We show that computational problem of testing the behaviour of quantum circuits is hard for QMA. This generalizes previous techniques to prove QMA-hardness for circuit problems. We apply this result to show the hardness of a weak version of detecting the insecurity of a symmetric-key quantum encryption system, or alternately the problem of determining when a quantum channel is not private. We also give a QMA protocol for this problem to show that it is QMA-complete.

Testing quantum circuits

Given a circuit C, does this circuit act like some known circuit C_0 on a large subspace of inputs, or does it act like some other known circuit C_1 on the whole input space? We show this problem is hard for any two families of quantum circuits that are not too close.

Problem ($\mathrm{CT}(\varepsilon, \delta, \mathcal{C}_0, \mathcal{C}_1)$)**.** Let $0 < \varepsilon < 1$, $0 < \delta \leq 1$, and $\mathcal{C}_0, \mathcal{C}_1$ be two uniform families of quantum circuits. The input is a circuit $C \in \mathbf{T}(\mathcal{X}, \mathcal{Y})$. Let C_0 and C_1 be the circuits from $\mathcal{C}_0$ and $\mathcal{C}_1$ that have the same input/output spaces as C. The problem is to decide:

Yes: there is a subspace S of $\mathcal{X}$ with $\dim S \geq (\dim \mathcal{X})^{1-\delta}$ such that for any $\mathcal{R}, \rho \in \mathbf{D}(S \otimes \mathcal{R})$

$$\|(C \otimes \mathbb{1}_{\mathcal{R}})(\rho) - (C_0 \otimes \mathbb{1}_{\mathcal{R}})(\rho)\|_{\mathrm{tr}} \leq \varepsilon,$$

No: $\|C - C_1\|_\diamond \leq \varepsilon$, i.e. for all $\mathcal{R}$ and any $\rho \in \mathbf{D}(\mathcal{X} \otimes \mathcal{R})$

$$\|(C \otimes \mathbb{1}_{\mathcal{R}})(\rho) - (C_1 \otimes \mathbb{1}_{\mathcal{R}})(\rho)\|_{\mathrm{tr}} \leq \varepsilon.$$

This problem is well-defined only for families $\mathcal{C}_0$ and $\mathcal{C}_1$ that do not violate the promise, i.e. any circuits whose output is not too close together. These are the C_0 and C_1 such that there does not exist a subspace T of $\mathcal{X}$ of size $\dim T > \dim \mathcal{X}^\delta$ such that for any input states $\rho \in \mathbf{D}(T \otimes \mathcal{R})$ we have

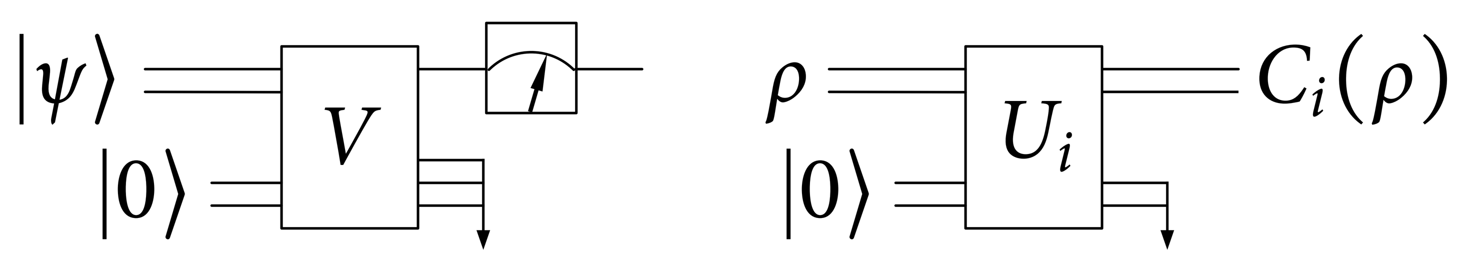
$$\|(C_0 \otimes \mathbb{1}_{\mathcal{R}})(\rho) - (C_1 \otimes \mathbb{1}_{\mathcal{R}})(\rho)\|_{\mathrm{tr}} \leq 2\varepsilon. \quad (1)$$

Note that $\mathcal{C}_0, \mathcal{C}_1$ are part of the problem definition: an algorithm to solve the problem may depend non-uniformly on these families. Notice also than when $\delta = 1$ the problem asks if there are *any* inputs ρ for which $C(\rho) \approx C_0(\rho)$ or if $C(\rho) \approx C_1(\rho)$ for all ρ.

QMA Hardness of circuit testing

Theorem. *$\mathrm{CT}(\varepsilon, \delta, \mathcal{C}_0, \mathcal{C}_1)$ is QMA-hard for any $0 < \varepsilon < 1$ such that $\varepsilon \geq 2^{-p}$ for some polynomial p, any constant $0 < \delta \leq 1$, and any uniform circuit families $\mathcal{C}_0, \mathcal{C}_1$ satisfying* (1).

