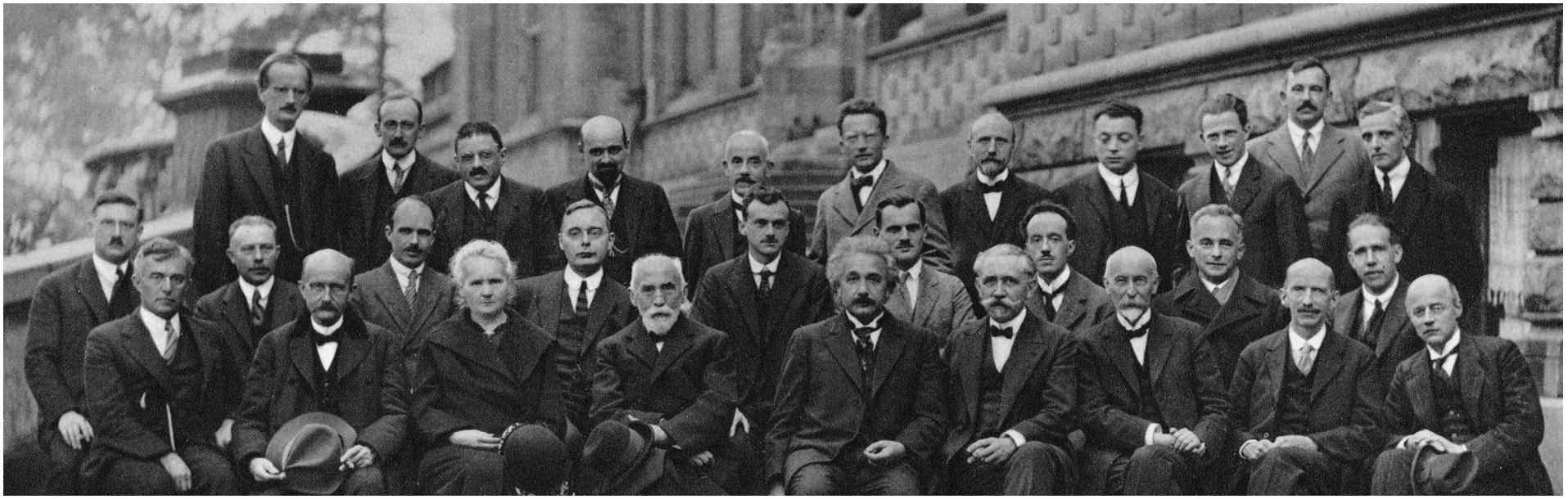
Quantum Computation & Quantum Error Correction

Mark M. Wilde

McGill University

LSU Center for Computation and Technology Seminar,
Baton Rouge, Louisiana, April 5, 2012

The Quantum Revolution

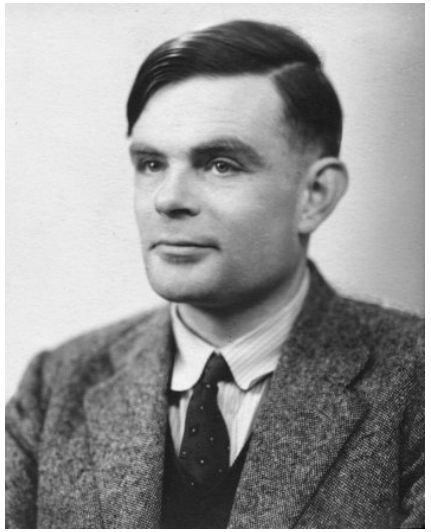


Solvay Conference in Brussels 1927

Quantum Theory developed from 1900-1925

Ideas such as **indeterminism**,
Heisenberg uncertainty, **superposition**,
interference, and **entanglement**
are part of quantum theory

The Computing Revolution



In 1936, **Alan Turing** revolutionized the
theory of computation
with a breakthrough paper:

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

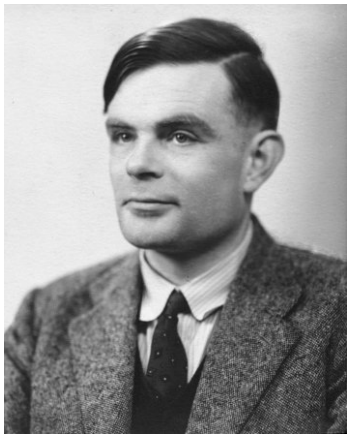
By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*.

The Church-Turing Thesis

A **computing problem** can be solved
on *any* computer that we could hope to build,
if and only if it can be solved
on an abstract **Turing machine**.

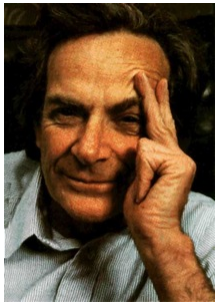


Turing machine consists of

- a **finite set of states**
- An **infinite tape** for reading and writing with a moving head
- A **transition function** specifying next state in terms of current one and symbol pointed to by the head.

Variation: **Complexity-theoretic Church-Turing thesis**:
A probabilistic Turing machine can efficiently simulate
any realistic model of computation.

The Quantum Computing Revolution



Feynman

Grover

Shor

Deutsch

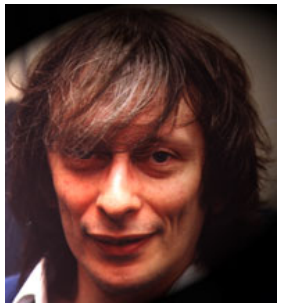
Kitaev

"The Second Quantum Revolution" *or*
"The Second Computing Revolution"

"Putting quantum weirdness to use"

Ideas such as **quantum Fourier transform**, **amplitude amplification**, **phase estimation**, and **quantum parallelism** are important here

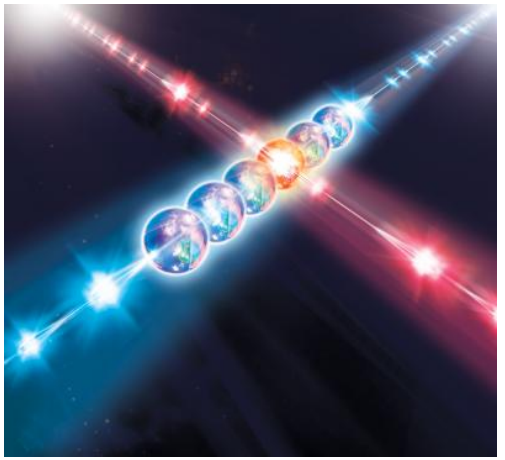
Revising the Church-Turing Thesis



Strong quantum Church-Turing thesis:
A **quantum Turing machine** can
efficiently simulate any realistic
model of computation.

It appears that classical physics is *not powerful enough*
to simulate quantum physics

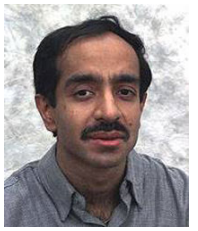
Exponential slowdown when
simulating quantum physics



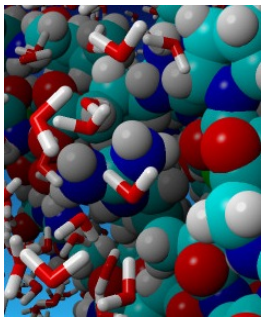
What are quantum computers good for?

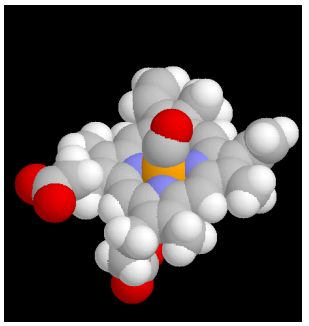
- Shor's algorithm (1994) breaks the RSA public key cryptography algorithm in polynomial time.

- Grover's algorithm (1997) gives a quadratic speedup for unstructured search.



