Explicit Receivers for Optical Communication and Quantum Reading

Mark M. Wilde

School of Computer Science,
McGill University

Joint work with **Saikat Guha** and **Si-Hui Tan**

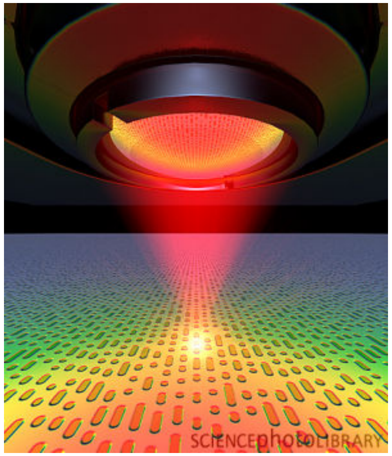
arXiv:1202.0518

Nagoya Winter Workshop 2012,
Nagoya, Japan, February 14, 2012

Overview

- Sequential decoding for a pure-state classical-quantum channel
- Sequential decoding for a pure-loss bosonic channel

- Sequential decoding in quantum reading

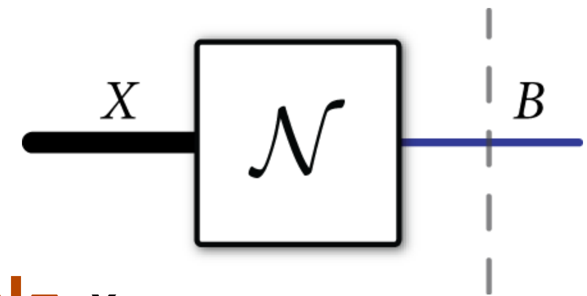


- Further applications of sequential decoding

Simple Model for a Quantum Channel

A pure-state, classical-quantum channel:

$$x \longrightarrow |\psi_x\rangle$$



Upon inputting **classical variable** *x*,
the channel prepares a **pure quantum state** at the output

