

#### **Motivations for quantum information processing**

- Quantum computing (QC)
  - Extended Church-Turing Thesis: Anything physically efficiently computable can be computed efficiently on my laptop
  - QC: Extended Church-Turing Thesis is false; there are exponentially-faster algorithms (for interesting problems) by using quantum mechanics
- Cryptography
  - Breaks RSA public-key cryptosystem
  - Gives unconditionally secure key distribution

- Simulation & modeling
  - for quantum devices,
  - chemistry,
  - materials (high-T superconductors, new states of matter?)
- Quantum sensing
  - Precise measurement and lithography
  - Atomic clocks
- Basic science
  - Investigate measurement/ decoherence, quantum/classical boundary
  - Test qu. mechanics on new scales

(but no free lunch...)

#### **Quantum information**



• State of n qubits = unit vector in  $\mathbb{C}^{2^n}$ 



# Quantum information• "Qubit": $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ • "Qubit": $|\alpha_0|^2 + |\alpha_1|^2 = 1$ • State of n qubits = unit vector in $\mathbb{C}^{2^n}$ • $(\alpha'_x)_{x \in \{0,1\}^n}$

- Computation by local gates, rotate the state vector
- Observing/measuring system collapses it to a single classical bitstring x
  - No exponential parallelism
  - Have to "finesse" the quantum system to output the classical information you want

#### **Classical information processing**

• Classical state is a vector of probabilities:

$${p_x}_{x \in {0,1}^n} \quad p_x \ge 0 \quad \sum_x p_x = 1$$

• Valid operations are stochastic maps

## **Quantum information processing**

• Quantum state is also a vector

$$\{\alpha_x\}_{x \in \{0,1\}^n} \quad \sum_x |\alpha_x|^2 = 1$$

• Valid operations are rotations (unitaries)

The universe is quantum mechanical but it looks classical because of noise...





## **Quantum computing in 2008**

#### • Ion traps

- can trap and cool 16-18 qubits
- can entangle 6-8 qubits in a trap
- microfabrication of trap arrays on chips, dealing with increased noise



- in next 2-3 years may be able to compute with 40-60 qubits
- challenges: controlling thousands of traps with dozens of detection channels and lasers along the surface of the chip...

#### Superconducting qubits

- 2 qubit local interactions becoming routine
- nonlocal movement
  & interactions now possible



noise levels seem promising...

#### • Other technologies:

• Photonic qubits, quantum dots...

• Scaling these systems is a major engineering challenge



- But the basic technologies have been proven, there are intermediate rewards
- And there are no known fundamental difficulties, except...

## Common obstacle is noise!

- Physically reasonable noise rates are ~1% error per gate, or *maybe* 0.1%
  - ... Only 100 operations before an error can occur and propagate through the system
- Factoring a 2048-bit number uses
  - 6 x 10<sup>11</sup> gates on
  - 10,000 qubits
  - Need error  $\lesssim 1/10^{12}$  per gate

K-bit number: 72 K<sup>3</sup> gates 5 K qubits

72 K<sup>3</sup> gates versus  $e^{K^{1/3}}$  classically

# Noise is fundamental problem for quantum computers: entangled systems are fragile



- "Both dead and alive," in superposition; but collapses to one or the other when observed
- A single stray photon can collapse it and also analogous states in a quantum computer
- Physically reasonable noise rates are ~1% error per gate, or perhaps 0.1%

#### How to deal with noise?

- I. Engineering
  - Not enough— noise is fundamental in quantum systems
- 2. Fault tolerance

[Von Neumann '56]

- Enough to engineer the noise rate beneath a constant threshold,
- Then effective noise rate can be decreased arbitrarily (and efficiently) using errorcorrecting codes



Replacing a bad tube meant checking among ENIAC's 19,000 possibilities.