- Simulation of quantum processes such as chemical reactions and molecular dynamics perhaps has the most potential.





Overview

- Brief review of quantum computation
- Quantum error correction

Quantum Cheat Sheet

I. Quantum states are represented by *rays in Hilbert space.*

II. States evolve according to **unitary operators**.

III. The states of composite systems are rays in a **tensor-product Hilbert space**.

IV. **Immediate repetition** of a measurement gives the same outcome.

IV a? **Born rule**: Probability of an outcome given by square of a probability amplitude

Note: Born forgot to square the amplitude in original version, did so in a footnote, and later won the Nobel Prize for the footnote

Quantum States

Simplest quantum system is a **qubit** (*quantum bit*).

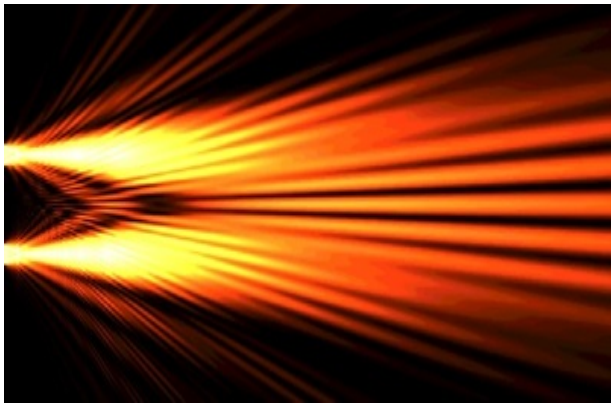
A qubit state can be classical ("*here or there*"):

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Any superposition (*"here and there"*) of these classical states is a possible quantum state:

$$\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

where $|\alpha|^2 + |\beta|^2 = 1$



Reading out information

Can “read out” information by performing **quantum measurements**

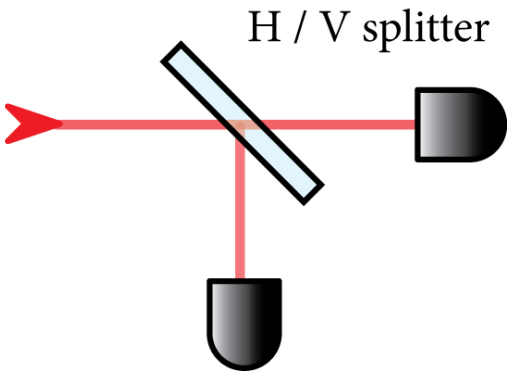
For classical states $|0\rangle$ or $|1\rangle$, a “**computational-basis**” measurement gives a *definite outcome* and *state is unchanged*.

For superposed state $\alpha|0\rangle + \beta|1\rangle$

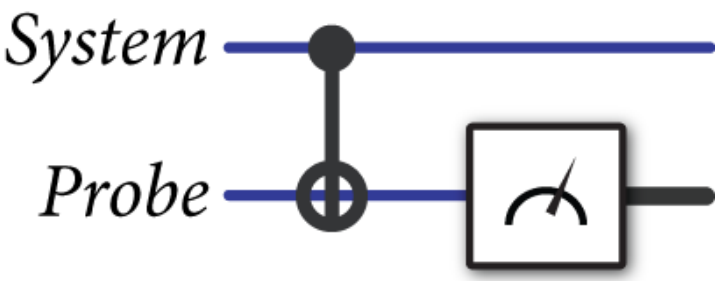
Such a measurement gives outcome $|0\rangle$ with probability $|\alpha|^2$

or outcome $|1\rangle$ with probability $|\beta|^2$

Optical example:



Typical QIP implementation of measurement:



How is quantum different from classical?

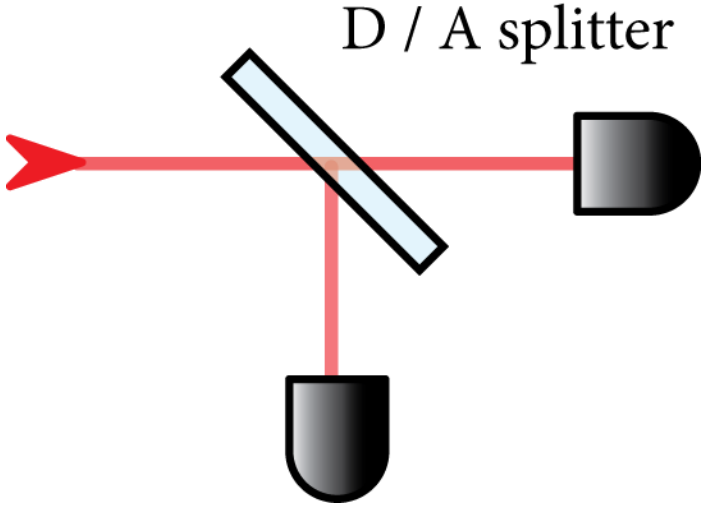
Superposed state: $\alpha|0\rangle + \beta|1\rangle$

Mixture: $|0\rangle$ with probability $|\alpha|^2$

$|1\rangle$ with probability $|\beta|^2$

Is superposed state physically different from mixture? ***Yes!***

Can see this by performing a different measurement:



Superposition gives 0 w/ prob. $|\alpha + \beta|^2/2$

and 1 w/ prob. $|\alpha - \beta|^2/2$

Quantum interference!

Mixture gives 0 or 1 w/ equal prob. 1/2...

Entanglement

Suppose Alice and Bob are in distant labs and each possess a qubit

States of two qubits might be $|0\rangle^A \otimes |0\rangle^B$ or $|1\rangle^A \otimes |1\rangle^B$

But by the **superposition principle**, the state could also be

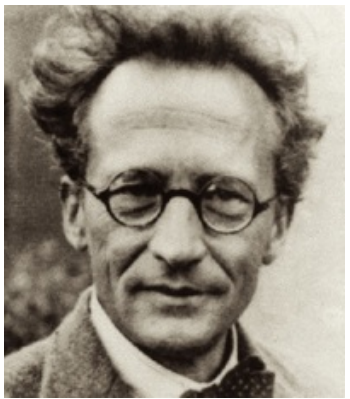
$$\frac{1}{\sqrt{2}}(|0\rangle^A \otimes |0\rangle^B + |1\rangle^A \otimes |1\rangle^B)$$