For example, channel could be

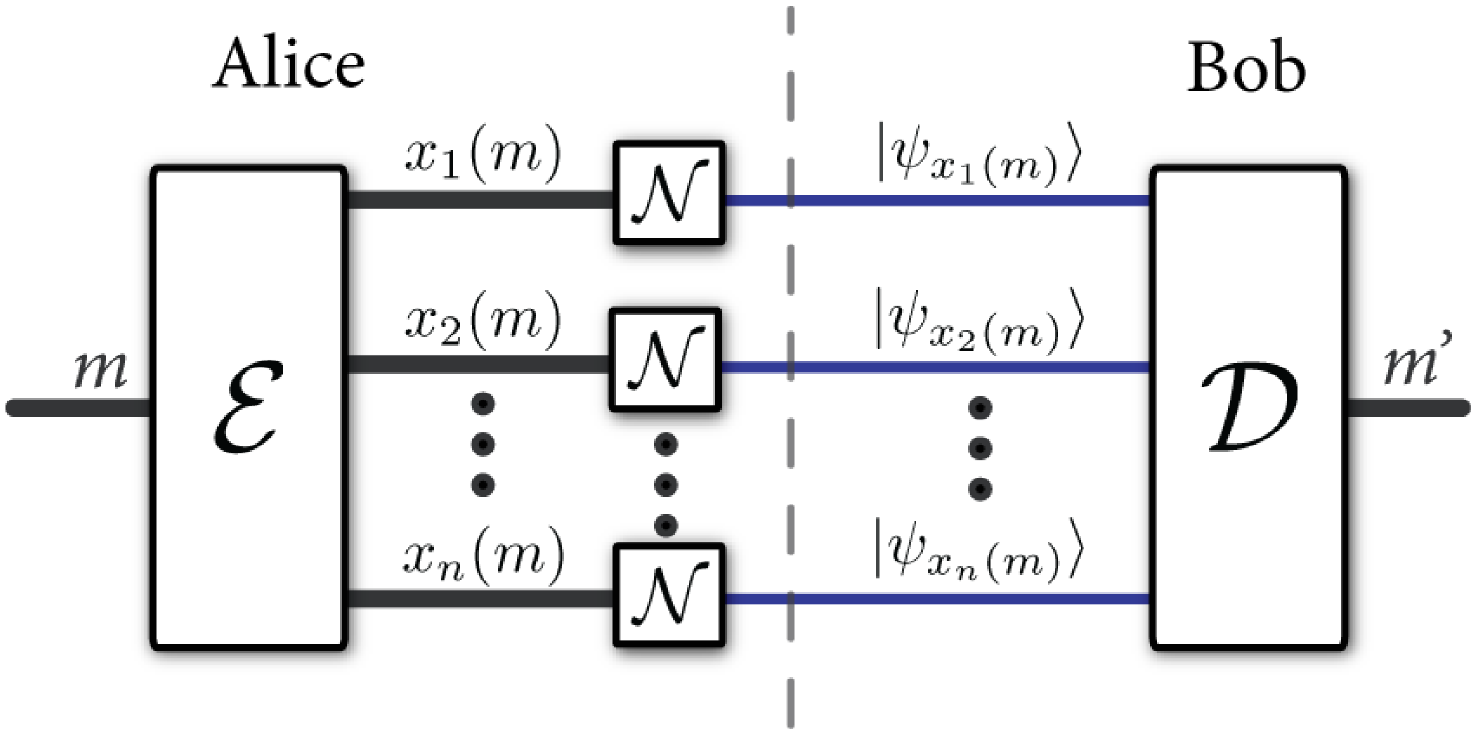
$$0 \rightarrow |0\rangle$$

$$1 \rightarrow |+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Inputting *codewords* 00 and 11 and performing **collective measurement** at receiver would outperform inputting 0 and 1 and doing "single-symbol" measurements

Classical Codes for a Quantum Channel

Use the channel *n* times:



Encoder just maps classical message *m* to a **classical codeword**:

$$x^n(m) \equiv x_1(m) \cdots x_n(m) \rightarrow |\psi_{x^n(m)}\rangle \equiv |\psi_{x_1(m)}\rangle \otimes \cdots \otimes |\psi_{x_n(m)}\rangle$$

Decoder performs a **collective measurement** to determine transmitted classical signal

How to build the decoding measurement with **optical devices**?

Achievable Rates

Two measures of performance:

1) The **rate R** of a code is equal to **bits per channel use**:

$$R \equiv \frac{\log_2 |\mathcal{M}|}{n}$$

2) The **probability of error** P_e is equal to

$$\Pr\{M' \neq M\}$$

In Shannon theory, we demand that $P_e \to 0$ as $n \to \infty$ at a fixed rate R

(*so that rate R becomes only performance measure*)

Define a rate R to be **achievable** if there exists a sequence of codes of rate R such that $P_e \to 0$ as $n \to \infty$.

Capacity of a Pure-State CQ Channel

Definition: The capacity is the **supremum** of all achievable rates.

Theorem: The capacity of a pure-state CQ channel is equal to

$$\max_{p(x)} H\left(\sum_x p(x)|\psi_x\rangle\langle\psi_x|\right)$$

where $$H(\rho) \equiv -\text{Tr}\{\rho \log_2 \rho\}$$

NOTE: This is **NOT** the capacity for the most general definition of a quantum channel as a Kraus map.

HJSWW96 proved the above theorem by employing the so-called **"square-root measurement"**

We will show that **sequential decoding** works just as well...

P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, W. Wootters. Phys. Rev. A 54 (1996)

Sequential Decoding

First consider **sequential decoding** for a **classical channel**.

1) Suppose the receiver obtains a sequence y^n as the output of an IID channel $p(y|x)$

2) Sequential decoding has the receiver ask, for every codeword $x^n(m)$, "*Is $x^n(m)$ a* ***reasonable cause*** *for y^n?*"

3) Receiver declares the message to be m as soon as the answer to the above question is "Yes!"

