Efficient Noise Estimation With MUBs

Christoph Dankert

Institute for Quantum Computing

University of Waterloo

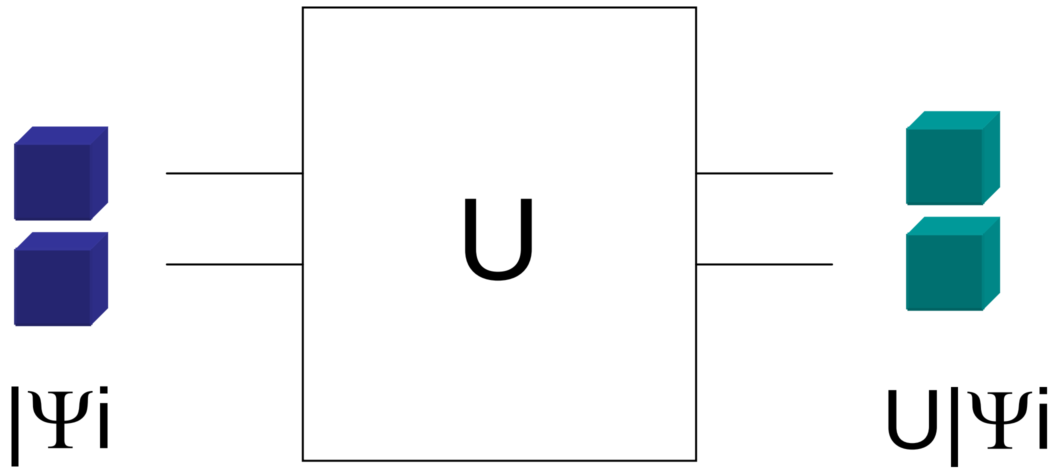
CS-QIC Calgary 2005

Joint work with Richard Cleve, Joseph Emerson, Etera Livine

Outline

- Noise in Quantum Computation
- Figure of Merit for Implementations
- Estimating the Average Gate Fidelity
- Mutually-Unbiased Bases
- Efficient Noise Estimation with MUBs

Quantum Algorithms

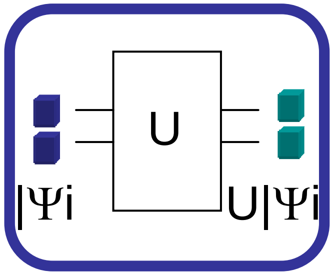


+ Measurement

Shor's Factoring Algorithm,
Discrete Log Algorithm,
Fourier Transform,
. . .

Noise in Quantum Computation

Goal: Compute U|ψi perfectly for some algorithm U and starting state |ψi 2 C^d

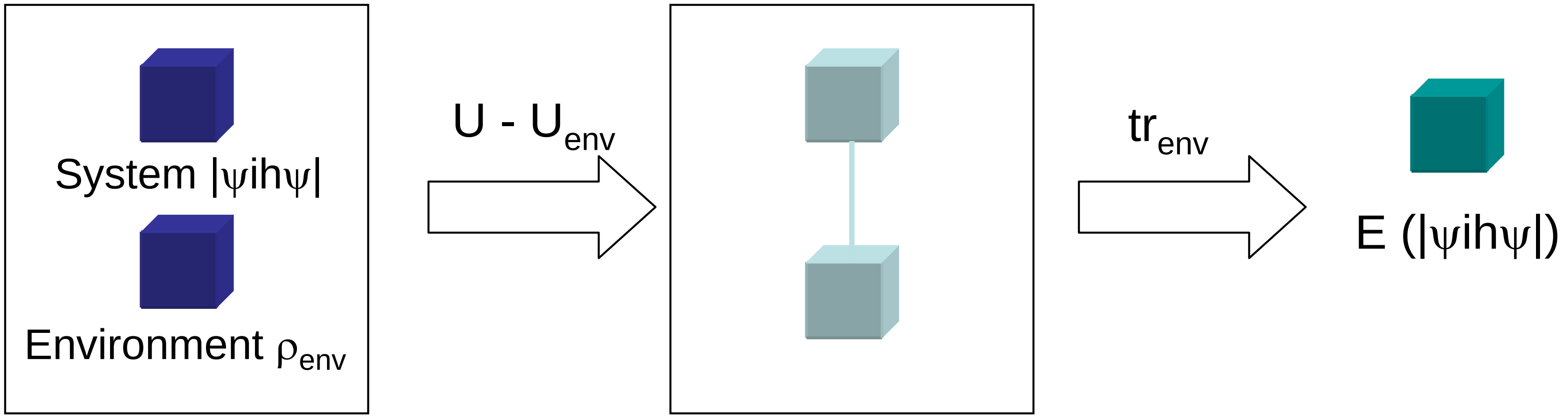

U

|Ψi

U|Ψi

Actual: Noisy implementation that introduces phase errors, bit flips, and decoherence. Have mixed states, i.e. we need density operators.

