Complexity Resources and Sinks in Noisy Quantum Computation

ITT

Engineered for life

Marco Lanzagorta

Quantum Technologies Group

Advanced Engineering & Sciences

ITT Corporation

Collaborators:

Keye Martin, US Naval Research Laboratory

Jeffrey Uhlmann, University of Missouri-Columbia

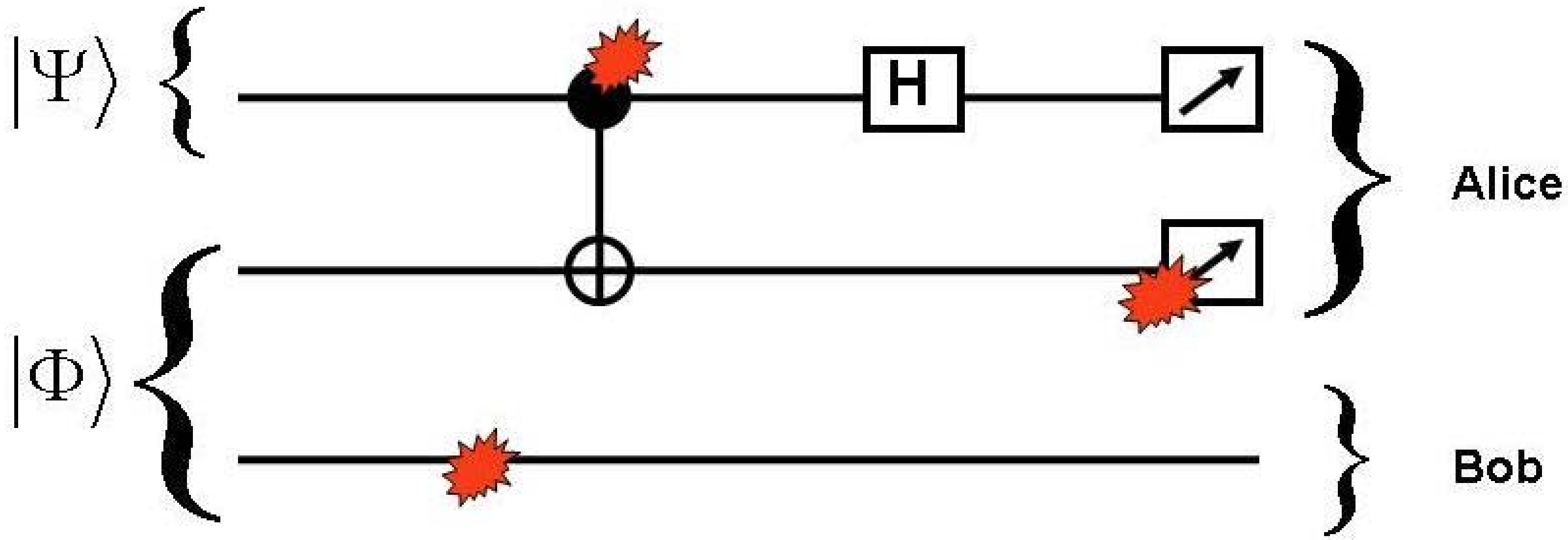
ITT - AES

- One of the largest providers of technology solutions and research services to the US Department of Defense.
  - Sensors, communication, information processing, cryptology, C^4I, radar, sonar, electronic warfare, tracking, guidance, NBCR, and night vision systems.
- Selected as the Top Performing Aerospace / Defense Company by *Aviation Week & Space Technology* magazine in 2007.
- Quantum Technologies Group
  - Quantum Sensing and Communications.
  - Mathematics and Algorithmics of Quantum Information.
  - Quantum Effects in Biological Systems.

Outline

- Noisy Quantum Computation and the Threshold Theorem
- Constant Errors Change Algorithmic Complexity
- Error Scaling Avoids Algorithmic Complexity Penalties
- Circuit Size Complexity Overheads and Tradeoffs
- Quantum Errors as Complexity Sinks
- Noisy Entanglement as a Resource/Sink in Teleportation
- Conclusions

Noisy Quantum Computation



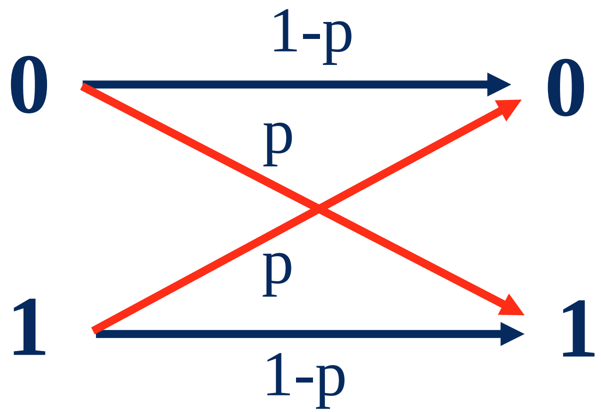
- Quantum information is very susceptible to noise.
- In order to exploit all the advantages of QIS, we require protocols and systems that guarantee fault tolerance.