A little more precise: The question above can be stated more formally as "Is $x^n(m)$ jointly typical with y^n?"

Cover and Thomas. Elements of Information Theory.

Quantum Sequential Decoding

Ask, "*Is it the m^{th} codeword*?", by performing the measurement

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

Receiver declares the message to be *m* as soon as the answer to the above **quantum question** is "Yes!"

Probability of correctly decoding message *m*:

$$\mathrm{Tr}\left\{ \phi_{x^n(m)} \hat{\Pi}_{m-1} \cdots \hat{\Pi}_1 \phi_{x^n(m)} \hat{\Pi}_1 \cdots \hat{\Pi}_{m-1} \phi_{x^n(m)} \right\}$$

where

$$\phi_{x^n(m)} \equiv \left| \phi_{x^n(m)} \right\rangle \left\langle \phi_{x^n(m)} \right|,$$

$$\hat{\Pi}_i \equiv I^{\otimes n} - \left| \phi_{x^n(i)} \right\rangle \left\langle \phi_{x^n(i)} \right|.$$

Giovannetti, Lloyd, and Maccone. PRA 2012. arXiv:1012.0386, Sen. arXiv:1109.0802

Quantum Sequential Decoding (ctd.)

Analyze instead average error probability

$$1 - \mathop{\mathbb{E}}_{X^n,M} \mathrm{Tr}\left\{\phi_{X^n(M)} \hat{\Pi}_{M-1} \cdots \hat{\Pi}_1 \phi_{X^n(M)} \hat{\Pi}_1 \cdots \hat{\Pi}_{M-1}\right\}.$$

under the assumptions that

1) Alice chooses message *m* uniformly at random

2) Codewords $x^n(m)$ are selected IID according to $p(x)$ and independent of the message *m* to be sent

Can show that the above error is approximately equal to

$$\mathbb{E}\mathrm{Tr}\left\{\Pi\phi_{X^n(M)}\Pi\right\} - \mathbb{E}\mathrm{Tr}\left\{\phi_{X^n(M)} \hat{\Pi}_{M-1} \cdots \hat{\Pi}_1 \Pi \phi_{X^n(M)} \Pi \hat{\Pi}_1 \cdots \hat{\Pi}_{M-1} \phi_{X^n(M)}\right\}$$

where Π is the typical projector for the average state $\rho \equiv \sum_x p(x) |\psi_x\rangle\langle\psi_x|$

Sen. ArXiv:1109.0802. Guha, Tan, Wilde. arXiv:1202.0518

Key Tool: Noncommutative Union Bound

Holds for a subnormalized state ρ and projectors Π_1, …, Π_N:

$$1 - \mathrm{Tr}\{\Pi_N \cdots \Pi_1 \rho \Pi_1 \cdots \Pi_N\} \leq 2\sqrt{\sum_{i=1}^{N} \mathrm{Tr}\{(I - \Pi_i)\rho\}}$$

Consider similarity with union bound:

$$\Pr\{(A_1 \cap \cdots \cap A_N)^c\} = \Pr\{A_1^c \cup \cdots \cup A_N^c\} \leq \sum_{i=1}^{N} \Pr\{A_i^c\}$$

Should find **widespread application** in quantum info. theory

P. Sen, "Achieving the Han-Kobayashi inner bound ...", arXiv:1109.0802

Error Analysis

Analyze **error probability**:

$$\mathbb{E}\mathrm{Tr}\left\{\Pi\phi_{X^n(M)}\Pi\right\} - \mathbb{E}\mathrm{Tr}\left\{\phi_{X^n(M)}\hat{\Pi}_{M-1}\cdots\hat{\Pi}_1\Pi\phi_{X^n(M)}\Pi\hat{\Pi}_1\cdots\hat{\Pi}_{M-1}\phi_{X^n(M)}\right\}$$

Upper bound this using the **noncommutative union bound**:

$$1 - \mathrm{Tr}\{\Pi_N\cdots\Pi_1\rho\Pi_1\cdots\Pi_N\} \leq 2\sqrt{\sum_{i=1}^{N}\mathrm{Tr}\{(I-\Pi_i)\rho\}}$$

