Non-isometry testing is QMA-complete

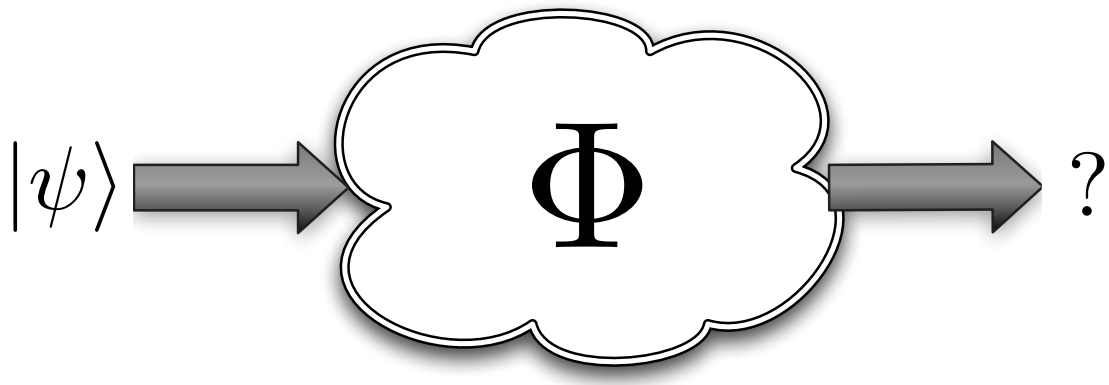
Bill Rosgen

Centre for Quantum Technologies
National University of Singapore

April 15, 2010

Detecting non-isometry

- How hard is it to test that a channel Φ is noisy?
- i.e. is there some $|\psi\rangle$ for which $\Phi(|\psi\rangle\langle\psi|)$ has large entropy?



- This is a weak process tomography problem.
- Estimating worst-case behaviour of a channel.
- Formalized properly: QMA-complete.

Outline

Representations of channels

- A *channel* is a linear CPTP map.
- Two representations we will need:

Choi: A channel may be represented by the matrix

$$\mathrm{C}(\Phi) = (\Phi \otimes I)(|\phi^+\rangle\langle\phi^+|)$$

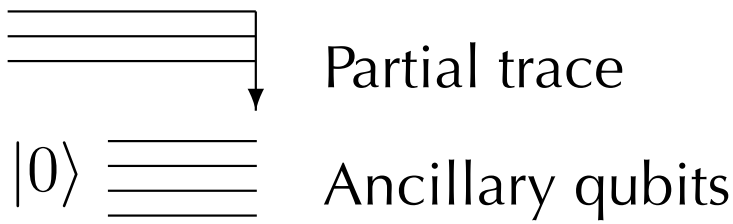
Kraus: There exist r operators A_i such that

$$\sum_{i=1}^{r} A_i^* A_i = \mathbb{1} \text{ and } \Phi(X) = \sum_{i=1}^{r} A_i X A_i^*$$

where $r = \operatorname{rank} \mathrm{C}(\Phi)$.

Mixed-state quantum circuits

- A channel can also be represented as a circuit, using unitary gates plus two non-unitary gates:

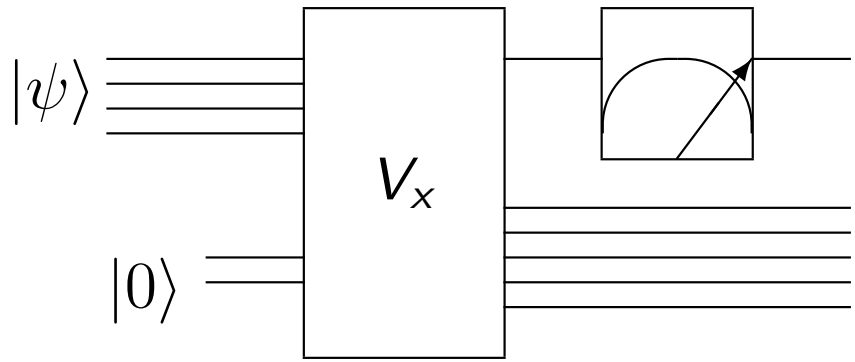


For efficient quantum computations this representation

- is exponentially smaller than a matrix representation,
- allows small modifications (i.e. controlled-Φ)