FTQC: Typical Assumptions

- **Physical Error Models**
  - Random Errors
  - Uncorrelated Errors
  - Error Rate Independent on Number of Qubits
  - No Leakage Errors
- **Error Correction Protocols**
  - Perfect Parallelism
  - Gate Non-Locality
  - Large Supply of Ancilla Qubits

Quantum Error Correction

- Redundancy: encode logical qubit states in multi-qubit states.



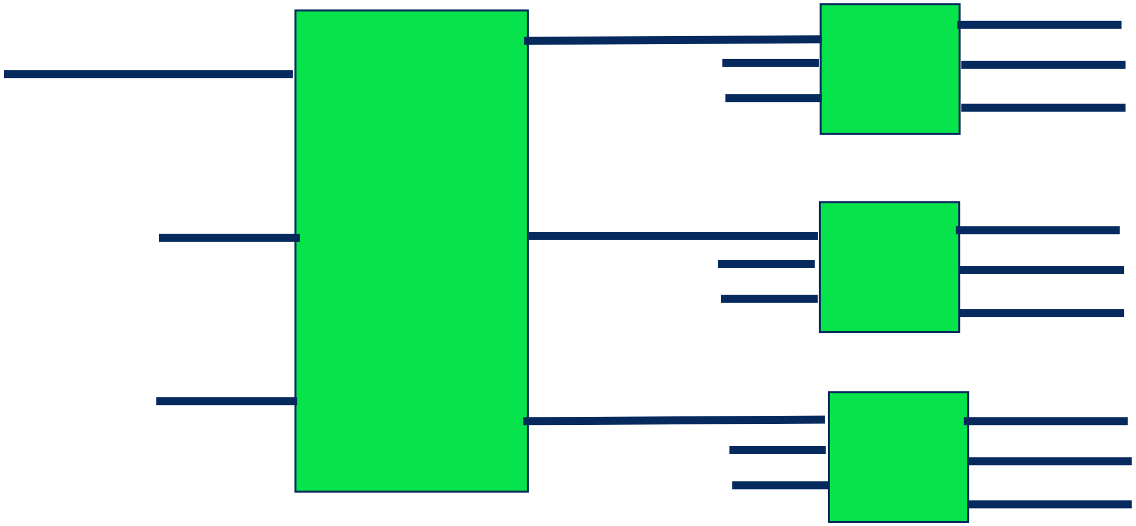
$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

3-qubit bit flip Error QEC

- QEC does not cancels out errors, it merely reduces them.

$$p \rightarrow 3p^2(1-p) + p^3 = 3p^2 - 2p^3 = \mathcal{O}(p^2)$$

Concatenated QEC

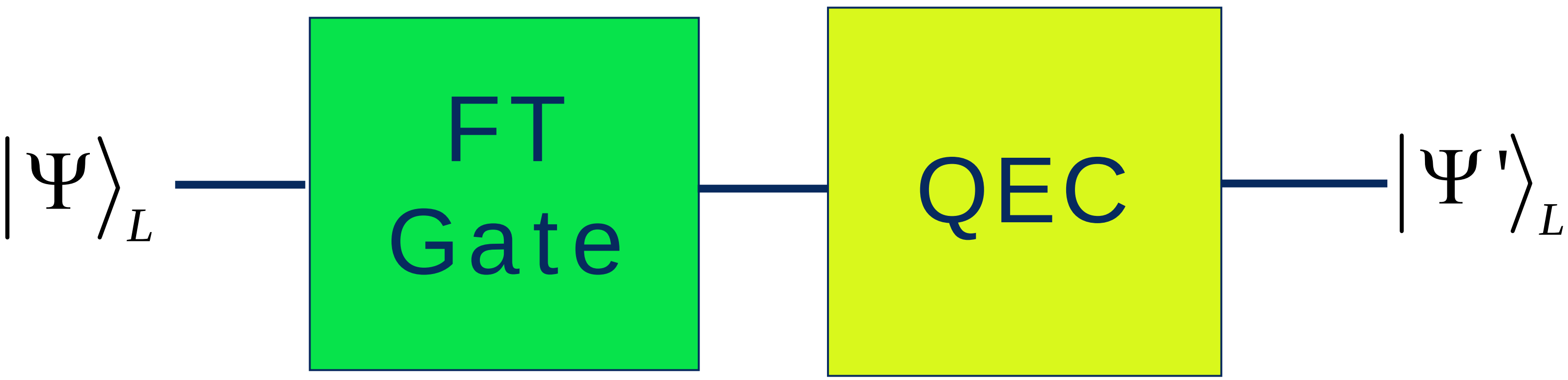


$$\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha|000\rangle+\beta|111\rangle$$

