Quantum Convolutional Coding Techniques

Mark M. Wilde

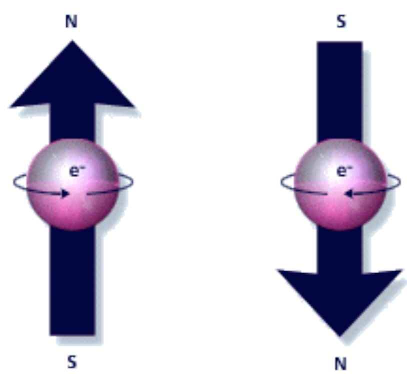
Communication Sciences Institute,
Ming Hsieh Department of Electrical Engineering,
University of Southern California,
Los Angeles, California 90089

cQIST
USC
Center *for*
Quantum Information Science
and Technology

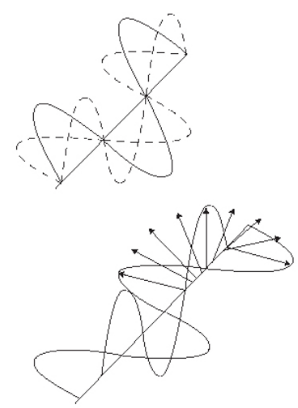
What is a qubit?

A **qubit** is a quantum system with two degrees of freedom.

Examples



Electron Spin

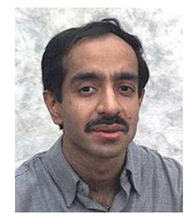


Photon Polarization

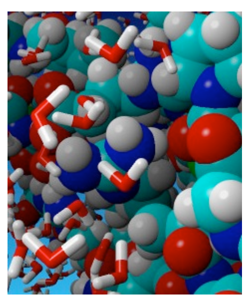
What are qubits good for?

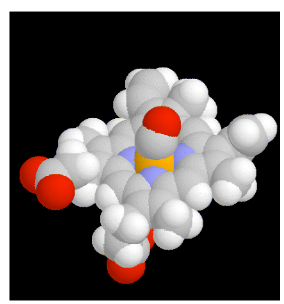
- Shor's algorithm (1994) breaks the RSA public key cryptography algorithm in polynomial time.

- Grover's algorithm (1997) gives a quadratic speedup for database search. Google YAHOO!



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





Tell me more about a **qubit**

A 2D complex vector represents the state of a qubit:

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

Measurement projects the qubit

to state $|0\rangle$ w/ prob. $|\alpha|^2$

to state $|1\rangle$ w/ prob. $|\beta|^2$

What can I do to a **qubit**?

Pauli matrices act on a single qubit:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

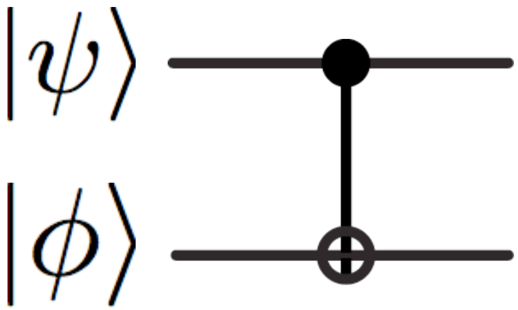
The Pauli group acts on multiple qubits:

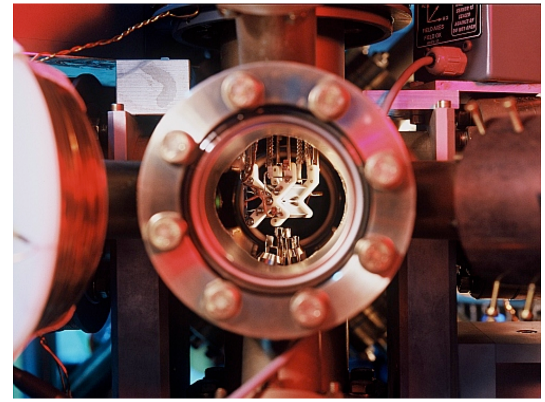
$$\Pi^n = \{A_1 \otimes \cdots \otimes A_n : A_j \in \Pi\}$$

E.g., $(Z \otimes Z) \, |\psi\rangle \otimes |\phi\rangle$

What can I do to **two qubits**?

A Controlled-NOT gate acts on two qubits:





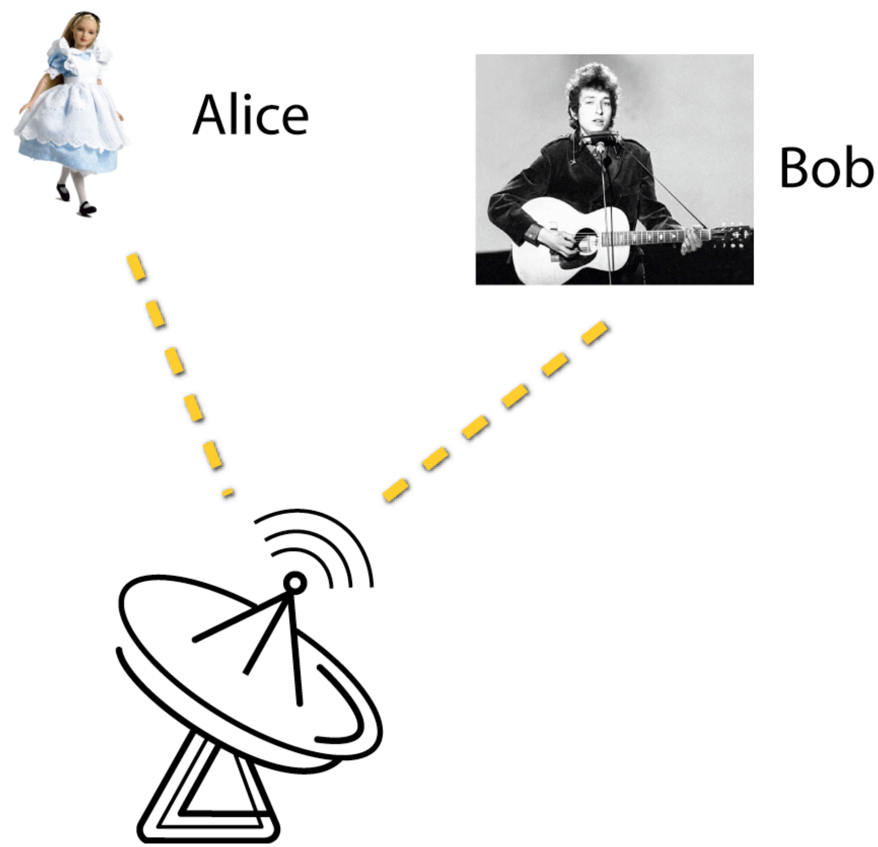
CNOT in an ion trap

Action of CNOT on computational basis:

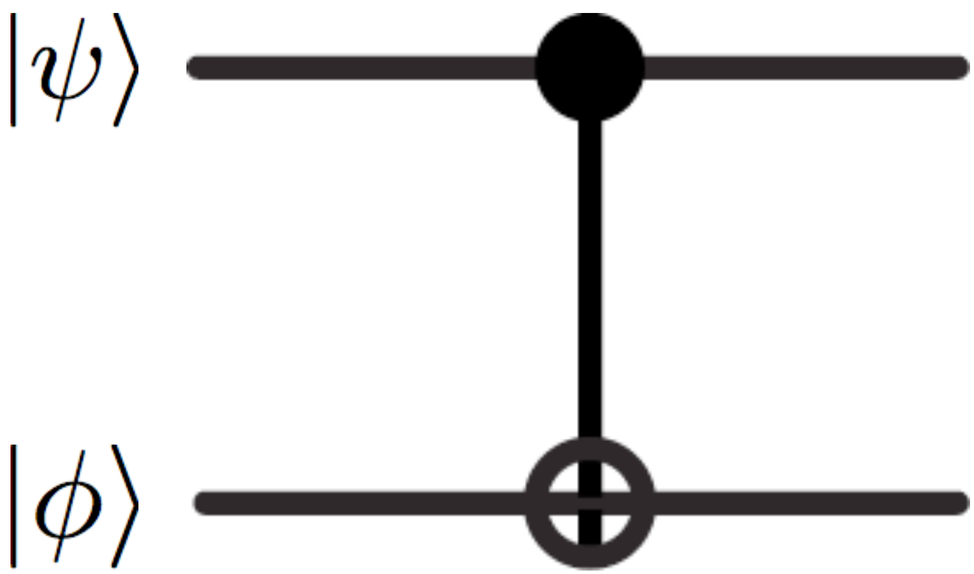
$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |11\rangle \\
|11\rangle &\rightarrow |10\rangle
\end{aligned}
$$

What is **Quantum Entanglement?**

Quantum entanglement is the resource that fuels a quantum computer or a quantum communication network.



Quantum Information and Noise



Alice

Eve

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

Can We Correct **Quantum Errors**?