QMA

QMA is the set of all languages L for which there exist polynomial-time unitary circuits V such that:



- When $x \in L$, $\exists |\psi\rangle$ such that outcome is $|1\rangle$ with Pr $\geq 1 - \varepsilon$
- When $x \notin L$, $\forall |\psi\rangle$ the outcome is $|1\rangle$ with Pr $\leq \varepsilon$

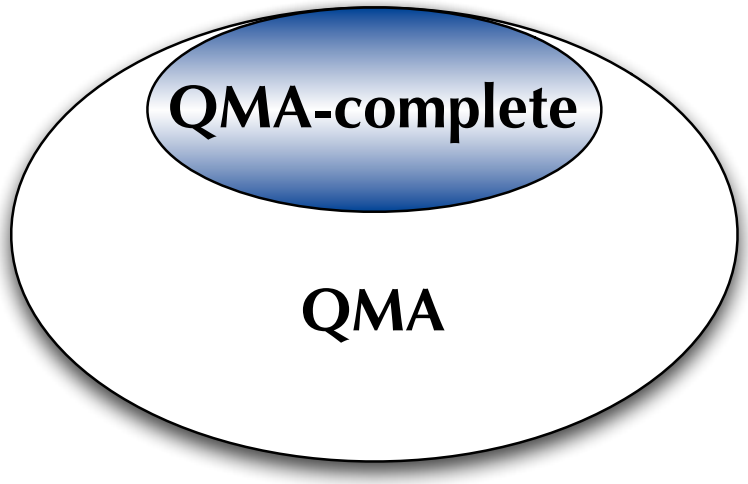
i.e. there is a $|\psi\rangle$ verifier accepts (w.h.p.) if and only if $x \in L$.

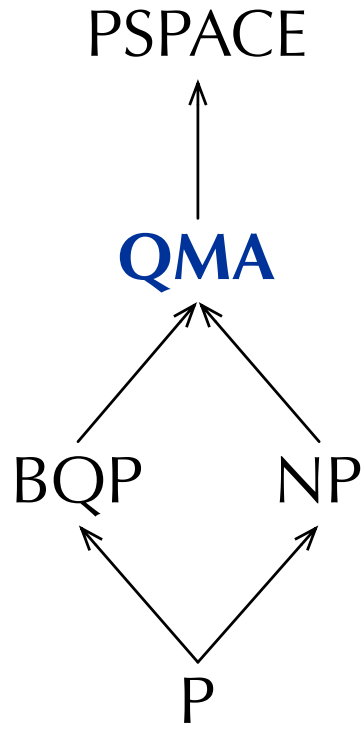
QMA-completeness

QMA has complete problems, i.e. problems

1. as hard as any problem in QMA,
2. contained in QMA.

Example: 2-local Hamiltonian [KKR 2006].





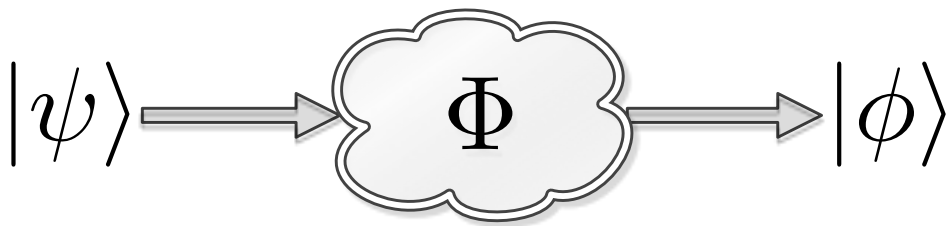
Outline

Rank non-increasing channels

- A channel Φ is *rank non-increasing* if for all ρ

$$\text{rank}(\rho) \geq \text{rank}(\Phi(\rho)))$$

- By linearity Φ does not increase rank if and only if it maps pure states to pure states.