$$\rightarrow \alpha|(000)(000)(000)\rangle+\beta|(111)(111)(111)\rangle$$

$$\Rightarrow\ p \rightarrow \mathcal{O}(p^2) \rightarrow \mathcal{O}(p^4)$$

Fault Tolerant Gates



- Fault tolerant quantum gates operate on *h*-layers of encoded logical qubit states.
- Syndrome measurement and recovery procedures applied after the FT gate.
- c is the total number of places where a failure may occur.

$$\Rightarrow \epsilon \equiv \frac{(cp)^{2^h}}{c}$$

The Threshold Theorem

- Further layers of QEC will decrease the net error probability as long as:

$$\lim_{h \to \infty} \frac{(cp)^{2^h}}{c} = 0 \Leftrightarrow p < 1/c \equiv p_{th}$$

- Therefore, FTQC is only possible if the probability of error p is under a certain threshold value.
- In practice:

$$p_{th} \in \left[10^{-6}, 10^{-5}\right]$$

Fault Tolerant Quantum Computing

- To achieve algorithmic accuracy $\tilde{\epsilon}$ with a circuit of s noisy gates we require:

$$\frac{(cp)^{2^h}}{c} \leq \frac{\tilde{\epsilon}}{s}$$

- Circuit size overhead:

$$O(s \times \log^r (s/\tilde{\epsilon}))$$

$$r = \log d$$

d is the maximum number of operations used in FT for a single gate.

Beyond the Threshold Theorem

$$\frac{(cp)^{2^h}}{c} \leq \frac{\tilde{\epsilon}}{s}$$

- LHS has received lots of attention:
  - More realistic physical error models (*p*).
  - Improved quantum error correction protocols (*c*).
- RHS usually ignored:
  - First order approximation incompatible with complexity theory.

Full Error Model

- Complexity theory: take the **asymptotic limit** of the scaling variable and do **not** make any assumptions about constants.
- Assume a quantum algorithm made of *m* repeated applications of an unitary operator *U*.
- State after *1* iteration:

$$\rho^{(1)} = (1-\epsilon)\hat{U}\rho^{(0)}\hat{U}^{\dagger} + \epsilon\hat{U}_f\rho^{(0)}\hat{U}_f^{\dagger}$$

- State after *m* iterations:

$$\rho^{(m)} = (1-\epsilon)\hat{U}\rho^{(m-1)}\hat{U}^{\dagger} + \epsilon\hat{U}_f\rho^{(m-1)}\hat{U}_f^{\dagger}$$

$$\Rightarrow \rho^{(m)} = (1-\epsilon)^m\hat{U}^m\rho^{(0)}\hat{U}^{\dagger m} + \ldots$$

Constant Error Probability Analysis

- We define *P(j)* as the probability that after *m* iterations the algorithm is completed with *j* errors.

$$P(j) = (1-\epsilon)^{m-j} \epsilon^{j} \binom{m}{j} \qquad \sum_{i=0}^{m} P(i) = 1$$

- Then, the probability that the algorithm will be completed with at least one error is:

$$P_{err} \equiv \sum_{i=1}^{m} P(i) = 1 - P(0) = 1 - (1-\epsilon)^{m}$$

$$\Rightarrow P_{err} \approx 1 - (1 - m\epsilon) = m\epsilon$$

Probability Amplification

- Error will diminish the accuracy of the algorithm. How many times do we need to run it to obtain a target accuracy?

$$\left(P_{err}\right)^k = \left(1-\left(1-\epsilon\right)^m\right)^k \approx \delta \Rightarrow k \approx \frac{\log \delta}{\log\left(1-\left(1-\epsilon\right)^m\right)}$$