Proof Sketch: We reduce an arbitrary (promise) problem in QMA to $\mathrm{CT}(\varepsilon, \delta, \mathcal{C}_0, \mathcal{C}_1)$. To prove that CT is QMA-hard, we embed the problem of deciding if an arbitrary QMA verifier V accepts into an equivalent instance of the CT problem.



(a) QMA verifier (b) Circuit C_i

Figure 1: The starting point for the reduction is a QMA verifier. The circuits implementing C_0 and C_1 are part of the problem definition and do not depend on V.

Using these circuits, the reduction constructs a circuit C that runs the verifier V and then behaves like either C_0 or C_1 depending on whether the verifier would have accepted part of the input state. C is a "yes" instance of CT if and only if V can be made to accept.

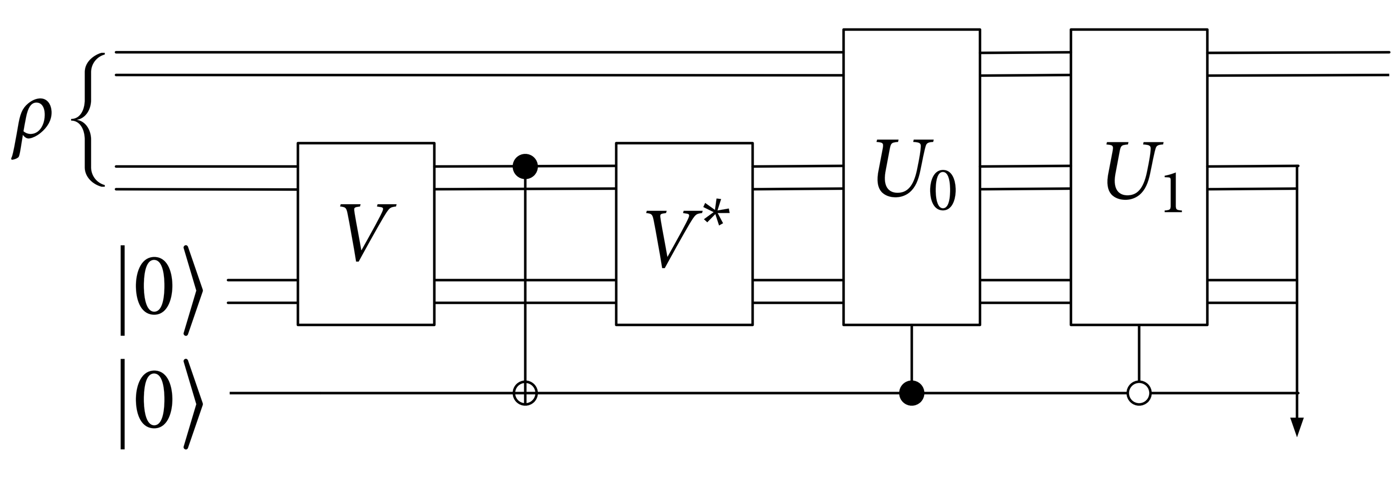


Figure 2: Instance C of the CT problem produced by the reduction.

Essential to the argument is that if the verifier V accepts or rejects with high probability, the result is essentially a "gentle measurement" of the output qubit. The portion of the input that is sent only to the circuits U_0 and U_1 serves to ensure that if V accepts any state, then V must "accept" on a subspace of dimension at least $(\dim \mathcal{X})^{1-\delta}$. Using this we show that the instance C is equivalent to deciding if V accepts some input state. □

Other QMA hardness results

The hardness of many circuit problems follows immediately from the hardness of the circuit testing problem, which can be used as a general tool to prove QMA-hardness. What follows is a list of some of these problem. Ω is the completely depolarizing channel.

Problem ((Mixed) Non-identity Check **(See [2])**)**.** Let $0 < \varepsilon < 1$. On input a circuit $C \in \mathbf{T}(\mathcal{X}, \mathcal{X})$, the promise problem is to decide between:

Yes: $\|C - \mathbb{1}\|_\diamond \geq 2 - \varepsilon$ and there exists an efficient unitary U such that on some pure state $|\psi\rangle \in \mathcal{X}$ we have $\|C(|\psi\rangle\langle\psi|) - U|\psi\rangle\langle\psi|U^*\|_{\mathrm{tr}} \leq \varepsilon$ and $\|U|\psi\rangle\langle\psi|U^* - |\psi\rangle\langle\psi|\|_{\mathrm{tr}} \geq 2 - \varepsilon$.

No: $\|C - \mathbb{1}\|_\diamond \leq \varepsilon$.

This is QMA-hard as $\mathrm{CT}(\varepsilon, 1, \mathcal{U}, \mathbb{1})$ is a special case for $\mathcal{U}$ is any uniform family of unitary quantum circuits that are not close to the identity. The requirement on yes instances that C is close to a unitary U on some input state is not needed for hardness, but is required for the phase-estimation based QMA verifier for this problem [2].

