Photonic Quantum Information Processing
OPTI 647: Lecture 24

Saikat Guha

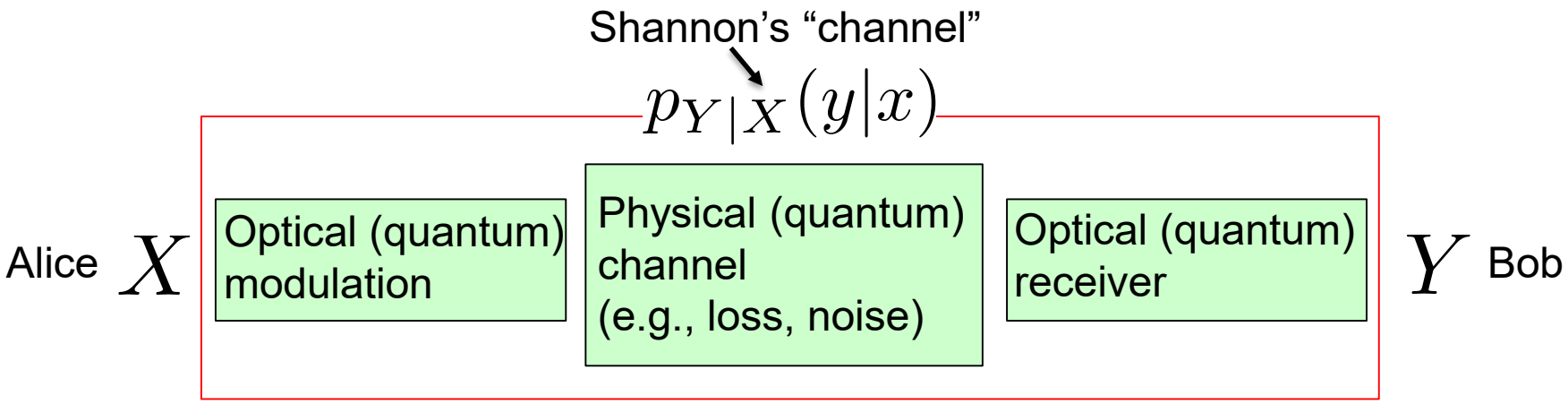
November 14, 2019
College of Optical Sciences
Meinel 523

Recap of previous lecture

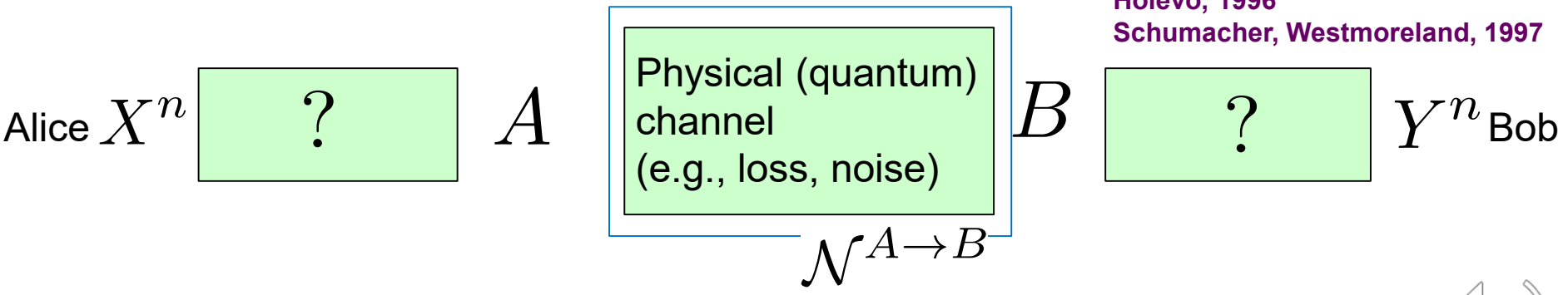
THE UNIVERSITY OF ARIZONA

- Trace distance
- Minimum probability of error state discrimination
- Multi-copy binary state discrimination and the Chernoff bound
- Examples where measurement that is optimal for single-copy state discrimination is suboptimal when presented with M copies, and vice versa
- Quantum illumination
  - 6 dB improvement in Chernoff error exponent
  - OPA receiver to achieve 3 dB improvement
  - Optimal receiver that uses squeezing and feedback

Quantum limit of classical communication



Shannon capacity C is a function of p(y|x), which depends upon the choice of transmitter modulation, and (more importantly) choice of receiver measurement. How do we calculate, and design a receiver to attain, the capacity of the underlying physical channel?

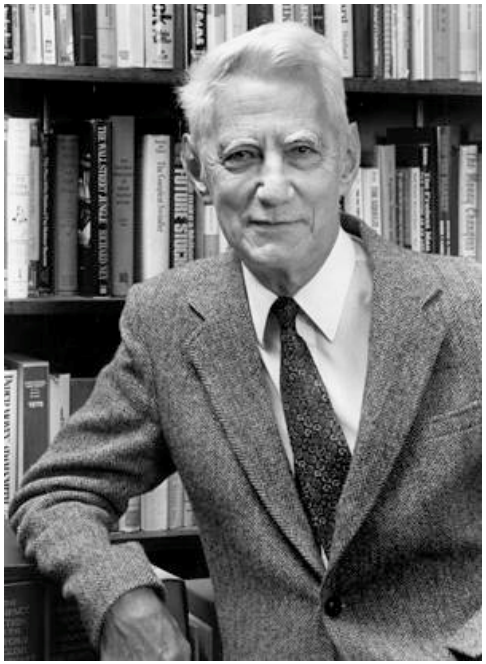


Holevo capacity, $\chi(\mathcal{N}) \geq C$

Bits per use of the *physical* channel

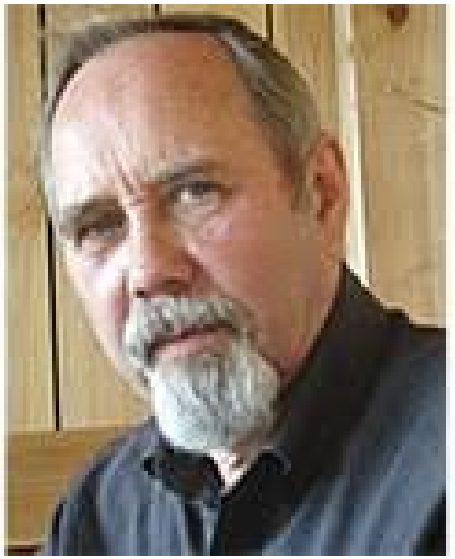
Shannon theory starts *after* detection
We will try to zoom inside that $p_{Y|X}(y|x)$

The stalwarts of Information theory



Claude Shannon
1916-2001

John von Neumann
1903 - 1957



Alexander Holevo
1943 –
Shannon Award – 2016

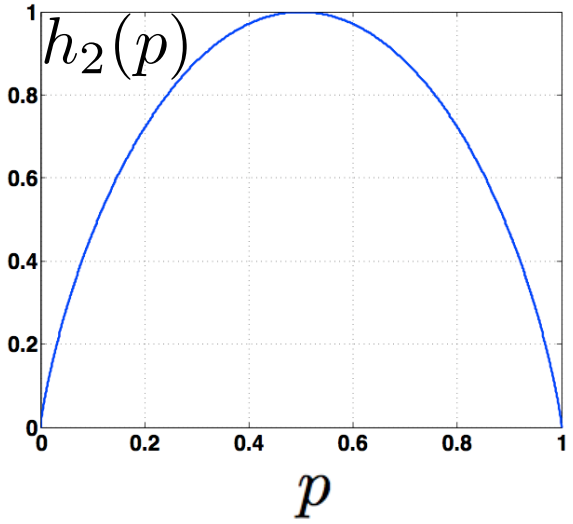
Information, entropy, compression

- Shannon entropy of a random variable X
  - Quantifies the "amount of uncertainly" in X