Think of noise as unitary operation in larger system followed by tracing out over the environment.


System |ψihψ|

Environment ρ_{env}

U - U$_{env}$

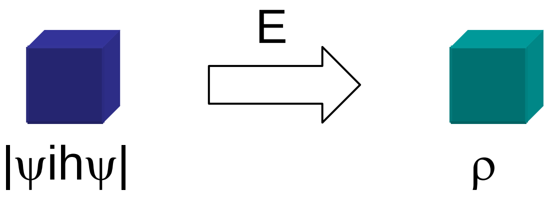
tr$_{env}$

E (|ψihψ|)

General Quantum Maps

An actual implementation of U is a quantum map E:

- Linear
- Trace-preserving or decreasing
- Completely positive
- Acts on density operators rather than states



Can decompose E using Kraus operators to describe noisy U:

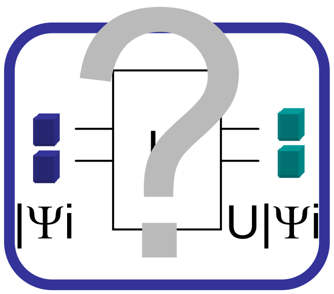
$$E(|\psi\rangle\langle\psi|) = \sum_{k=1}^{d^2} A_k|\psi\rangle\langle\psi|A_k^\dagger = \sum_{k=1}^{d^2} U E_k|\psi\rangle\langle\psi|E_k^\dagger U^\dagger$$

where

$$\sum_k A_k^\dagger A_k = \sum_k E_k^\dagger E_k = 1;$$

Figure of Merit for Implementations

How good does an implementation of U work?



How well does a quantum channel transmit information?

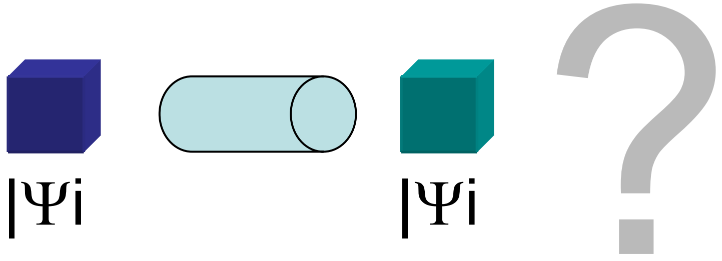
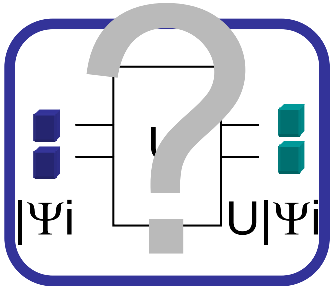


Figure of Merit for Implementations

How good does an implementation of U work?

How well does a quantum channel transmit information?



Fidelity as a distance measure between density operators:

$F(\rho, \sigma) = \mathrm{tr}(\rho\ \sigma^y)$ ⇐ Will use this one, but makes no big difference.

$F(\rho, \sigma) = \mathrm{tr}\ (\rho^{1/2}\sigma\rho^{1/2})^{1/2}$

For a quantum channel or a noisy implementation E, we have

$$F(U|\psi i h\psi|U^y, E(|\psi i h\psi|)) \quad = h\psi|U^y\ E(|\psi i h\psi|)\ U|\psi i$$
$$= 1 \text{ if } E = I, \text{ otherwise less than } 1$$

Will write $F(U, \{E_k\})$ instead.