#### What's different quantumly?

- Quantum problems:
  - Quantum states are continuous, not discrete—need to protect against continuous errors
  - No-cloning theorem: Can't copy a quantum state  $|\psi\rangle \mapsto |\psi\rangle |\psi\rangle$ , so no immediate analog of the repetition code  $0 \mapsto 0^n, 1 \mapsto 1^n$
  - But quantum ECCs do exist! [Shor '95]



## **Operational def. of QECC**

- Quantum problems:
  - Quantum states are continuous, not discrete—need to protect against continuous errors
  - No-cloning theorem: Can't copy a quantum state  $|\psi\rangle \mapsto |\psi\rangle |\psi\rangle$ , so no immediate analog of the repetition code  $0 \mapsto 0^n, 1 \mapsto 1^n$
  - But quantum ECCs do exist! [Shor '95] Operationally,



#### Quantum error-correcting codes exist

- Although quantum states are continuous, correcting a *discrete set* of errors (bit and phase flips) suffices
- Based on classical linear ECCs: QECC comes from *two* linear ECCs



(one for bit flips, one for phase flips)

#### Quantum error-correcting codes exist

- Although quantum states are continuous, correcting a *discrete set* of errors (bit and phase flips) suffices
- Based on classical linear ECCs: QECC comes from two linear ECCs
- How can we use these codes?
  - Need operations as well as memory
  - Error recovery must be resilient to faults during recovery
  - How to encode into them in the first place?? (qu problem)



(one for bit flips, one for phase flips)

#### **Fault-tolerance intuition**

• Compile ideal circuit into "faulttolerant" (noise-resistant) version, fails to commute starting with small QECC:





- Concatenate (i.e., repeat) for arbitrarily improved reliability (so arb<sup>ly</sup> long calcs), if starting below a constant noise threshold
- Problem: Noise model at encoded level is not the same as the physical noise model!

- 1996-97: First fault-tolerance results: QECCs, threshold proofs Shor, Steane, Calderbank, Aharonov, Ben-Or, Kitaev, Knill, Laflamme, Zurek, ...
  - Proved existence of some *positive* tolerable noise rate using concatenated qu. codes of distance ≥5
  - No explicit lower bounds on tolerable noise rate, but estimates were 10<sup>-6</sup>-10<sup>-5</sup> noise per gate
  - Moral: Fault tolerance makes quantum computers plausible in the real world



#### **Proofs**

- I997: Aharonov/Ben-Or, Kitaev: Prove positive tolerable noise rate for codes of distance d≥5
- 2005: R, Aliferis/Gottesman/Preskill: First explicit numerical threshold lower bounds, threshold for distance-3 codes

# Estimates & simulations

- 2002: Steane: Correct bit flip errors all at once, and then phase flip errors all at once
  - based on simulations, estimates 3x10<sup>-3</sup> tolerable noise rate per gate

#### Simulations using distance-3 codes

- Basic estimates:
  - Aharonov & Ben-Or '97
  - Gottesman '97
  - Knill-Laflamme-Zurek '98
  - Preskill '98

- Optimized estimates:
  - Zalka **'97**
  - R '04
  - Svore-Cross-Chuang-Aho '05

- 2D locality constraint
  - Szkopek et al '04
  - Svore-Terhal-DiVincenzo '05

#### **Proofs**

- I997: Aharonov/Ben-Or, Kitaev: Prove positive tolerable noise rate for codes of distance d≥5
- 2005: R, Aliferis/Gottesman/Preskill: First explicit numerical threshold lower bounds, threshold for distance-3 codes

# Estimates & simulations

- 2002: Steane: Correct bit flip errors all at once, and then phase flip errors all at once
  - based on simulations, estimates 3x10<sup>-3</sup> tolerable noise rate per gate

#### Postselection

#### Improved threshold result [R '04]

 Modification of standard error correction scheme increases *estimated* threshold 3x, to almost 1%.



