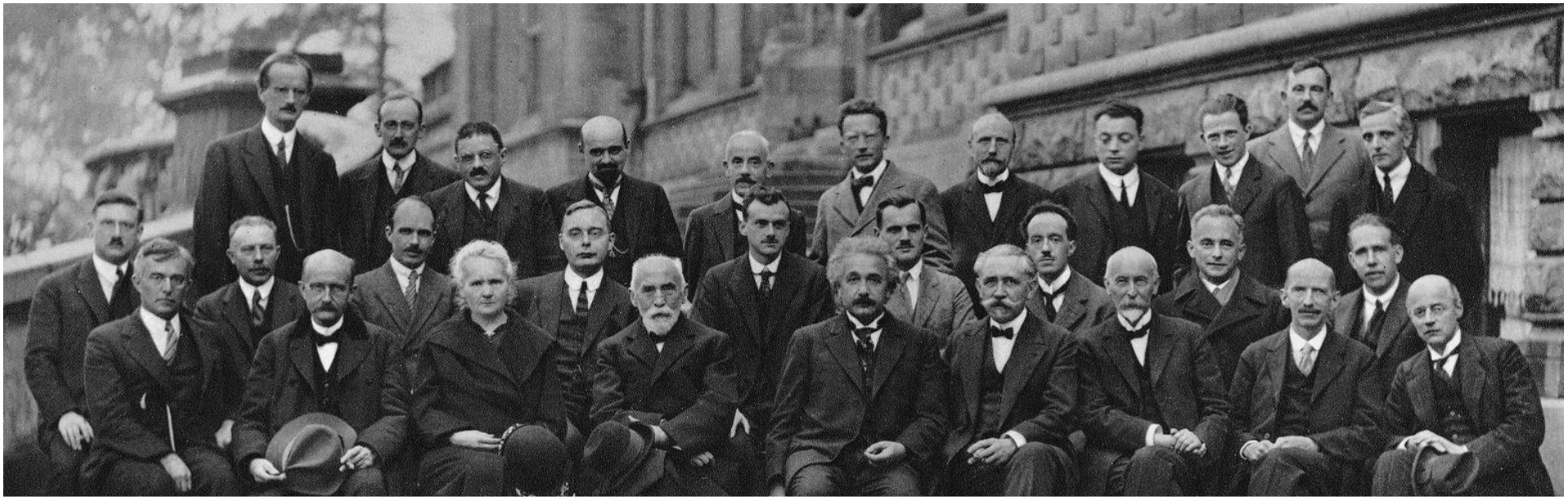
Quantum Information & Optical Communication

Mark M. Wilde

McGill University

LSU Physics & Astronomy Colloquium,
Baton Rouge, Louisiana, April 5, 2012

The Quantum Revolution

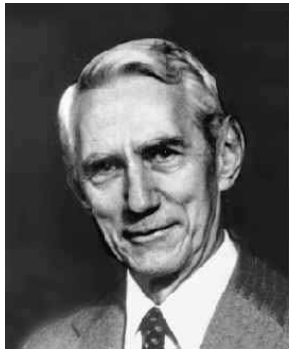


Solvay Conference in Brussels 1927

Quantum Theory developed from 1900-1925

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

The Information Revolution



In 1948, **Claude Shannon** revolutionized the **theory of information storage and transmission** with a breakthrough publication:

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

"Einstein of the Information Age"

The Quantum Information Revolution

Shor

Bennett

Holevo

Schumacher

Westmoreland

"The Second Quantum Revolution" *or*
"The Second Information Revolution"

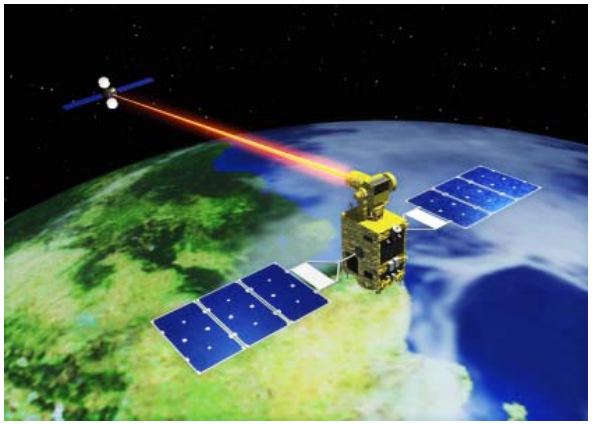
"Putting quantum weirdness to use"

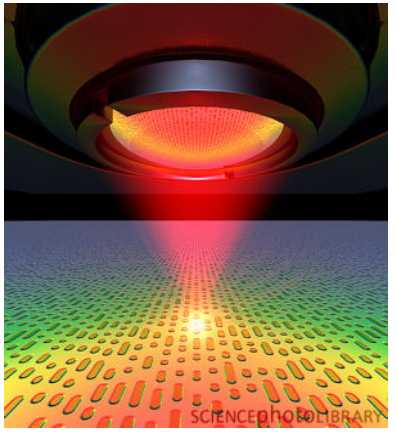
Ideas such as **teleportation**, **superdense coding**, the **Schumacher qubit**, **quantum compression**, and **capacity of a quantum channel** are important here

Overview

- Quantum weirdness

- Putting quantum weirdness to use





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*).

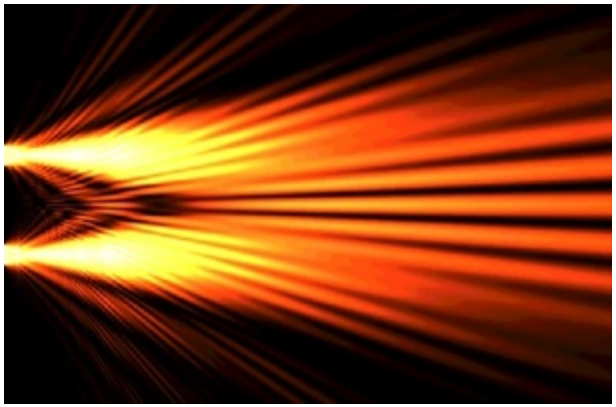
A qubit state can be classical ("*here or there*"):

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

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**

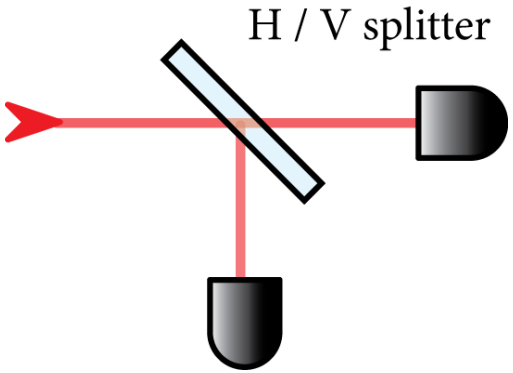
For classical states $|0\rangle$ or $|1\rangle$, a “**computational-basis**” measurement gives a *definite outcome* and *state is unchanged*.

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

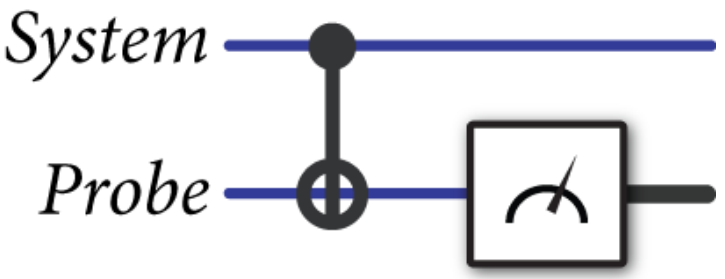
Such a measurement gives outcome $|0\rangle$ with probability $|\alpha|^2$

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

Optical example:



Typical QIP implementation of measurement:



How is quantum different from classical?