This state is "entangled" because it cannot be written as

$$|\psi\rangle^A \otimes |\phi\rangle^B$$

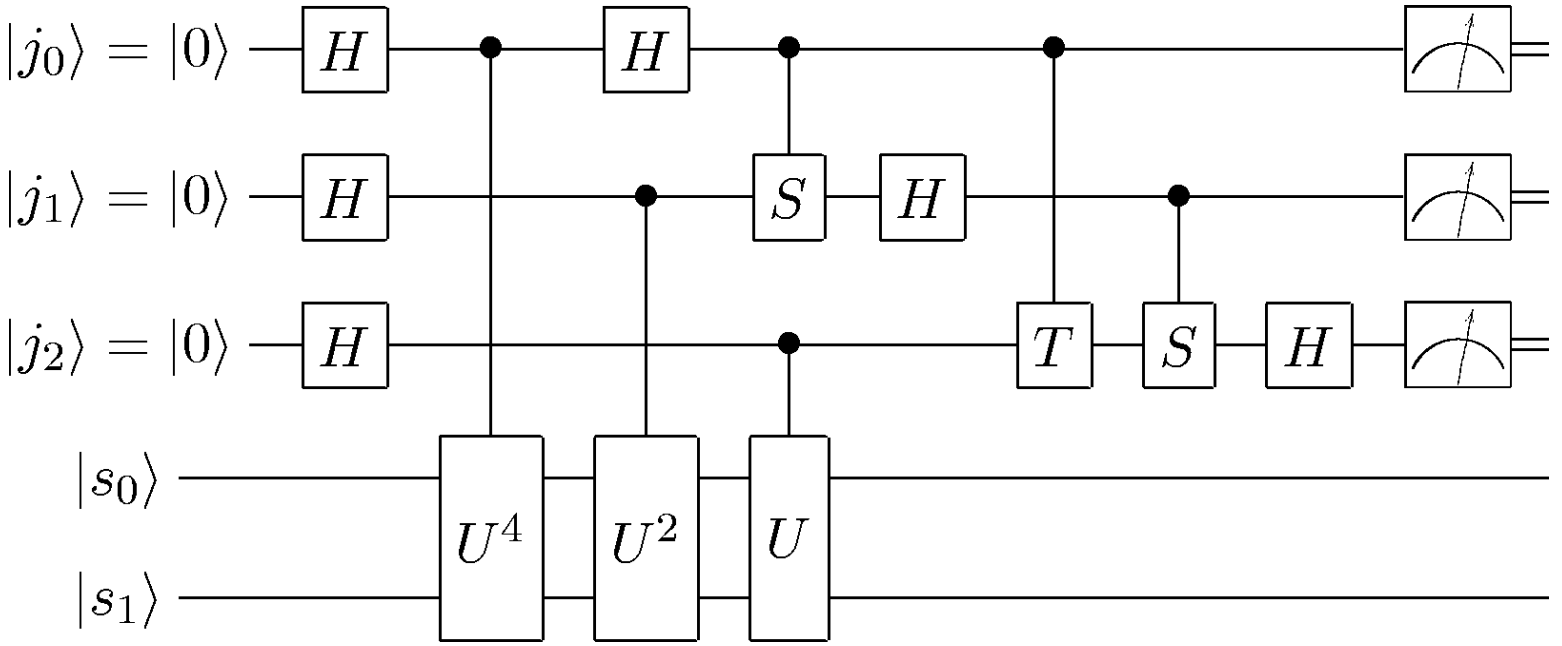
Entanglement confounded Schrodinger:

"I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."



Circuit Model of Quantum Computing

Example quantum algorithm:



Quantum circuit model is universal for quantum computation

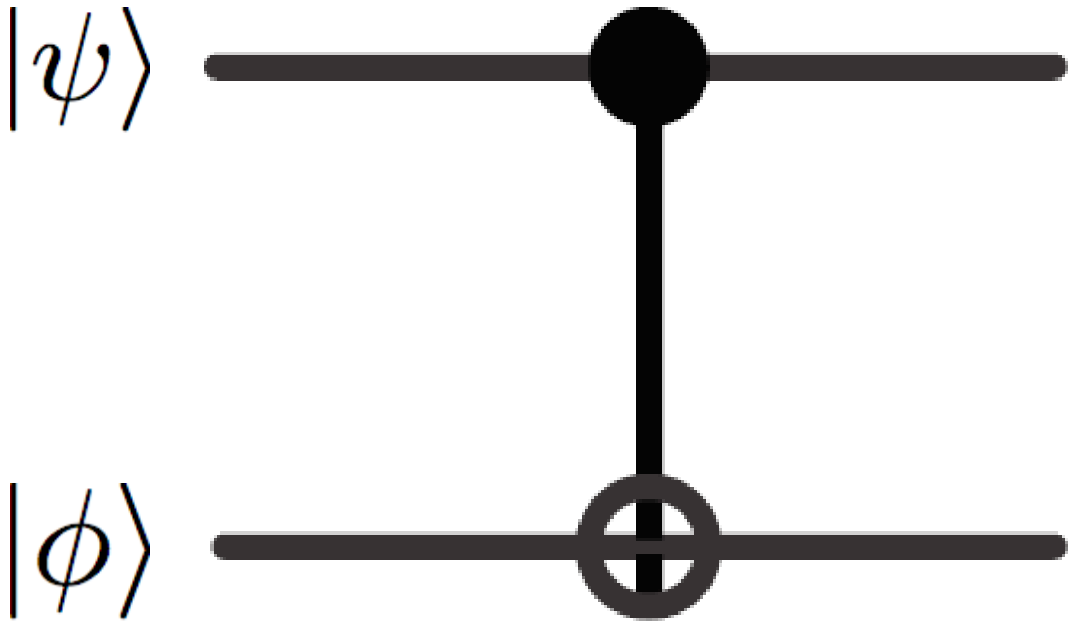
1) **Initialize** qubits

2) They **interact** by some controlled unitary operations

3) **Read out** by performing measurements at the end

Other models of quantum computation exist but circuit model is most prevalent

Quantum Information and Noise



Alice

Eve

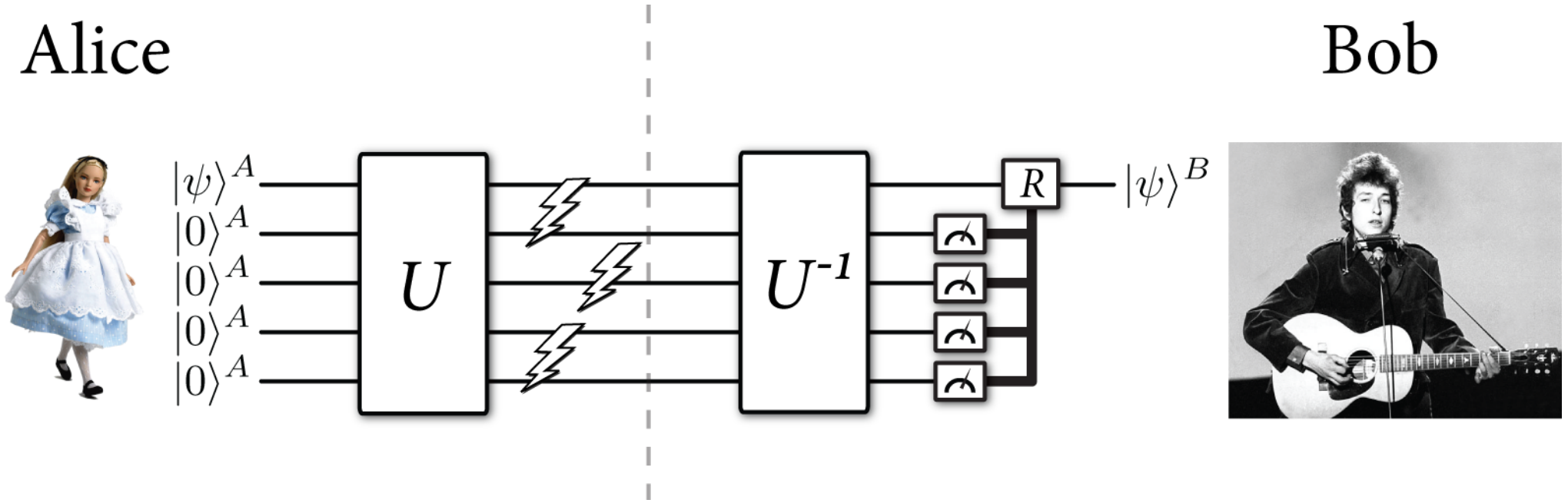
Environment **Eve** correlates with **Alice**'s qubits and destroys the fragile nature of a quantum state

This can happen at any stage of computation (preparation, evolution, or read-out)

Quantum Error Correction

Quantum error correction and its variants
appear to be the only viable way
to fight decoherence in a quantum computer

Main idea of quantum error correction:



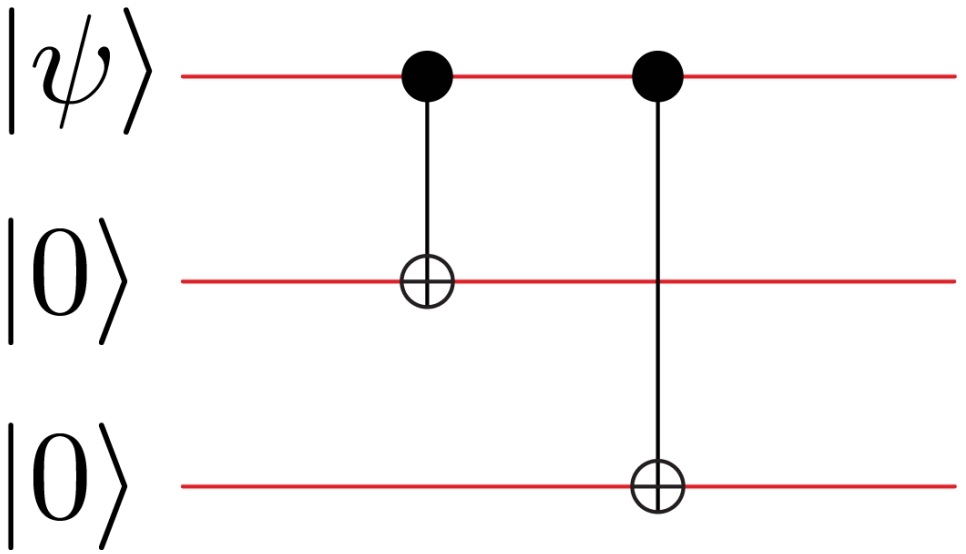
*Shor, PRA **52**, pp. R2493-R2496 (1995).*

Example Bit-Flip Code

Would like to protect a single qubit against classical bit flip noise:

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

Encode it with the help of other ancilla qubits:



State then transforms to

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \rightarrow \alpha|0\rangle|0\rangle|0\rangle + \beta|1\rangle|1\rangle|1\rangle$$

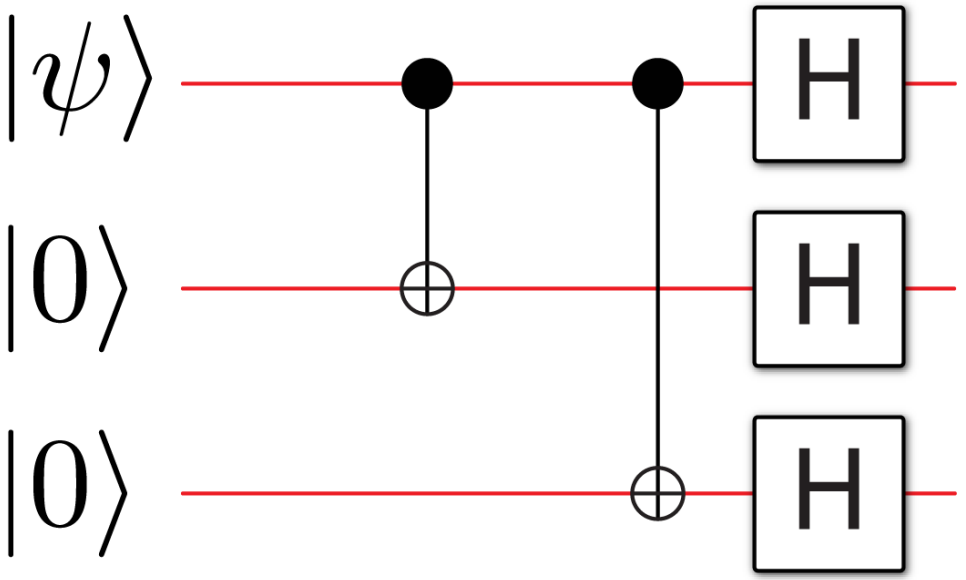
Quantum data encoded into the correlations between qubits.
More difficult for local bit-flip noise to destroy this quantum data

Example Phase-Flip Code

Would like to protect a single qubit against quantum phase-flip noise:

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

Encode it with the help of other ancilla qubits and change basis:



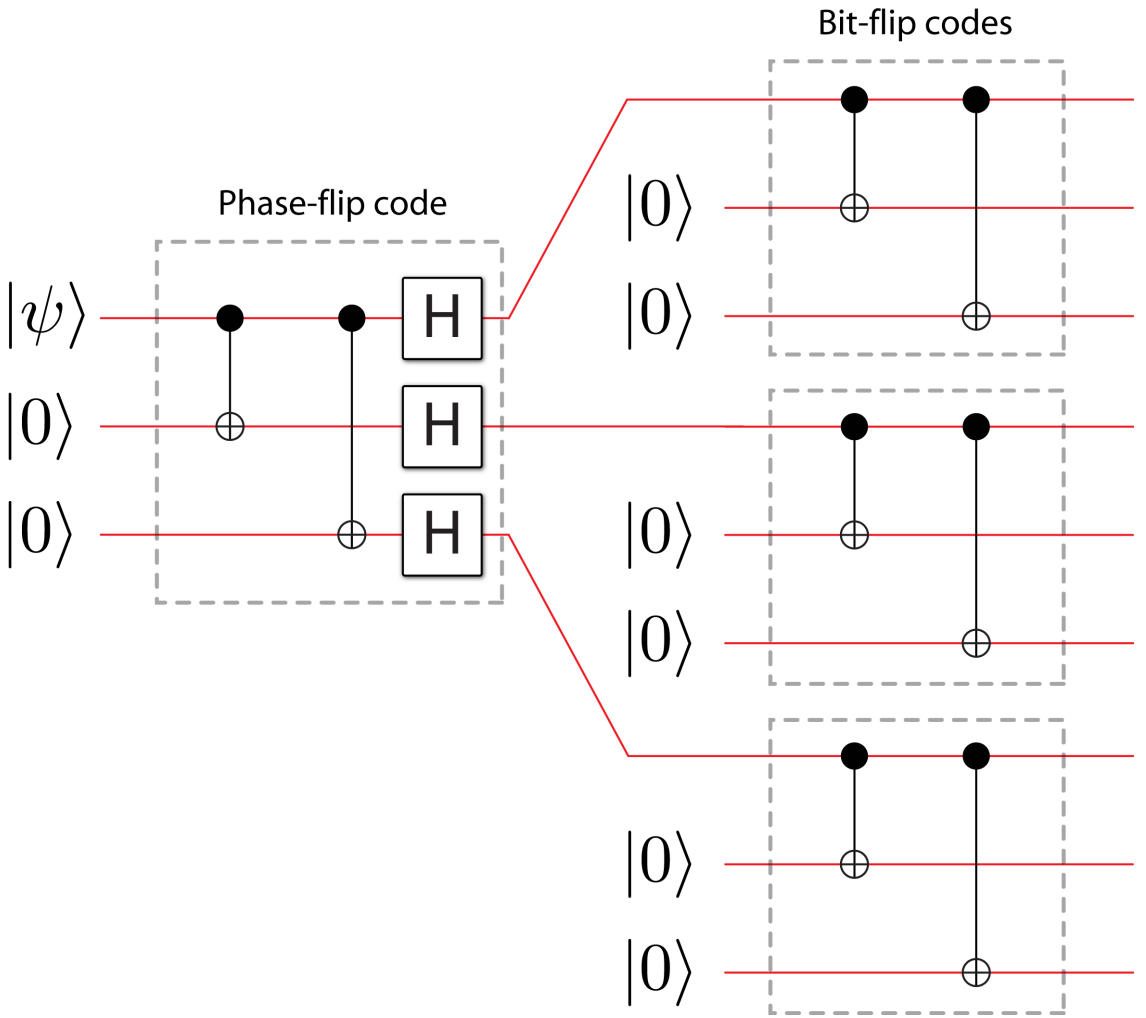
State then transforms to

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \rightarrow \alpha|+\rangle|+\rangle|+\rangle + \beta|-\rangle|-\rangle|-\rangle$$

More difficult for local phase-flip noise to destroy this quantum data

Shor Code

Shor's idea: To protect against arbitrary bit-flip and phase-flip noise, Concatenate the two schemes!



Preskill's interpretation: If you try to “read one page of this 9-page quantum book, then you won't get any information”!

Which quantum errors can we correct?