$$H(X) = -\sum_{x=1}^{|\mathcal{X}|} p_X(x) \log_2 p_X(x) \text{ bits}$$

- Binary entropy, $p_X(0) = p, p_X(1) = 1 - p$

$$H(X) = -p \log_2 p - (1-p) \log_2 (1-p) \triangleq h_2(p)$$



Max H(X) for given $|\mathcal{X}|$:
(uniform prior) = $\log_2(|\mathcal{X}|)$

- Data compression

X (i.i.d. source) ➡ 10010100100100011111010001
$[n$ source symbols$]$

⬇

H(X): bits per source symbol

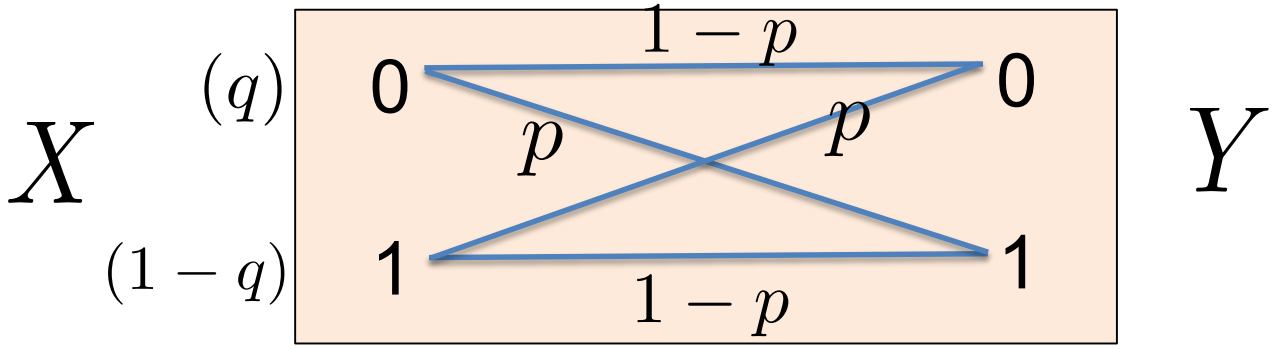
00101100101010010101
$[nH(X)$ bits$]$

Channel capacity, Binary Symmetric Channel (BSC)

THE UNIVERSITY OF ARIZONA

$p_X[0] = q, p_X[1] = 1 - q$

Shannon's "channel"
$p_{Y|X}(y|x), x \in \mathcal{X}, y \in \mathcal{Y}$



- Mutual information

Claude Shannon, 1948

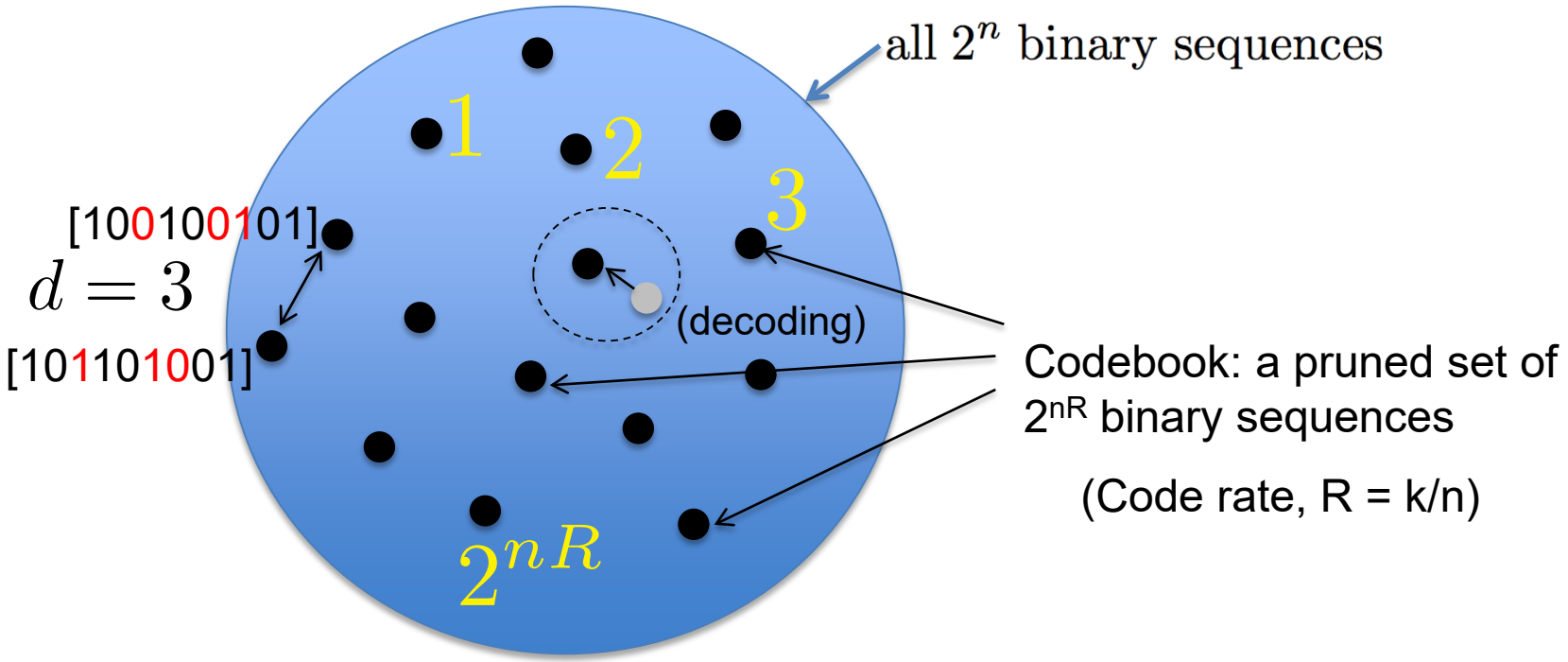
$$I(X;Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$$

$$H(X|Y) = \sum_y p_Y(y) H(X|Y = y)$$

- Capacity, $C = \max_{p_X(x)} I(X;Y) = 1 - h_2(p)$ bits/use
  - Noise does not preclude error-free digital communication
  - Need error correction to achieve capacity

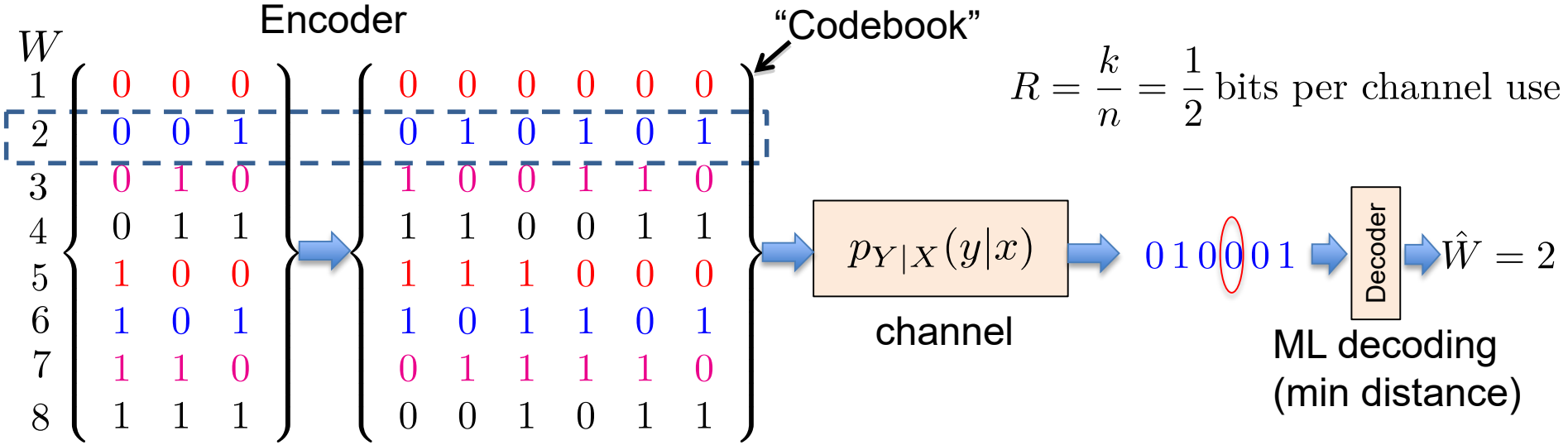
Channel coding

- Driving down errors via redundancy, (n,k,d) code



- For R < C, there exists a sequence of (n, nR, d_n) codes, s.t., $P_e^{(n)} \to 0$ as $n \to \infty$