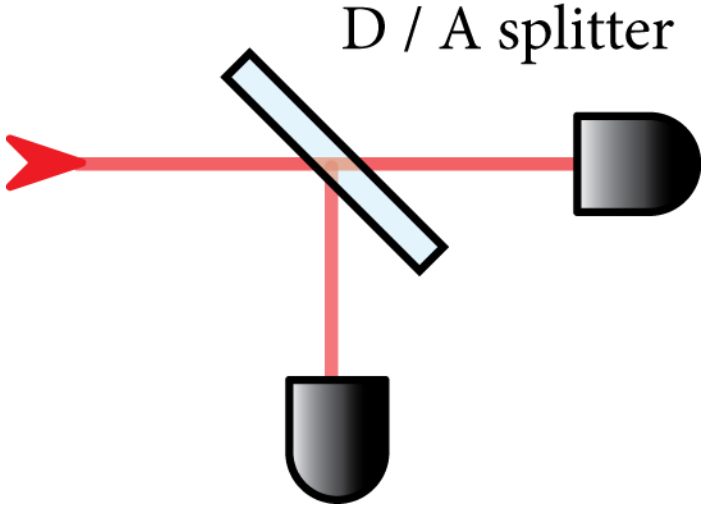
Superposed state: $\alpha|0\rangle + \beta|1\rangle$

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

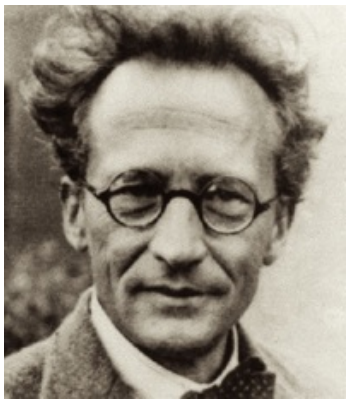
$$\frac{1}{\sqrt{2}}(|0\rangle^A \otimes |0\rangle^B + |1\rangle^A \otimes |1\rangle^B)$$

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."



Entanglement Games

Entanglement is often the “fuel” in QIP

Can understand this *supercorrelation* with the CHSH game

Referee sends bits *x* and *y* to **Alice** and **Bob**

They respond with *a* and *b*

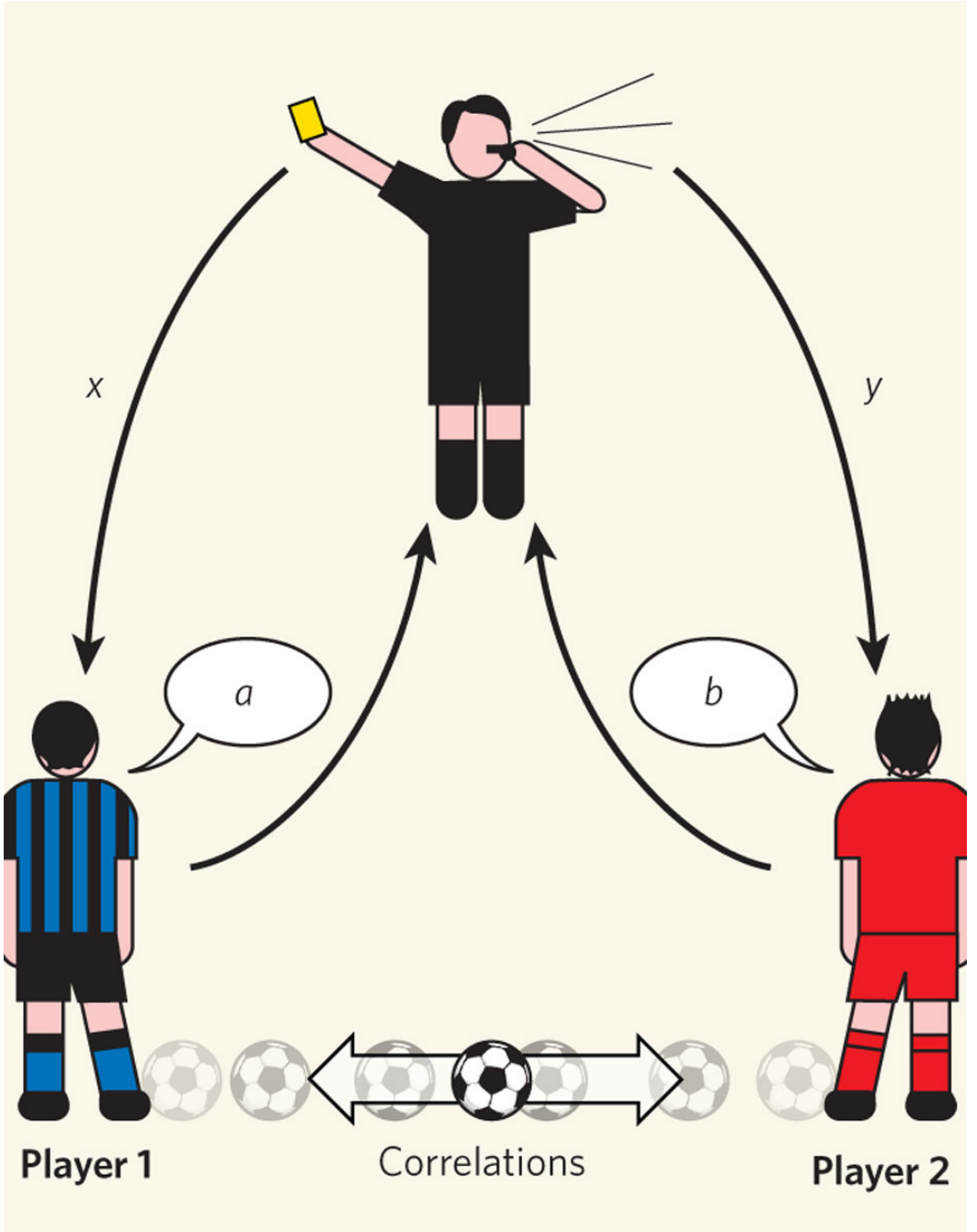
They win if

$$x \wedge y = a \oplus b$$

Maximal classical winning prob. is 3/4
(*at least one question pair is answered incorrectly*)

Quantum strategy has winning prob.:

$$\cos^2(\pi/8) \approx 0.85$$

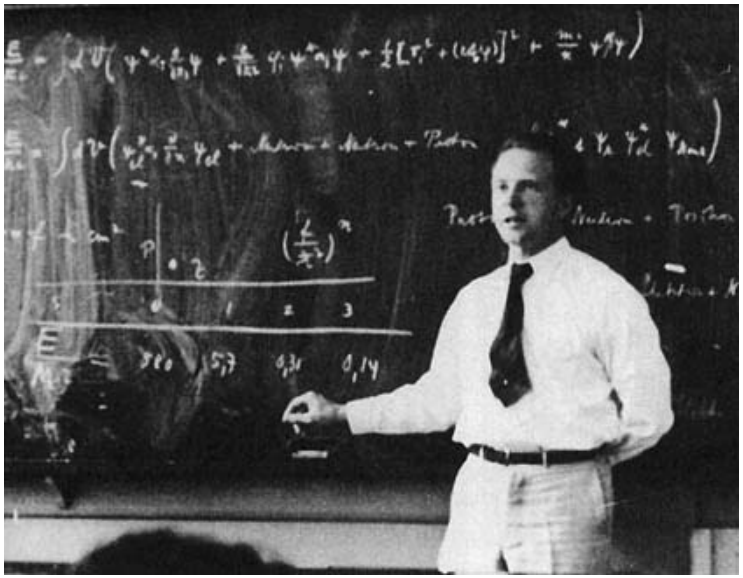


Uncertainty Principle

Heisenberg-Robertson relation:

$$(\Delta X) \times (\Delta Z) \geq \frac{1}{2}|\langle\psi|[X, Z]|\psi\rangle|$$

The "uncertainty product" has a fundamental, state-dependent lower bound in terms of "non-commutativity" two observables



Correct Interpretation:

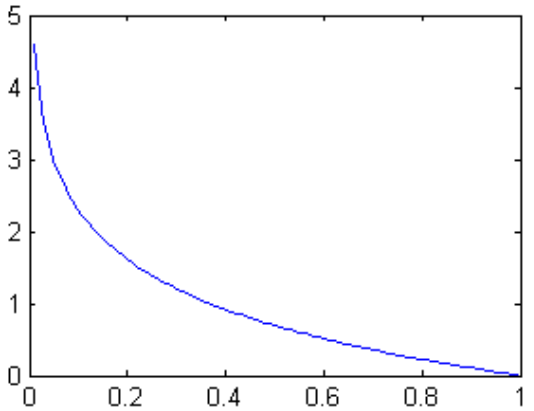
1) Do many measurements of *X* with system in state $|\psi\rangle$
2) Calculate Δ*X*
3) Do many measurements of *Z* with system in state $|\psi\rangle$
4) Calculate Δ*Z*
5) Uncertainty product obeys the above lower bound.