A **quantum error-correcting code** can only correct certain errors.

Which ones?

Let $|0\rangle$ and $|1\rangle$ be the logical 0 and 1 states for a logical qubit in a QECC

Then it can correct an error set $\{E_a\}$ if these states remain **distinguishable** under any two different errors from the set

$$E_a|0\rangle \perp E_b|1\rangle$$

(*these conditions are the same as the classical conditions*)

For QECC, we also require that the dual basis states remain distinguishable

$$E_a(|0\rangle + |1\rangle) \perp E_b(|0\rangle - |1\rangle)$$

How to build a fault-tolerant quantum computer

Need to make sure that procedures are robust to failure while doing

1) Preparation
2) Evolution
3) Read-out
4) Even when doing nothing!

Then continue **concatenating codes** like we did for Shor code!
Replace every circuit operation with a **fault-tolerant version** and perform **error correction** after every operation

How to build a fault-tolerant quantum computer

If reduction in error is from p to cp^2,
then there is some **accuracy threshold** for quantum computing if $p < 1/c$

Constant c is very important in practice---depends on quantum code chosen

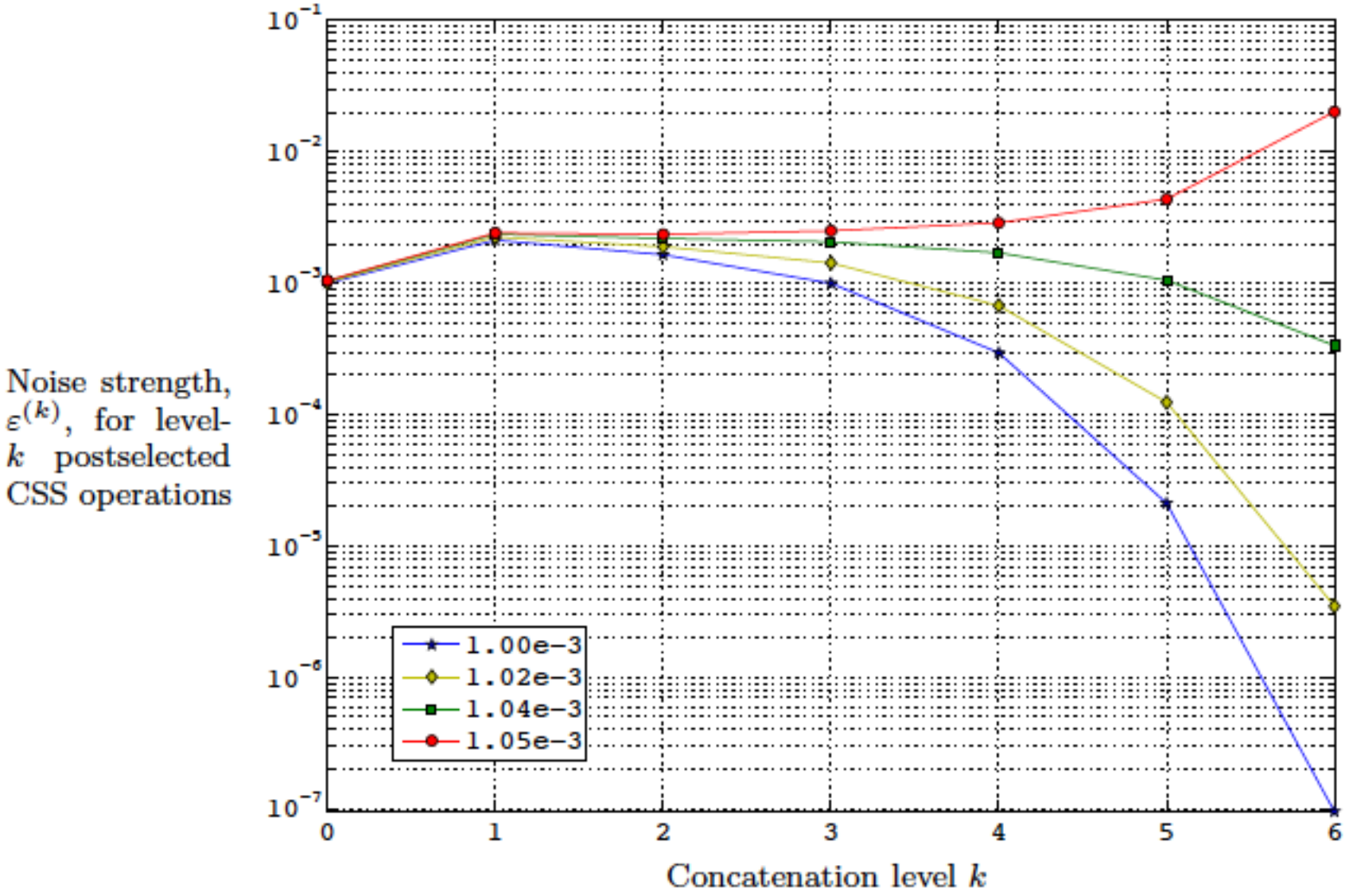
For any accuracy $\epsilon > 0$, we require a quantum circuit size that is only polylogarithmic in inverse accuracy:

$$O\left(\text{poly}\left(\log\left(\frac{1}{c\epsilon}\right)\right)\right)$$

Why? Under concatenation,
failure probability is **doubly exponentially small**
in number of levels of concatenation, whereas
circuit size only increases **exponentially**