Example of a code



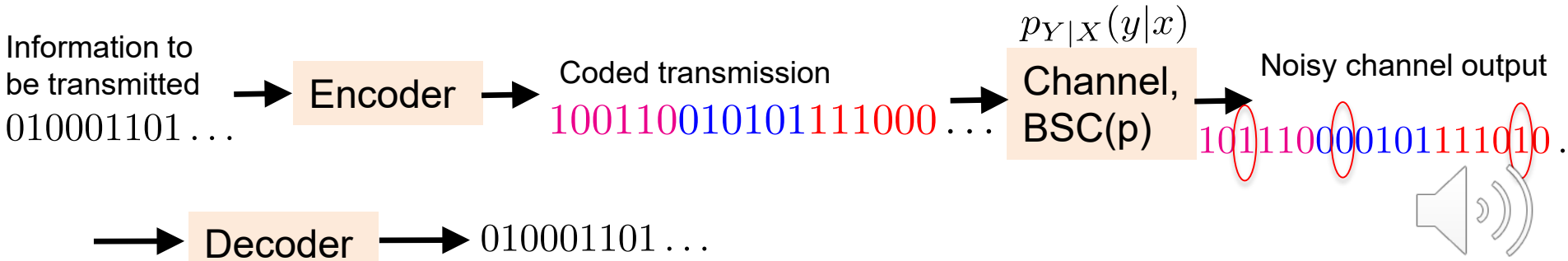
$$R = \frac{k}{n} = \frac{1}{2} \text{ bits per channel use}$$

$k = 3$ bit message
$K = 2^k = 8$ codewords

$(6, 3, 3)$ code
(n, k, d)

(d-1)/2 errors can be deterministically corrected

$P_e^{(n)} = \mathrm{P}[\hat{W} \neq W]$



Differential entropy

- Continuous random variable X, $p_X(x), x \in \mathbb{R}$
- Differential entropy $h(X) = -\int p_X(x) \log_2 p_X(x) dx$
  - Translation invariant; *h(X)* independent of mean μ_X
- Entropy of a Gaussian random variable

$$p_X(x) = \frac{1}{\sqrt{2\pi\sigma_X^2}} e^{-(x-\mu_X)^2/2\sigma_X^2} \quad \Rightarrow \quad h(X) = \frac{1}{2}\log_2(2\pi e\sigma_X^2)$$

  - For given variance σ_X^2, Prove that Gaussian *X* with that variance maximizes *h(X)* **Problem 91**
  - If $E[X^2] = P \Rightarrow h(X) \leq \frac{1}{2}\log_2(2\pi eP)$
- Mutual information, $I(X;Y) = h(Y) - h(Y|X)$
  $= h(X) - h(X|Y)$

Capacity of the AWGN channel

THE UNIVERSITY OF ARIZONA

- Additive white Gaussian noise (AWGN) channel

  $Y = X + Z,\ Z \sim \mathcal{N}(0, N),\ E[X^2] = P$ Input power constraint

- Capacity, $C = \max_{p_X(x)} I(X;Y)$, modulo $\int_{\infty}^{\infty} x^2 p_X(x) dx = P$
- Expanding

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) \\ &= h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z|X) \quad \text{mean independent} \\ &= h(Y) - h(Z) \quad \text{Z independent of X} \end{aligned}$$

  - $h(Z) = \frac{1}{2}\log_2(2\pi e N)$
  - $E[Y^2] = E[(X+Z)^2] = E[X^2] + 2E[X]E[Z] + E[Z^2] = P + N$
  - $h(Y) \le \frac{1}{2}\log_2(2\pi e(P+N))$. So, $\forall p_X(x)$,
  - $I(X;Y) \le \frac{1}{2}\log_2(2\pi e(P+N)) - \frac{1}{2}\log_2(2\pi e N) = \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right)$
  - Hence, $C = \max_{p_X(x)} I(X;Y) \le \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right)$

Capacity of the AWGN channel (contd.)

- Now, let us find a lower bound to the capacity C
- Since, $C = \max_{p_X(x)} I(X;Y)$, if we pick a particular $p_X(x)$ modulo the input power constraint $\int_{\infty}^{\infty} x^2 p_X(x)dx = P$, we will get a lower bound to C
- Let us pick, $p_X(x) = \frac{1}{\sqrt{2\pi P}} e^{-x^2/2P}$
- We obtain $C = \max_{p_X(x)} I(X;Y)$

$$\geq h(Y) - h(Y|X)$$

$$= \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right)$$

We get this by lower bound by choosing a specific p_X

- This proves that: $C = \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right)$

Optical communication capacity of a lossless channel with homodyne detection

THE UNIVERSITY OF ARIZONA

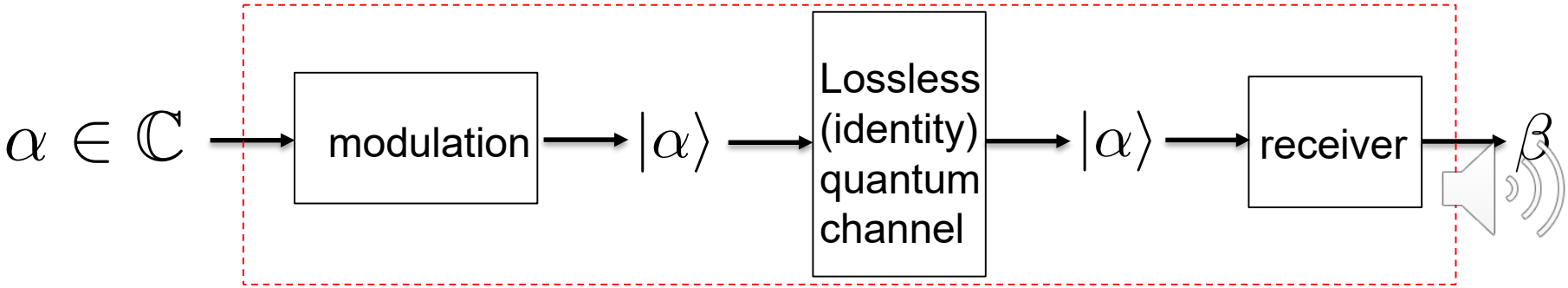
- Use coherent state modulation $|\alpha\rangle, p(\alpha) = \frac{1}{\pi N} e^{-|\alpha|^2/N}$
- Homodyne detection output

$$\beta = \alpha + Z, \;\; Z \sim \mathcal{N}\left(0, \frac{1}{4}\right)$$

- Capacity $C(N) = \frac{1}{2}\log_2\left(1 + \frac{N}{1/4}\right)$

$$= \frac{1}{2}\log_2\left(1 + 4N\right) \quad \text{bits per mode}$$

Classical "channel" $p(\beta|\alpha)$



Optical communication capacity of a lossless channel with heterodyne detection

THE UNIVERSITY OF ARIZONA

- Use coherent state modulation $|\alpha\rangle, p(\alpha) = \frac{1}{\pi N} e^{-|\alpha|^2/N}$
- Heterodyne detection output(s)