Aside: Information and Entropy

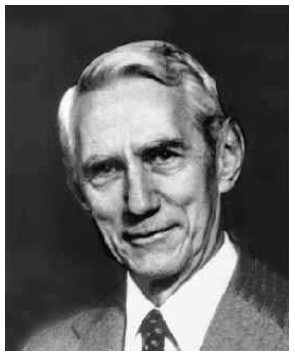
Information Content is a *Measure of Surprise*

Given random variable *X* with outcome *x*,
the surprise is

$$i(x) \equiv -\log(p_X(x))$$



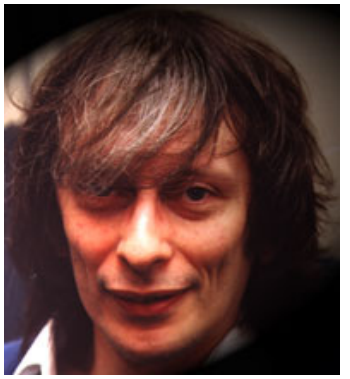
Entropy is the ***expected surprise***:



$$\begin{aligned} H(X) &\equiv \mathbb{E}_X\{i(X)\} \\ &= \sum_x p_X(x) i(x) \end{aligned}$$

Entropic Uncertainty Relation

Deutsch advocated for a state-independent, entropic uncertainty relation



Why? Consider state $|0\rangle$ in Robertson's relation

Also, standard deviation is a poor measure of uncertainty (*depends on values*)

Eventually, Maassen and Uffink proved the following:

$$H(X) + H(Z) \geq 1$$

(More general lower bound for other observables)

Interpretation again is in terms of many independent experiments

Not just conceptual, but useful operationally! (more coming up...)

Entropic Uncertainty Relation for Entanglement

How to unify uncertainty and entanglement?

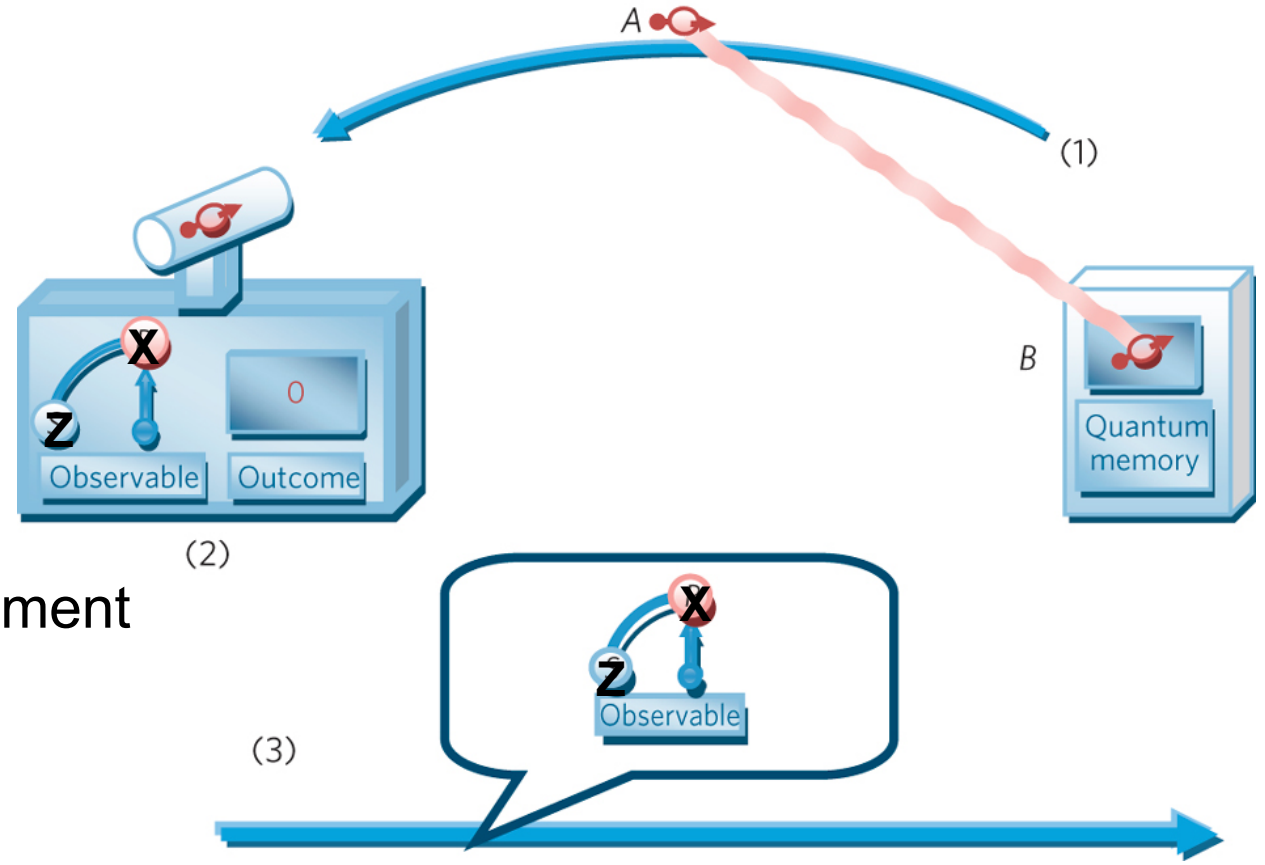
Consider another game!

1) Bob prepares two-qubit state and sends one to Alice

2) Alice measures *X* or *Z* on her received particle

3) She tells Bob which measurement she performed

Bob must guess her measurement outcome



Berta, Christandl, Colbeck, Renes, Renner. *Nature Physics* (2010)

Entropic Uncertainty Relation for Entanglement

Entropic Uncertainty Relation:

$$H(X|B) + H(Z|B) \geq 1 + H(A|B)$$

$H(X|B)$ quantifies Bob's ability
to **guess** the outcome of X given his system B

Similar statement for $H(Z|B)$ and Z

The quantity $H(A|B)$ indicates how **entangled** initial particles are

Example 1: Maximally entangled state has a lower bound of **zero**

Example 2: Uncorrelated state has a lower bound of 1 + $H(A)$
(*improvement over Maassen-Uffink*)

Berta, Christandl, Colbeck, Renes, Renner. *Nature Physics* (2010)

Entropic Uncertainty Relation for Entanglement

Other tripartite variation:

$$H(X|B) + H(Z|E) \geq 1$$

Interpretation: If Bob can guess X, then Eve can't guess *Z*!
(and vice versa)

This is the basis of a secure communication scheme and a scheme for quantum error correction

Wilde and Renes. arXiv:1203.5794 and arXiv:1201.2906

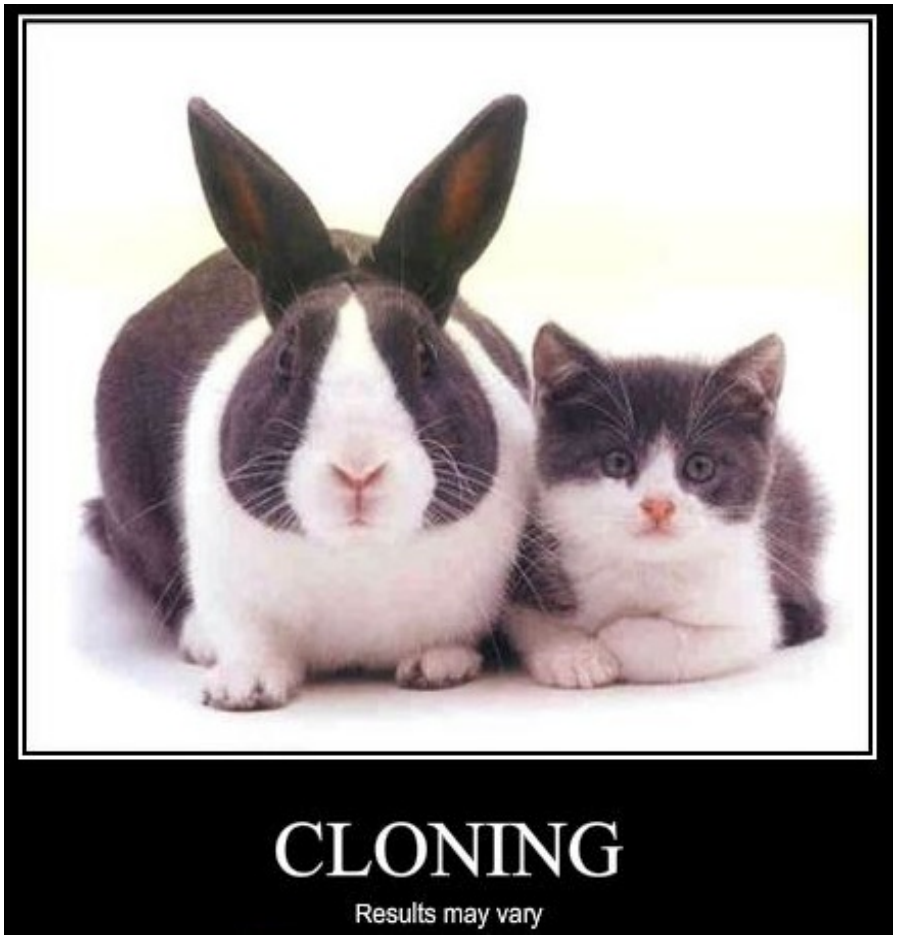
No-cloning theorem

Cannot copy arbitrary quantum states.