Shor's Solution

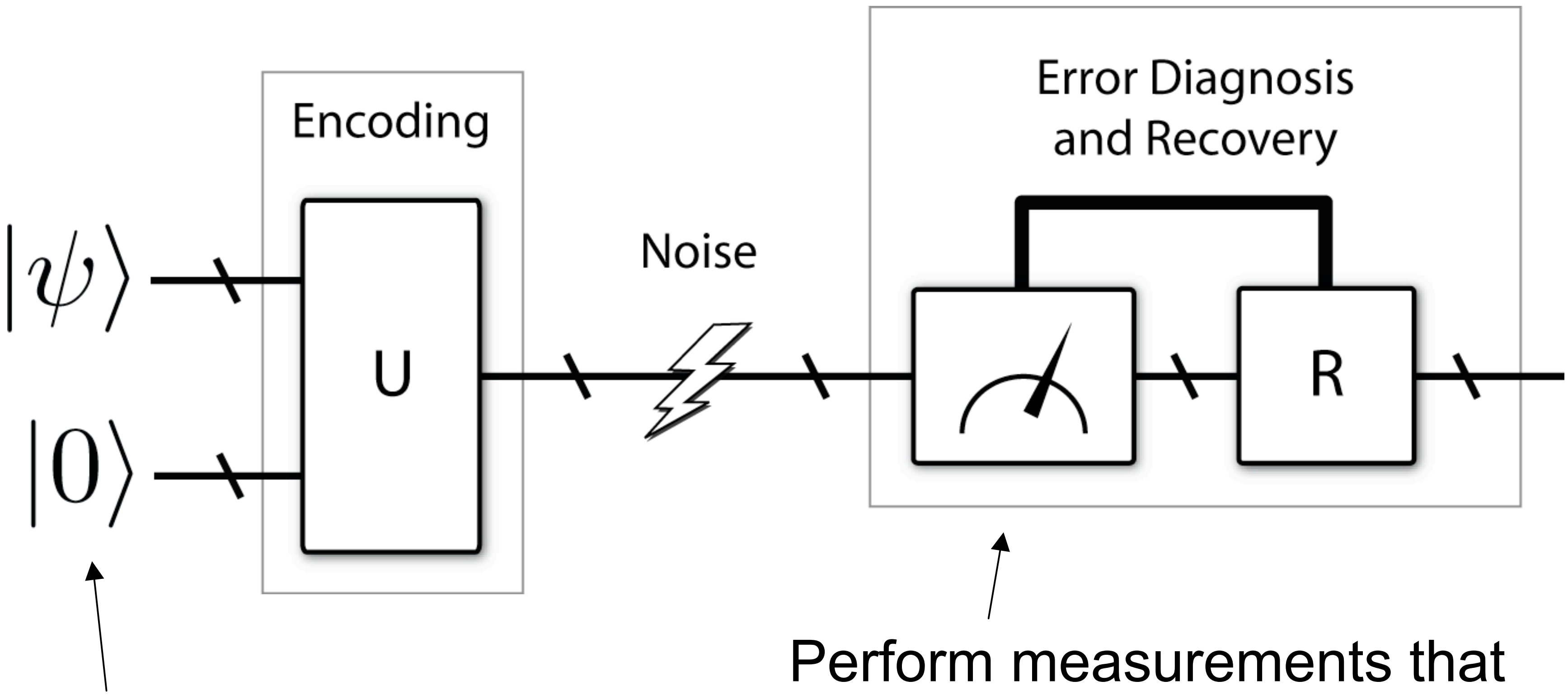
• Use extra ancilla qubits for redundancy

• Perform particular measurements that learn only about errors

• Measurement projects the encoded qubits and effectively digitizes the errors.

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

Shor Code



Encode qubits with ancillas

Perform measurements that learn only about errors

Our Research @ USC

Novel forms of Quantum Error Correction

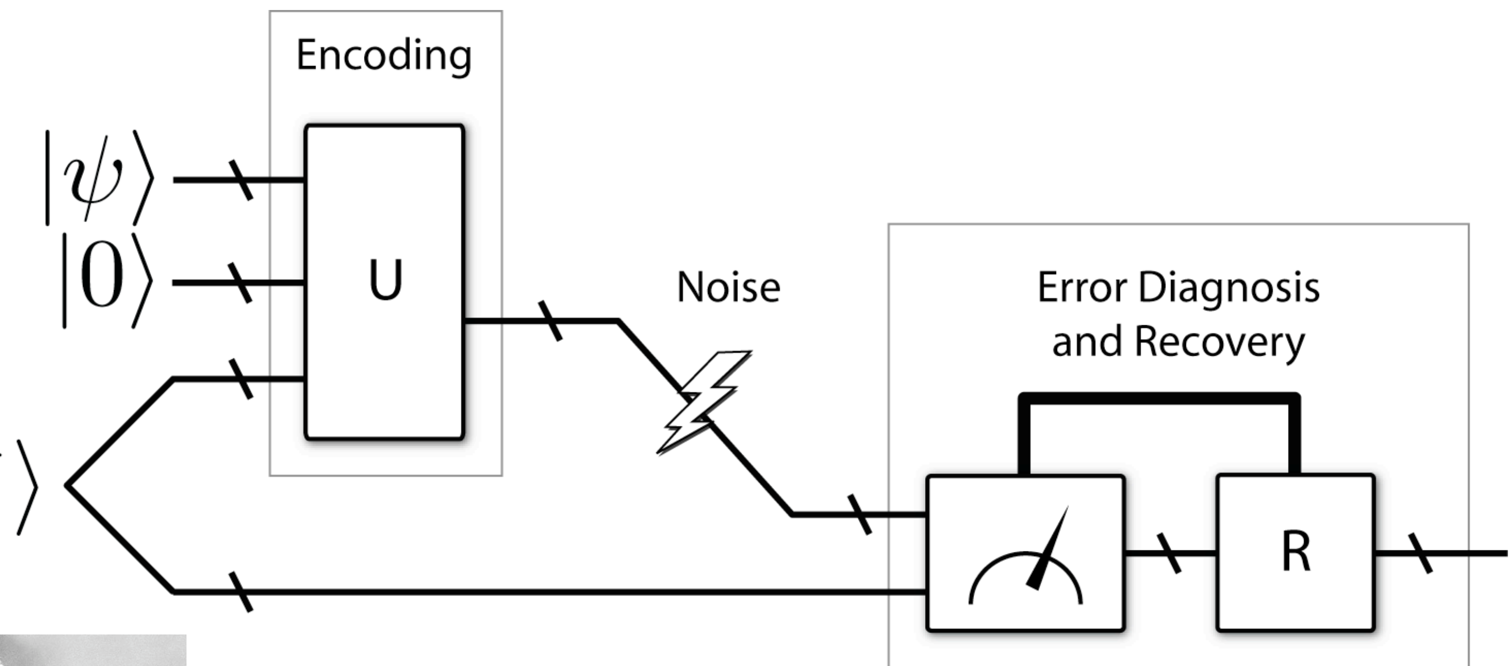
Decoherence-free subspaces and subsystems (Lidar)