#### **Error-detection-based fault-tolerance**

• Compile ideal circuit into "faulttolerant" (noise-resistant) version, fails to commute starting with small QECC:





- In simulations, tolerates much higher noise rates than error-correction-based FT schemes
- But (previously) no proven positive threshold!



#### **Proofs**

- I997: Aharonov/Ben-Or, Kitaev: Prove positive tolerable noise rate for codes of distance d≥5
- 2005: R, Aliferis/Gottesman/Preskill: First explicit numerical threshold lower bounds, threshold for distance-3 codes

#### Postselection

# Estimates & simulations

- 2002: Steane: Correct bit flip errors all at once, and then phase flip errors all at once
  - based on simulations, estimates 3x10<sup>-3</sup> tolerable noise rate per gate

#### Improved threshold result [R '04]

- Modification of standard error correction scheme increases *estimated* threshold 3x, to almost 1%.
- Postselection + Teleportation

#### Knill's threshold result [Knill '04]

 Estimated 3-6% threshold for independent depolarizing errors.



#### **Applying teleportation to fault tolerance**

I. Encoding 2. Decoding 3. Error correction 4. Computation



## Applying teleportation to fault tolerance I. Error correction 2. Computation



\* decoding measurements using classical computer

# Applying teleportation to fault tolerance I. Error correction 2. Computation



\* operation U should be "C<sub>2</sub>"

# Applying teleportation to fault tolerance Error correction + Encoded Computation



- Teleportation allows for correcting bit flip errors, phase flip errors, and doing one step of computation all at once.
- (Provided that we can prepare reliably the necessary resource states.)

#### **Teleported EC + encoded computation**



- Teleportation allows for correcting bit flip errors, phase flip errors, and doing one step of computation all at once.
- (Provided that we can prepare reliably the necessary resource states.)
- Note: We can prepare very good ancilla states, e.g., throwing away all ancillas with any detected errors ("postselection"). We wouldn't want to throw away the data—but the data is isolated from the ancilla state.

#### **Teleported EC + encoded computation**



- Teleportation allows for correcting bit flip errors, phase flip errors, *and* doing one step of computation all at once.
- (Provided that we can prepare reliably the necessary resource states.)
- Note: We can prepare very good ancilla states, e.g., throwing away all ancillas with any detected errors ("postselection"). We wouldn't want to throw away the data—but the data is isolated from the ancilla state.

# Quantum disadvantages

- States are continuous (i.e., analog)
- No-cloning theorem

#### Quantum advantage!

• Quantum teleportation allows isolating the data from errors

 Problem: Although Knill estimated tolerable noise rate was 3-6%, proofs could not show that postselection-based schemes tolerated any noise at all!

#### **Renormalization frustrates previous proofs**



#### Intuition for Aharonov/Ben-Or's proof

• Idea: Maintain inductive invariant of goodness. (A level-k block is good "if it has at most one bad level-(k-1) subblock.")



#### Problems:

- Inefficient analysis: Logical error rate for a distance-d code drops as c p<sup>(d-1)/2</sup> instead of c p<sup>(d+1)/2</sup>
  - .:. Can't hope for very good rigorous lower bounds on the noise threshold
- No threshold at all for concatenated d=3 codes, or for postselection-based schemes



(one level k-1 error is already too many)

- Problem: Although Knill estimated tolerable noise rate was 3-6%, proofs could not show that postselection-based schemes tolerated any noise at all!
  - Renormalizing the error distribution leads to bad correlations.

#### **Results** [R '06]

- *Existence* of tolerable noise rates for many fault-tolerance schemes, including:
  - Schemes based on error-detecting codes, not just ECCs (Knill-type)
  - Distance-3 codes, and more efficient "Fibonacci"-type schemes (d=2 codes)
- Tolerable threshold lower bounds\*
  - 0.1% simultaneous depolarization noise†
  - I.1%, if error model known *exactly*





†Versus .02% best lower bound for errorcorrection-based FT scheme [Aliferis, Cross 2006]

#### **Techniques**

- Main new technique is to maintain close control over the distribution of errors in the quantum computer (Previous threshold proofs had used a "worst-case" criterion for error behavior that blew up during renormalization.)
  - Rewrite true error distribution as a mixture of nearby distributions whose error distributions lack nasty correlations



#### Bitwise-independent noise is nice...

• **Def:** Noisy encoder = perfect encoder, followed by bitwise-indep. noise at rates  $\leq p$ .