Proof follows from superposition principle

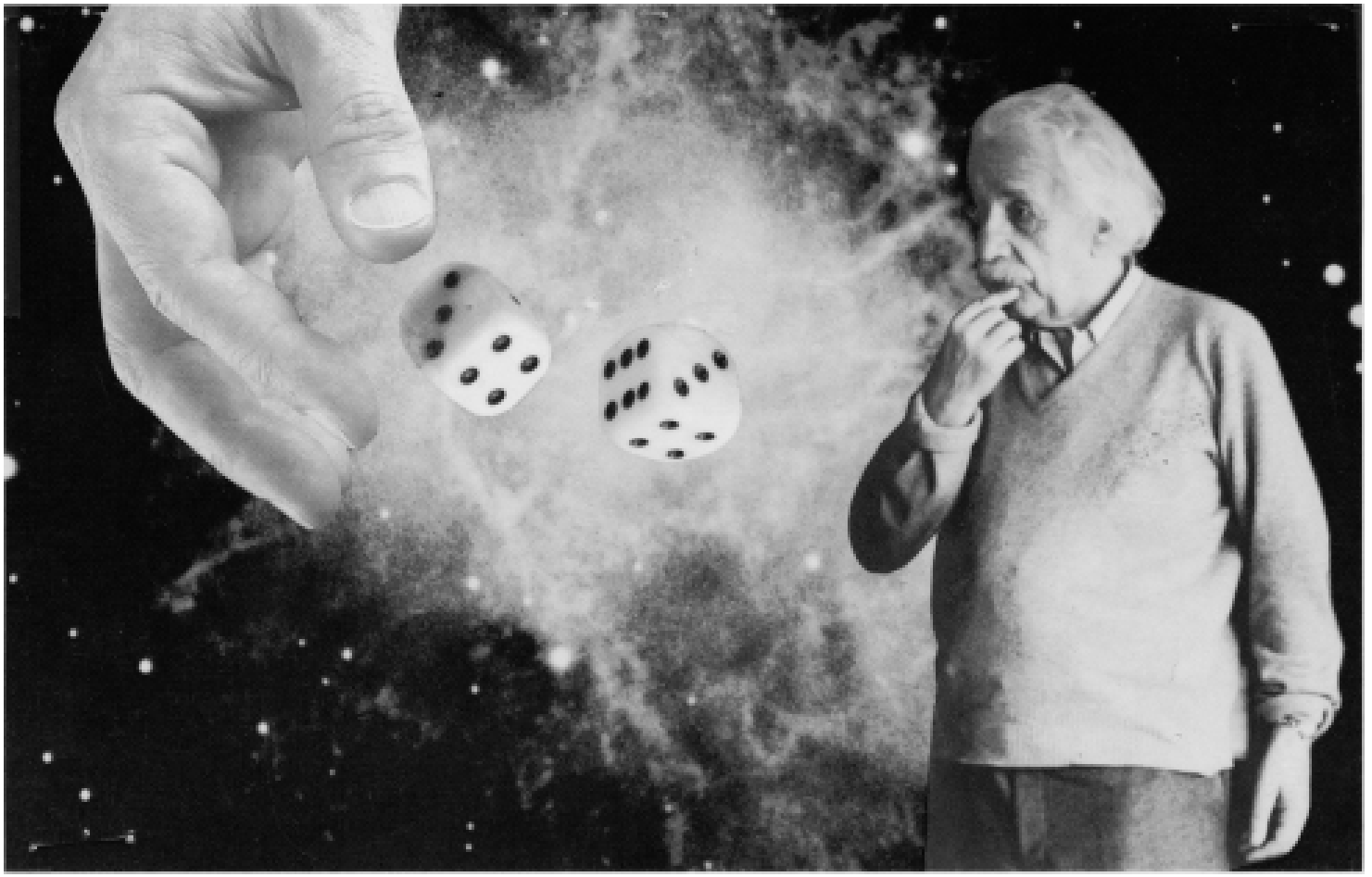
Suppose *U* is some universal copier

$$U|0\rangle|0\rangle = |0\rangle|0\rangle$$
$$U|1\rangle|0\rangle = |1\rangle|1\rangle$$
$$U(\alpha|0\rangle + \beta|1\rangle)|0\rangle$$
$$= U(\alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle)$$
$$= \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle$$
$$= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$$
$$\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

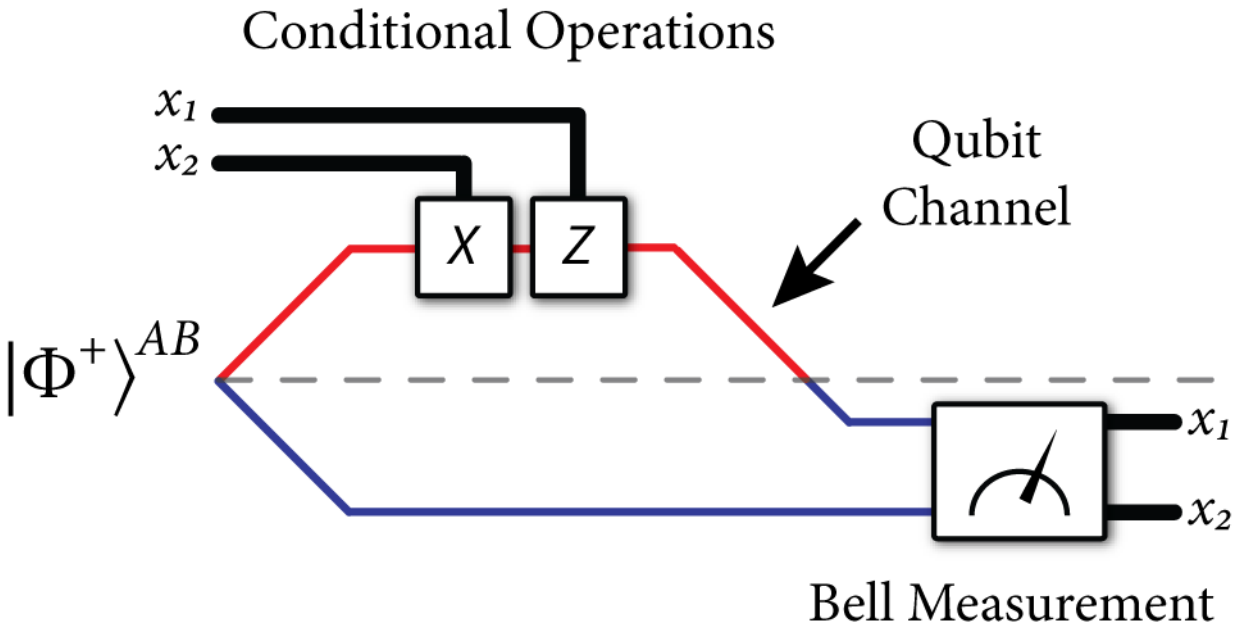


At the heart of our understanding of quantum information!