1) Probability that correct codeword does **not "click"**:

$$\mathbb{E}\mathrm{Tr}\left\{(I^{\otimes n} - \phi_{X^n(M)})\Pi\phi_{X^n(M)}\Pi\right\} \leq \epsilon$$

2) Probability that **some other codeword "clicks"**:

$$\mathbb{E}\sum_{i=1}^{M-1}\mathrm{Tr}\left\{\phi_{X^n(i)}\Pi\phi_{X^n(M)}\Pi\right\} \leq 2^{-n[H(\rho)-\delta]}\ |\mathcal{M}|$$

Result: Entropy Rate is Achievable

The **error probability**

$$\mathbb{E}\mathrm{Tr}\left\{\Pi\phi_{X^n(M)}\Pi\right\} - \mathbb{E}\mathrm{Tr}\left\{\phi_{X^n(M)}\hat{\Pi}_{M-1}\cdots\hat{\Pi}_1\Pi\phi_{X^n(M)}\Pi\hat{\Pi}_1\cdots\hat{\Pi}_{M-1}\phi_{X^n(M)}\right\}$$

has the following upper bound:

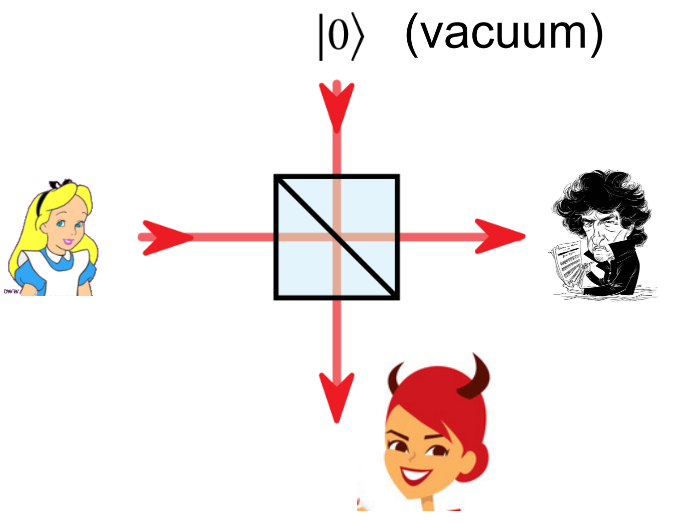
$$\epsilon + 2^{-n[H(\rho)-\delta]}\ |\mathcal{M}|$$

As long as rate $R \approx H(\rho)$, conclude there exists a particular sequence of codes with $P_e \to 0$ as $n \to \infty$

Application to Pure-Loss Bosonic Channels

Pure-Loss Bosonic Channel

(*models fiber optic or free space transmission*)



Heisenberg input-output relation for channel:

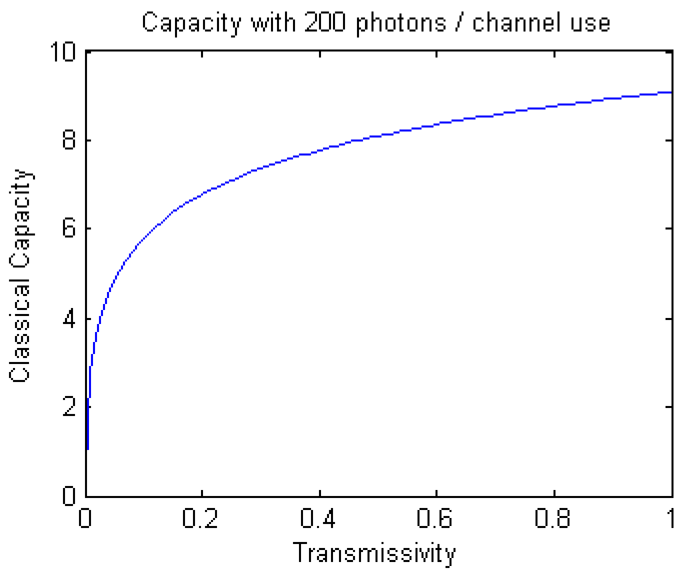
$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}$$