- In the asymptotic limit:

$$k \approx -\log \delta \times \left(\frac{1}{1-\epsilon}\right)^m$$

Algorithmic Complexity

- It can be observed that k is a non-trivial function of m (unless the constant uncorrected error is exactly zero)
- Also, m is a scaling function that depends on the number of qubits, gates, and iterations.
- The “true” algorithmic complexity for noisy circuits is:

$$\mathcal{O}(f) \rightarrow \mathcal{O}(f \times k)$$

- **As a consequence, even if they are arbitrarily small, constant uncorrected errors affect algorithmic complexity.**

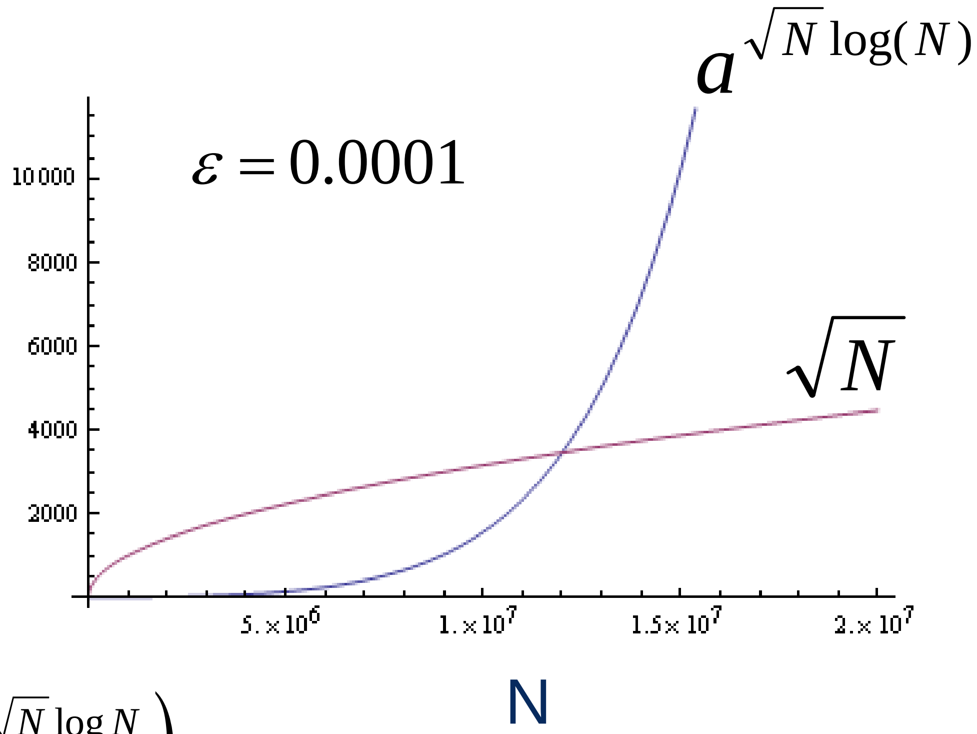
Grover's Algorithm – Complexity

- The values of m and k are:

$$m = O(n \times 2^{n/2})$$

$$k \approx -\log \delta \times \left(\frac{1}{1-\epsilon}\right)^{n\, 2^{n/2}}$$

$$\Rightarrow k = \mathcal{O}\left(a^{\sqrt{N}\log N}\right)$$



- The overall complexity is:

$$\mathcal{O}\left(\sqrt{N} \times k\right) \approx \mathcal{O}\left(\sqrt{N} \times a^{\sqrt{N}\log N}\right)$$