These channels need not be isometries, however:

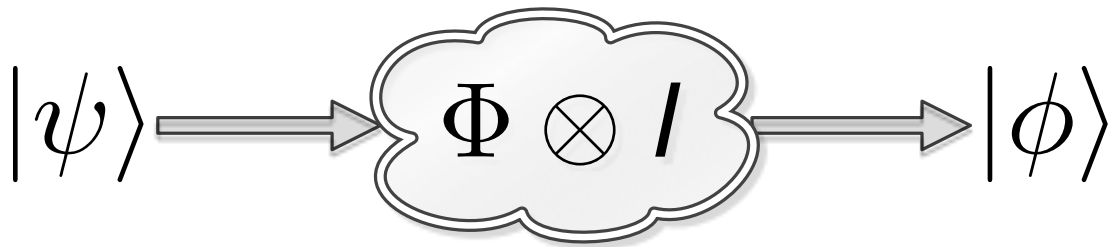
- $\Psi(\rho) = |0\rangle\langle 0|$ does not increase rank.

Completely rank non-increasing channels

- A channel Φ is *completely* rank non-increasing if for all spaces $\mathcal{F}$ and all states ρ

$$\text{rank}(\rho) \geq \text{rank}((\Phi \otimes I_{\mathcal{F}})(\rho)))$$

- This property characterizes the isometries.

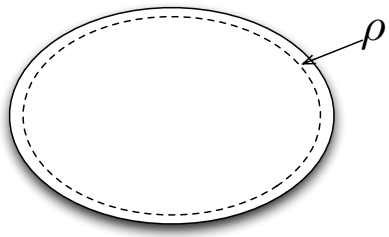


- $\Psi(\rho) = |0\rangle\langle 0|$ is not completely rank non-increasing:

$$\Psi(|\phi^+\rangle\langle\phi^+|) = |0\rangle\langle 0| \otimes \mathbb{1}$$

Approximately pure states

- QMA algorithms fail with small probability.
  - Need to define the approximate isometries



Definition

A state ρ is ε-*pure* if $\min_{|\psi\rangle} \|\rho - |\psi\rangle\langle\psi|\|_{\text{tr}} \leq \varepsilon$.

- Equivalent definitions (up to constants):
  - $\text{tr}(\rho^2) \geq 1 - \varepsilon$,
  - $\|\rho\|_\infty \geq 1 - \varepsilon$.

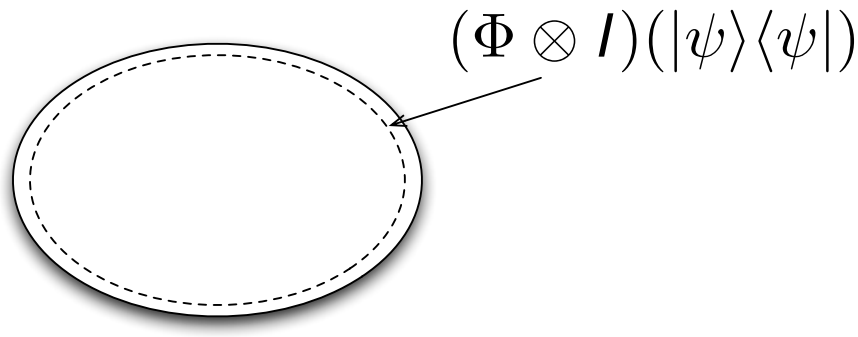
Approximate isometries

Definition

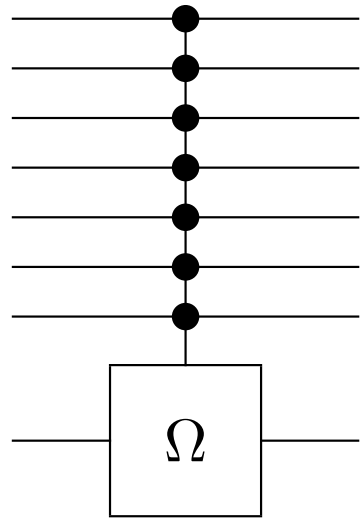
Φ is an approximate isometry if

$$(\Phi \otimes I)(|\psi\rangle\langle\psi|) \text{ is } \varepsilon\text{-pure}$$

for all $|\psi\rangle$.



