Algorithmic aspects of optimal channel coding.

Input: Classical channel W, integer M.

Output: maximize $p_{succ}(E,D)$ over all M-codes (E,D) for W.

← success prob.

W is general, objective is to compute optimal success probability.

Additional motivation: understand if entanglement between sender & receiver helps.

Define optimization problem:

$$p_{succ}(W,M) = \max_{(E,D)} \frac{1}{M} \sum_{\substack{s \in [M] \\ y \in \mathcal{Y}}} D_s(y) W(y|E(s))$$

$$\text{s.t.} \quad \sum_{s \in [M]} D_s(y) = 1 \quad \forall y.$$

$$D_s(y) \geq 0.$$

Claim: $p_{succ}(W,M) = \frac{1}{M} \max_{\substack{C \subseteq \mathcal{X} \\ |C| \leq M}} f_W(C)$ with $f_W(C) = \sum_y \max_{x \in C} W(y|x)$.

$$\sum_{\substack{s \in [M] \\ y \in \mathcal{Y}}} D_s(y) W(y|E(s)) \leq \sum_{y \in \mathcal{Y}} \max_{s \in [M]} W(y|E(s))$$

$$= \sum_{y \in \mathcal{Y}} \max_{x \in C} W(y|x) \quad \text{where } C = \{x \in \mathcal{X} : \exists s, E(s) = 1\}$$

Achieved by taking $D_s(y) = 1$ if s maximizing $W(y|s)$

Observation: f_W is submodular i.e., for $C \subseteq C'$, $x \notin C'$

$$f_W(C \cup \{x\}) - f_W(C) \geq f_W(C' \cup \{x\}) - f_W(C')$$

and monotone.

Th (Nemhauser, Wolsey, Fisher, 1978)

Greedy algorithm for monotone submodular function achieves approximation $1-\frac{1}{e}$.

Greedy algorithm:

$C = \emptyset$

Repeat M times:

- Let $x = \operatorname{argmax} f_W(C \cup \{x\}) - f_W(C)$.
- $C \leftarrow C \cup \{x\}$

Corollary: Output C_{greedy} of greedy algorithm satisfies

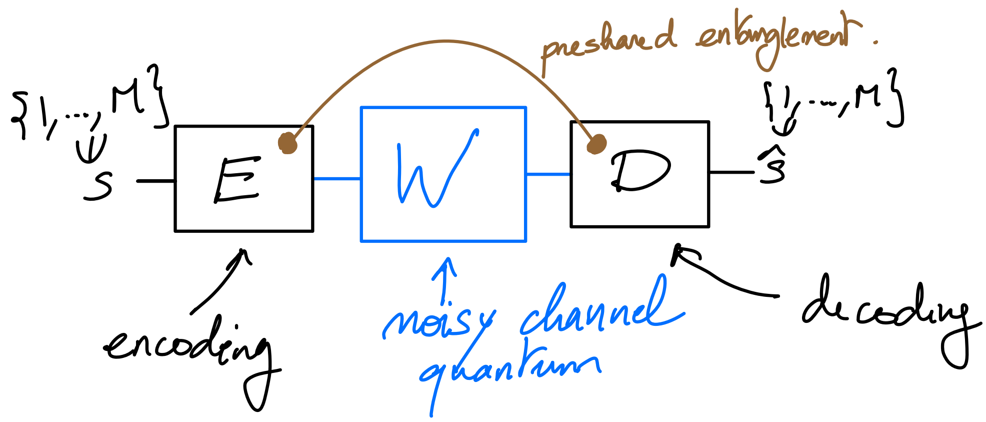
$$\frac{1}{M} f_W(C_{greedy}) \geq \left(1-\frac{1}{e}\right) p_{succ}(W, M)$$

This approximation ratio is optimal by a simple reduction to Max Coverage.

i.e. approximating $p_{succ}(W, M)$ with ratio $\left(1-\frac{1}{e}+\varepsilon\right) \Rightarrow P = NP$.

Can we find efficient upper bounds on $p_{succ}(W, k)$?

Motivation: can entanglement help?



encoding POVMs decoding POVMs.

$$p^{Q}_{succ}(W,M) = \max_{\substack{\mathcal{H},\, |\psi\rangle \in \mathcal{H}\otimes\mathcal{H} \\ E(x|s)\in \mathrm{Pos}(\mathcal{H}) \\ D(s|y)\in \mathrm{Pos}(\mathcal{H})}} \frac{1}{M} \sum_{x,y,s}' W(y|x) \langle\psi| E(x|s)\otimes D(s|y) |\psi\rangle$$

$$\sum_x' E(x|s) = I \quad \forall s$$

$$\sum_s' D(s|y) = I \quad \forall y.$$

Clear: $p_{succ}(W,M) \leq p^{Q}_{succ}(W,M)$

Inequality can be strict for some choice of W.