Error Scaling

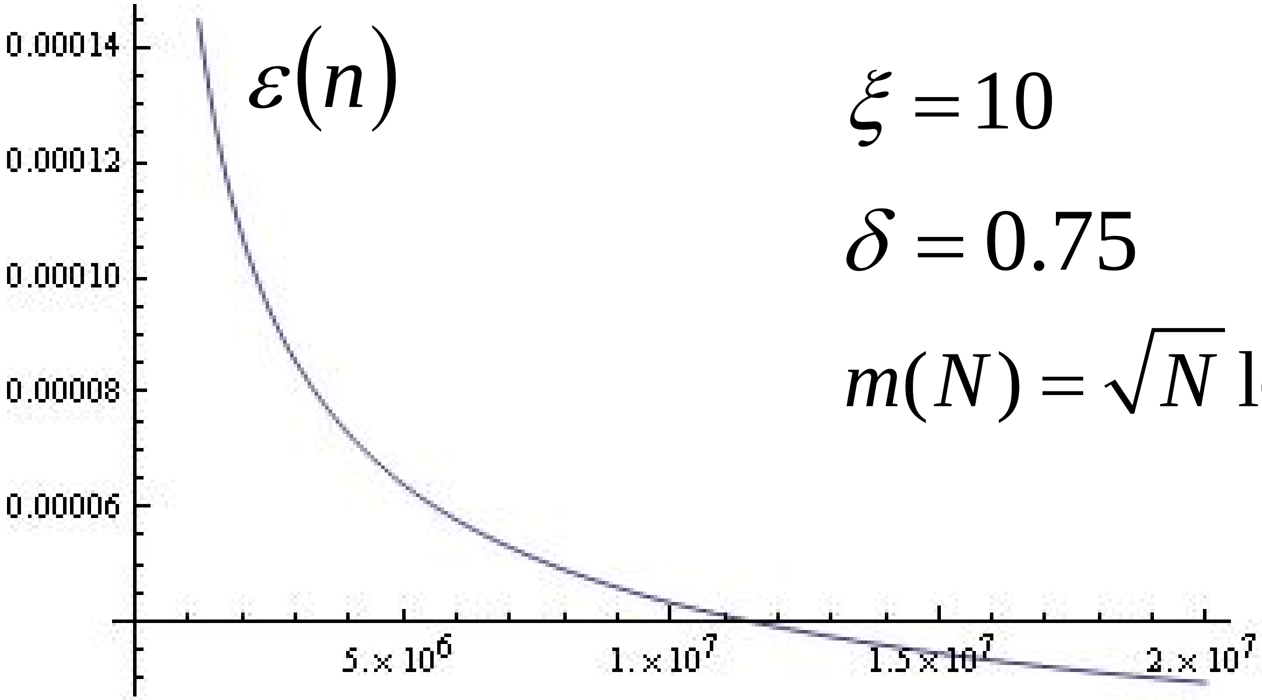
- If we demand that the algorithmic complexity remains the same in the presence of errors, then we need to include a functional dependency between the uncorrected error probability and *m*.

$$k \approx -\log \delta \times \left(\frac{1}{1-\epsilon} \right)^{m} \equiv \xi = \mathcal{O}(1)$$

$$\Rightarrow \epsilon(N) = 1 - \left(\frac{-\log \delta}{\xi} \right)^{1/m(N)}$$

Grover's Algorithm – Error Scaling

- The error scaling in Grover's algorithm looks like:



$$\xi = 10$$

$$\delta = 0.75$$

$$m(N) = \sqrt{N} \log N$$

$$N = 2^n$$

Circuit Complexity Bounds

- A more adequate expression for the inequality in the threshold theorem, consistent with complexity theory, is:

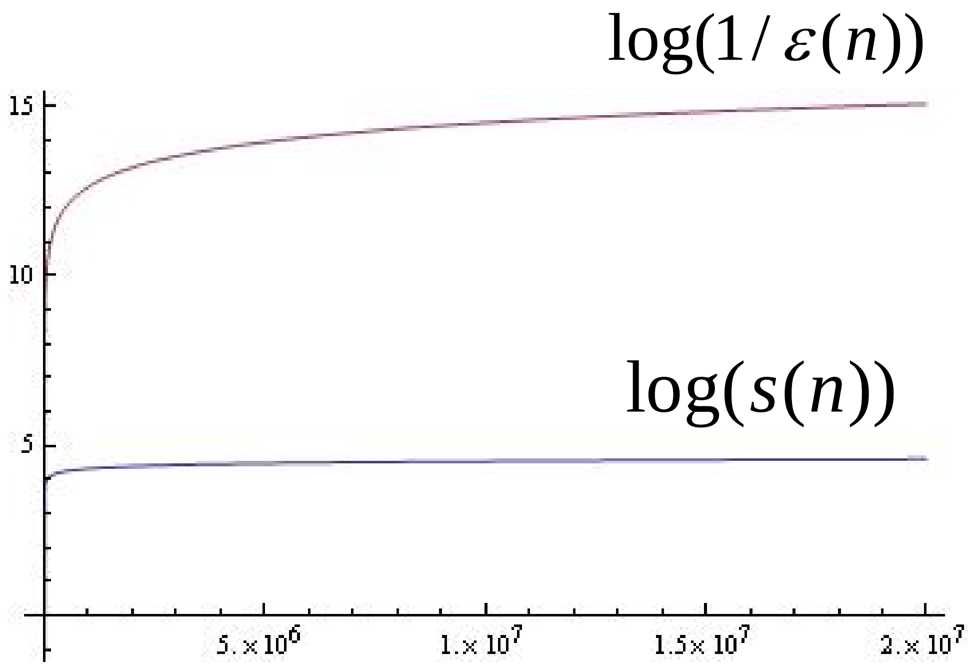
$$\frac{(cp)^{2^{h(N)}}}{c} \leq \epsilon(N) = 1 - \left(\frac{-\log \delta}{\xi} \right)^{1/m(N)}$$