Entanglement-assisted quantum error correction (Brun, Devetak, Hsieh)

Entanglement-assisted quantum convolutional coding (Wilde, Brun)

Convolutional entanglement distillation (Wilde, Krovi, Brun)

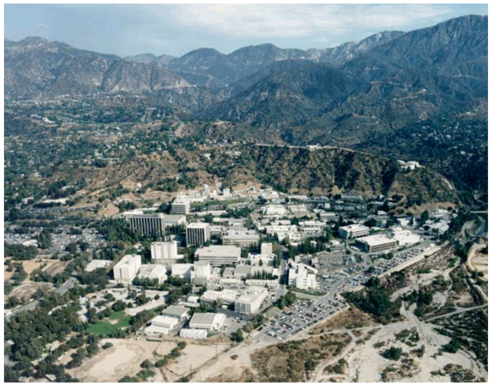
Entanglement-Assisted Quantum Error Correction



Brun et al., Science ***314****, 436-439 (2006).*

Classical Convolutional Coding

Convolutional Coding techniques have application in



cellular and **deep space** communication

Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm

ANDREW J. VITERBI, SENIOR MEMBER, IEEE

Abstract—The probability of error in decoding an optimal convolutional code transmitted over a memoryless channel is bounded from above and below as a function of the constraint length of the code. For all but pathological channels the bounds are asymptotically (exponentially) tight for rates above R_0, the computational cutoff rate of sequential decoding. As a function of constraint length the performance of optimal convolutional codes is shown to be superior to that of block codes of the same length, the relative improvement increasing with rate. The upper bound is obtained for a specific probabilistic nonsequential decoding algorithm which is shown to be asymptotically optimum for rates above R_0 and whose performance bears certain similarities to that of sequential decoding algorithms.

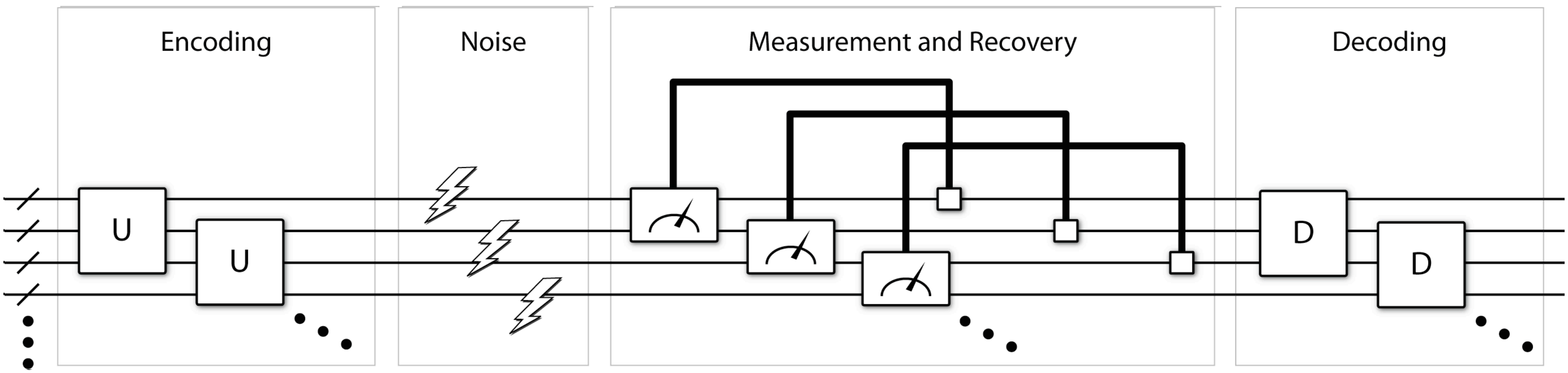
Manuscript received May 20, 1966; revised November 14, 1966. The research for this work was sponsored by Applied Mathematics Division, Office of Aerospace Research, U. S. Air Force, Grant AFOSR-700-65.

I. Summary of Results

SINCE Elias[1] first proposed the use of convolutional (tree) codes for the discrete memoryless channel, it has been conjectured that the performance of this class of codes is potentially superior to that of block codes of the same length. The first quantitative verification

