Bosonic Dirty Paper Coding

Uzi Pereg

Institute for Communications Engineering
Technical University of Munich (TUM)

ISIT 2021

Motivation

- Optical communication forms the backbone of the Internet

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

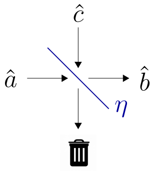
Motivation

- Optical communication forms the backbone of the Internet
- The bosonic (Gaussian) channel is a simple quantum-mechanical model for optical communication over free space or optical fibers

Bosonic Model

For a single-mode lossy bosonic channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is

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



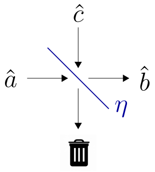
Bosonic Model

For a single-mode lossy bosonic channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is

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

where

- the noise mode $\hat{e}$ is in a thermal Gaussian state



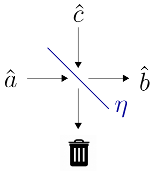
Bosonic Model

For a single-mode lossy bosonic channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is

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

where

- the noise mode $\hat{e}$ is in a thermal Gaussian state
- the transmissivity $\eta \in [0,1]$ depends on the absorption length of the optical fiber



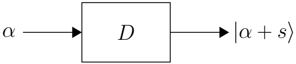
Bosonic Model (Cont.)

- The transmitter employs a coherent state protocol.
- A coherent state $|\alpha\rangle$ corresponds to an oscillation of the electromagnetic field,

$$|\alpha\rangle = D(\alpha)|0\rangle$$
$$D(\alpha) \equiv \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a})$$

Main Contributions

We consider the single-mode lossy bosonic channel with a coherent-state protocol and non-ideal modulation:



- Applications
  - classical interference in the transmission equipment
  - watermarking with a quantum embedding

Main Contributions (Cont.)

- Homodyne and heterodyne detection
- Joint detection
  - DPC lower bound
  - MMSE coefficient is sub-optimal

Background

In the Gel'fand-Pinsker model,

- the channel depends on a random parameter, $S \sim p_S$, while the transmitter has channel side information (CSI).
- Applications:
  - cognitive radio in wireless systems
  - memory storage
  - digital watermarking

Background (Cont.)

Theorem (GP, 1980; Heegard and El Gamal, 1983)

The capacity of a random-parameter classical channel $W_{Y|X,S}$ with CSI at the transmitter is given by

$$C(W) = \max_{p_{U,X|S}} (I(U;Y) - I(U;S))$$

where $U \multimap (X,S) \multimap Y$ form a Markov chain.

Background: Dirty Paper

Gaussian Channel with Additive Interference

Consider

$$Y = X + S + Z$$

with Gaussian noise $Z \sim \mathcal{N}_{\mathbb{R}}(0, \sigma^2)$ and interference S.

Background: Dirty Paper

Gaussian Channel with Additive Interference

Consider

$$Y = X + S + Z$$

with Gaussian noise $Z \sim \mathcal{N}_{\mathbb{R}}(0, \sigma^2)$ and interference S.

Theorem (Costa, 1983)

The capacity of the Gaussian channel with additive interference and CSI at the transmitter is the same as if there is no interference, i.e. $C(W) = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$.

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Background: Dirty Paper (Cont.)

$$Y = X + S + Z$$

Theorem (Costa, 1983)

The capacity of the Gaussian channel with additive interference and CSI at the transmitter is the same as if there is no interference, i.e. $C(W) = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$.

- It is not obvious. The trivial strategy is to send $X = U - S$ such that $U \perp S$, resulting in an intereference-free output, $Y = U + Z$. However, this strategy would waste transmission power.

Q.Link.X Verbundprojekt Quanten-Link-Erweiterung

Background: Dirty Paper (Cont.)

Dirty Paper Coding (DPC) Strategy

Set

$$U = X + tS\,,$$

where $X \sim \mathcal{N}_{\mathbb{R}}(0, P)$, such that X is statistically independent of S.

Background: Dirty Paper (Cont.)

Dirty Paper Coding (DPC) Strategy

Set

$$U = X + tS\,,$$

where $X \sim \mathcal{N}_{\mathbb{R}}(0, P)$, such that X is statistically independent of S.