- This is a worst-case definition.
- Average case (purity of $C(\Phi)$) is in BQP.
- If Ψ is the n-controlled completely depolarizing channel:
  1. Ψ is not a $1/2$-isometry
  2. $C(\Psi)$ is $1/2^n$-pure



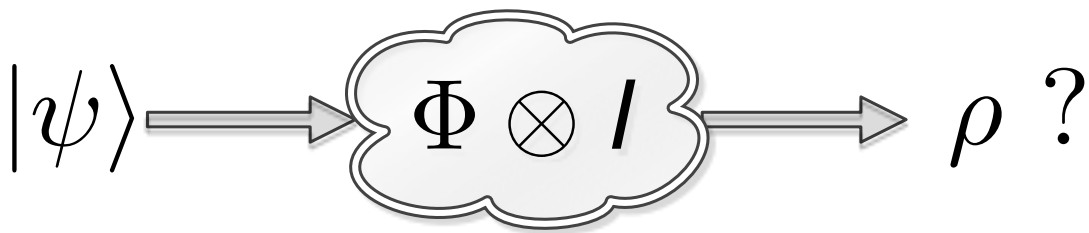
Computational problem

Non-isometry$_\varepsilon$

Given a mixed-state circuit Φ, decide between

Yes: For some $|\psi\rangle$, $(\Phi \otimes I)(|\psi\rangle\langle\psi|)$ is $2-\varepsilon$ far from pure,

No: Φ is an approximate isometry.

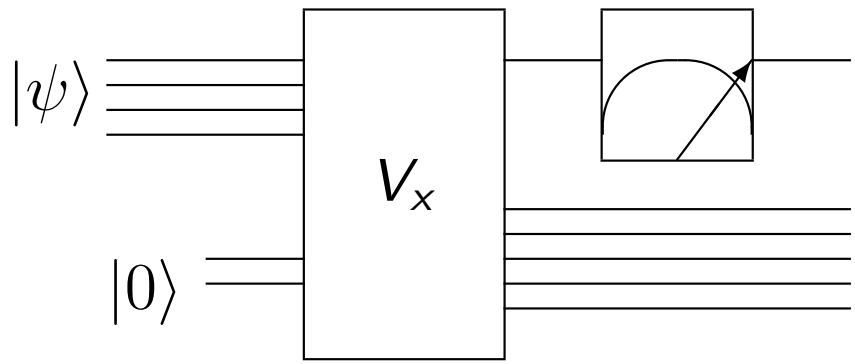


Is there pure input $|\psi\rangle$ on which $\Phi \otimes I$ outputs a highly mixed state, or is the output of $\Phi \otimes I$ always close to pure?

Outline

QMA proof system

- Given an arbitrary QMA language L and input x, then if the measurement in the following circuit

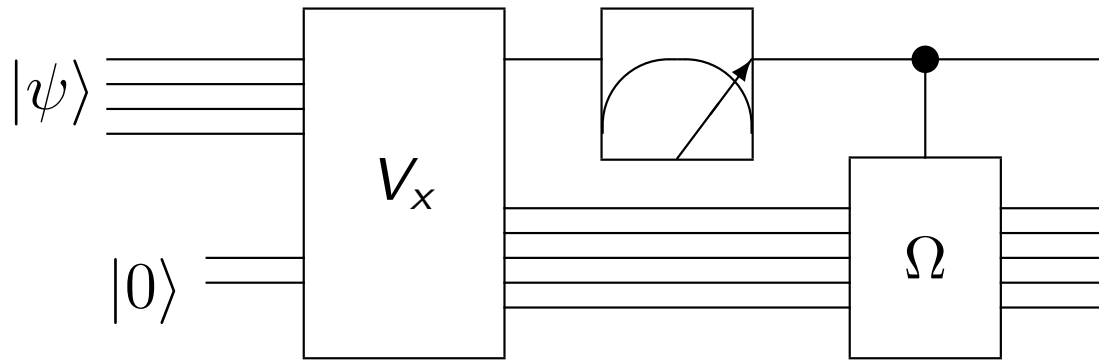


- is $|1\rangle$ with probability $1-\varepsilon$ on some $|\psi\rangle$, then $x \in L$
- is $|1\rangle$ with probability at most ε on all $|\psi\rangle$, then $x \notin L$.