$$\beta_1 = \alpha_1 + Z_1, \; Z_1 \sim \mathcal{N}\left(0, \frac{1}{2}\right)$$

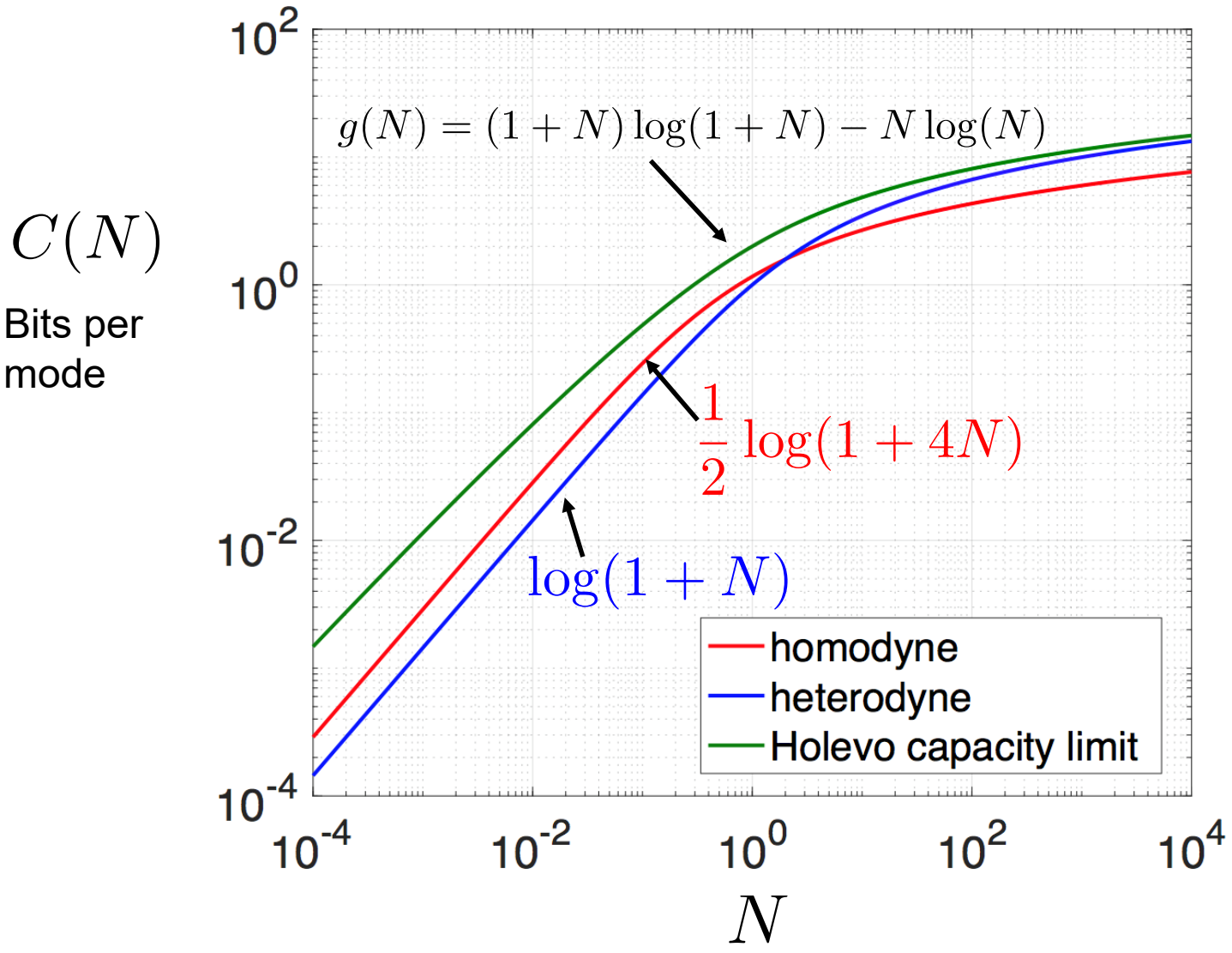
$$\beta_2 = \alpha_2 + Z_2, \; Z_2 \sim \mathcal{N}\left(0, \frac{1}{2}\right)$$

- Capacity is the sum of capacities of two independent AWGN channels

$$C(N) = 2 \times \frac{1}{2} \log_2 \left(1 + \frac{N/2}{1/2}\right)$$

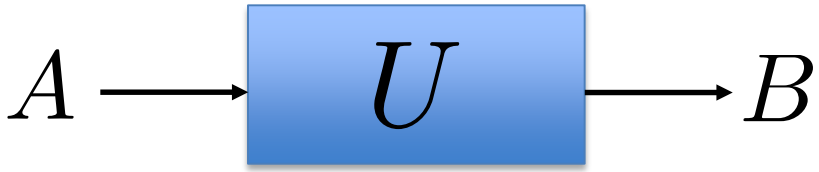
$$= \log(1 + N)$$

Capacity of homodyne and heterodyne



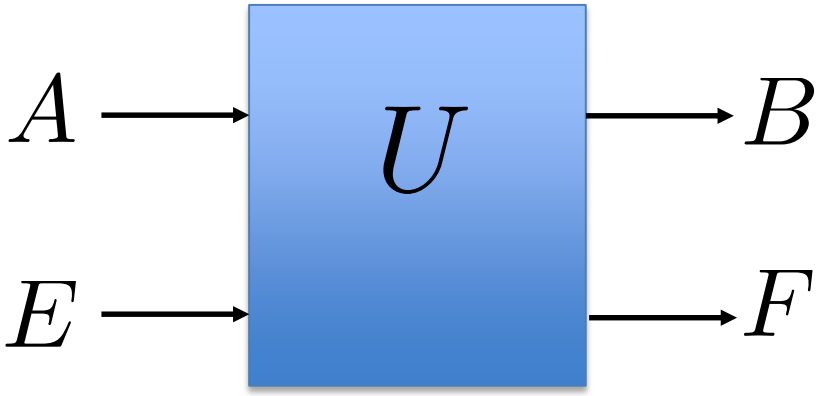
Quantum unitary and quantum channel

- Unitary transformation
  - Most general transformation of a closed quantum system



$$\rho_B = U \rho_A U^\dagger$$

- Quantum channel
  - completely positive trace preserving (CPTP) map



$$\rho_{BF} = U \rho_{AE} U^\dagger$$

$$\rho_B = \mathrm{Tr}_F(\rho_{BF})$$

$$\rho_B = \mathcal{N}(\rho_A)$$

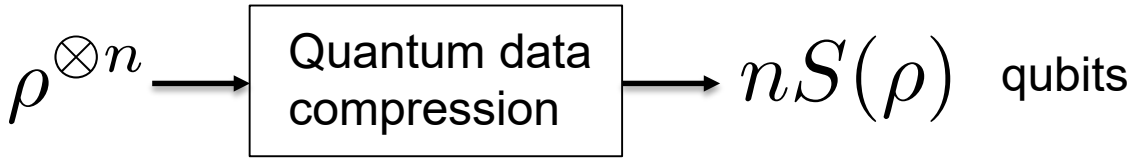
Quantum version of entropy

THE UNIVERSITY OF ARIZONA

- **von Neumann Entropy** (pure state has zero entropy)

$$S(\rho) = -\mathrm{Tr}\left(\rho \log_2 \rho\right) = -\sum_i \lambda_i \log_2 \lambda_i \; = H(\{\lambda_i\})$$

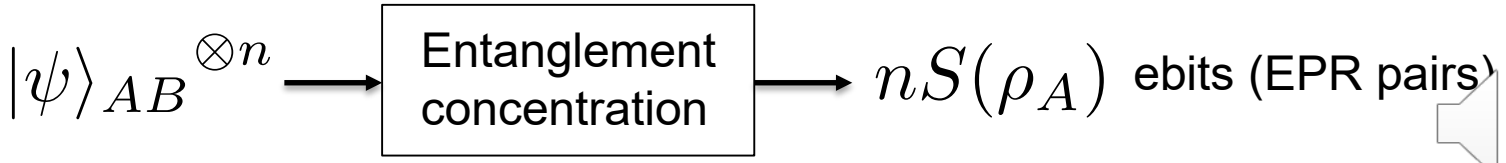
  - Shannon entropy of eigenvalues of density operator
- **Interpretation 1: quantum data compression**



  - need (ϵ, δ) to make above statement precise for finite n

Benjamin Schumacher, 1995

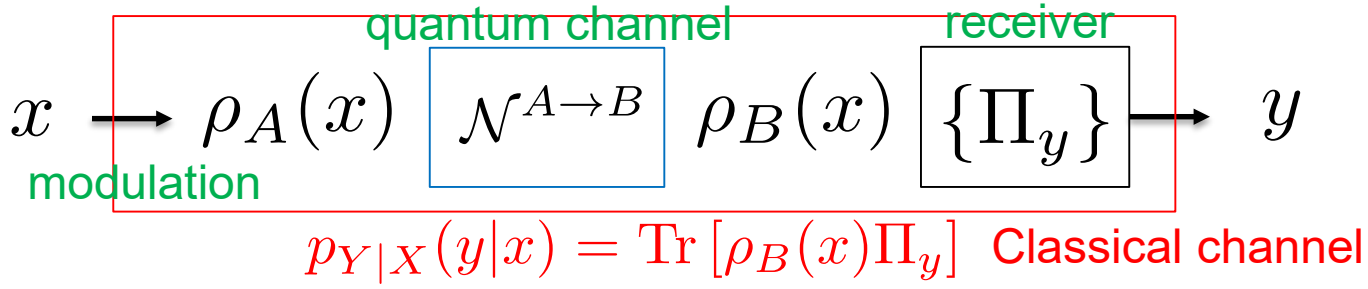
- **Interpretation 2: entanglement concentration**