- The optimal choice for t turns out to be the same as that of the minimum mean-square error (MMSE) estimator $\widehat{X} = t(X + Z)$, i.e.

$$t = \frac{P}{P + \sigma_Z^2}.$$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Background: Dirty Paper (Cont.)

Dirty Paper Coding (DPC) Strategy

Set

$$U = X + tS\,,$$

where $X \sim \mathcal{N}_{\mathbb{R}}(0, P)$, such that X is statistically independent of S.

- The optimal choice for t turns out to be the same as that of the minimum mean-square error (MMSE) estimator $\widehat{X} = t(X + Z)$, i.e.

$$t = \frac{P}{P + \sigma_Z^2}.$$

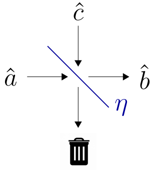
- Explicit lattice codes were proposed e.g. by [Erez and ten Brink, 2005].

Q.Link.X Verbundprojekt Quanten-Link-Erweiterung

Lossy Bosonic Channel

The channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is another mode,

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



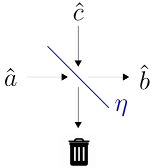
Lossy Bosonic Channel

The channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is another mode,

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

where

- the noise mode $\hat{e}$ is in a thermal state, $\tau(N_E) \equiv \int_{\mathbb{C}} d^2\alpha \frac{e^{-|\alpha|^2/2N_E}}{\pi N_E} |\alpha\rangle\langle\alpha|$



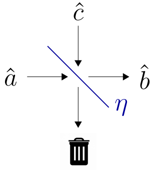
Lossy Bosonic Channel

The channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is another mode,

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

where

- the noise mode $\hat{e}$ is in a thermal state, $\tau(N_E) \equiv \int_{\mathbb{C}} d^2\alpha \frac{e^{-|\alpha|^2/2N_E}}{\pi N_E} |\alpha\rangle\langle\alpha|$
- $0 \leq \eta \leq 1$ is the transmissivity, which depends on the absorption length of the optical fiber



Bosonic Model (Cont.)

Coding with CSI

- Alice chooses $m \in \{1, 2, \ldots, \mathrm{M}\}$
  Encoding: $m \mapsto (\alpha_i(m, s_1, \ldots, s_n))_{i=1}^n$, $|\alpha_i| \leq N_A$.

Bosonic Model (Cont.)

Coding with CSI

- Alice chooses $m \in \{1, 2, \ldots, \mathrm{M}\}$
  Encoding: $m \mapsto (\alpha_i(m, s_1, \ldots, s_n))_{i=1}^n$, $|\alpha_i| \leq N_A$.
- Non-ideal modulation: $\alpha_i \longrightarrow |\alpha_i + s_i\rangle$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Bosonic Model (Cont.)

Coding with CSI

- Alice chooses $m \in \{1, 2, \ldots, \mathrm{M}\}$
  Encoding: $m \mapsto (\alpha_i(m, s_1, \ldots, s_n))_{i=1}^n$, $|\alpha_i| \leq N_A$.
- Non-ideal modulation: $\alpha_i \longrightarrow |\alpha_i + s_i\rangle$
- Bob receives the channel output
  Decoding measurement: $\rho_{B^n} \mapsto \hat{M}$

Bosonic Model (Cont.)

Coding with CSI

- Alice chooses $m \in \{1, 2, \ldots, \mathrm{M}\}$
  Encoding: $m \mapsto (\alpha_i(m, s_1, \ldots, s_n))_{i=1}^n$, $|\alpha_i| \leq N_A$.
- Non-ideal modulation: $\alpha_i \longrightarrow |\alpha_i + s_i\rangle$
- Bob receives the channel output
  Decoding measurement: $\rho_{B^n} \mapsto \hat{M}$

The coding rate is defined as $R = \frac{\log(\mathrm{M})}{n}$ [bits per transmission], and the maximal probability of error is denoted by $P_e^{(n)} = \max_m \Pr(\hat{M} \neq m | m)$. A rate $R > 0$ is called achievable if there exists a sequence of $(\lceil 2^{nR} \rceil, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$. The operational capacity $C(\mathcal{E})$ is defined as the supremum of achievable rates.