Accuracy: $\epsilon = c^{-1}(cp)^{2^a}$ Circuit size: d^a

Estimate on the Quantum Accuracy Threshold

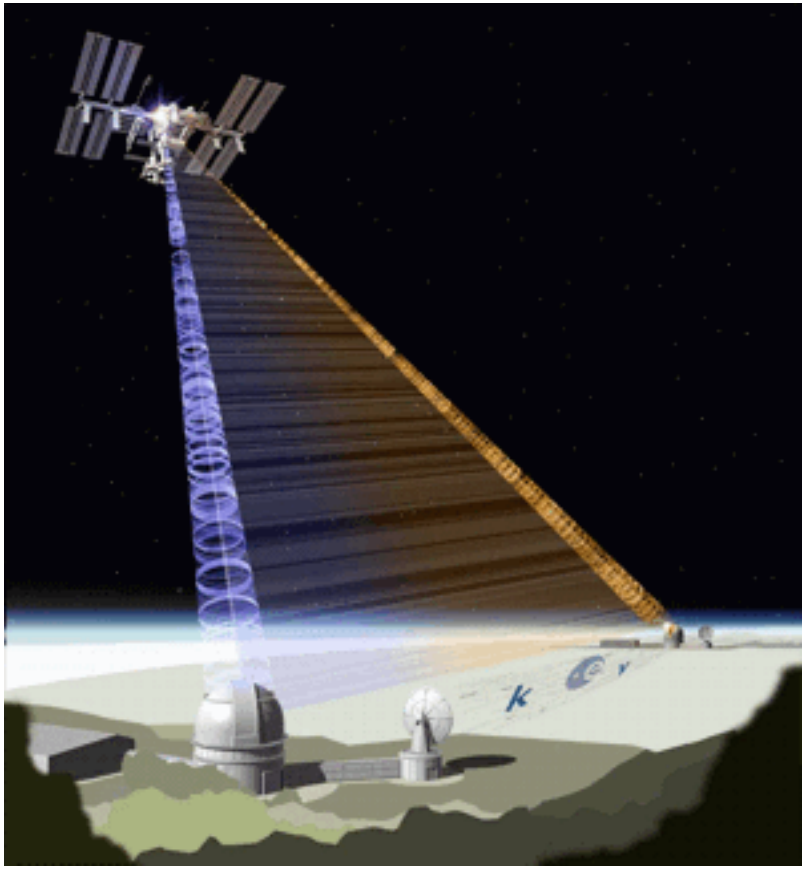


$p = 1.04 \times 10^{-3}$

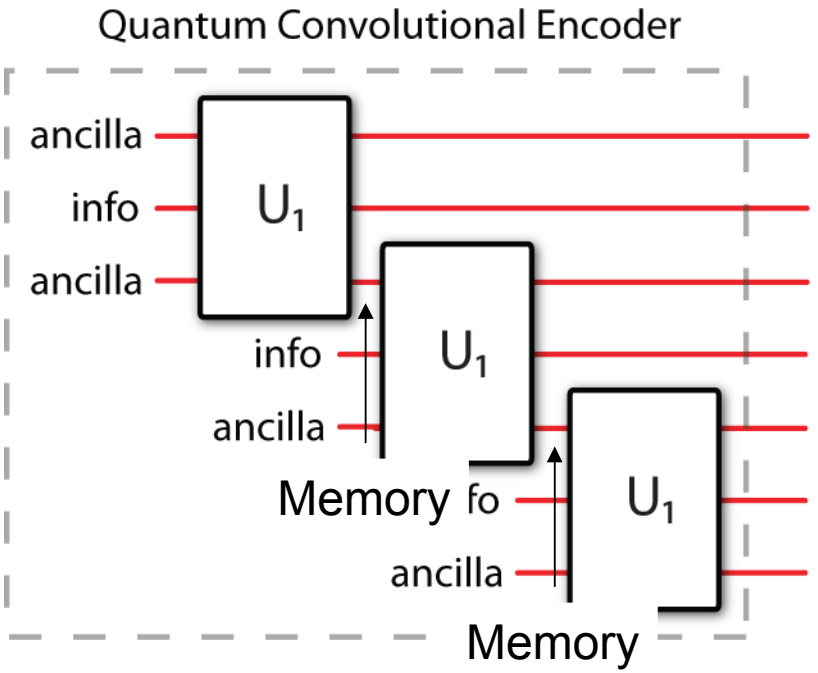
(Though, for some quantum algorithms, may only require 2 or 3 levels of concatenation)

Aliferis, Gottesman, Preskill. arXiv:quant-ph/0703264

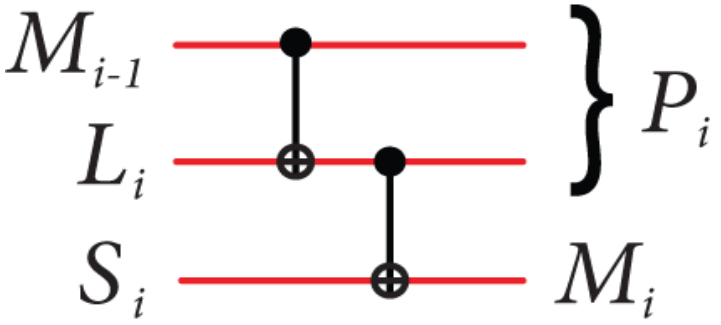
Quantum Error Correction for Communication



Quantum Convolutional Codes

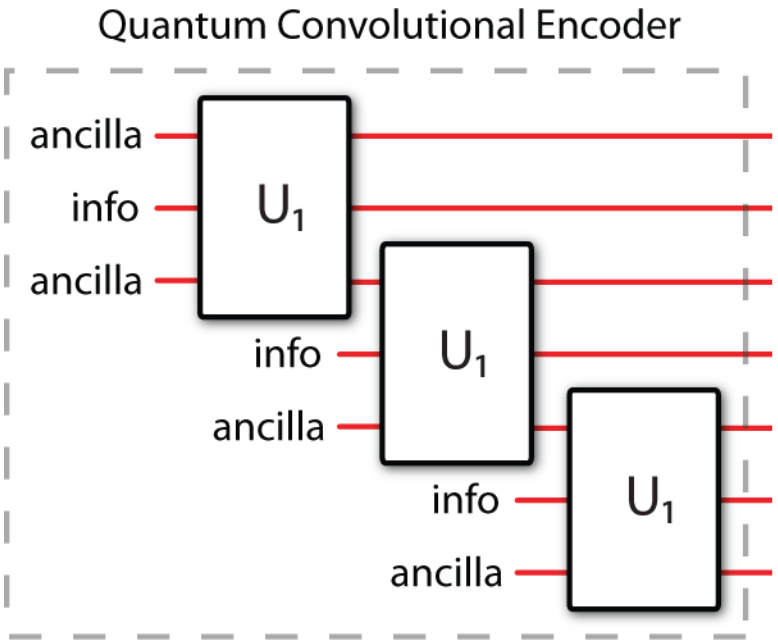


Example:



H. Ollivier and J.-P. Tillich, “Description of a quantum convolutional code,” PRL (2003)

Quantum Turbo Codes



A **quantum turbo code** consists of two interleaved and serially concatenated quantum convolutional encoders

Performance **appears to be good** for q. comm. from the results of numerical simulations

D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776– 2798, June 2009.
M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes." arXiv:1010.1256

Simulations

Selected an encoder **randomly**
with one information qubit, two ancillas, and three memory qubits

Non-catastrophic and **quasi-recursive**

Distance spectrum:

$$11x^5 + 47x^6 + 253x^7 + 1187x^8 + 6024x^9 + 30529x^{10} + 153051x^{11} + 771650x^{12}$$

Serial concatenation with itself gives
a rate 1/9 quantum turbo code

Replacing both ancillas with ebits gives EA encoder

Non-catastrophic and **recursive**

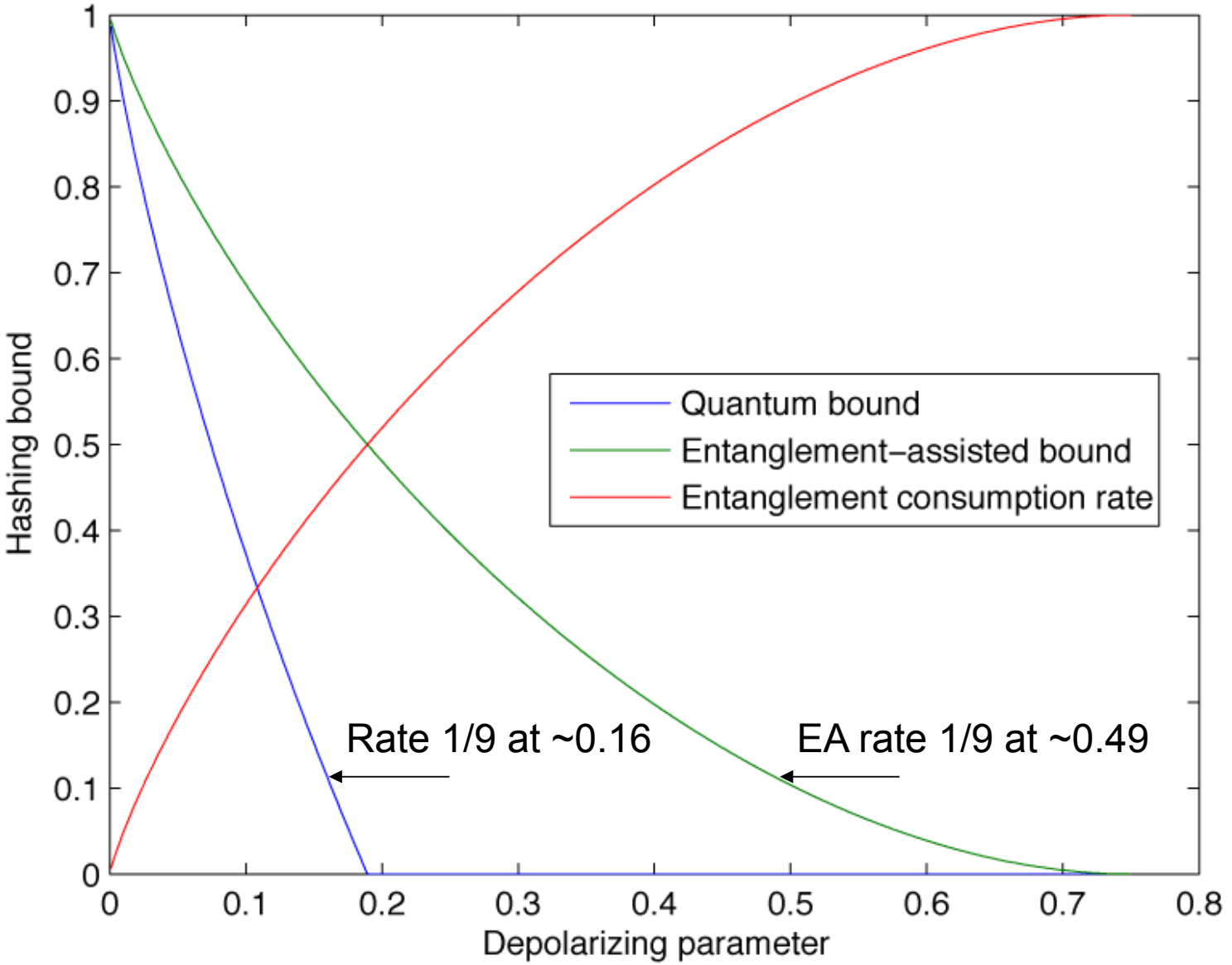
Distance spectrum improves dramatically:

$$2x^9 + x^{10} + 5x^{11} + 8x^{12}$$

Serial concatenation with itself gives
a rate 1/9 quantum turbo code
with 8/9 entanglement consumption rate

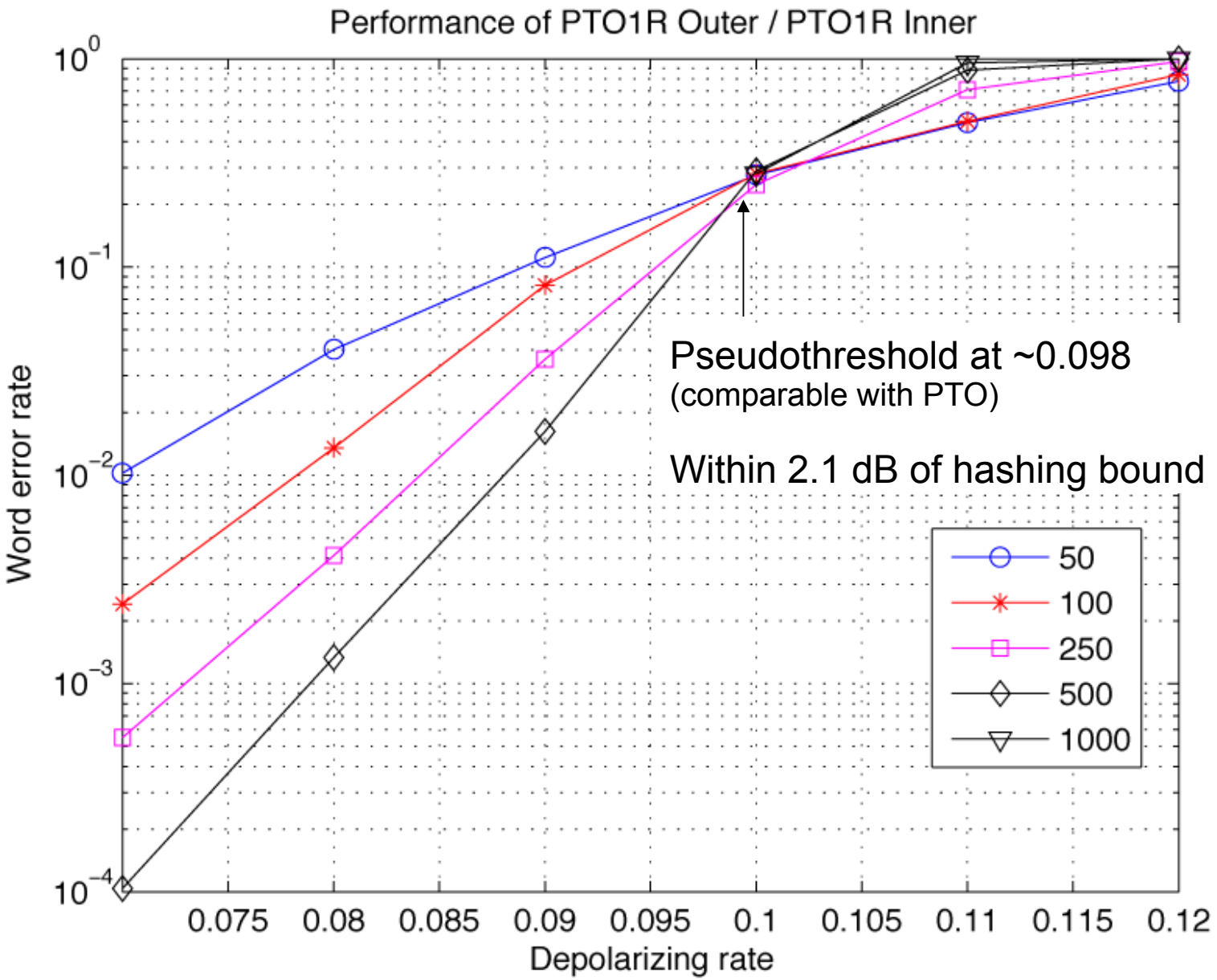
M. M. Wilde and M.-H. Hsieh, “Entanglement boosts quantum turbo codes,” arXiv:1010.1256.

Compare with the Hashing Bounds



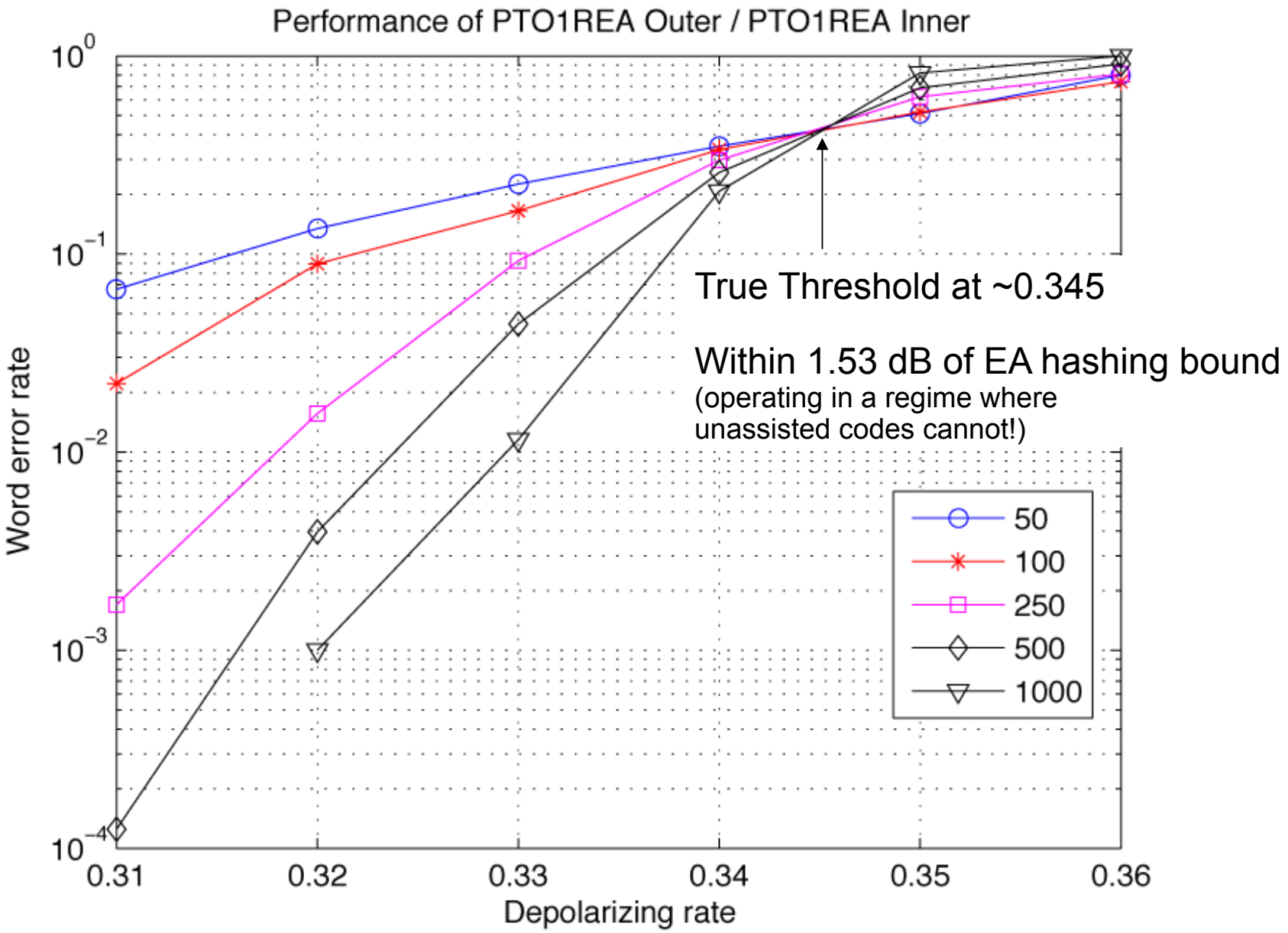
Bennett *et al*., “Entanglement-assisted classical capacity,” (2002)
Devetak *et al*., “Resource Framework for Quantum Shannon Theory (2005)