Shannon vs. Holevo capacity

THE UNIVERSITY OF ARIZONA

- **Shannon capacity** of a given receiver that detects each channel symbol one at a time (all standard optical and RF receivers)



  - E.g. AWGN (RF antenna, Optical heterodyne), Poisson (Optical photon detection)
  - Highest capacity with symbol-by-symbol detection, $C_{1,1} = \max_{\{\Pi_y\},p(x)} I(X;Y)$

- **Holevo capacity** of the *quantum* channel

Holevo information: $\chi(p_X, \rho_A(x), \mathcal{N}) = S\left[\sum_x p_X(x)\rho_B(x)\right] - \sum_x p_X(x) S\left[\rho_B(x)\right] = I(X;B)$

Holevo capacity with product-state encoding: $C_{1,\infty}(\mathcal{N}) = \sup_{p_X,\rho_A(x)} \chi\left(p_X, \rho_A(x), \mathcal{N}\right)$

Ultimate capacity: $C_{\infty,\infty}(\mathcal{N}) = \sup_n \frac{C_{1,\infty}(\mathcal{N}^{\otimes n})}{n} \triangleq C(\mathcal{N})$

Superadditivity conjecture [settled by Hastings, 2009]: $C_{\infty,\infty}(\mathcal{N}) > C_{1,\infty}(\mathcal{N})$

Holevo capacity for two pure states

THE UNIVERSITY OF ARIZONA

$$x \in \{0,1\} \longrightarrow \boxed{\text{Modulation, and quantum, channel}} \longrightarrow \rho_B(x)$$

$$\rho_B(x) = |\psi_x\rangle\langle\psi_x|, \; \langle\psi_0|\psi_1\rangle = \sigma$$

$$S(p|\psi_0\rangle\langle\psi_0| + (1-p)|\psi_1\rangle\langle\psi_1|)$$

$$= S\left(\frac{1}{2}\begin{bmatrix} 1+\sigma & (1-2p)\sqrt{1-\sigma^2} \\ (1-2p)\sqrt{1-\sigma^2} & 1-\sigma \end{bmatrix}\right)$$

$$= H(\lambda_+, \lambda_-), \; \lambda_\pm(p,\sigma) = \frac{1 \pm \sqrt{1-4p(1-p)(1-\sigma^2)}}{2}$$

$$C_\infty(\sigma) = \max_{p\in(0,1)} S\left(p|\psi_1\rangle\langle\psi_1| + (1-p)|\psi_2\rangle\langle\psi_2|\right)$$

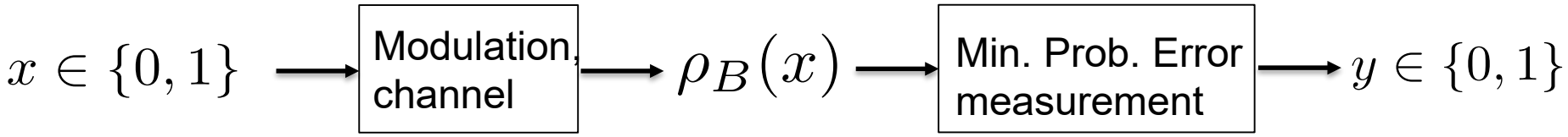
$$= h_2\left(\frac{1-\sigma}{2}\right) \text{ bits per channel use}$$

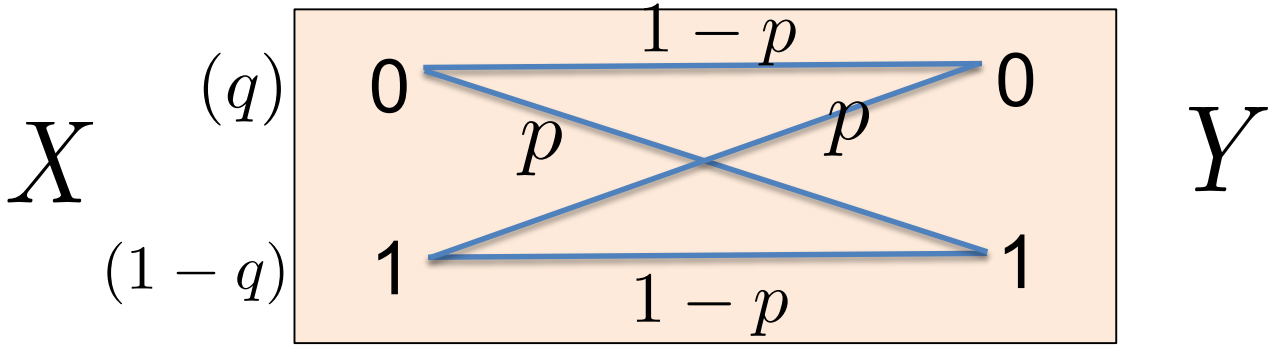
Problem 92

Derive the expression of the eigenvalues, $\lambda_\pm$ and prove this expression for Holevo capacity

Shannon capacity for two pure states

- Lets pick the optimal measurement to distinguish the two pure states





$$p = \frac{1}{2}\left[1 - \sqrt{1-\sigma^2}\right]$$

$$C_1(\sigma) = 1 - h_2(p) \text{ bits per channel use}$$

Shannon vs. Holevo capacities

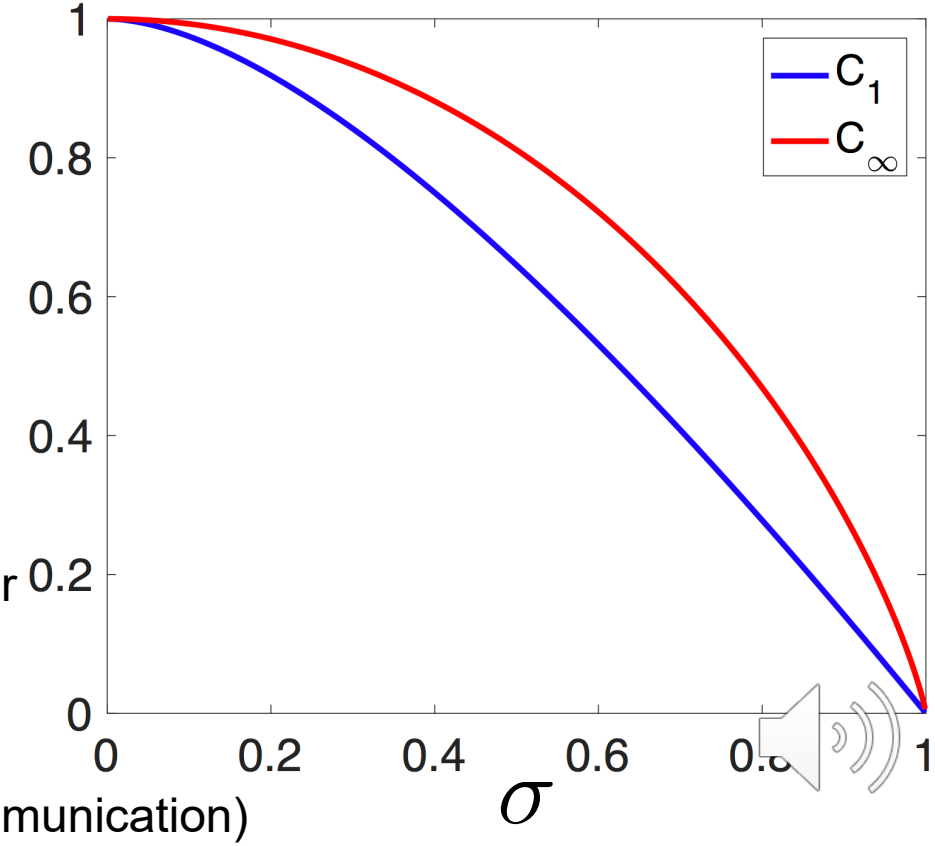
THE UNIVERSITY OF ARIZONA

$$C_1 = 1 - h_2\left(\frac{1}{2}\left[1 - \sqrt{1 - |\sigma|^2}\right]\right)$$

$$C_\infty = h_2\left(\frac{1 - \sigma}{2}\right)$$

$$\lim_{\sigma \to 1} \frac{C_\infty(\sigma)}{C_1(\sigma)} = \infty$$

$$C_1 \leq C_2 \leq \ldots \leq C_\infty$$



Example: BPSK coherent state alphabet: $\{|\alpha\rangle, |-\alpha\rangle\}, \alpha \in \mathbb{R}$