Verbundprojekt Quanten-Link-Erweiterung

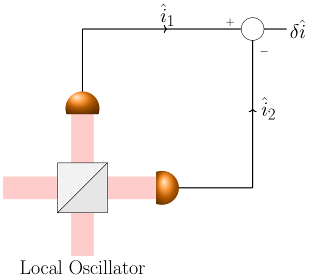
Watermarking

This can be viewed as a watermarking model with a quantum embedding.

- Given a classical host data sequence $s_1, \ldots, s_n$, Alice encodes an authentication message m into a watermark $(\alpha_i(m, s_1, \ldots, s_n))_{i=1}^n$.
- Next, she performs a quantum embedding of the watermark; she prepares a *watermarked state* $|\alpha_i + s_i\rangle$ ("stegotext"') and transmits it to Bob through the optical fiber.
- The capacity of the random-parameter bosonic channel represents the optimal rate at which the authenticator, Bob, can recover the messages with high fidelity.

Q.Link.X Verbundprojekt Quanten-Link-Erweiterung

A homodyne measurement of a quadrature observable is implemented by combining the target quantum mode with an intense local oscillator at a 50:50 beam splitter, and measuring the photocurrent difference of the outgoing modes using two photodetectors.



Homodyne Measurement (Cont.)

When homodyne detection is used with a coherent-state protocol, the resulting channel $\mathcal{E}_{\text{hom}}$ is the classical Gaussian channel

$$Y = \sqrt{\eta}(\alpha + S) + Z_{\text{hom}}$$

with a real-valued $S \sim \mathcal{N}_{\mathbb{R}}(0, N_S)$ and noise $Z_{\text{hom}} \sim \mathcal{N}_{\mathbb{R}}\left(0, \frac{1}{4}\left[2(1-\eta)N_E + 1\right]\right)$

Results: Homodyne Measurement

Using the DPC scheme, $\alpha \sim \mathcal{N}_{\mathbb{R}}(0, N_A)$ and

$$U = \alpha + t_0 S$$

such that α and S are uncorrelated, with $t_0 = \frac{\eta N_A}{\eta N_A + \text{var}(Z_{\text{hom}})}$.

The effect of the interference is thus removed, and the capacity is given by

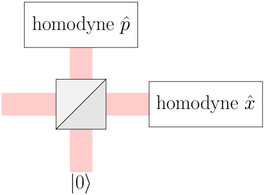
$$C(\mathcal{E}_{\text{hom}}) = \frac{1}{2} \log_2 \left(1 + \frac{4\eta N_A}{2(1-\eta)N_E + 1} \right)$$

as without interference.

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Heterodyne Measurement

In heterodyne detection, two quadratures are measured by combining the measured mode with a vacuum mode into a 50:50 beam splitter, and homodyning the quadratures of the outcome modes.



Heterodyne Measurement (Cont.)

Heterodyne detection is described by a random-parameter channel $\mathcal{E}_{\text{het}}$ with complex-valued Gaussian noise,

$$Y = \sqrt{\eta}(\alpha + S) + Z_{\text{het}}$$

with a complex-valued circularly-symmetric Gaussian random parameter $S \sim \mathcal{N}_{\mathbb{C}}(0, \frac{1}{2}N_S)$ and noise $Z_{\text{het}} \sim \mathcal{N}_{\mathbb{C}}(0, \frac{1}{2}[(1-\eta)N_E + 1])$.

Results: Heterodyne Measurement

Using the DPC scheme, $\alpha \sim \mathcal{N}_{\mathbb{C}}(0, \frac{1}{2}N_A)$ and

$$U = \alpha + t_1 S$$

such that α and S are uncorrelated, with $t_1 = \frac{\eta N_A}{\eta N_A + \mathrm{var}(Z_{\mathrm{het}})}$.

