Algorithmic aspects of optimal channel coding.

Input: Classical channel $W$, integer $M$.
Output: maximize $\text{Psucc}(E,D)$ over all $M$-codes $(E,D)$ for $W$.

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

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

Define optimization problem:

$$\text{Psucc}(W, M) = \max_{(E,D)} \frac{1}{M} \sum_{y \in Y} D_{y}(g)W(g|E(y))$$

subject to:

$$\sum_{y \in Y} D_{y}(g) = 1 \quad \forall y.$$

$$D_{y}(g) \geq 0.$$

Claim: $\text{Psucc}(W, M) = \frac{1}{M} \max_{C \subseteq X, |C| \leq M} f_{W}(C)$

with $f_{W}(C) = \sum_{y \in C} \max_{x \in E(y)} W(g|E(y))$.

$$\sum_{y \in Y} D_{y}(g)W(g|E(y)) \leq \sum_{y \in Y} \max_{x \in E(y)} W(g|E(y))$$

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

Achieved by taking $D_{y}(g) = 1$ if $g = \max_{x \in E(y)} W(g|x)$

Achieved by taking $D_{y}(g) = 1$ if $g = \max_{x \in E(y)} W(g|x)$

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.
The (Neuhaus, Wolsey, Fisher, 1978)

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

Greedy algorithm:
\[
C = \emptyset \\
\text{repeat } M \text{ times:} \\
\quad \alpha = \arg \max f(C \cup \{a\}) - f(C) \\
\quad C \leftarrow C \cup \{a\}
\]

Corollary: Output $C_{\text{greedy}}$ of greedy algorithm satisfies
\[
\frac{1}{M} \sum f(C_{\text{greedy}}) \geq (1 - \frac{1}{e}) \text{psucc}(W, M)
\]

This approximation ratio is optimal by a simple reduction to Max Coverage. i.e. approximately $\text{psucc}(W, M)$ with ratio $(1 - \frac{1}{e} + \epsilon) \Rightarrow P = NP$.

Can we find efficient upper bounds on $\text{psucc}(W, k)$?

Motivation: can entanglement help?

- Encoding
- Decoding
- Noisy channel
- Preshared entanglement.
\[ p_{\text{succ}}^Q(W, M) = \max_{H, H \in \mathbb{H}, E \in \mathbb{E}(H)} \frac{1}{M} \sum_s W(y|x_s) <\psi| E(x_s) \otimes D(s|y) |\psi> \]

Clear: \[ p_{\text{succ}}^Q(W, M) \leq p_{\text{succ}}^Q(W, M) \]

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 \( p_{\text{succ}}(W, M) \):

Linear programming relaxation.

\[ p_{\text{succ}}^{LP}(W, M) := \max_{p_x \geq 0, r_{x,y} \geq 0} \frac{1}{M} \sum_x W(y|x) r_{x,y} \]

\[ \sum_x r_{x,y} \leq 1 \quad \forall y, \quad r_{x,y} \leq p_x + r_{x,y} \]

\[ \sum_x p_x = M \]

Claim: \[ p_{\text{succ}}^Q(W, M) \leq p_{\text{succ}}^{LP}(W, M) \]

Set \( r_{x,y} = \sum_s <\psi| E(x_s) \otimes D(s|y) |\psi> \).

and \( p_x = \sum_s <\psi| E(x_s) \otimes I |\psi> \).

Check \[ \sum_x r_{x,y} = \sum_s <\psi| \sum_x E(x_s) \otimes D(s|y) |\psi> = 1 \]

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

\[ \sum_x p_x = \sum_s <\psi| \mathbb{I} \otimes \mathbb{I} |\psi> = M. \]
Recap

\[ P_{\text{succ}}(W,M) \leq P_{\text{succ}}(W,\hat{M}) \leq P_{\text{succ}}(W,H) \leq \frac{P_{\text{succ}}(W)}{\epsilon} \]

**Th.:** For any \( M, \epsilon \leq M \):

\[ \frac{M}{\epsilon} (1-e^{-2\phi}) P_{\text{succ}}(W,M) \leq P_{\text{succ}}(W,\epsilon) \]

**Ex.:** \((1-\frac{1}{2}) P_{\text{succ}}(W,M) \leq P_{\text{succ}}(W,M) \)

\[ 0.99 P_{\text{succ}}(W,M) \leq P_{\text{succ}}(W,\frac{M}{2^6}) \]

**Rk.:** Factor \( \frac{M}{\epsilon} (1-e^{-2\phi}) \) optimal.

**Consequences:**

1. Entanglement can increase success probability by at most \( \frac{M}{\epsilon} \).
2. Taking \( W^{\otimes n} \), this implies that entanglement does not change capacity:
   - If \( M \leq 2^{2\phi} \), \( P_{\text{succ}}(W^{\otimes n},M) \to 1 \)
   - If \( M > 2^{2\phi} \), \( P_{\text{succ}}(W^{\otimes n},M) \to 0 \)

**Proof:** Roundy. Assume \( \epsilon = M \).

Let \( C = \{X_1, X_2, \ldots, X_m\} \) with \( X_i \) indep with distribution \( P_\phi \). \( X_i \) are independent, average probability of success is at least \( 0.99 P_\phi \).
\[ E \left[ \frac{f_W(C)}{C} \right] = \frac{1}{M} \sum_{y} E \left[ \max_{x \in C} W(y|x) \right] \]

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

\[ E \left[ \max_{x \in C} W(y|x) \right] = \alpha \cdot P \left[ x_1 \in C \land x_2 \in C \ldots \land x_t \in C \right] \]

\[ = \alpha \cdot \left( 1 - \left( 1 - \frac{1}{M} \right)^t \right) \]

\[ \geq \alpha \cdot \left( 1 - \left( 1 - \frac{1}{M} \right)^t \right) \cdot \sum_{x} \frac{x_{y|x}}{n} \]

\[ \geq \left( 1 - \frac{1}{e} \right) \sum_{x} \frac{x_{y|x}}{n} W(y|x) \]

\[ E \left[ \frac{f_W(C)}{C} \right] \geq \left( 1 - \frac{1}{e} \right) P_{\text{succ}}(W, M). \]

Open question: does the same hold forcq channels?