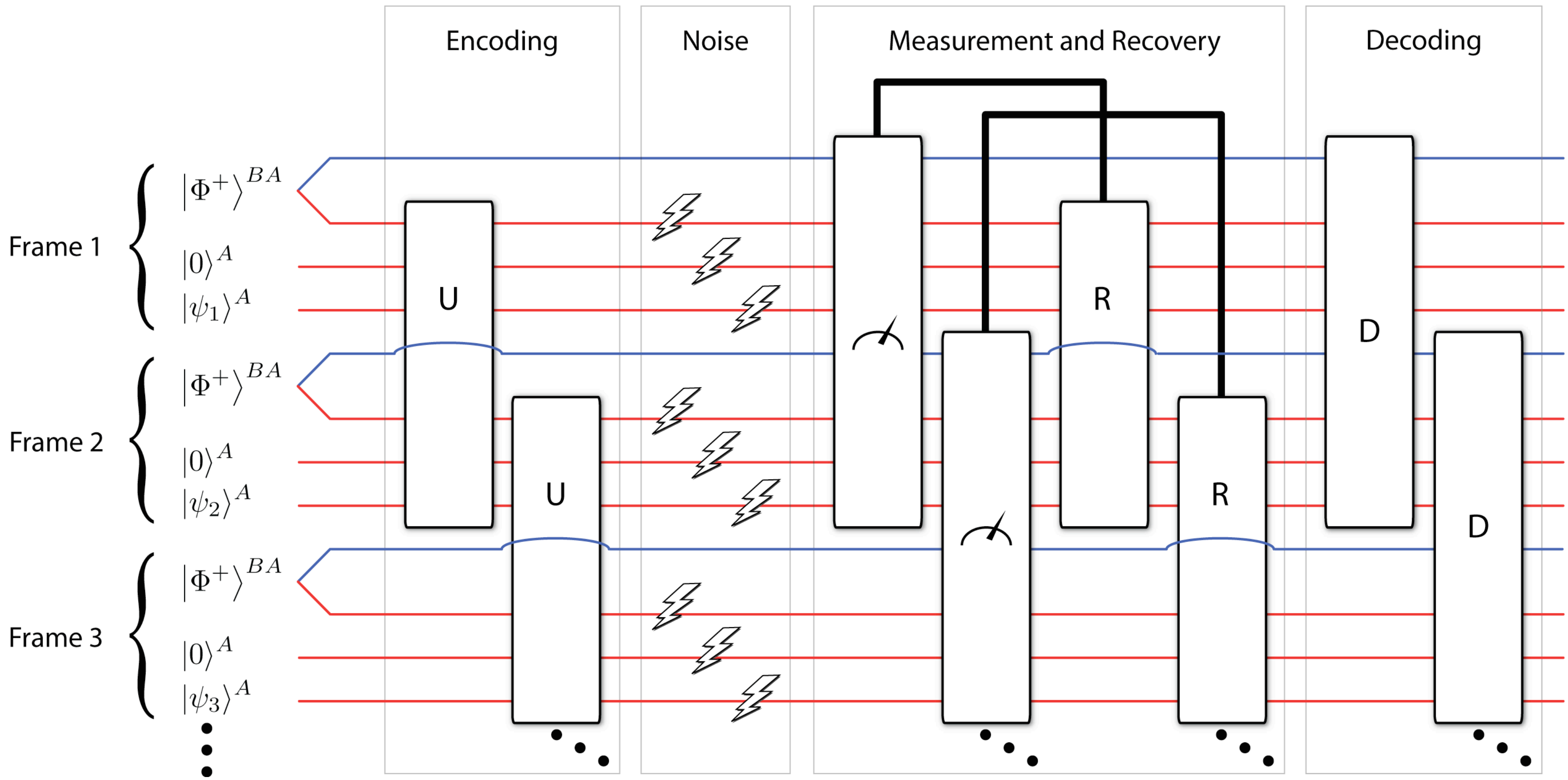
Viterbi Algorithm is most popular technique for determining errors

Quantum Convolutional Coding



*Ollivier and Tillich, PRL **91,** 177902 (2003).*
*Forney et al., IEEE Trans. Inf. Theory **53**, 865-880 (2007).*

Entanglement-Assisted Quantum Convolutional Coding



Wilde and Brun, In preparation (2007).

Advantages of EAQCC

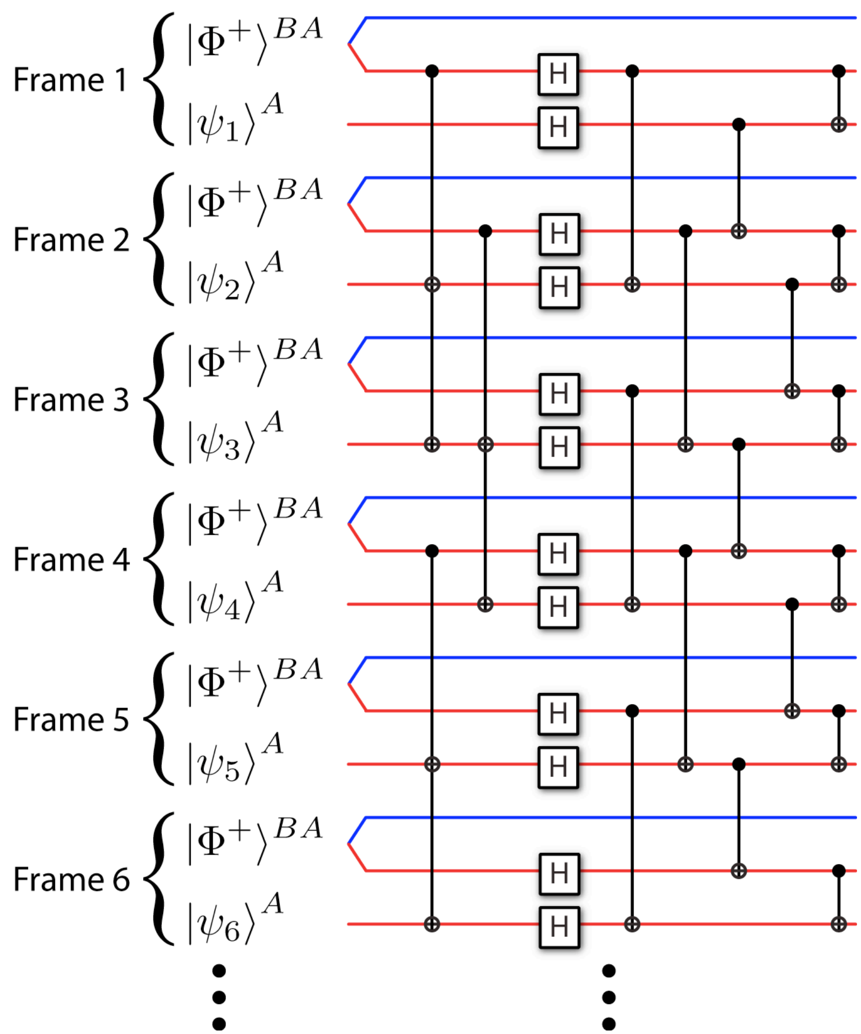
Can produce an EAQCC from two arbitrary classical binary convolutional codes:

$$\left[\begin{array}{c|c} H_1(D) & 0 \\ 0 & H_2(D) \end{array}\right]$$

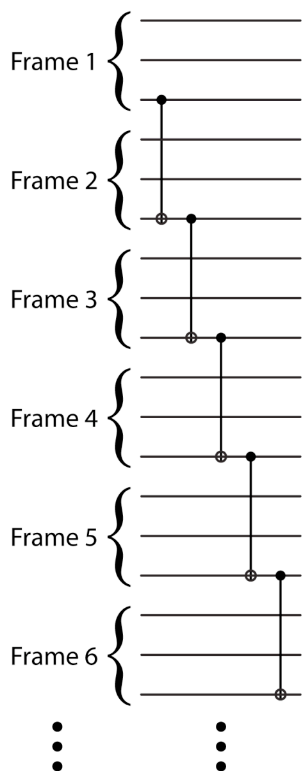
The rate and error-correcting properties of the classical codes translate to the EAQCC.
(high-performance classical codes => high-performance quantum codes)

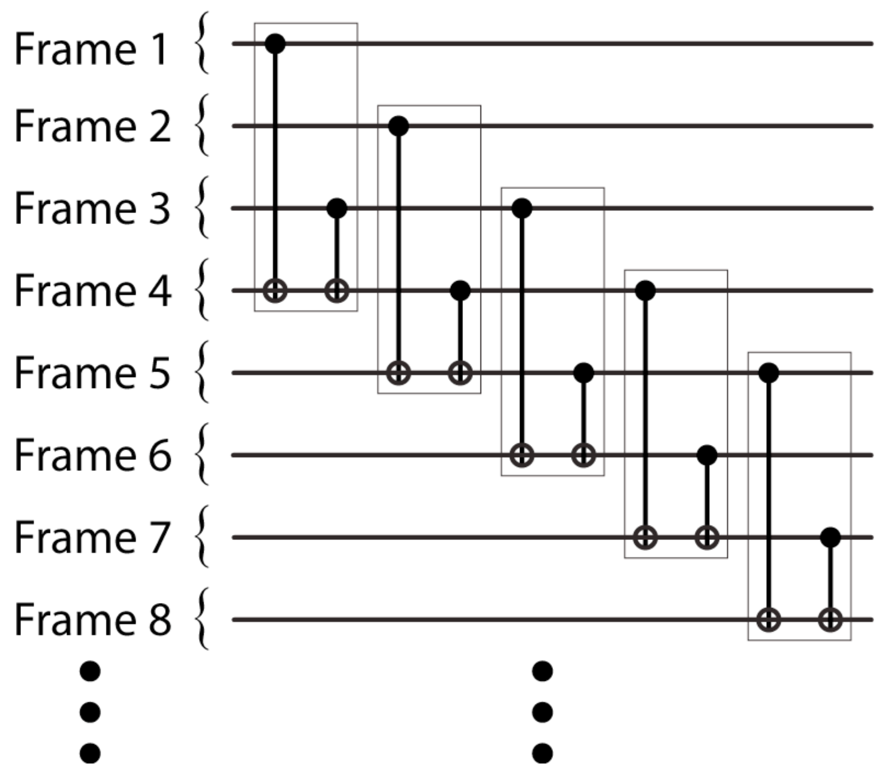
$$\begin{array}{c} [n, k_1] \\ [n, k_2] \end{array} \Rightarrow [n, k_1 + k_2 - n + c; c]$$