$\sigma = \langle\alpha|-\alpha\rangle = e^{-2N}, N = |\alpha|^2$

Capacity gain with a joint-detection receiver most pronounced in the regime,

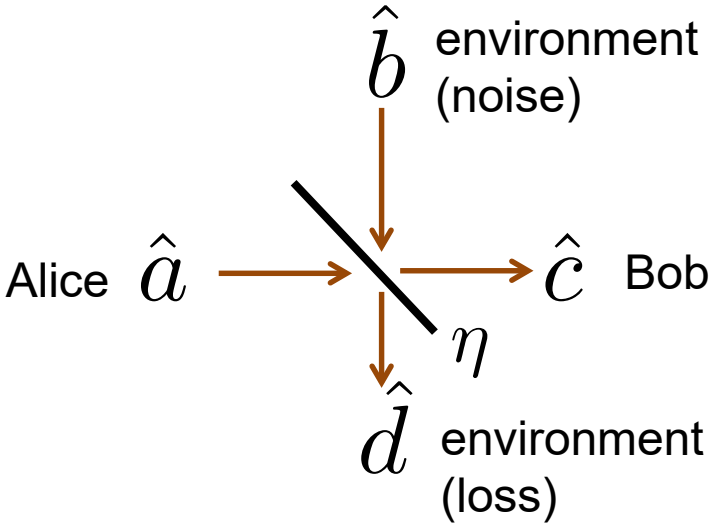
$\sigma \to 1$, or, $N \to 0$

(low photon number regime for optical communication)

Single-mode bosonic channel

- The beamsplitter

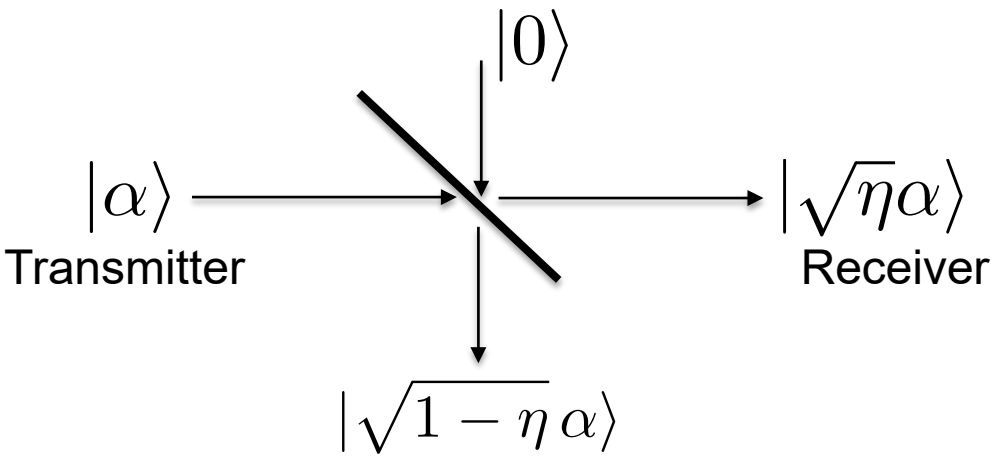
$$\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$$
$$\hat{d} = -\sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{b}$$



- Single-mode bosonic channel, $\mathcal{N}_\eta^{N_b}$: $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$
  - Pure loss: $\rho_b = |0\rangle\langle 0|$ $(N_b = 0)$
  - Thermal noise: $\rho_b = (1/\pi N_b) \int e^{-|\alpha|^2/N_b} |\alpha\rangle\langle\alpha| d^2\alpha$
  - Mean power (photon number) constraint, $\langle \hat{a}^\dagger \hat{a} \rangle = N$
  - Only state that retains its purity through the pure loss channel is the coherent state, $|\alpha\rangle \rightarrow |\sqrt{\eta}\alpha\rangle$
  - Mean photon number at output, $\langle \hat{c}^\dagger \hat{c} \rangle = \eta N + (1-\eta) N_b$

Pure loss bosonic channel

- Coherent state transmission



  - With a mean photon number constraint N at the input, which implies a mean photon number constraint ηN at the output, how many bits can be transmitted per use of this channel? (each use = one transmitted mode)
  - Example: use BPSK modulation $\{|\alpha\rangle, |-\alpha\rangle\}$, $|\alpha|^2 = N$
    - Maximum capacity (achieved at high N) is 1 bit per mode
    - Max capacity with 4-PSK (high N) is 2 bits per mode, etc.

Maximum entropy state

- For a given mean photon number, the thermal state maximizes the von Neumann entropy
  - For $\mathrm{Tr}\left(\hat{a}^\dagger \hat{a}\rho\right) = N,\ S(\rho) \leq g(N)$

$$g(x) = (1+x)\log_2(1+x) - x\log_2(x)$$

  - With equality attainted by the thermal state,

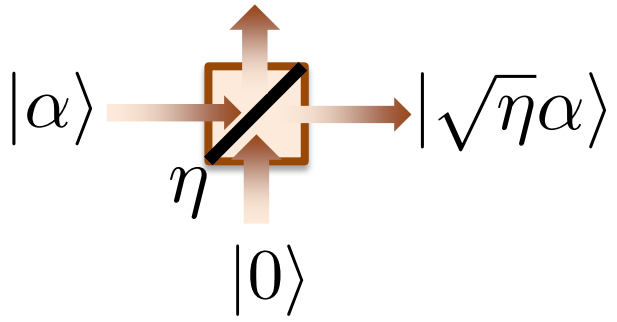
$$\rho = \sum_{n=0}^{\infty} \frac{N^n}{(1+N)^{n+1}} |n\rangle\langle n| \quad = \frac{1}{\pi N} e^{-|\alpha|^2/N} |\alpha\rangle\langle\alpha| d^2\alpha$$

- For a k-mode state with total mean photon number given by M, a tensor product thermal state of those k modes with M/k mean photon number in each mode, maximizes the entropy

Prove both of the above statements

Advanced Problem 18

Holevo capacity of pure-loss channel



$$\left\{|\alpha\rangle, p(\alpha) = \frac{1}{\pi N} e^{-|\alpha|^2/N}\right\}$$

Achievability $C(\eta, N) \geq S\left(p(\alpha)|\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|d^2\alpha\right) = g(\eta N)$

$$g(x) = (1+x)\log(1+x) - x\log x$$

Converse

$$\begin{aligned} C(\eta, N) &= \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) - \sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ &\leq \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) \right] - \min_{\{p_j, \hat{\rho}_j\}} \left[\sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ &\leq \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) \right] - \min_{\hat{\rho}} \left[S(\mathcal{E}_\eta^N(\hat{\rho})) \right], \\ &\leq g(\eta N) - 0 \end{aligned}$$