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:

$$\alpha \to \left|\sqrt{\eta}\alpha\right\rangle$$ (WLOG, set η = 1)

And choose codewords **randomly** according to

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

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

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

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

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

Sequential Decoding for pure-loss channel

Sequential decoding measurements are

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

Observing that

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

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

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

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

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

3) If "NOT VAC," displace back:

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

Guha, Tan, Wilde. arXiv:1202.0518

Sequential Decoding for pure-loss channel

Result: Sequential decoding achieves the capacity of the pure-loss channel

Observation: This scheme also achieves the **private capacity** of the pure-loss channel:

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

How? Pick $2^{ng(\eta N_S)}$ coherent-state codewords

Put them into $2^{n[g(\eta N_S)-g((1-\eta)N_S)]}$ groups,

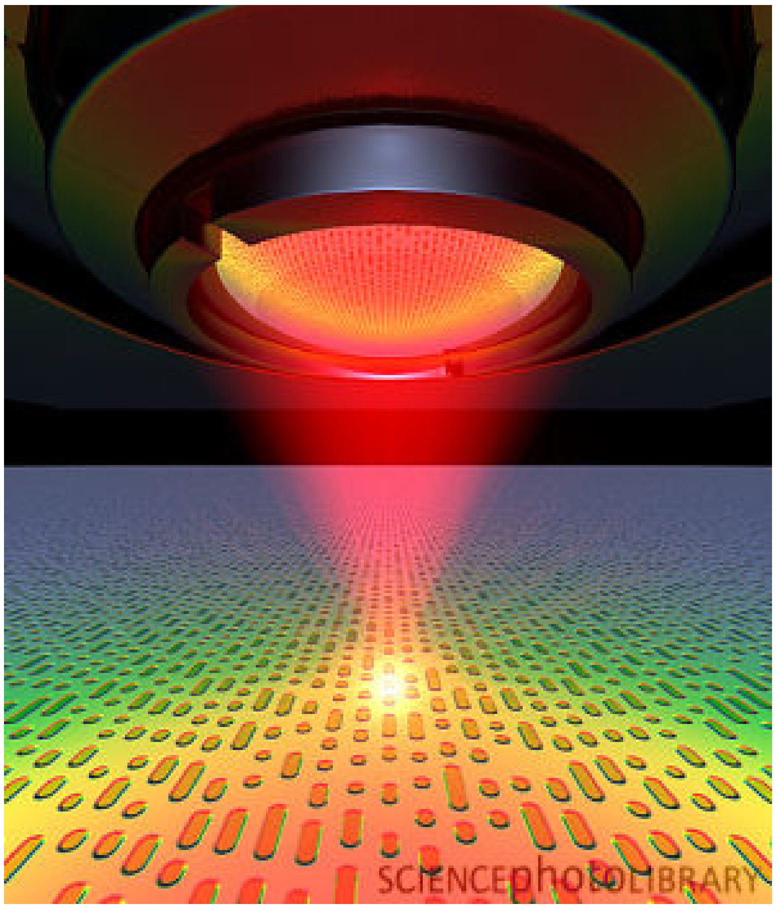
each labeled by *m* and consisting of $2^{ng((1-\eta)N_S)}$ codewords

To send message *m*, pick a codeword from m^{th} group **uniformly at random** and transmit