Putting Quantum Weirdness to Use



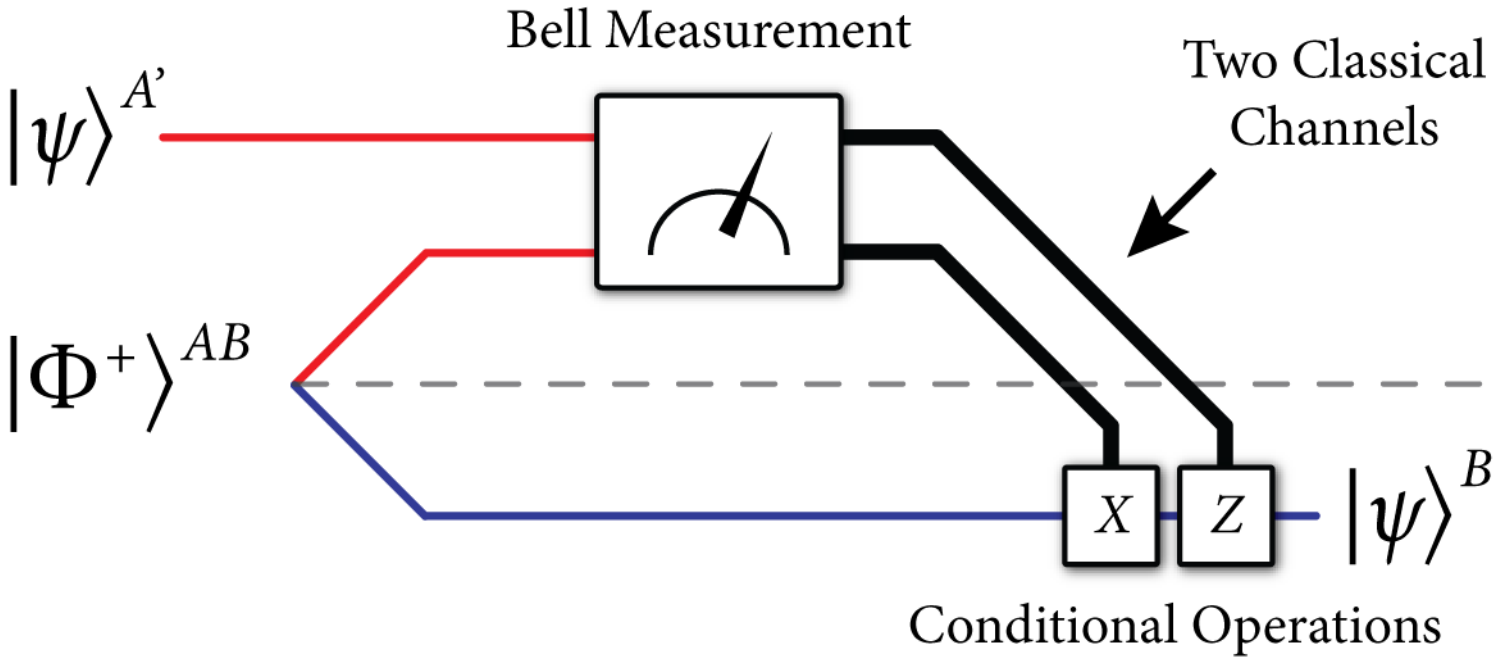
Super-dense Coding



One noiseless ebit and **one noiseless qubit channel** generates **two classical bit channels**

Bennett and Wiesner, *Physical Review Letters* 69, 2881 (1992)

Teleportation



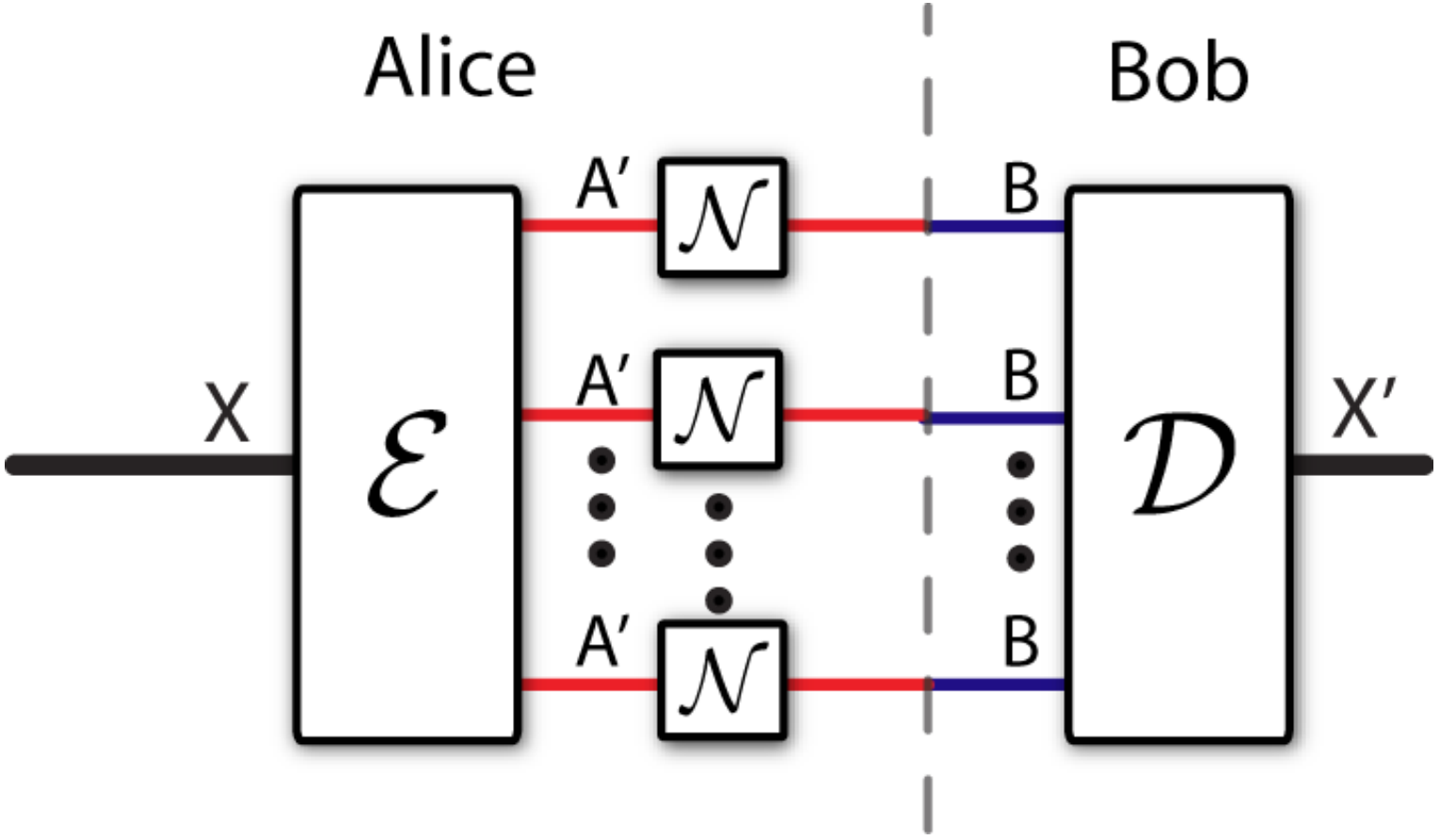
One noiseless ebit and **two classical bit channels** generates a **noiseless qubit channel** from Alice to Bob

Bennett *et al.*, *Physical Review Letters* 70, 1895 (1993)

Classical Capacity

Fundamental question:

What is the maximum rate for error-free comm. over a quantum channel?