- Goal: Using V_x, build a circuit that outputs a highly mixed state if and only if $x \in L$

Isometry testing problem

- Add a controlled application of the completely depolarizing channel:



- if $x \in L$, there is $|\psi\rangle$ with output $(1-2\varepsilon)$-far from pure
- if $x \notin L$, output state is 2ε-pure for any $|\psi\rangle$

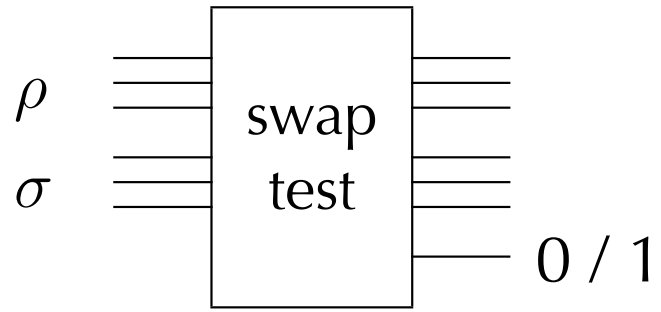
- This circuit is close to an isometry if and only if $x \notin L$
- Non-isometry$_\varepsilon$ is QMA-hard for any $\varepsilon \geq \text{poly}(1/n)$.

Outline

Verifying non-isometry

Idea: given $|\psi\rangle$, check that $(\Phi \otimes I)(|\psi\rangle\langle\psi|)$ is mixed.

- The swap test measures the symmetric and antisymmetric subspaces.



Antisymmetric outcome occurs with probability:

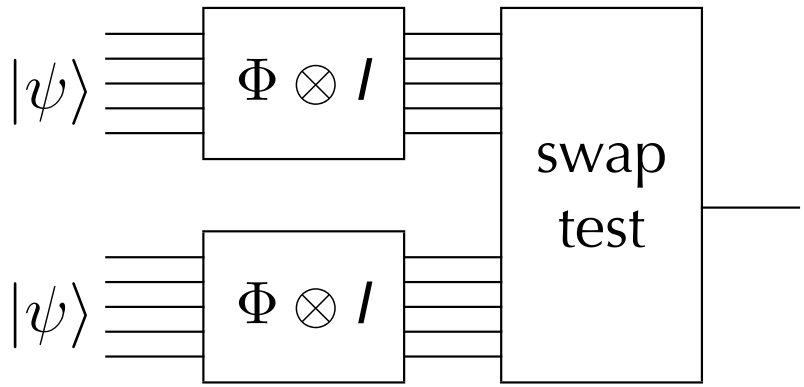
$$\frac{1}{2}(1 - |\langle\phi|\psi\rangle|^2) \text{ on input } |\psi\rangle \otimes |\phi\rangle$$

$$\frac{1}{2}(1 - \mathrm{tr}(\rho^2)) \text{ on input } \rho \otimes \rho$$

The swap test provides a test for purity (given two copies).

QMA protocol: first attempt

- Idea: on two copies run circuit in parallel, do swap test.



- The output is 'antisymmetric' with probability

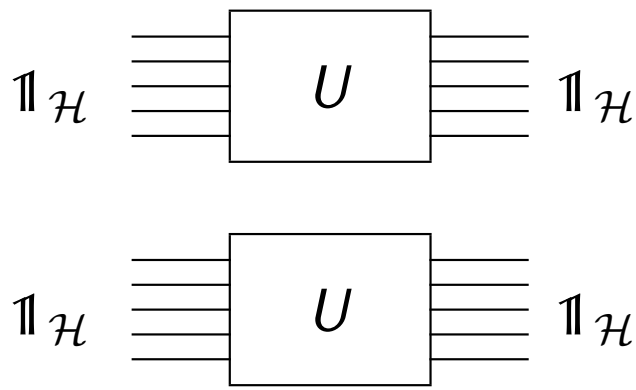
$$\frac{1}{2} - \frac{1}{2} \operatorname{tr}\left[(\Phi \otimes I)(|\psi\rangle\langle\psi|)^2\right]$$

- i.e. given input $|\psi\rangle \otimes |\psi\rangle$ on which the channel produces a highly mixed state, can solve the non-isometry problem.