EAQCC Example 1



Infinite-Depth Operations

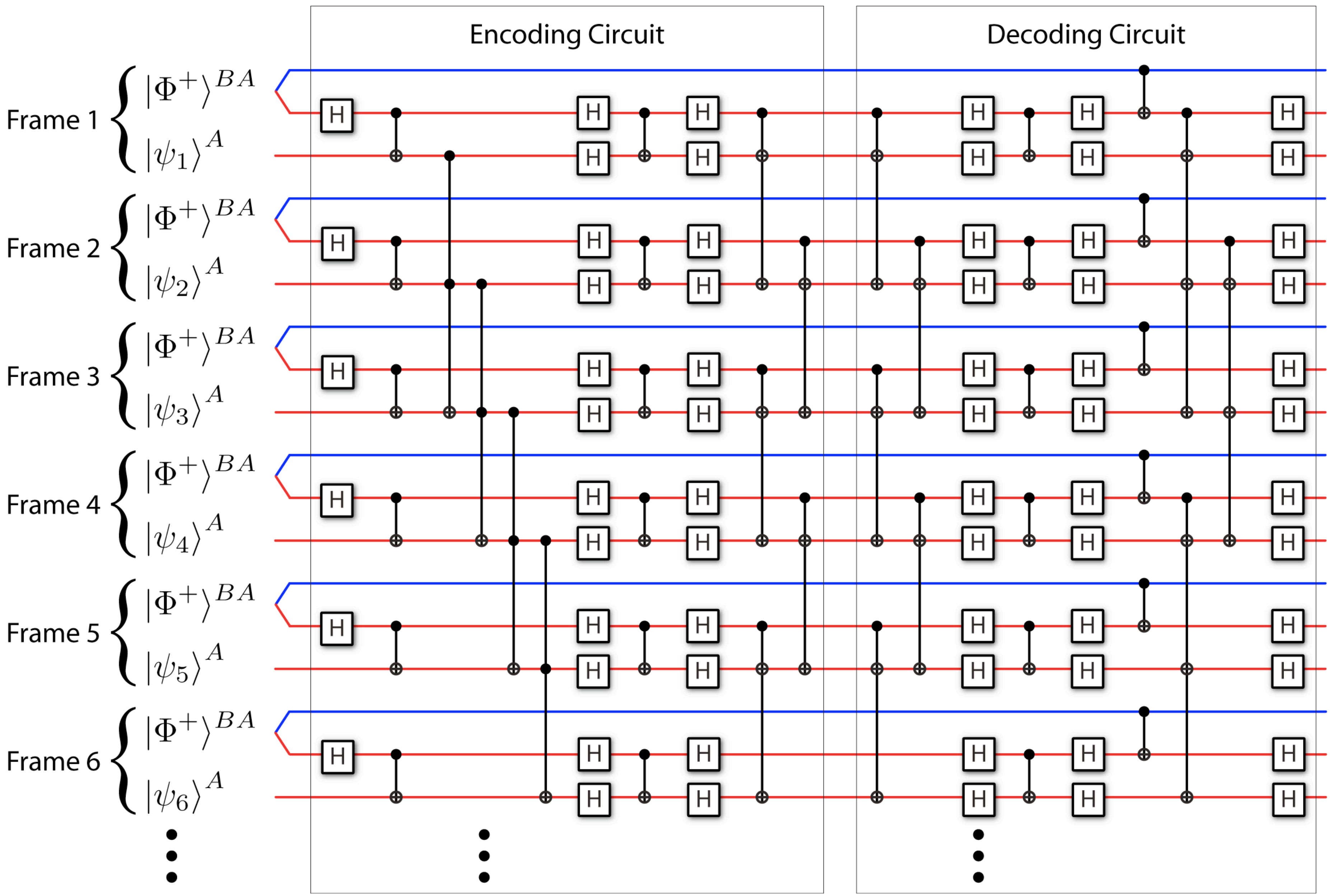




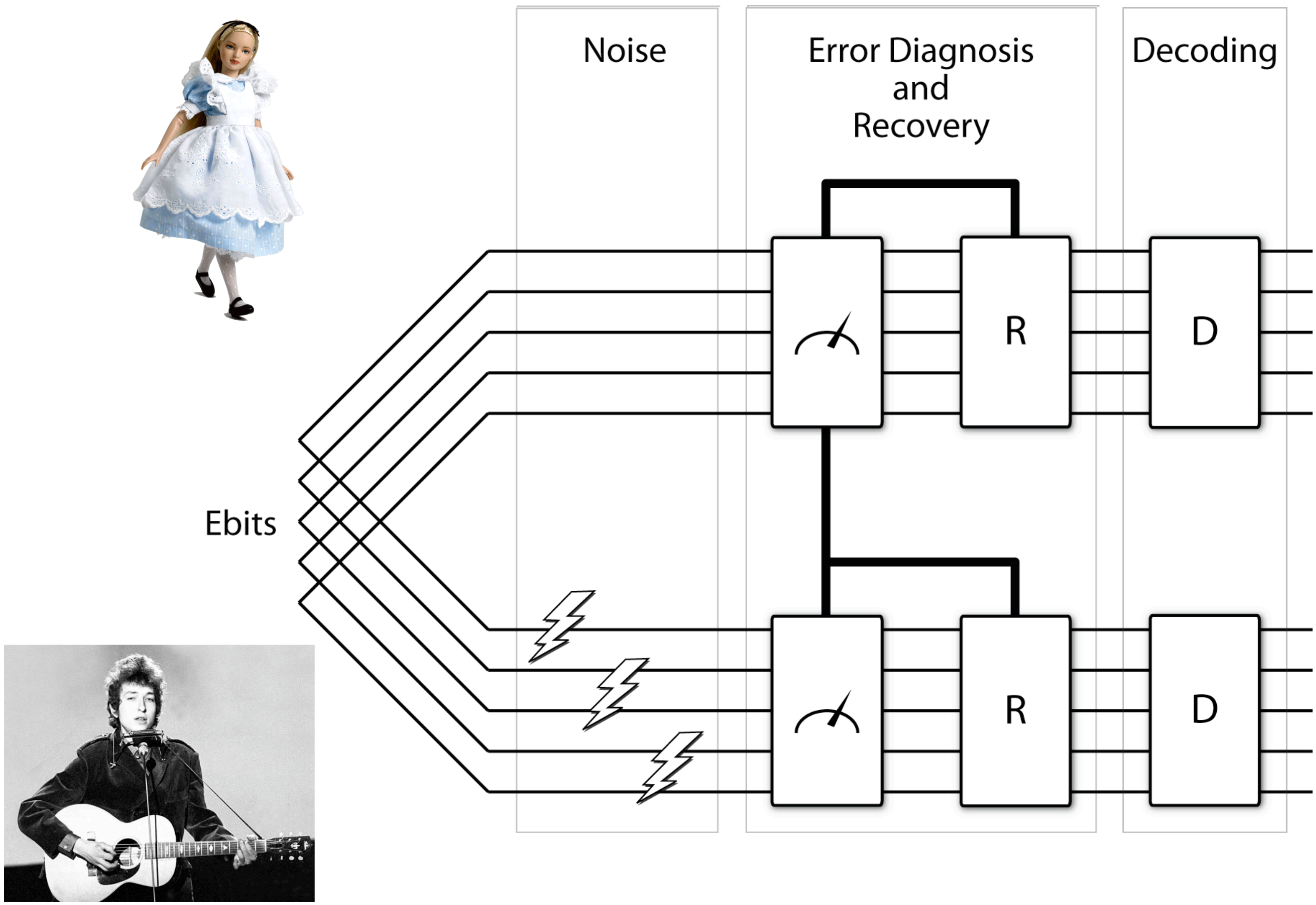
Implements 1/(1+D)