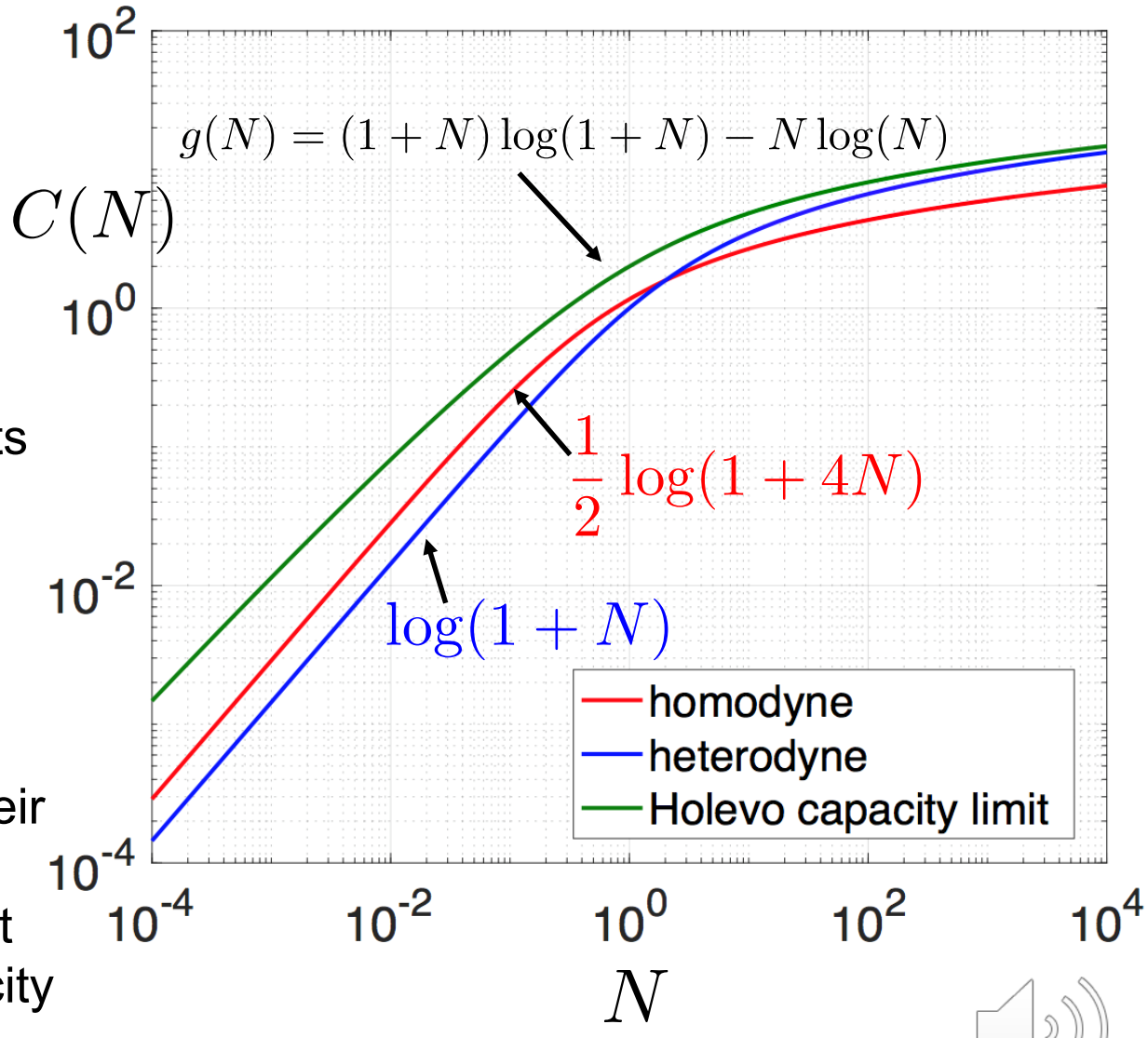
$C = g(\eta N)$ bits per mode

Capacity/coding analysis can pretend N is at the output

Giovannetti, Guha, Lloyd, Macconne, Shapiro, Yuen, PRL, 92, 027902 (2004)

Holevo capacity of pure-loss channel

- For coherent state transmission, no other distribution (other than Gaussian) attains a higher Holevo capacity
- Modulation using no other states at the inputs (such as number or squeezed states) can attain a higher capacity
- Homodyne and/or heterodyne detection receiver, even under their ideal (quantum noise limit) operations, cannot attain the Holevo capacity

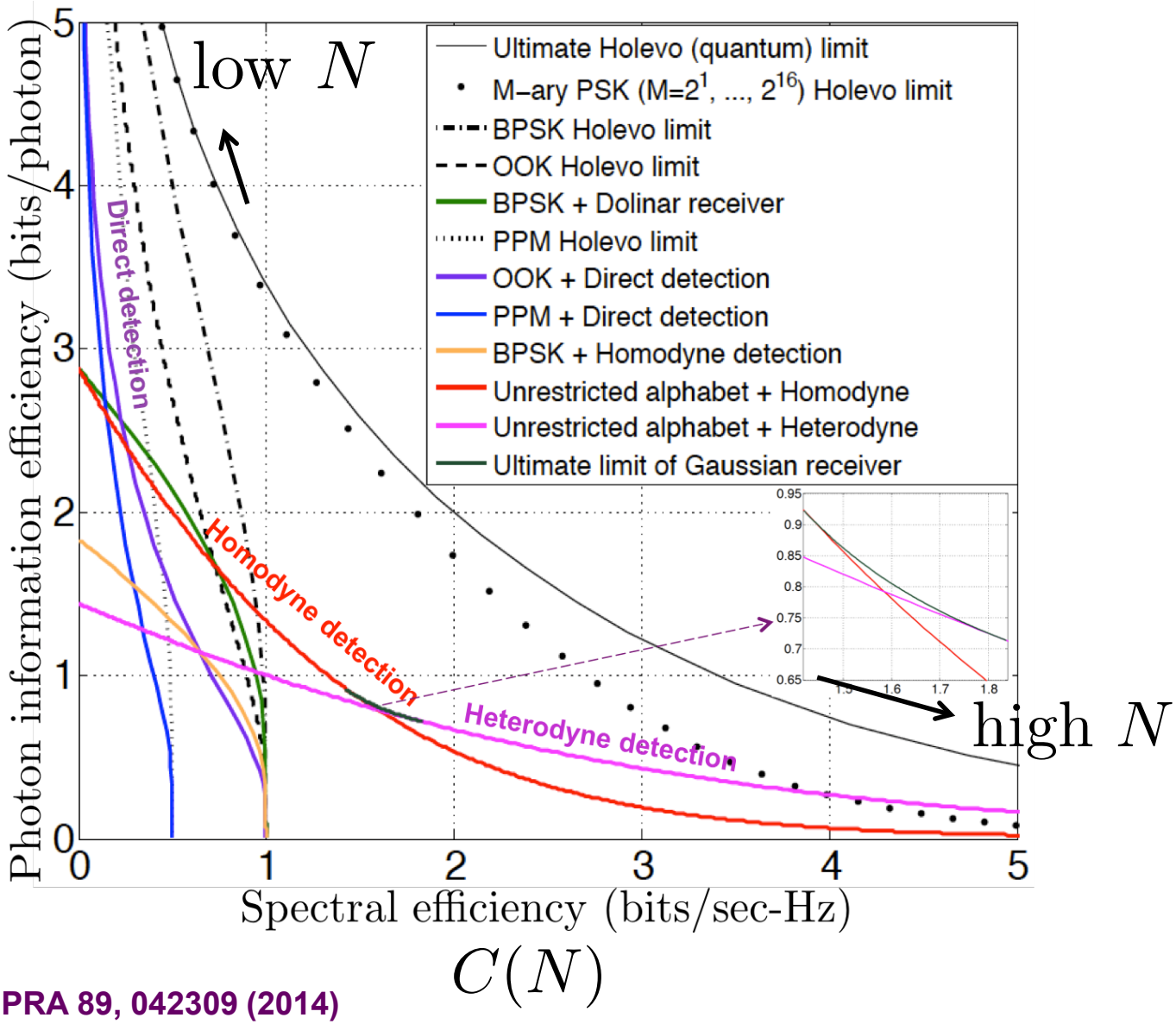


$N \rightarrow \eta N$ Pure loss: we can take N to be the output mean photon number per mode

Photon vs. spectral efficiency

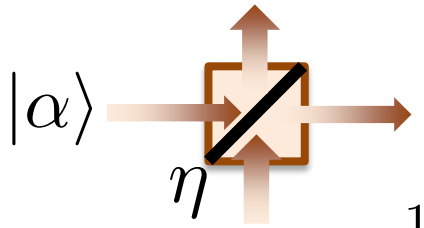
THE UNIVERSITY OF ARIZONA

$\frac{C(N)}{N}$



Takeoka, Guha, PRA 89, 042309 (2014)

Holevo capacity with loss and noise



Coherent state modulation

$$\left\{ |\alpha\rangle, p(\alpha) = \frac{e^{-|\alpha|^2/N_S}}{\pi N_S} \right\}$$

$$\rho_{\rm th} = \frac{1}{N} \int e^{-|\mu|^2/N} |\mu\rangle\langle\mu| d^2\mu$$