- The circuit size overhead is given by:

$$\mathcal{O}\left(s(N) \times \log^{r}(1/\epsilon(N)) \right)$$

Grover's Algorithm – Circuit Size

- The scaling of the circuit size overhead looks like:



$$N = 2^n$$

$$\xi = 10$$

$$\delta = 0.75$$

$$m(N) = \sqrt{N}\log N$$

$$\lim_{N\to\infty} \frac{\log\left(1/\epsilon(N)\right)}{\log\left(s(N)\right)} = \infty$$

"*Negligible*" Complexity Overheads

- QC constantly requires poly-logarithmic circuit size overheads
  - FTQC.
  - Approximation of an arbitrary unitary operator using a finite universal set.
- Most of the time these terms are considered as "negligible" (in comparison to leading order polynomial or exponential terms).
- These terms are commonly omitted when talking about the potential physical realization of a general purpose quantum computer.
- Are they really negligible from a practical standpoint?

A Lesson from Computational Geometry

- Linear space multi-dimensional searches require:

$$\mathcal{O}(N)\ \text{space} \qquad \mathcal{O}(N^{\alpha})\ \text{time}$$

- Space-time tradeoff:

$$\mathcal{O}(N)\ \text{space} \rightarrow \mathcal{O}(N \log N)\ \text{space} \Rightarrow \mathcal{O}(\log^{\eta} N)\ \text{time}$$

- In most real-time systems of interest, the “small” space overhead makes the tradeoff unfeasible and impractical.
- Quantum algorithmic efficiency could be offset by poly-logarithmic overheads or could be rendered impractical.

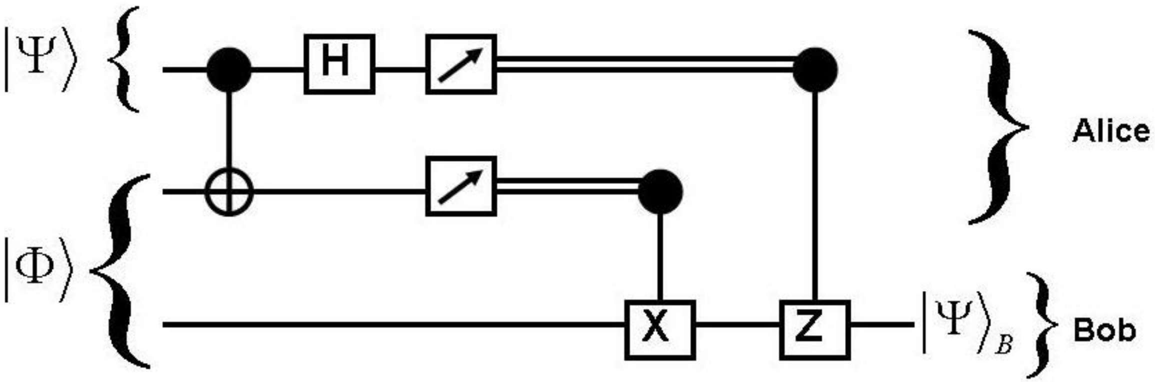
Smart Quantum Compilers

- Assigning levels of QEC independently of the algorithm leads to a waste of valuable resources.
- Dynamic quantum compilers should be able to decide at run time the optimal amount of QEC required to accomplish a specific algorithmic task.
- If circuit size overheads are non-trivial expenses, then the compiler should decide the most optimal algorithmic accuracy given hardware constraints.
- Error scaling formula provides a general guideline to establish optimal space-time tradeoffs in noisy QC.

Complexity Resources and Sinks

- Complexity theory attempts to describe how easy or how difficult is to find the solution of a computational problem.
- Complexity resources are those necessary to carry out a computation (space, time, and circuit size): they reflect the theoretical difficulty of solving a computational problem.
- Errors act as “Complexity Sinks”: they consume nontrivial amounts of resources and do not reflect the theoretical difficulty of solving a computational problem.
- What about entanglement? Is it a complexity resource? Or is it a complexity sink?