(tool for analysis—such encoders don't actually exist)

#### **Induction claim?**

(much stronger than Aharonov/Ben-Or's claim)



bitwise-independent errors preceding encoded gate bitwise-independent errors following perfect gate, plus quadratically suppressed independent logical errors



#### encoded FT circuit

• Since the error model is preserved (level-one logical errors have the same form as physical errors), the analysis can be repeated to give a threshold

#### Bitwise-independent noise is nice...

• **Def:** Noisy encoder = perfect encoder, followed by bitwise-indep. noise at rates  $\leq p$ .



(tool for analysis—such encoders don't actually exist)

#### **Induction claim**

(much stronger than Aharonov/Ben-Or's claim)



bitwise-independent errors preceding encoded gate bitwise-independent errors following perfect gate, plus quadratically suppressed independent logical errors

## Details in proving that mixing works

• Numerical approach (for numerical threshold lower bounds)



- Existence argument (for threshold existence proofs):
  - characterize convex hull of dit-wise independent distributions (a simplex)
  - "pull back" actual distribution onto distribution on dits
- Must also obtain universality CNOT and similar "linear" gates can be efficiently simulated on a classical computer. Need a nonlinear operation (AND or Toffoli). Use "magic states distillation."

#### **Conclusions**

- Conclusion: Mixing argument shows that concatenation works to reduce errors. Error events are correlated, but error correlations do *not* explode.
- Correlations manifest themselves as asymmetries in the conditional error models



- With postselection, gate error rates that are asymmetrically too low can be just as bad as error rates that are too high
- Are Knill's simulations too optimistic?

#### More fault-tolerance work...

- Magic states distillation (for teleporting into a universal gate set) [R'05, '06]
- Optimizing ancilla verification [R'06]
- Higher-order-accurate composite pulses, based on quantum search algorithm, for eliminating noise *without encoding* [R'05]

### **Open questions in fault tolerance**

- Quantum computers need fault-tolerance techniques if they are to scale, but...
- Current FT schemes are not good enough
  - Need to increase tolerable noise rate, reduce overhead
  - So far, the biggest improvements have come *not* from optimizations or customizations, but rather from new quantum concepts that unify. The next division to remove is the code concatenation levels.
- Foundations:
  - Extend applicability of threshold proofs
  - Improve threshold upper bounds
- Connecting full-blown fault-tolerance schemes to implementations
  - Specialized, low-level error prevention (e.g., composite pulses, DFSs)









#### Farhi, Goldstone, Gutmann '07 algorithm

• **Theorem** ([FGG '07, CCJY '07]): A balanced binary NAND formula can be evaluated in time N<sup>1/2+o(1)</sup>.  $x_1 = x_2 = x_3 = x_4 = x_5 = x_6 = x_7 = x_8$ 

#### **Questions:**

- I. Why does it work?
- 2. How does it connect to what we know already?
- 3. How does it generalize?
- 4. What kinds of problems can we hope to solve with this technique?



#### Farhi, Goldstone, Gutmann '07 algorithm

• **Theorem** ([FGG '07, CCJY '07]): A balanced binary NAND formula can be evaluated in time N<sup>1/2+o(1)</sup>.

#### **Questions:**

**Answers:** 

- I. Why does it work?
- 2. How does it connect to what we know already?