Guha, Tan, Wilde. arXiv:1202.0518

Quantum Reading

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



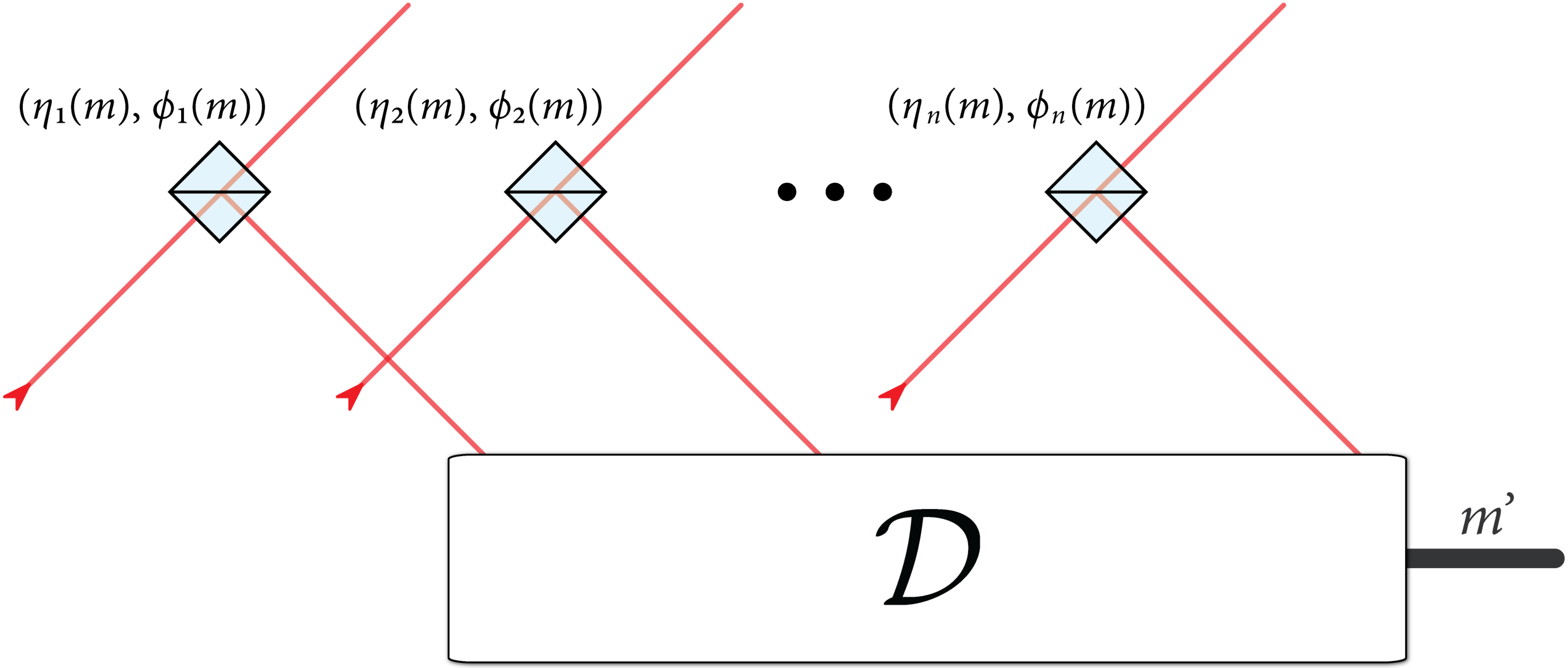
In a **DVD** or **CD**, information is encoded into "pits" etched onto the disc.

(*"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

Achieving Capacity of Quantum Reading

How to achieve capacity of quantum reading?

1) Put transmitter in the state:

$$\sum_{n=0}^{\infty} \sqrt{\frac{N_S^n}{(N_S+1)^{n+1}}} |n\rangle$$

(Avg. photon number is N_S)

2) For codewords, choose $\eta_i = 1$ and phases φ_i randomly

Avg. state of ensemble is then a **dephased version** of the above state:

$$\sum_{n=0}^{\infty} \frac{N_S^n}{(N_S+1)^{n+1}} |n\rangle\langle n|$$

Achieves capacity of $g(N_S)$!

Though, how to implement strategy?

Guha, Dutton, Nair, Shapiro, Yen. In preparation (2012)

Sequential Decoding for Quantum Reading

Since we don't know how to implement the previous strategy, analyze a strategy where transmitter retains an idler mode.