Unassisted Turbo Code



M. M. Wilde and M.-H. Hsieh, “Entanglement boosts quantum turbo codes,” arXiv:1010.1256.

Fully Assisted Turbo Code



M. M. Wilde and M.-H. Hsieh, “Entanglement boosts quantum turbo codes,” arXiv:1010.1256.

Quantum Polar Codes

Polar codes were invented by Arikan for classical error correction,
and we have now figured out how to
exploit these ideas for quantum error correction

Result: The first class of explicit quantum codes
that provably achieve the hashing bound and
have an efficient encoding and decoding

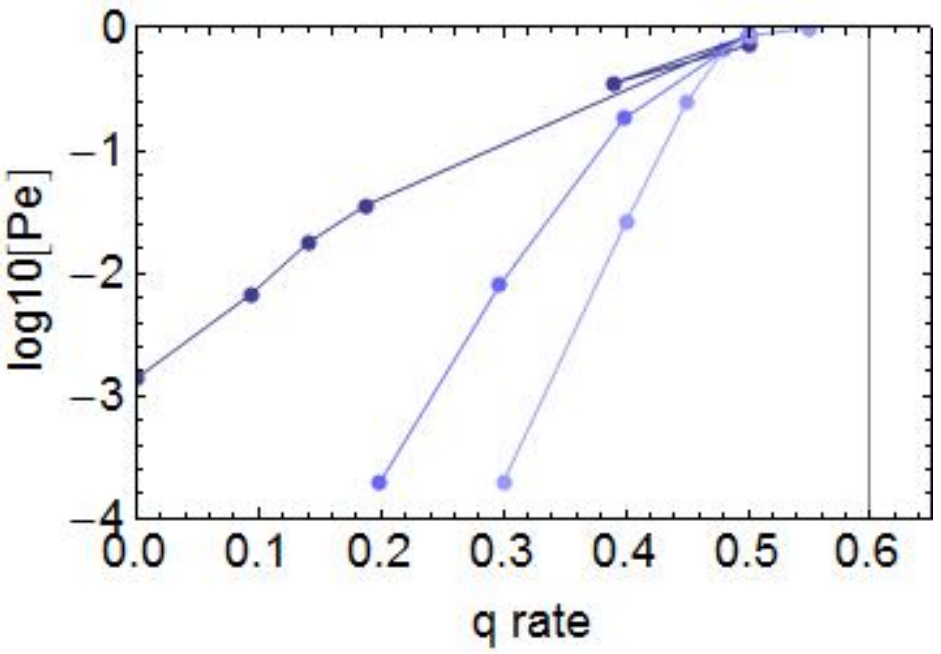
The scheme relies on *channel polarization*:
A recursive encoding induces a set of synthesized channels
of which a fraction are **perfect** and the other fraction are **useless**

Many theoretical papers on this topic, now starting numerical work

Erdal Arikan, “Channel polarization: A method for constructing capacity-achieving codes ... ,” arXiv:0807.3917.
M. M. Wilde and S. Guha, “Polar codes for classical-quantum channels,” arXiv:1109.2591.
M. M. Wilde and S. Guha, “Polar codes for degradable quantum channels,” arXiv:1109.5346.
M. M. Wilde and J. M. Renes, “Quantum polar codes for arbitrary channels,” arXiv:1201.2906.
S. Guha and M. M. Wilde, “Polar coding to achieve the Holevo capacity of a pure-loss optical channel,” arXiv:1202.0533.
M. M. Wilde and J. M. Renes, “Polar codes for private classical communication,” arXiv:1203.5794.

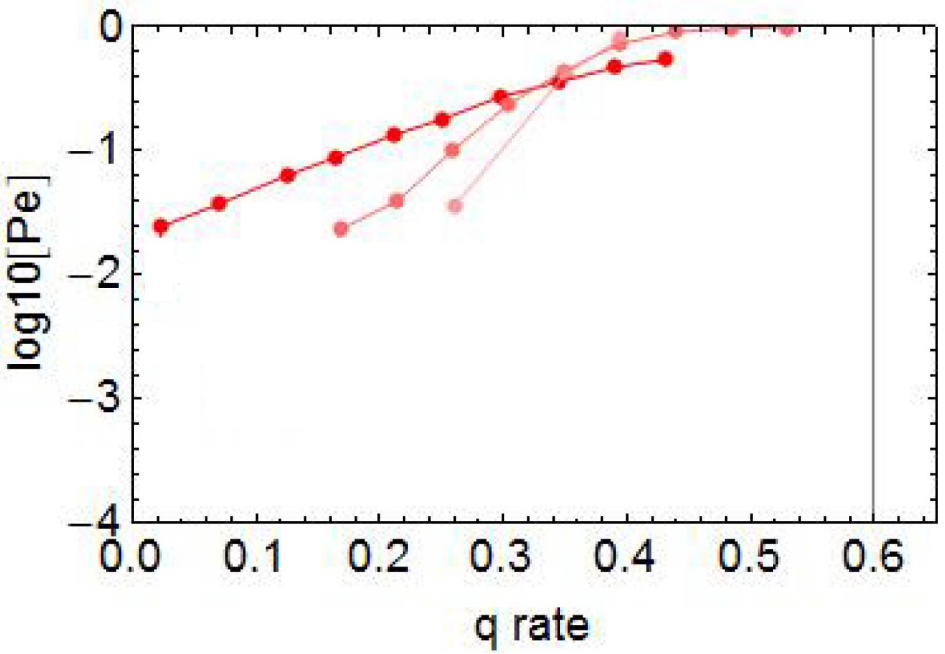
Preliminary Simulation Results for Quantum Polar Codes

Quantum erasure channel



Erasure probability – 0.2

Quantum depolarizing channel



Depolarizing probability – 0.063

Block sizes of codes are 128, 1024, 4096

Results are preliminary...

Z. Dutton, S. Guha, and M. M. Wilde, In preparation (2012)

Future Directions

The goal of the **second quantum revolution** is to narrow down all scenarios in which we have a “quantum supremacy” and to realize this supremacy

Much remains to be understood

Much work regarding quantum code performance is numerical in order to make statements to experimentalists regarding device design