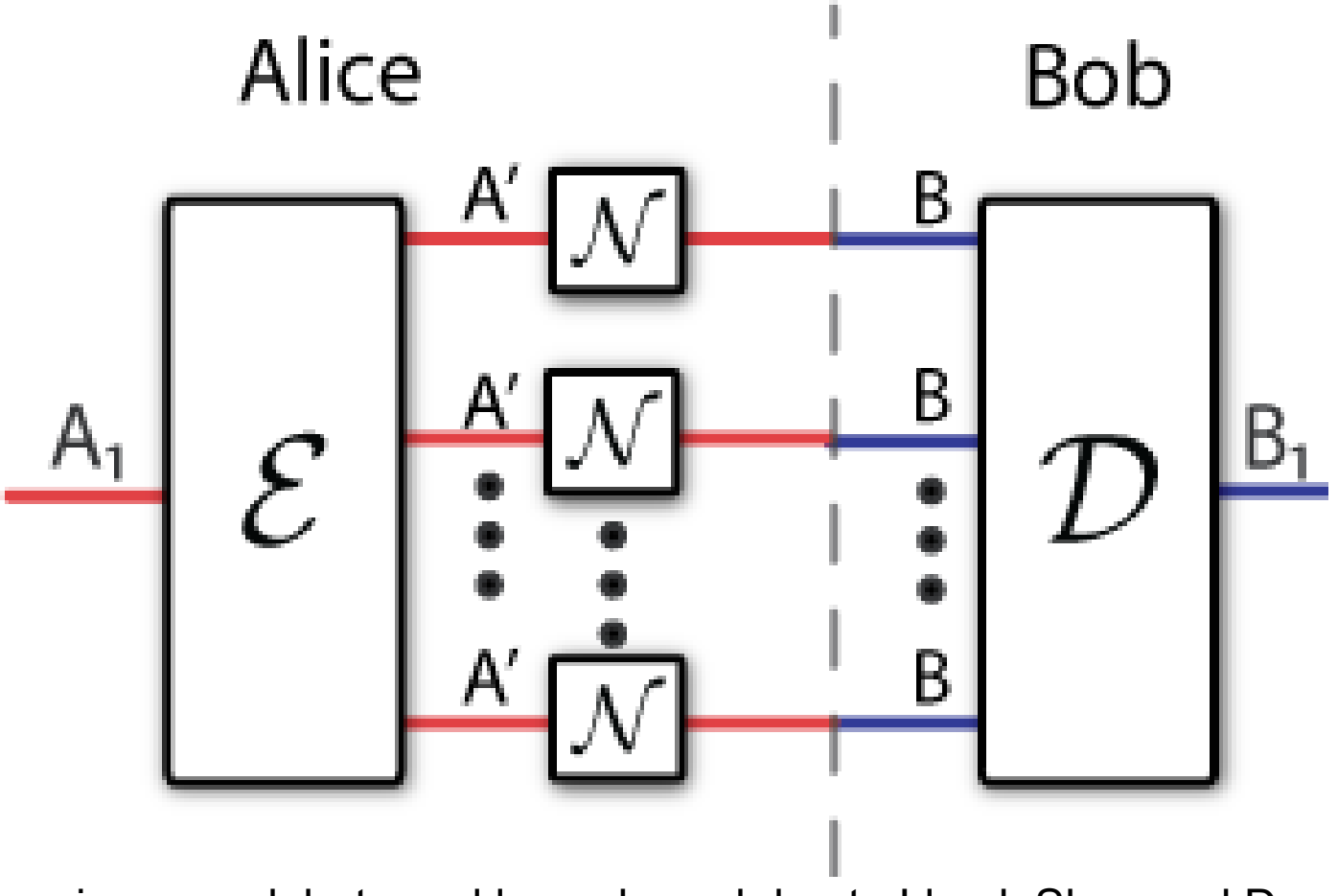
Not known in general, but good lower bound due to Holevo, Schumacher, and Westmoreland



Quantum Capacity

Fundamental question:

What is the maximum rate for error-free *quantum* comm. over a channel?



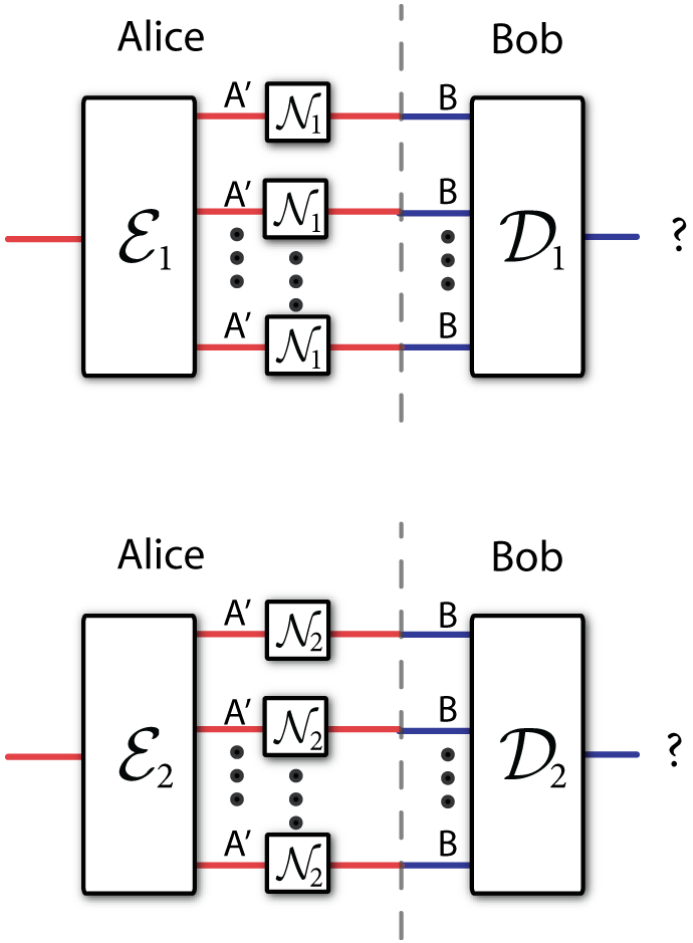
Not known in general, but good lower bound due to Lloyd, Shor, and Devetak (LSD)

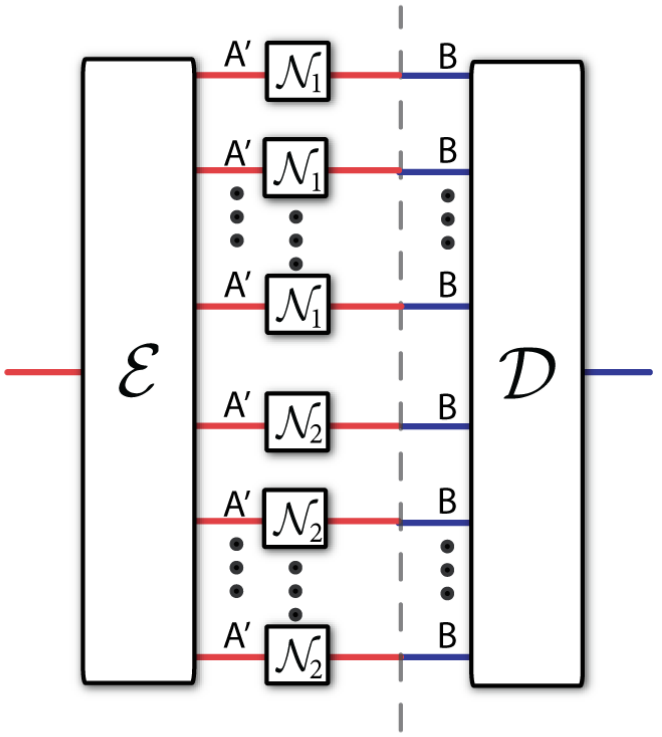


Superactivation

In fact, solving the quantum capacity problem in general will be very difficult

because 0 + 0 > 0 !





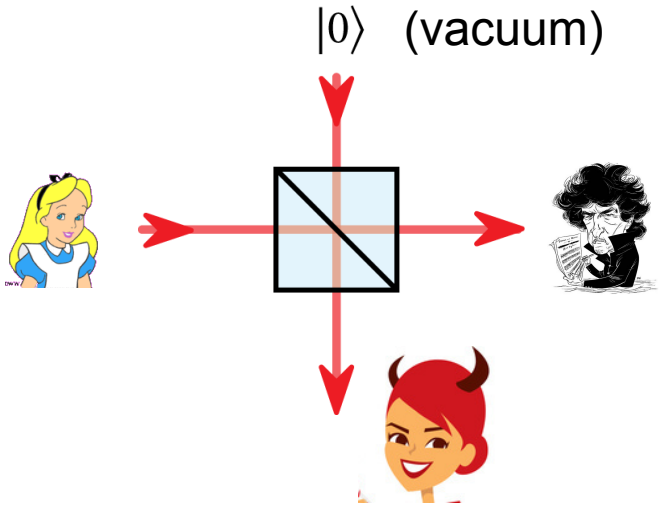
Explicit codes that exhibit this effect:
Wilde and Renes. arXiv:1201.2906

Smith and Yard, *Science* (2008)

Application to Pure-Loss Bosonic Channels

Pure-Loss Bosonic Channel

(*models fiber optic or free space transmission*)



Heisenberg input-output relation for channel:

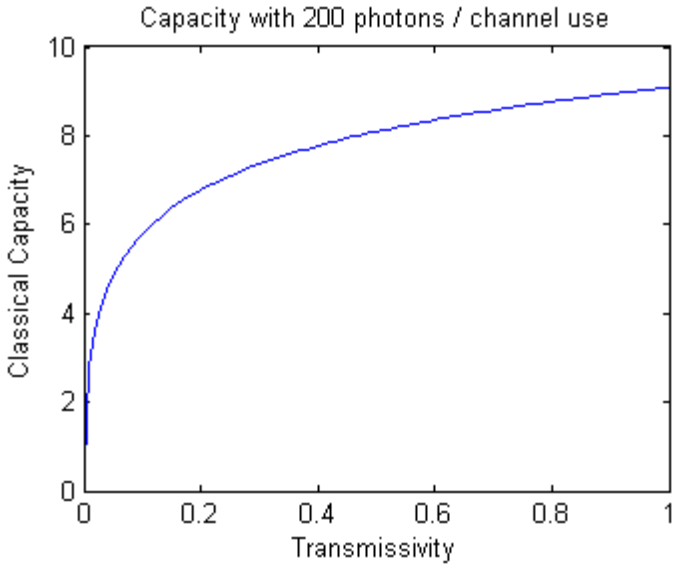
$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}$$

Weedbrook *et al*., Gaussian Quantum Information, *Reviews of Modern Physics* (2011).