1) Put transmitter in the state:

$$\sum_{n=0}^{\infty} \sqrt{\frac{N_S^n}{(N_S+1)^{n+1}}} |n\rangle |n\rangle$$

(Avg. photon number of one mode is N_S)

2) For codewords, again choose $\eta_i = 1$ and phases φ_i randomly

Avg. state of ensemble is then a **dephased version** of the above state:

$$\sum_{n=0}^{\infty} \frac{N_S^n}{(N_S+1)^{n+1}} |n\rangle\langle n| \otimes |n\rangle\langle n|$$

Achieves rate of $g(N_S)$!

Don't know whether this is optimal, but we know how to implement receiver

Guha, Tan, Wilde. arXiv:1202.0518

Sequential Decoding for Quantum Reading

Consider that phase-encoded light is a tensor product of the states

$$\left(P\left(\theta_i\left(m\right)\right) \otimes I\right) S\left(r\right) \left|0\right\rangle^{\otimes 2}$$

where P is a **phase-shifter** and $S(r)$ is a **two-mode squeezer**

We can now see sequential decoding strategy for the m^{th} round:

1) Phase shift the first mode of the i^{th} pair by $-\theta_i(m)$
2) Apply an unsqueezing operator $[S(r)]^{-1}$ to every pair.
3) Perform a “vacuum-or-not” measurement:

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

4) If “NOT VAC”, squeeze back and phase-shift back

Guha, Tan, Wilde. arXiv:1202.0518

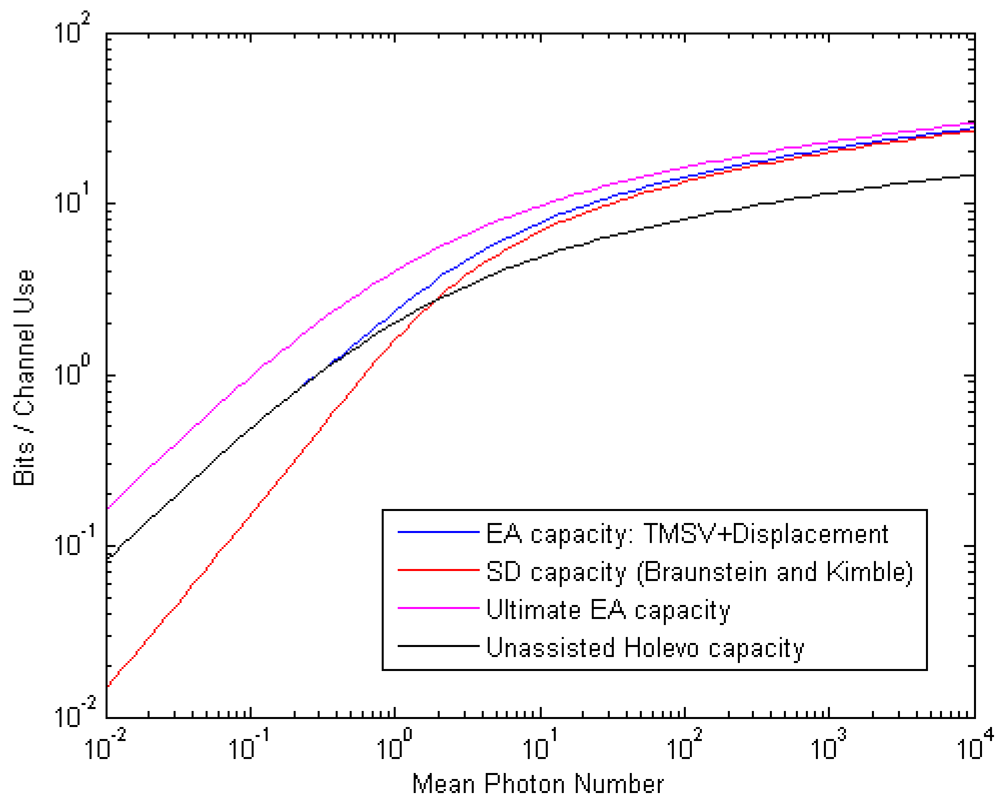
Sequential Decoding in EA comm.