Implements $1/(1+D+D^3)$

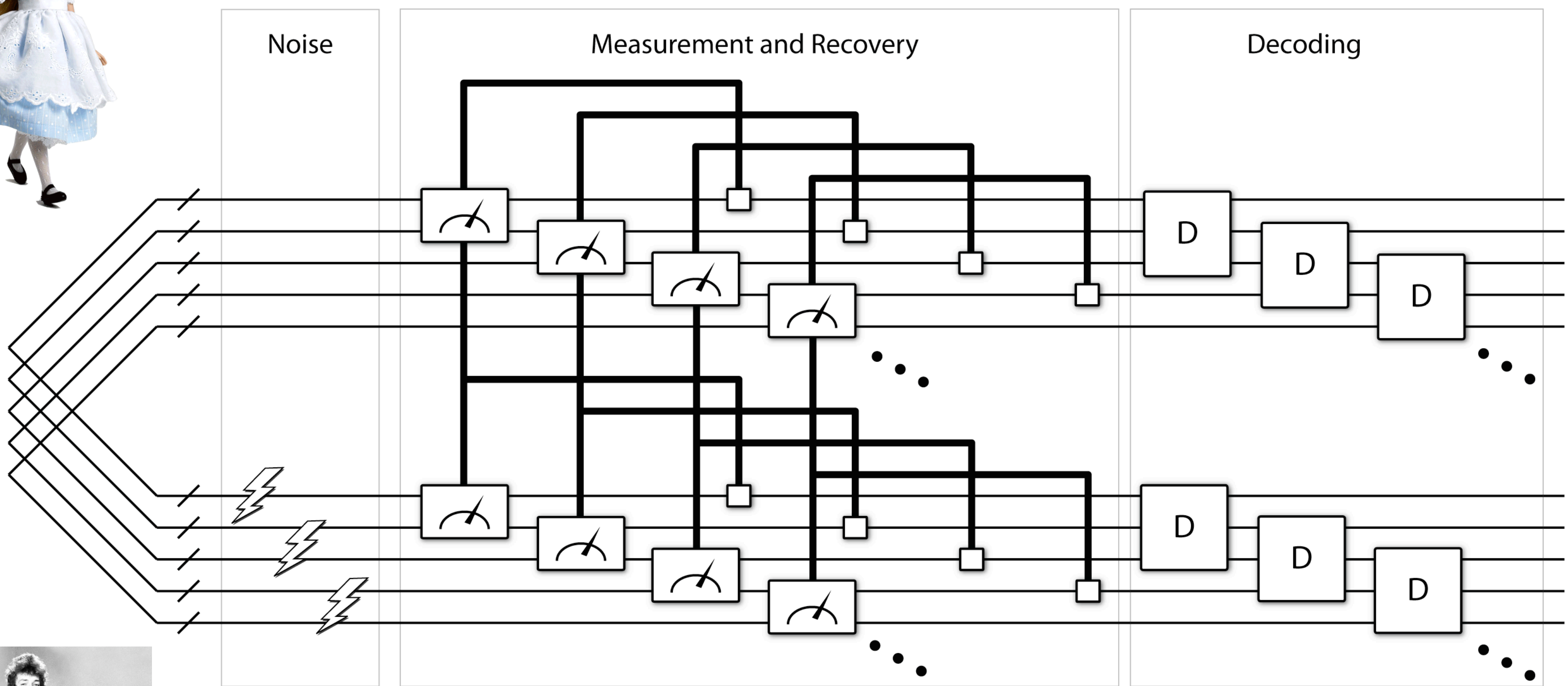
EAQCC Example 2



Block Entanglement Distillation



Convolutional Entanglement Distillation



Wilde et al., arXiv:0708.3699 (2007).

Conclusion

- **Quantum computing** and **quantum communication** are the future of computing and communication
- **Quantum error correction** is the way to make quantum computing and communication practical
- **Quantum error correction** also leads to private classical communication
- There is still much to explore in these areas (QEC07@USC)