Can be seen as a "two player game" where quantum value > classical value.

Question: By how much can entanglement increase success prob.?

Upper bound on $p_{succ}(W,M)$:

Linear programming relaxation.

$$p^{LP}_{succ}(W,M) := \max_{\substack{p_x\geq 0 \\ r_{x,y}\geq 0}} \frac{1}{M}\sum_{x,y}' W(y|x)\, r_{x,y}.$$

$$\sum_x' r_{x,y} \leq 1 \quad \forall y, \qquad r_{x,y} \leq p_x \quad \forall x,y$$

$$\sum_x' p_x = M$$

<u>Claim:</u> $p^{Q}_{succ}(W,M) \leq p^{LP}_{succ}(W,M)$

Set $r_{x,y} = \sum_s' \langle\psi| E(x|s)\otimes D(s|y) |\psi\rangle$.

and $p_x = \sum_s' \langle\psi| E(x|s)\otimes I |\psi\rangle$.

Check $\sum_x' r_{x,y} = \sum_s' \langle\psi| \sum_x' E(x|s)\otimes D(s|y) |\psi\rangle = 1.$

$D(s|y) \leq I \Rightarrow r_{x,y} \leq p_x$

$\sum_x' p_x = \sum_s' \langle\psi| I\otimes I |\psi\rangle = M.$

Rk: $p_{succ}^{LP}(W, M)$ is the optimal success probability with arbitrary non-signalling correlations between Sender & Receiver.

Recap

$$p_{succ}^{greedy}(W,M) \le p_{succ}(W,M) \le p_{succ}^{Q}(W,M) \le p_{succ}^{LP}(W,M)$$

efficient. efficient

$1 - 1/e$.

<u>Th</u>: For any M, $\ell \le M$:

$$\frac{M}{\ell}\left(1 - e^{-\ell/M}\right) p_{succ}^{LP}(W,M) \le p_{succ}^{greedy}(W,\ell)$$

Ex: • $\left(1 - \frac{1}{e}\right) p_{succ}^{LP}(W,M) \le p_{succ}^{greedy}(W,M)$

• $0.99\, p_{succ}^{LP}(W,M) \le p_{succ}^{greedy}\left(W, \frac{M}{2^6}\right)$

Rk: factor $\frac{M}{\ell}\left(1 - e^{-\ell/M}\right)$ optimal.

Consequences: * Entanglement can increase success probability by at most $\frac{1}{1-\frac{1}{e}}$.

* Taking $W^{\otimes n}$, this implies that entanglement does not change capacity: even non signalling.

if $M < 2^{C(W)}$, $p_{succ}(W^{\otimes n}, M^n) \xrightarrow[n\to\infty]{} 1$

if $M > 2^{C(W)}$, $p_{succ}^{LP}(W^{\otimes n}, M^n) \xrightarrow[n\to\infty]{} 0$

<u>Proof</u>: Rounding. Assume $\ell = M$.

Let $C = \{X_1, X_2, \dots, X_M\}$ with X_i indep with distribution $\left\{\frac{p_x}{\ell}\right\}_{x\in\mathcal{X}}$

$$\mathop{\mathbb{E}}_{C} f_W(C) = \frac{1}{M} \sum_{y}{}' \mathop{\mathbb{E}}_{C} \left\{ \max_{x \in C} W(y|x) \right\}$$

Focus on a fixed y. Assume for simplicity $W(y|x_1) = \dots = W(y|x_t) = \alpha$ and $W(y|x_{t+1}) = \dots = W(y|x_{|\mathcal{X}|}) = 0$

$$\begin{aligned}
\mathop{\mathbb{E}}_{C} \left\{ \max_{x \in C} W(y|x) \right\} &= \alpha \cdot \mathbb{P}\{x_1 \in C \text{ or } x_2 \in C \dots \text{ or } x_t \in C\} \\
&= \alpha \cdot \left(1 - \left(1 - \frac{p_{x_1} + p_{x_2} \dots + p_{x_t}}{M} \right)^M \right) \\
&\geq \alpha \left(1 - \left(1 - \frac{r_{x_1,y} + r_{x_2,y} + \dots + r_{x_t,y}}{M} \right)^M \right) \\
&\geq \left(1 - \left(1 - \frac{1}{M} \right)^M \right) \left(r_{x_1,y} + \dots + r_{x_t,y} \right) \alpha \\
&\geq \left(1 - \frac{1}{e} \right) \underbrace{\sum_{x}{}' r_{x,y} W(y|x)}_{\text{what appears in objective function of LP.}}
\end{aligned}$$

$$\mathop{\mathbb{E}}_{C} \left\{ f_W(C) \right\} \geq \left(1 - \frac{1}{e} \right) P^{LP}_{succ}(W, M). \qquad \blacksquare$$

Open question: does the same hold for cq channels?