Quantum Teleportation with Imperfect (Noisy) Entanglement



- The state to be teleported is:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- The imperfectly entangled state is:

$$|\Phi\rangle = a|00\rangle + b|11\rangle$$

Communication Using Teleportation

- We use qubits to encode classical bits:

$$|0_L\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$|1_L\rangle = \beta|0\rangle - \alpha|1\rangle$$

- Alice teleports these qubits to Bob. The probability that Alice sends a "X_L" and Bob measures a "Y_L" is given by $P(X_L, Y_L)$:

$$P(0|0) = P(1|1) = 1 - 2\left(1 - 2ab\right)\alpha^2\beta^2$$
$$P(0|1) = P(1|0) = 2\left(1 - 2ab\right)\alpha^2\beta^2$$

Entanglement as a Complexity Resource

- *Conventional thinking* leads one to believe that that the degree of entanglement is an accurate measure of a teleportation device's ability to transmit information.
- This implies that entanglement should be considered as a complexity resource.
- Note, however, that Gross et.al. (2009) showed that high degrees of entanglement may actually reduce the computational power in the measurement-based quantum computing model.

Degree of Entanglement

- The standard measure of entanglement in a bipartite state is the Shannon entropy of the moduli squared of the Schmidt coefficients:

$$E(|\psi\rangle) = -\sum_k |\lambda_k|^2 \log(|\lambda_k|^2)$$

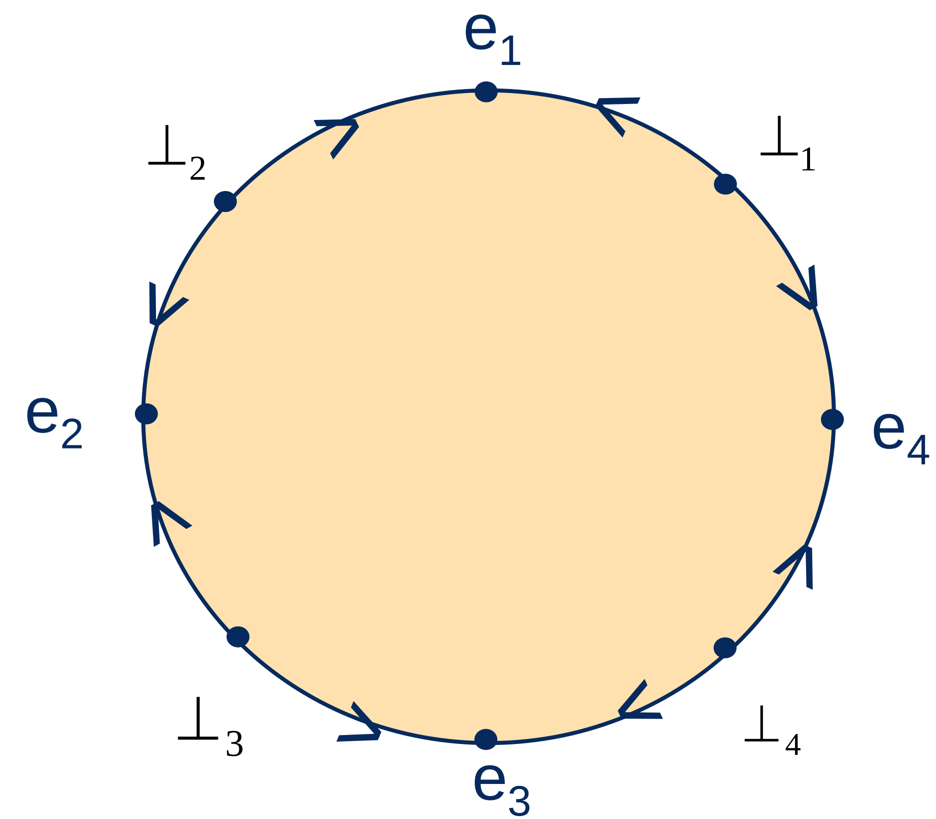
- For the state:

$$|\Phi\rangle = a|00\rangle + b|11\rangle$$

the Schmidt coefficients are given by:

$$\lambda_1^{\,2} = a^2 \qquad \lambda_2^{\,2} = b^2$$

The Circle as a Domain: Entanglement



$$e_1 = (0,1)$$

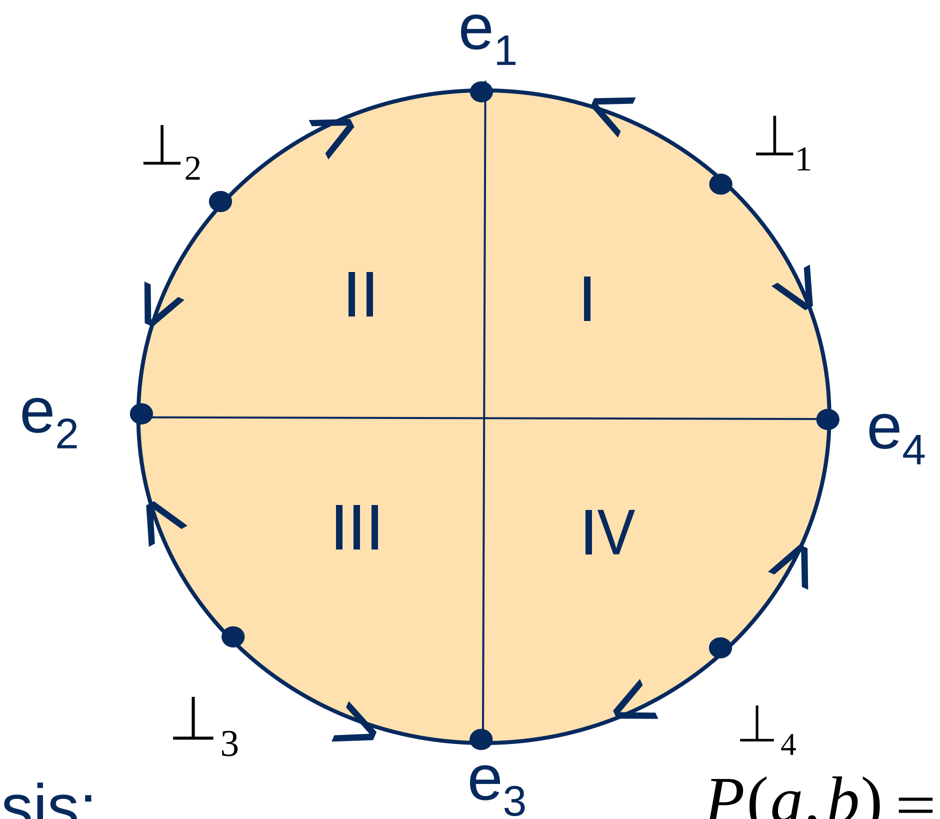
$$e_4 = (1,0)$$

$$\perp_1 = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right)$$

- Entanglement decreases as we move up in the order.

$$E(a,b) = -a^2 \log a^2 - b^2 \log b^2$$

Probability of Success on the Circle



$$e_1 = (0,1)$$

$$e_4 = (1,0)$$

$$\perp_1 = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$$

For a fixed basis:

$$P(a,b) = 1 - 2(1 - 2ab)\alpha^2\beta^2$$

- Probability of success decreases in odd quadrants as we move up in the order.
- Probability of success increases in even quadrants as we move up in the order.

Entanglement and Capacity

- As we have seen, in the even quadrants, the degree of entanglement and the probability of success do not move in the same direction.
  - Entanglement always decreases as we move up in the order.
  - The success probability decreases in the odd quadrants as we move up in the order.
  - The success probability increases in the even quadrants as we move up in the order.
- **As a consequence, in the even quadrants, the degree of entanglement and the channel capacity do not move in the same direction.**

Noisy Entanglement: Resource and Sink

- **Entanglement as a resource:** there are cases where as the degree of entanglement increases, so too does the amount of information we can transmit.
- **Entanglement as a sink:** there are cases where as the degree of entanglement *increases*, the amount of information we can transmit *decreases*.
- Furthermore, it is possible to teleport information with an acceptable error rate *despite* the fact that the entangled states posses a degree of entanglement that is *near zero*.
- Therefore, noisy entanglement acts as a complexity resource, but also as a complexity sink.

Conclusions

- Even if they are arbitrarily small, constant uncorrected errors affect algorithmic complexity. To avoid such an algorithmic penalty, uncorrected errors have to depend on the scaling variable.
- Error scaling requires a substantially larger circuit size overhead for FTQC. Then, scaling errors act as non-trivial “complexity sinks”.
- Entanglement: it can be considered as a complexity resource, but also as a sink (at least within the context of noisy teleportation).
- **The complexity of noisy QC is still not well understood.**

Advertisement

- Synthesis Lectures on Quantum Computing (Morgan & Claypool).
- Graduate level books on almost anything related to “quantum stuff”.
- Current and upcoming titles:
  - *Quantum Walks for Computer Scientists* by S. Venegas
  - *Quantum Computer Science* by M. Lanzagorta & J. Uhlmann
  - *Broadband Quantum Cryptography* by D. Rogers
  - *Quantum Simulators* by S. Venegas, F. Delgado, & J.L. Gomez
  - *Relativistic Quantum Information* by P. Alsing
  - *Algebraic Quantum Information Theory* by K. Martin
  - *Nonlinear Quantum Filtering* by S. Julier, M. Lanzagorta & J. Uhlmann
- Currently looking for new book proposals.