The capacity is given by

$$C(\mathcal{E}_{\mathrm{het}}) = \log\left(1 + \frac{\eta N_A}{(1-\eta)N_E + 1}\right)$$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Background

the quantum counterpart of the classical channel with additive white Gaussian noise (AWGN)

Results: Joint Detection

For joint detection, the channel does not have a classical description.

Applying the previous result in [P., 2020] for a quantum channel with random parameters, and using the DPC strategy, we obtain the lower bound $C(\mathcal{E}_{\text{joint}}) \geq \mathsf{R}_{\text{DPC}}(t)$,

$$\mathsf{R}_{\text{DPC}}(t) \equiv I(\gamma; B) - I(\gamma; S)\Big|_{\gamma=\alpha+tS}$$

DPC Lower Bound

$$
\begin{aligned}
\mathrm{R}_{\mathrm{DPC}}(t) = {} & g(\eta(N_A + N_S) + (1-\eta)N_E) \\
& - g\left(\frac{\eta(1-t)^2 N_A N_S}{N_A + t^2 N_S} + (1-\eta)N_E\right) - \log_2\left(\frac{N_A + t^2 N_S}{N_A}\right)
\end{aligned}
$$

where

$$
g(N) = \begin{cases} (N+1)\log_2(N+1) - N\log_2(N) & N > 0 \\ 0 & N = 0. \end{cases}
$$

Results: Joint Detection (Cont.)

Pure-Loss Bosonic Channel

For $N_E \to 0$,

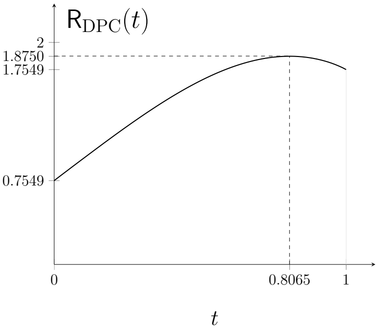
$$R_{\mathrm{DPC}}(t) = g(\eta(N_A + N_S)) - g\left(\frac{\eta(1-t)^2 N_A N_S}{N_A + t^2 N_S}\right) - \log\left(\frac{N_A + t^2 N_S}{N_A}\right)$$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Results: Joint Detection (Cont.)

For example, suppose that $N_A = N_S = 2$ and $\eta = \frac{1}{2}$. Then,

$$\mathsf{R}_{\mathsf{DPC}}(t) = g(2) - g\left(\frac{(1-t)^2}{1+t^2}\right) - \log(1+t^2)$$



Results: Joint Detection (Cont.)

Achievable Rates

- Ignoring the CSI: $\mathsf{R}_{\mathsf{DPC}}(t=0) = 0.7549$

Results: Joint Detection (Cont.)

Achievable Rates

- Ignoring the CSI: $\mathsf{R}_{\mathsf{DPC}}(t = 0) = 0.7549$
- Using DPC with MMSE coefficient $t_0 = \frac{2}{2+0} = 1$, we obtain a better rate: $\mathsf{R}_{\mathsf{DPC}}(t = 1) = 1.7549$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Results: Joint Detection (Cont.)

Achievable Rates

- Ignoring the CSI: $\mathsf{R}_{\mathsf{DPC}}(t=0) = 0.7549$
- Using DPC with MMSE coefficient $t_0 = \frac{2}{2+0} = 1$, we obtain a better rate: $\mathsf{R}_{\mathsf{DPC}}(t=1) = 1.7549$
- Optimal DPC coefficient is $t_{\max} = 0.8065 \Rightarrow \mathsf{R}_{\mathsf{DPC}}(t_{\max}) = 1.8750$

Q.Link.X
Verbundprojekt
Quanten-Link-
Erweiterung

Results: Joint Detection (Cont.)

Achievable Rates

- Ignoring the CSI: $R_{\text{DPC}}(t=0) = 0.7549$
- Using DPC with MMSE coefficient $t_0 = \frac{2}{2+0} = 1$, we obtain a better rate: $R_{\text{DPC}}(t=1) = 1.7549$
- Optimal DPC coefficient is $t_{\max} = 0.8065 \Rightarrow R_{\text{DPC}}(t_{\max}) = 1.8750$
- joint-detection capacity without interference: $g(1) = 2$.

Thank you