Minimum and Average Fidelity

Minimum Fidelity:

$F_{min} = \min_{\psi} F(U, \{E_k\})$

Average Fidelity:

$F_{avg} = s\ F(U, \{E_k\})\ d\psi$ using the unitarily invariant measure
$= s\ h\psi|U^{y}\ E(|\psi i h\psi|)\ U|\psi i\ d\psi$ on C^{d}

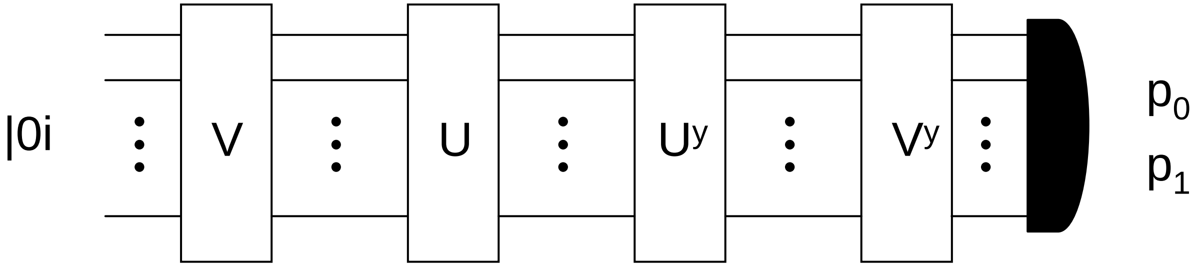
How to measure F_{avg}?

1. Quantum Process/State Tomography to get the E_k; costly (see Nielsen, 2002 – quant-ph/0205035)

2. Random Sampling ← We chose this approach.

Estimating the Average Fidelity

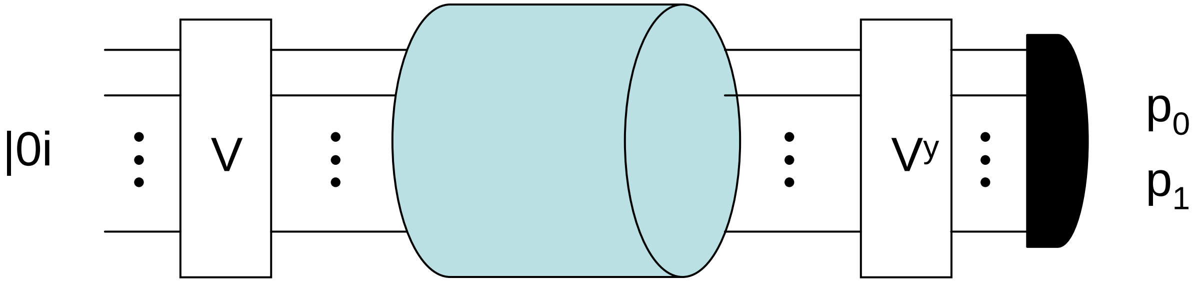
Naive approach: Generate random states using random circuits V.



$p_0 = F_{avg}$ if noise of U and U^y does not cancel out and
noise introduced by V, V^y is neglibible compared to noise in U

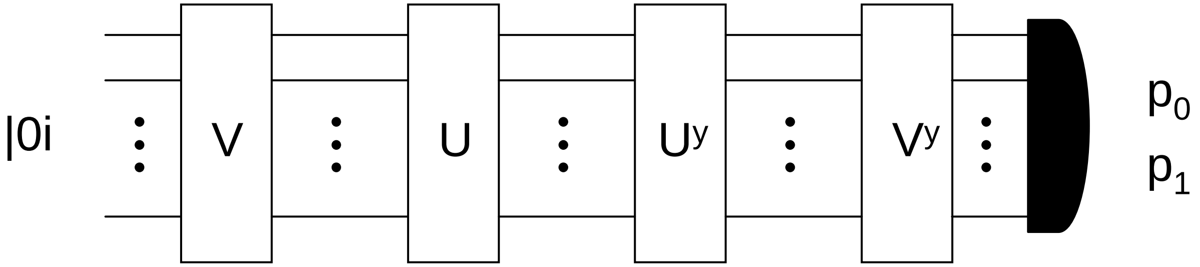
Estimating the Average Fidelity

Works as well for Quantum Channels:



$p_0 = F_{avg}$ if noise of U and U^y does not cancel out and
noise introduced by V, V^y is neglibible compared to noise in U

Estimating the Average Fidelity



$p_0 = F_{avg}$ if noise of U and U^y does not cancel out and
noise introduced by V, V^y is neglibible compared to noise in U

Problem: Generating the V's is costly, of order 2^n gates for most V needed.

Solutions:

1. Efficient Random Circuits
   (see Emerson, Alicki, Zyczkowski 2005 – quant-ph/0503243)

2. Random Sampling over subset of C^d

Outline

- Noise in Quantum Computation
- Figure of Merit for Implementations
- Estimating the Average Gate Fidelity
- Mutually-Unbiased Bases
- MUBs for Efficient Noise Estimation

Mutually-Unbiases Bases (MUB)

An orthonormal basis B for C^d: $B = \{\psi_1, ..., \psi_d\}$

Can we find other orthonormal bases that are orthogonal to B? No.