Problem (Non-isometry [3])**.** Let $0 < \varepsilon < 1/2$. On input a circuit $C \in \mathbf{T}(\mathcal{X}, \mathcal{Y})$ the promise problem is to decide between:

Yes: There exists $|\psi\rangle \in \mathcal{X}$ such that $\|(\Phi \otimes \mathbb{1}_{\mathcal{X}})(|\psi\rangle\langle\psi|)\|_\infty \leq \varepsilon$,

No: For all $|\psi\rangle \in \mathcal{X}$, $\|(\Phi \otimes \mathbb{1}_{\mathcal{X}})(|\psi\rangle\langle\psi|)\|_\infty \geq 1 - \varepsilon$.

This is QMA-hard as $\mathrm{CT}(\varepsilon, 1, \Omega, \mathbb{1})$ is a special case.

Problem (Pure Fixed Point)**.** Let $0 < \varepsilon < 1$. On input a circuit $C \in \mathbf{T}(\mathcal{X}, \mathcal{X})$ the promise problem is to decide between:

Yes: There exists $|\psi\rangle \in \mathcal{X}$ such that $\|C(|\psi\rangle\langle\psi|) - |\psi\rangle\langle\psi|\|_{\mathrm{tr}} \leq \varepsilon$

No: For any $|\psi\rangle \in \mathcal{X}$, $\|C(|\psi\rangle\langle\psi|) - |\psi\rangle\langle\psi|\|_{\mathrm{tr}} \geq 2 - \varepsilon$

This is QMA-hard as $\mathrm{CT}(\varepsilon, 1, \mathbb{1}, \Omega)$ is a special case.

Let $S_{\min}(C) = \min_\rho S(C(\rho))$ be the minimum output entropy of the channel C (where S is the von Neumann entropy). This problem is related to a problem in [1].

Problem (Minimum Output Entropy)**.** Let $0 < \varepsilon < 1/2$. On input a circuit $C \in \mathbf{T}(\mathcal{X}, \mathcal{X})$ the promise problem is to decide between:

Yes: $S_{\min}(C) \leq \varepsilon \log \dim \mathcal{X}$

No: $S_{\min}(C) \geq (1 - \varepsilon) \log \dim \mathcal{X}$

This is QMA-hard as $\mathrm{CT}(\varepsilon/2, 1, \mathbb{1}, \Omega)$ is a special case, by the Fannes Inequality.

Detecting insecure encryption

How difficult is it to verify the security of a symmetric-key quantum encryption scheme that acts on n qubits, given a full circuit implementation? The QMA-hardness of this problem implies that you cannot verify an encryption system from an untrusted party.

Problem (Detecting Insecure Encryption)**.** For $0 < \varepsilon < 1$ and $0 < \delta \leq 1$ an instance of the problem consists of a quantum circuit E that takes as input a quantum state as well as a m classical bits, such that for each $k \in \{0,1\}^m$ the circuit implements a quantum channel $E_k \in \mathbf{T}(\mathcal{X}, \mathcal{Y})$ with $\dim \mathcal{Y} \geq \dim \mathcal{X}$. The promise problem is to decide between:

Yes: There exists a subspace S of $\mathcal{X}$ with $\dim S \geq \dim \mathcal{X}^{1-\delta}$ such that for any reference space $\mathcal{R}$, any $\rho \in \mathbf{D}(S \otimes \mathcal{R})$, and any key k, $\|(E_k \otimes \mathbb{1}_{\mathcal{R}})(\rho) - \rho\|_{\mathrm{tr}} \leq \varepsilon$.

No: E is an ε-private channel, i.e. $\left\|\Omega - \frac{1}{2^m}\sum_{k \in \{0,1\}^m} E_k\right\|_\diamond \leq \varepsilon$, where Ω is the completely depolarizing channel in $\mathbf{T}(\mathcal{X}, \mathcal{Y})$, and there exists a polynomial-size quantum circuit D such that for all k we have $\|D_k \circ E_k - \mathbb{1}_{\mathcal{X}}\|_\diamond \leq \varepsilon$.

Informally, the problem is to distinguish two cases: either the circuit fails to encrypt a large subspace of the input (for all keys), or the channel is close to perfect.

The QMA-hardness of this problem follows from the hardness of CT. A QMA verifier can be constructed for this problem using the swap test.

Theorem. *For $0 < \varepsilon < 1/8$ and $0 < \delta \leq 1$, the problem $\mathrm{DI}_{\varepsilon,\delta}$ is QMA-complete.*

References

[1] S. Beigi and P. W. Shor. On the complexity of computing zero-error and Holevo capacity of quantum channels, 2007. EPRINT: arXiv:0709.2090v3 [quant-ph].

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

[3] B. Rosgen. Testing non-isometry is QMA-complete. In *Proc. TQC*, pp. 63–76. 2010.