"span programs" [Karchwer/Wig. 93]

- 3. How does it generalize?
- 4. What kinds of problems can we hope to solve with this technique?

formula evaluation problem over extended gate sets

#### Farhi, Goldstone, Gutmann '07 algorithm

• **Theorem** ([FGG '07, CCJY '07]): A balanced binary NAND formula can be evaluated in time N<sup>1/2+o(1)</sup>.

#### **Questions:**

- I. Why does it work?
- 2. How does it connect to what we know already?
- 3. How does it generalize?
- 4. What kinds of problems can we hope to solve with this technique?

5. No, really, WHY does it work?

formula evaluation problem over extended gate sets



"span programs" [Karchwer/Wig.'93]

**Answers:** 



#### **Recursive 3-bit majority tree**



# [RŠ '08] algorithm

Theorem: A balanced ("adversary bound-balanced") formula φ over a gate set including all three-bit gates (and more...) can be evaluated in O(ADV(φ)) queries (optimal!).

(Some gates, e.g., AND, OR, PARITY, can be unbalanced—but not most!)

- Best quantum lower bound is  $\Omega(ADV(\varphi) = 2^d)$  [LLS'05]
- Expand majority into {AND, OR} gates:  $MAJ_3(x_1, x_2, x_3)$   $= (x_1 \land x_2) \lor (x_3 \land (x_1 \lor x_2))$
- : {AND, OR} formula size is  $\leq 5^{d}$
- :.  $O(\sqrt{5^d}) = O(2.24^d)$ -query algorithm [ACRSZ '07]

New: O(2<sup>d</sup>)-query quantum algorithm

#### Span program definition

• **Def:** An n-bit span program P is\*:

[Karchmer, Wigderson '93]

- A target vector t in vector space V over **C**,
- n input subspaces, one for each bit

Span program P computes  $f_P: \{0, I\}^n \rightarrow \{0, I\}$ ,  $f_P(x) = I \Leftrightarrow t \text{ lies in the span of } \{subspace i : x_i = I\}$ 









- $\phi(x)=I \Rightarrow A_{G(x)}$  has  $\lambda=0$  eigenstate with  $\Omega(I)$  support on the root.
- $\phi(x)=0 \Rightarrow A_{G(x)}$  has no eigenvectors overlapping the root with  $|\lambda| < 1/2^d$ .

 $\Rightarrow O(2^d)$ -query (optimal!) recursive MAJ<sub>3</sub> evaluation algorithm

	Classical	Quantum
$x_1 x_2 \cdots x_N$	Θ(Ν)	Θ(√N) [Grover '96]
Balanced AND-OR		
AND	Θ(N <sup>0.753</sup> ) (fan-in two) [Sʻ85, SVVʻ86, Sʻ95]	Θ(√N) [FGG,AC <b>R</b> ŠZ '07]
General read-once AND-OR	Ω(N <sup>0.51</sup> ) [HW'91]	$\Omega(\sqrt{N}), \sqrt{N} \cdot 2^{O(\sqrt{\log N})}$
	Conj.: Ω(D(f) <sup>0.753</sup> ) [SW '86]	[BS '04] [AC <b>R</b> ŠZ '07]
Balanced MAJ <sub>3</sub>	Ω((7/3) <sup>d</sup> ), Ο((2.6537) <sup>d</sup> ) [JKS '03]	Θ(2 <sup>d</sup> =N <sup>log<sub>3</sub>2</sup> ) and much more [ <b>R</b> Š '08]

## **Open:**

- Extensions to larger gate sets...
- Unbalaned formulas over more gates...
- Why do span programs work so well? Connection to adversary lower bounds ADV(f) ≤ ADV<sup>±</sup>(f)?

# **Open ?: More quantum algorithms based on span programs?**

- Our quantum algorithm evaluates span programs. We've applied it by building a large span program by composing small ones for all the gates.
- New framework for developing quantum algorithms: Are there interesting quantum algorithms based directly on large span programs? (E.g., graph problems, Perfect Matching, ...) [notion of quantum recursion]