Consider entanglement-assisted communication over a noiseless bosonic channel

(CV dense coding: Braunstein and Kimble 1999)

Use a two-mode squeezed state and displacement operators for encoding

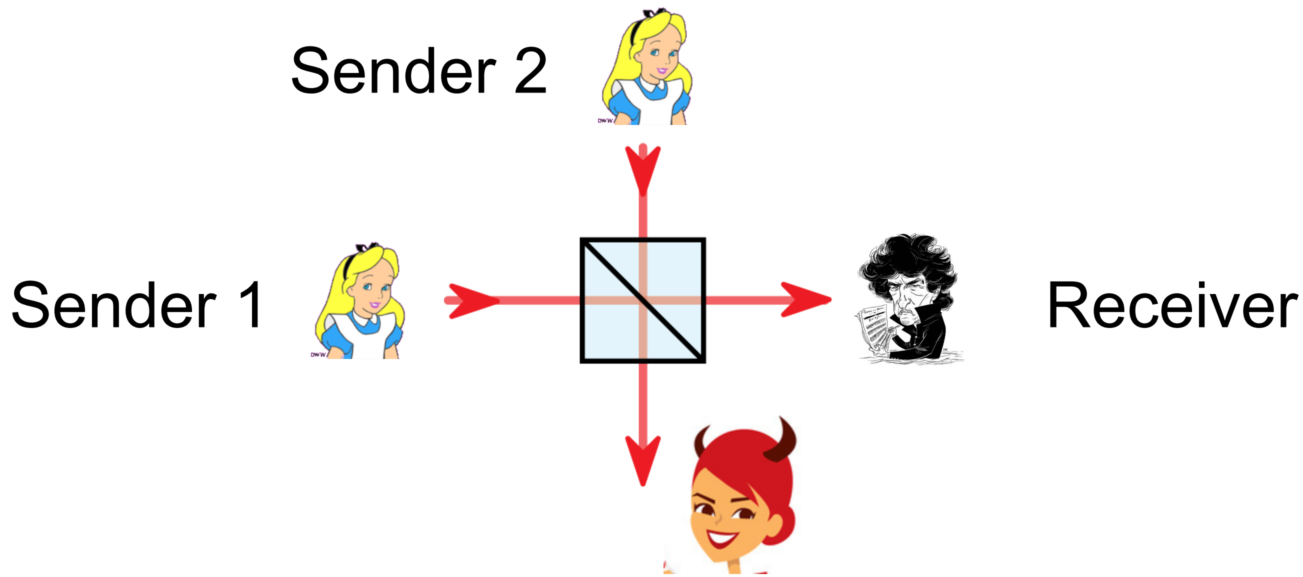
Sequential decoding works similarly as before
(*inverse displace*, *unsqueeze*, “VAC-OR-NOT”, *resqueeze*, *displace*)



Guha, Wilde. Unpublished Emails (2012)

Sequential Decoding in Multiple Access

Simple model of a "pure-interference" bosonic multiple access channel:



Coherent-state inputs $|\alpha\rangle$ and $|\beta\rangle$ lead to output

$$|\sqrt{\eta}\alpha + \sqrt{1-\eta}\beta\rangle$$

Sequential decoding works by testing all **pairs of codewords**

Can achieve capacity of "coherent-state MAC" in certain circumstances

Yen, Shapiro. PRA (2005). *Guha, Wilde. Unpublished Emails (2012)*

Conclusion and Current Work

Quantum sequential decoding leads to a "practical" receiver
("practical" in the sense that we can implement)

It is **impractical** because it requires
an exponential number of measurements

Open question: How to reduce the number of measurements?

Polar codes might be helpful here (arXiv:1202.0533)

Could any of the ideas here be helpful for
communicating quantum data?