Can we find orthonormal bases that are almost orthogonal to B? Yes.

To orthonormal bases B_1, B_2 are called mutually-unbiased iff vectors from different bases have overlap 1/d.

$$|\langle\psi|\varphi\rangle| = \frac{1}{\sqrt{d}}$$

Why MUBs?

1. State determination requires measurement wrt d+1 MUBs. (Schwinger, 1960; Ivanovic, 1981)
2. The BB84 Protocol makes use of MUBs.

Existence of MUBs

For prime d, there is a set of d+1 mutually-unbiased bases.
(Klappenecker and Rötteler, 2003 – quant-ph/0309120)

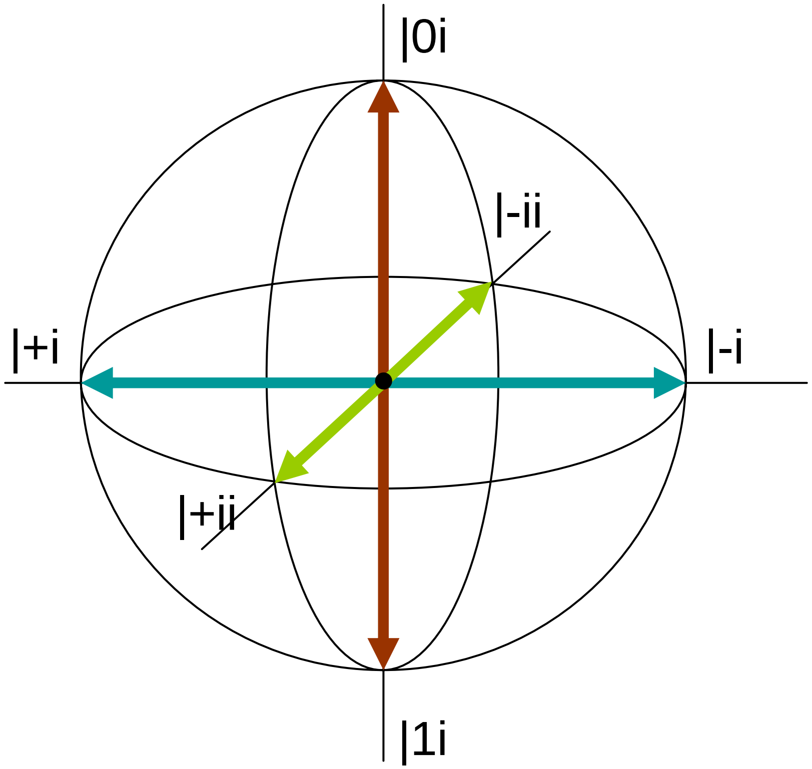
For non-prime d, there are at most d+1 mutually-unbiased bases.
(Wootters and Fields, 1989)

For $d = p_1^{\alpha 1}$ ¢ ¢ ¢ $p_k^{\alpha k}$, there exist $\min_i (p_i + 1)$ MUBs.

Open Problems:

1. How many MUBs exist in C^6 ?
   (Only trivial lower bound of 3 known so far.)
2. How many MUBs exist for general non-prime dimension d?

An Example



The 3 MUBs for a single qubit state.

Construction of MUBs for prime powers d

See Klappenecker & Rötteler, 2003 (quant-ph/0309120).

Denote B_a the a-th basis, and let B_a = {|$\psi^a{}_1$i, ..., |$\psi^a{}_d$i}. Let b denote the index of a vector in such a basis. Clearly a 2 {0, 1, ..., d}, and b 2 {1, ..., d}.

For odd prime powers d: $\text{jÃ}^a_b\text{i}$ 🖫 $\frac{\text{p}}{\text{d}}$ 🗀 $\text{X}^{\text{d}}_{\text{x}🖫🗀}$ $!^{♦☎\text{x}🗎✉\text{bx}➋}_{\text{d}}$ jxi

$e^{2\pi\ i\ /\ d}$

Using finite field arithmetic to compute the trace.