Achievability $C(\eta, N_S, N) \geq g(\eta N_S + (1-\eta)N) - g((1-\eta)N)$

$$g(x) = (1+x)\log(1+x) - x\log x$$

Converse

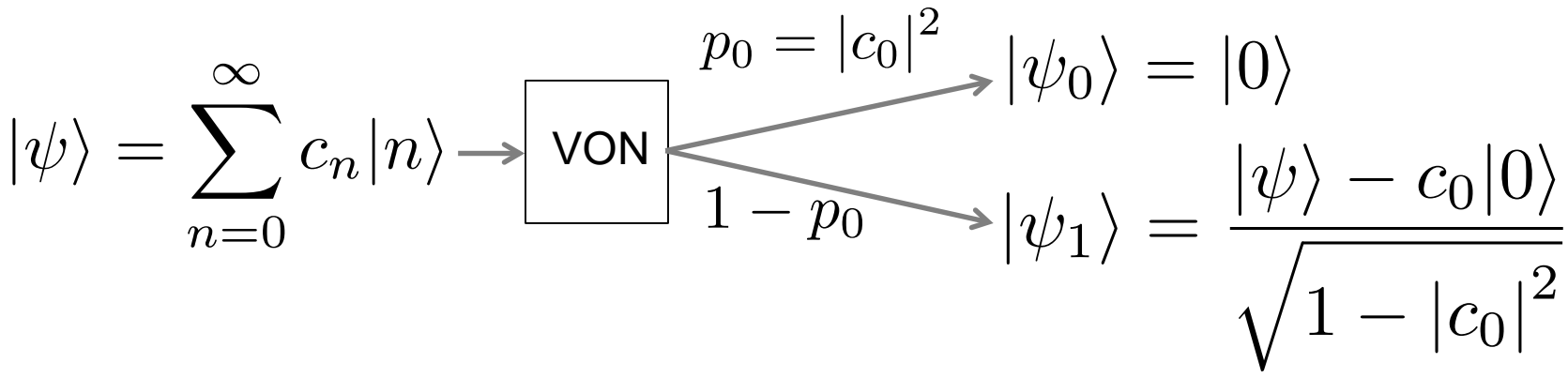
$$\begin{aligned} C(\eta, N_S, N) = & \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) - \sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ \leq & \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) \right] - \min_{\{p_j, \hat{\rho}_j\}} \left[\sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ \leq & \max_{\{p_j, \hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j \hat{\rho}_j)) \right] - \min_{\hat{\rho}} \left[S(\mathcal{E}_\eta^N(\hat{\rho})) \right], \\ \leq & \, g(\eta N_S + (1-\eta)N) - \min_{\hat{\rho}} \left[S(\mathcal{E}_\eta^N(\hat{\rho})) \right] \end{aligned}$$

Please note change in notation:
N_S = input photon number
N = thermal photon number

Minimum output entropy conjecture

V. Giovannetti, Guha, S. Lloyd, L. Maccone, J. H. Shapiro, Physical Review A 70, 032315 (2004)
V. Giovannetti, R. Garcia-Patron, N. J. Cerf, A. S. Holevo, Nature Photonics 8, 796-800 (2014)

“Vacuum or not” black box



- How do we realize the VON measurement using beam-splitters, phase-shifters, squeezers and cross-Kerr gates: $U_\kappa = e^{i\kappa(\hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b})}$?

Advanced Problem 19 (open)

The "vacuum or not" receiver to achieve the Holevo capacity

THE UNIVERSITY OF ARIZONA

- Random code with 2^{nR} codewords: A sequence of 2^{nR} "vacuum or not" binary non-destructive projective measurements plus phase-space displacements (beamsplitter & laser) can achieve capacity

$$|\boldsymbol{\alpha}^{(m)}\rangle = |\alpha_1^{(m)}\rangle|\alpha_2^{(m)}\rangle \dots |\alpha_n^{(m)}\rangle$$

$$1 \le m \le nR$$

$(j \to j+1)$

$|\psi'_j\rangle$

Displacement by negative of j[th] c.w. $|\boldsymbol{\alpha}^{(j)}\rangle$: array of n BS + lasers

$$|\psi_j\rangle = |\psi'_{j-1} - \boldsymbol{\alpha}^{(j)}\rangle$$

$$\left\{\hat{P}, \hat{I}_n - \hat{P}\right\}$$

$$\frac{(\hat{I}-\hat{P})|\psi^n\rangle}{\langle\psi_n|\hat{I}-\hat{P}|\psi_n\rangle}$$

$$\frac{\hat{P}|\psi^n\rangle}{\langle\psi_n|\hat{P}|\psi_n\rangle} = |0\rangle^{\otimes n}$$

$$\hat{P} = |0\rangle^{\otimes n}\langle 0|^{\otimes n}$$

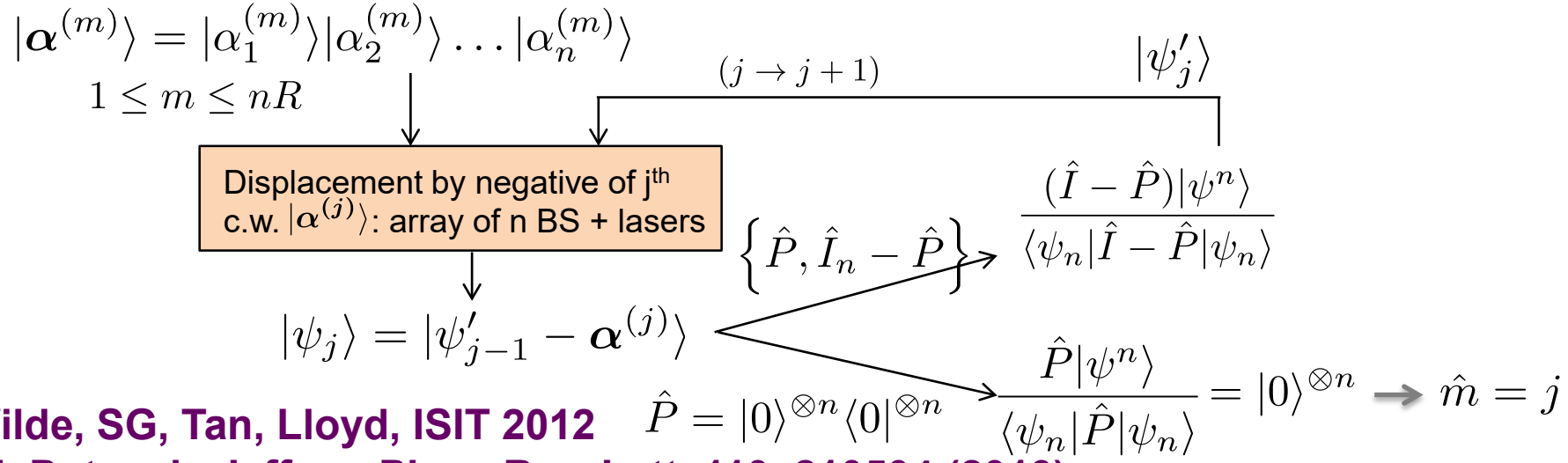
$$\hat{m} = j$$

Receiver cycles through multimode entangled coherent states…

Lloyd, Giovannetti, Maccone, Phys. Rev. Lett. 106, 250501 (2011)
Wilde, Guha, Tan, Lloyd, ArXiv: 1202.0518 (IEEE Int. Symp. Inf. Theory 2012)
"Measuring Nothing", Oi, Potocek, Jeffers, ArXiv:1207.3011, (PRL, 2012)

Holevo attaining joint detection receivers

- "vacuum or not" meas. and coherent feedback



Wilde, SG, Tan, Lloyd, ISIT 2012
Oi, Potocek, Jeffers, Phys. Rev. Lett. 110, 210504 (2013)

- Quantum polar code and successive cancellation

SG, Wilde, ISIT 2012
Wilde, SG, IEEE Trans. Inf. Theory, 59, no. 2, 1175-1187 (2013)

- Efficient joint measurements for symmetric codes

Krovi, SG, Dutton, da Silva, Phys. Rev. A 92, 062333 (2015)

- Slicing receiver

Da Silva, SG, Dutton, Phys. Rev. A 87, 052320 (2013)

Upcoming topics

- Wiretap channel – secure communication
- Quantum communication and entanglement distribution
- Quantum repeaters