Sending Classical Data over Bosonic Channels

Classical capacity of **lossy bosonic channel** is exactly

$$g(\eta N_S)$$



where η is **transmissivity** of channel,
N_s is the **mean input photon number**,
and $g(x) = (x+1)\log(x+1) - x \log x$
is the **entropy** of a **thermal state**
with photon number x

Can **achieve** this capacity by selecting **coherent states** randomly according to a complex, isotropic Gaussian prior with variance N_s

Giovannetti *et al.*, *Physical Review Letters* 92, 027902 (2004)

Codebook for pure-loss bosonic channel

Classical capacity result implies that it **suffices** to consider pure-state CQ channel:

$$\alpha \rightarrow \left|\sqrt{\eta}\alpha\right\rangle \qquad \text{(WLOG, set } \eta = 1\text{)}$$

And choose codewords **randomly** according to

$$p_{N_S}(\alpha) \equiv (1/\pi N_S)\exp\left\{-|\alpha|^2/N_S\right\}$$

Codebook is then of the form: $\left\{\left|\alpha^n(m)\right\rangle\right\}_m$

where $\left|\alpha^n(m)\right\rangle \equiv \left|\alpha_1(m)\right\rangle \otimes \cdots \otimes \left|\alpha_n(m)\right\rangle$

$$|\alpha\rangle \equiv D(\alpha)|0\rangle \equiv \exp\left\{\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right\}|0\rangle = e^{-\frac{|\alpha|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

Giovannetti *et al*., *Physical Review Letters* 92, 027902 (2004)

Sequential Decoding for pure-loss channel

Sequential decoding measurements are

$$\left\{ \left|\alpha^n\left(m\right)\right\rangle \left\langle \alpha^n\left(m\right)\right|,\ I^{\otimes n} - \left|\alpha^n\left(m\right)\right\rangle \left\langle \alpha^n\left(m\right)\right| \right\}$$

Observing that

$$\left|\alpha^n\left(m\right)\right\rangle = D\left(\alpha_1\left(m\right)\right) \otimes \cdots \otimes D\left(\alpha_n\left(m\right)\right) \left|0\right\rangle^{\otimes n}$$

1) Displace the *n*-mode codeword state by

$$D\left(-\alpha_1\left(m\right)\right) \otimes \cdots \otimes D\left(-\alpha_n\left(m\right)\right)$$

2) Perform a "vacuum-or-not" measurement:

$$\left\{ \left|0\right\rangle \left\langle 0\right|^{\otimes n},\ \ I^{\otimes n} - \left|0\right\rangle \left\langle 0\right|^{\otimes n} \right\}$$

3) If "NOT VAC," displace back:

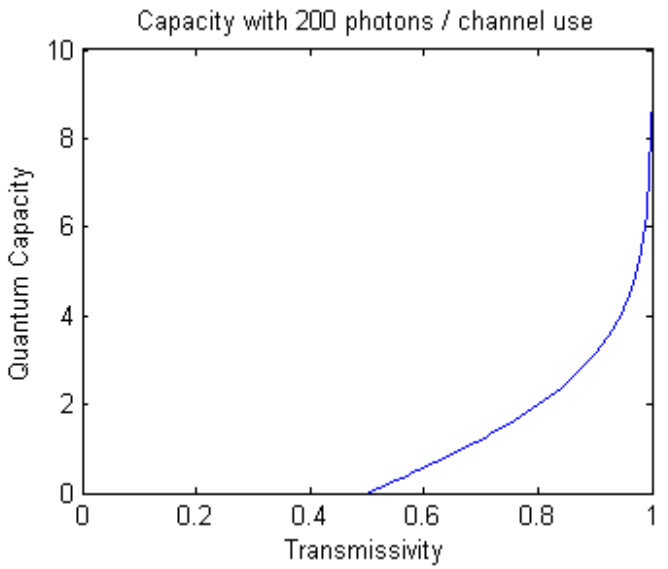
$$D\left(\alpha_1\left(m\right)\right) \otimes \cdots \otimes D\left(\alpha_n\left(m\right)\right)$$

Guha, Tan, Wilde. arXiv:1202.0518

Sending Quantum Data over Bosonic Channels

Quantum capacity of lossy bosonic channel is

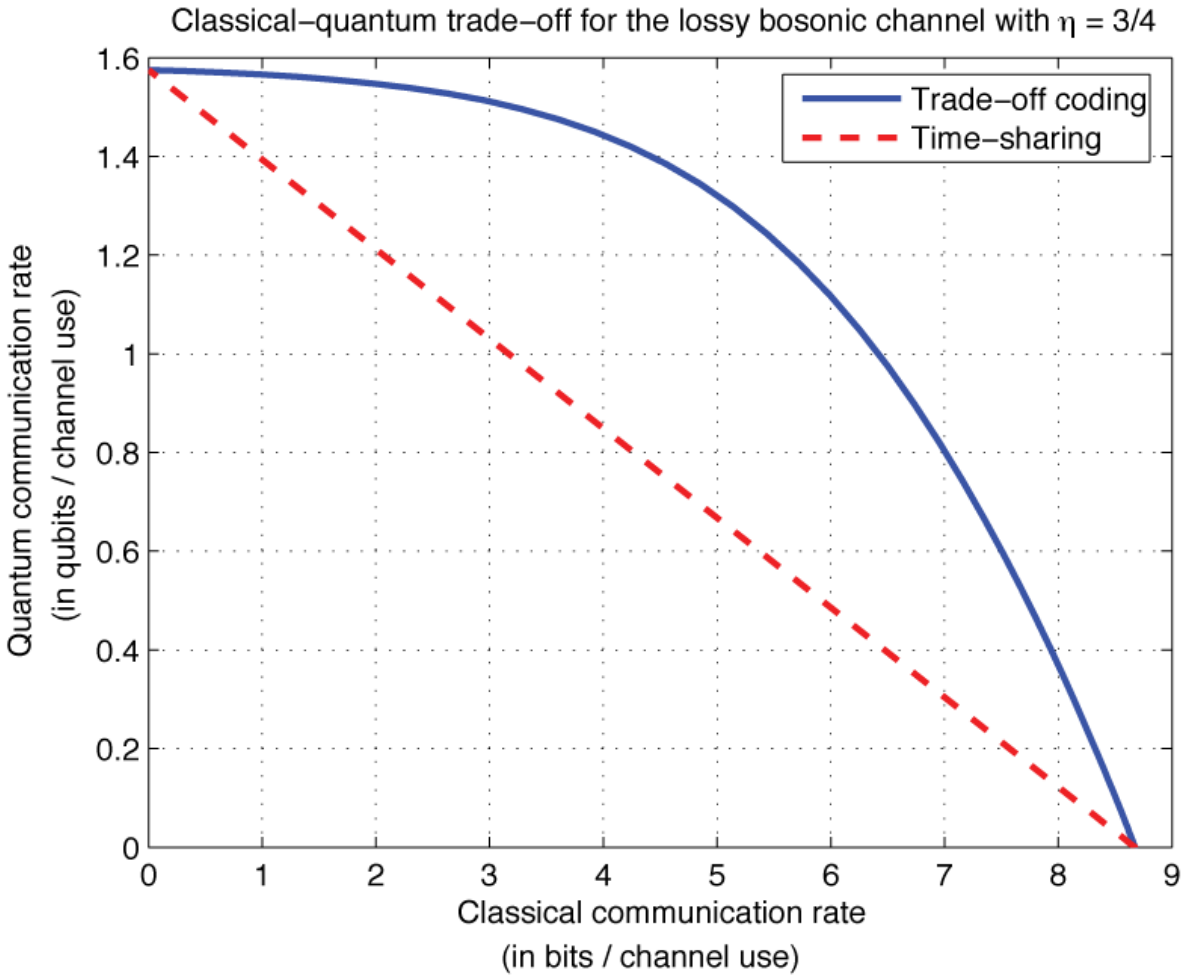
$$g(\eta N_S) - g((1-\eta)N_S)$$



An **achievable rate** is the *difference* of Bob and Eve's entropy

Holevo and Werner, *Physical Review A* 63, 032312 (2001)
Wolf *et al*., *Physical Review Letters* 98, 130501 (2007)
Guha *et al*., ISIT 2008, arXiv:0801.0841