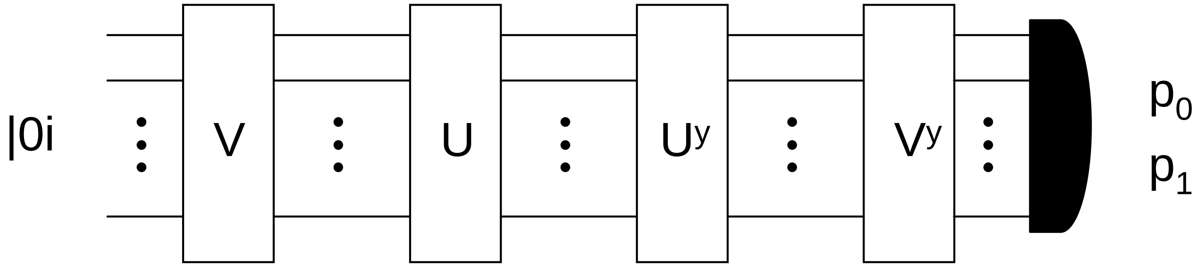
For d = 2^n: $\text{jÃ}^a_b\text{i}$ 🖫 $\frac{\text{p}}{\text{d}}$ 🗀 $\text{X}_{\text{x}\,2\,T_n}$ $!^{♦☎\text{a}✉🗎\text{b}➋\text{x}➋}_{🗐}$ jxi

$e^{2\pi\ i\ /\ 4}$

Using Galois ring arithmetic to compute the trace.

These d bases and the computational basis give d+1 MUBs.

Efficient Noise Estimation



Where V is a circuit that randomly generates an MUB vector $|\psi^a{}_b$i.

$$F_{\mathsf{avg}} = \int \langle\psi|U^\dagger \mathcal{E}(|\psi\rangle\langle\psi|)U|\psi\rangle d|\psi\rangle = \frac{\sum_k |\,\mathsf{tr}\, E_k|^2 + d}{d^2+d}$$

(Horodecki et al., PRA, 1999)

We showed that

$$\frac{1}{d^2+d}\sum_{a=0}^{d}\sum_{b=1}^{d}\langle\psi|U^\dagger \mathcal{E}(|\psi\rangle\langle\psi|)U|\psi\rangle = \frac{\sum_k |\,\mathsf{tr}\, E_k|^2 + d}{d^2+d}$$

⇨ "Cheap" average using MUBs is sufficient!

Proof (sketch)

Lemma 1: Let W be the subspace of all Hermitian traceless linear operators and let

$$W_a = \left\{ \sum_{b=0}^{d-1} r_b |\psi_b^a\rangle\langle\psi_b^a| : \sum_{b=1}^{d} r_b = 0 \right\}.$$

Then $W = \bigoplus_{a=0}^{d} W_a$.

Lemma 2: The operators

$$\Pi_a(V) = \sum_{b=1}^{d} |\psi_b^a\rangle\langle\psi_b^a|V|\psi_b^a\rangle\langle\psi_b^a|$$

on W form a complete set of orthogonal projectors on W.

Corollary 3: For $M, N \in W$,

$$\sum_{a=0}^{d} \mathrm{tr}\,(\Pi_a(M)\Pi_a(N)) = \mathrm{tr}\, MN.$$

Proof sketch (cont'd)

Theorem 4: ☹♏⧫ M ; N 2 W ♋❄⌘♏■

Xd X d hÃ a b jM jÃ a b i hÃ a b jN jÃ a b i ▣ ⧫□M N :

a▣ 🗀 b▣ 🗁

We can extend Theorem 4 to non-traceless Hermitian operators via the trick $\widetilde{M} = M - \frac{\operatorname{tr} M}{d}\mathbb{1}, \widetilde{N} = N - \frac{\operatorname{tr} N}{d}\mathbb{1}$

Corollary 5: ☹♏⧫ M ✍N ♌♏☞ ♏⬧⬧♋⬧♏ ◻◻♏⬧⧫◻◻ ♋❄⌘♏■

X d X d hÃ a b jM jÃ a b i hÃ a b jN jÃ a b i ▣ ⧫□M N ✉⧫□M ⧫□N :

a▣ 🗀 b▣ 🗁

Using another trick, we can extend this to general linear operators:

M 🗁▣ M ✉M y ; M 🖹 ▣ i ☎M ¡ M y ✆, N 🗁▣ N ✉N y ; N 🖹 ▣ i ☎N ¡ N y ✆:

Summing over all four combinations of these, we get Corollary 5 for all linear operators.

Proof sketch (finished)

📂 / d🗎 🖃d X^d X^d hÃjU^y E☎ÃihÃj➀UjÃi ■ P k j ♦□E k j🗎 🖃d / d🗎 🖃d

a■□b■📂

by using the last result and expanding E.

Summary

- Noise in Quantum Algorithms
- Figures of Merit
- Mutually-Unbiased Bases
- Noise Estimation works well with MUBs