Why this doesn't work

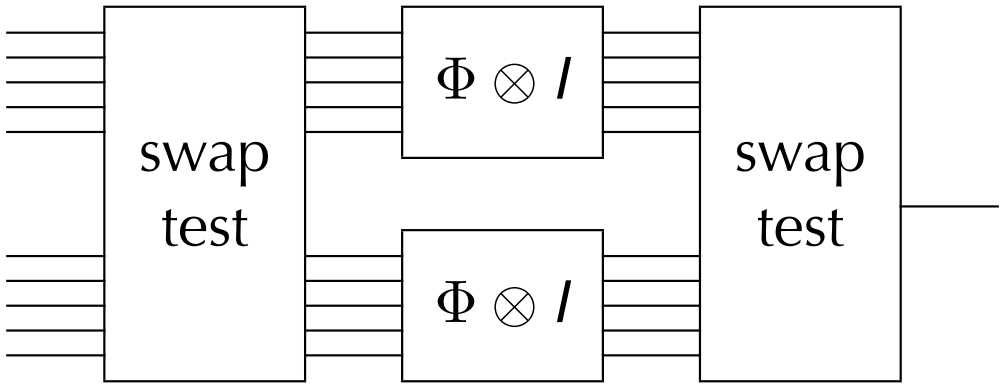
How can the Verifier check that the witness is $|\psi\rangle \otimes |\psi\rangle$?

- If the witness is $\mathbb{1}_{\mathcal{H}\otimes\mathcal{H}}$, the Verifier accepts unitaries as far from isometries with probability $1/2$.



- The Verifier can ensure the input is symmetric.
- The symmetry of states is preserved by isometries (or almost preserved, in the approximate case).

QMA protocol



1. V receives a witness state $\rho \in \mathbf{D}(\mathcal{H} \otimes \mathcal{H})$
2. V rejects if swap test on ρ returns antisymmetric
3. V computes $\sigma = [(\Phi \otimes I)^{\otimes 2}](\rho)$
4. V accepts if swap test on σ returns antisymmetric

- If the channel far from an isometry, there is a state $|\psi\rangle \otimes |\psi\rangle$ on which V accepts with probability $1/2 - \varepsilon$.

Isometries preserve symmetry

Claim: $(\Phi \otimes I)^{\otimes 2}$ preserves symmetry for Φ an isometry.

Proof.

Applying $(\Phi \otimes I)^{\otimes 2}$ to $|ij\rangle + |ji\rangle$ results in a state of the form

$$|\phi_i \phi_j\rangle + |\phi_j \phi_i\rangle.$$

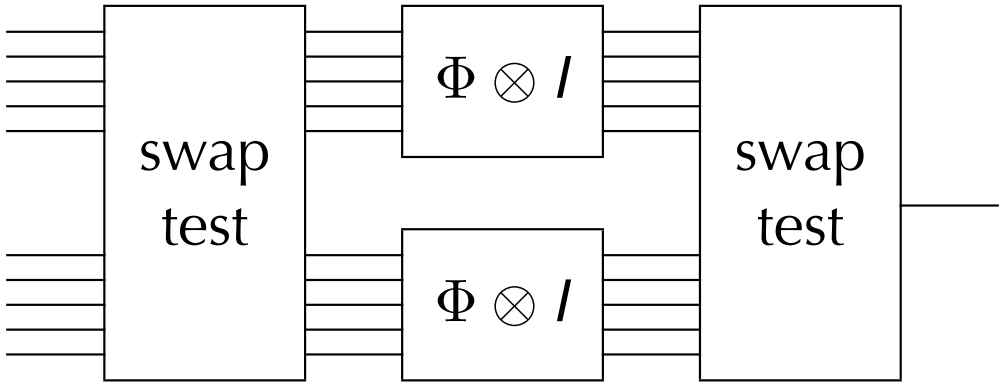
Swapping the two subsystem leaves the state unchanged:

$$\text{swap}(|\phi_i \phi_j\rangle + |\phi_j \phi_i\rangle) = |\phi_j \phi_i\rangle + |\phi_i \phi_j\rangle,$$

i.e. symmetry is preserved. □

- This implies that V never accepts an *exact* isometry.
- Approximate case is more work (see paper).

Containment in QMA



- When Φ is far from an isometry, there is a state that V accepts with probability $\geq \frac{1}{2} - \varepsilon$.
- When Φ is close to an isometry V accepts any input ρ with probability $\leq 9\varepsilon$.

- i.e. Non-isometry$_\varepsilon$ is in QMA for all $\varepsilon < \frac{1}{19}$.

QMA-completeness

Results:

- Non-isometry$_\varepsilon$ is QMA-complete, for any $\varepsilon < 1/19$.
- Detecting when a circuit can increase the rank of any input state (up to a perturbation of norm ε) is also QMA-complete.

Implications:

- Determining worst-case behaviour of systems is hard.
- Deciding when an operation is close to unitary in some model of quantum computation is intractable.