Trade-off Coding for Bosonic Channels

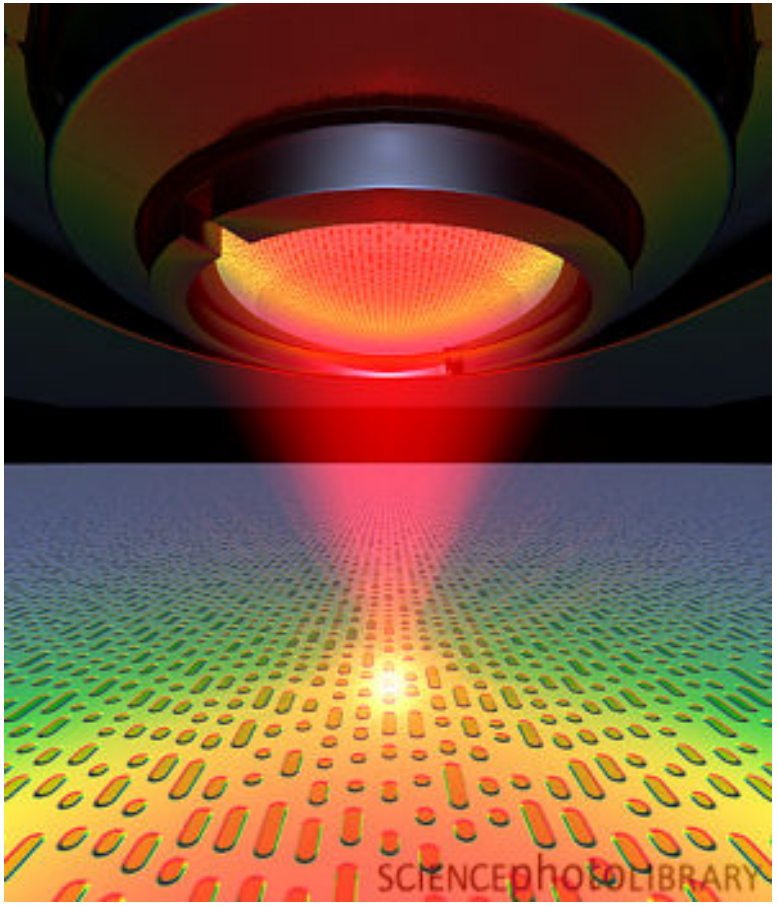


Trade-off is *so strong* for **bosonic channels**
that it would be **silly** not to use such a strategy

Wilde, Hayden, Guha. Physical Review Letters 108, 140501 (2012). arXiv:1105.0119

Quantum Reading

Idea: Use **quantum light** to improve performance of reading of a digital memory



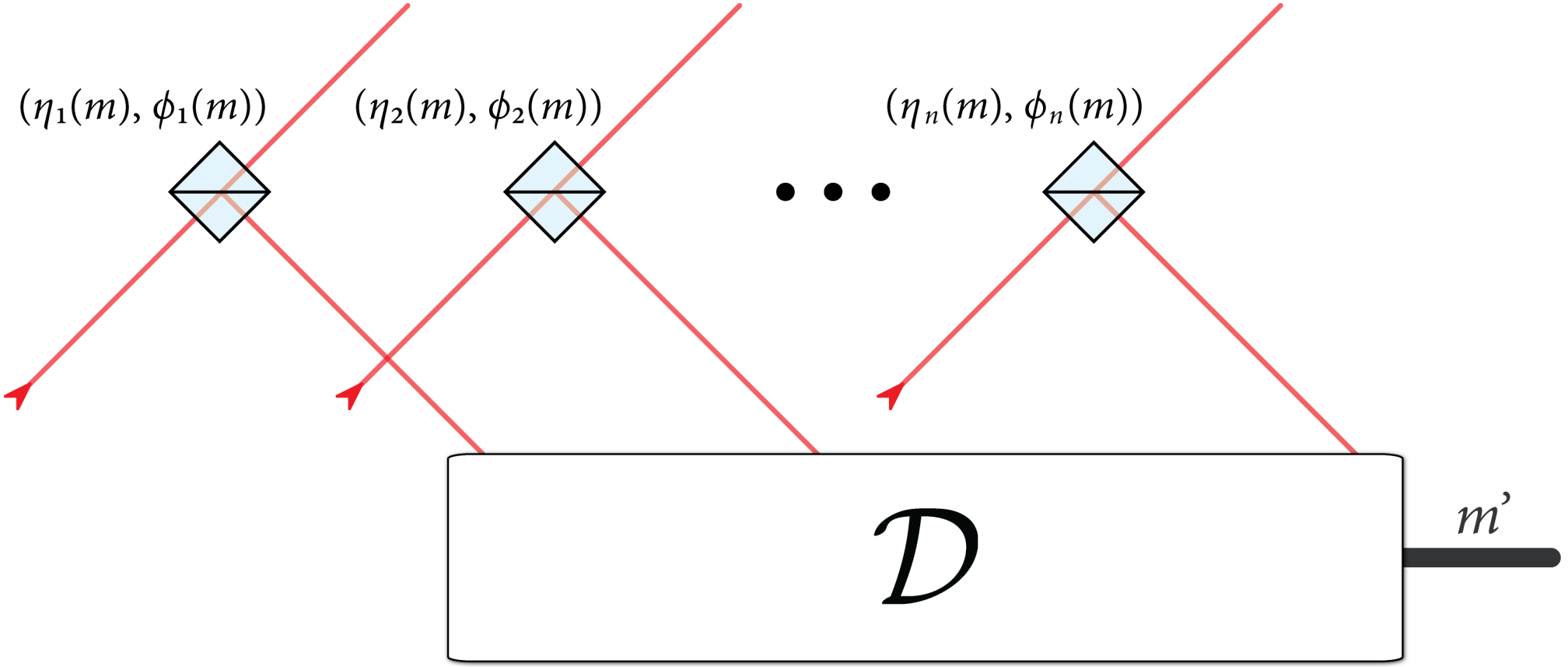
In a **DVD** or **CD**, information is encoded into "pits" etched onto the disc.

(*"pit" is 1 and "absence of pit" is 0*)

Model the information encoded onto a DVD as beamsplitters with certain reflectivity and phase

S. Pirandola, "Quantum reading of a classical digital memory," Physical Review Letters, vol. 106, p. 090504, March 2011

General Model for Quantum Reading



1) Irradiate memory cells with some quantum state of light with mean photon number N_s (*the same state for all cells*)

2) Information encoded into memory cells as

$$\hat{b}_i = \exp\{\mathrm{i}\phi_i\}\sqrt{\eta_i}\hat{a}_i + \sqrt{1-\eta_i}\hat{e}_i$$

3) Perform a collective measurement to recover classical message *m*

Capacity of Quantum Reading

If mean photon number of transmitter is N_s

and we do **not** allow for **retaining idler modes** at the transmitter, then the **capacity of quantum reading** is just

$$g(N_S)$$

Follows from **subadditivity of entropy** and that a thermal state of mean photon number N_s maximizes the entropy

If we allow for retaining idler modes, then the capacity is unknown

Sequential decoding strategy can work here as well

Guha, Tan, Wilde. arXiv:1202.0518

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

Where to learn more:

Quantum Information Theory by Mark M. Wilde

to be published by **Cambridge University Press** in late 2012

When does quantum reading beat classical?

Quantum strategy for reading always outperforms
a classical strategy for any photon number

At low photon number, classical strategy
gets close to quantum strategy using
“M-ary phase shift keying” of coherent states
(though, to achieve a given error rate,
quantum strategy requires fewer memory cells)

At high photon number, quantum strategy
significantly outperforms classical strategy

Guha and Shapiro, In preparation (2012).