One-Shot Capacity of Discrete Channels

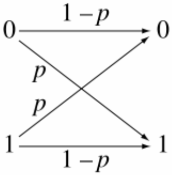
Rui A. Costa

Joint work with Michael Langberg and João Barros

Instituto de Telecomunicações
Faculdade de Ciências da Universidade do Porto, Portugal
rfcosta@fe.up.pt

Classical Channel Capacity

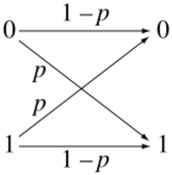
Binary Symmetric Channel



Shannon's Channel Capacity: $C = \sup_{p_X} I(X,Y) = 1 - H(p)$

Classical Channel Capacity

Binary Symmetric Channel



Shannon's Channel Capacity: $C = \sup_{p_X} I(X,Y) = 1 - H(p)$

Implicit in the definition:

- Arbitrarily large block length of the channel code
- Error probability goes to zero as the block length goes to infinity

Previous Approaches

- **Limited number of channel uses**
  - Rate at which the error probability decays to zero: **Error Exponents** (Shannon, Gallager, Berlekamp, 1967)
- **Error probability precisely zero**
  - Achievable rates with error probability is precisely zero: **Zero-Error Capacity** (Shannon, 1956)

The One-Shot Case

How many bits can we transmit over the channel if:

- **we can use the channel only once** and
- we allow the error probability to go up to a user-defined value

The One-Shot Case

How many bits can we transmit over the channel if:

- **we can use the channel only once** and
- we allow the error probability to go up to a user-defined value

Why do we care?

- Cases where power must be concentrated in a single transmission:
    - Military Scenarios
    - Random Short Encounters
    - Critical Systems

instituto de telecomunicações

The One-Shot Case

How many bits can we transmit over the channel if:

- **we can use the channel only once** and
- we allow the error probability to go up to a user-defined value

Why do we care?

- Cases where power must be concentrated in a single transmission:
    - Military Scenarios
    - Random Short Encounters
    - Critical Systems

Previous work has provided bounds for the one-shot capacity, but no precise characterization (Renner, Wolf, Wullschleger, 2006).

instituto de telecomunicações

Definitions

- A discrete channel is composed of:
  - An input alphabet $\mathcal{X}$ and an output alphabet $\mathcal{Y}$
  - The transition probabilities $\mathcal{P}(Y = y|X = x)$
- A **one-shot communication scheme** over a $P_{Y|X}$ channel is composed of:
  - A codebook $\underline{\mathcal{X}} \subseteq \mathcal{X}$
  - A decoding function $\gamma : \mathcal{Y} \to \underline{\mathcal{X}}$
- The **maximum error probability** associated with a pair $(\underline{\mathcal{X}}, \gamma)$ is defined as

$$\epsilon_{\underline{\mathcal{X}},\gamma} = \max_{x \in \underline{\mathcal{X}}} \mathcal{P}(\gamma(Y) \neq x | X = x)$$

Admissibility and Capacity

Definition (Admissible Codebooks)

The pair $(\underline{\mathcal{X}}, \gamma)$ is *maximum-ϵ-admissible* if $\epsilon_{\underline{\mathcal{X}},\gamma} \leq \epsilon$. The set of all ϵ-admissible pairs is denoted by $\mathcal{A}_\epsilon$.

Definition (One-Shot Capacity)

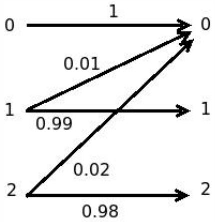
For $\epsilon \in [0, 1]$, the *ϵ-maximum one-shot channel capacity* is defined as

$$C_\epsilon = \max_{(\underline{\mathcal{X}},\gamma)\in\mathcal{A}_\epsilon} \log(|\underline{\mathcal{X}}|).$$

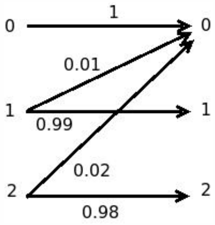
Zero-Error One-Shot Capacity

The Zero-Error One-Shot Capacity was fully characterized using a combinatorial approach: (Shannon, 1956; Korner, Orlitsky, 1998)

- Confusion Graph: two input symbols are connected if they can be "confused"
- Zero-Error One-Shot Capacity = Independence Number of the Confusion Graph.

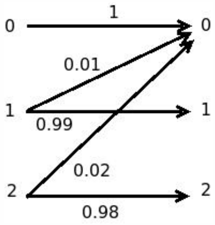


Can we transmit more?



- Zero-Error One-Shot Capacity = 0
- If we allow for a small error probability, can we transmit some bits in a single use of the channel?

Can we transmit more?



- Zero-Error One-Shot Capacity = 0
- If we allow for a small error probability, can we transmit some bits in a single use of the channel?
- "Yes, we can":

$$C_\epsilon = \begin{cases} 0 & \text{if } \epsilon < 0.01 \\ 1 & \text{if } 0.01 \leq \epsilon < 0.02 \\ \log(3) & \text{if } \epsilon \geq 0.02 \end{cases}$$

A family of examples

Definition (A Class of Discrete Channels)

- $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, n-1\}$
- $\mathcal{P}(Y = 0|X = 0) = 1$ and, with $0 < e_1 < e_2 < \cdots < e_{n-1} \leq 1$, for $i \in \mathcal{X} \setminus \{0\}$,

$$P(Y = y|X = i) = \begin{cases} 1 - e_i & \text{if } y = i \\ e_i & \text{if } y = 0 \\ 0 & \text{otherwise} \end{cases}$$

A family of examples

Definition (A Class of Discrete Channels)

- $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, n-1\}$
- $\mathcal{P}(Y = 0|X = 0) = 1$ and, with $0 < e_1 < e_2 < \cdots < e_{n-1} \leq 1$, for $i \in \mathcal{X} \setminus \{0\}$,

$$P(Y = y|X = i) = \begin{cases} 1 - e_i & \text{if } y = i \\ e_i & \text{if } y = 0 \\ 0 & \text{otherwise} \end{cases}$$

Lemma

For $e_i \leq \epsilon < e_{i+1}$, with $e_0 = 0$ and $e_n = 1$, we have that

$$C_\epsilon = \log(i + 1).$$

instituto de telecomunicações

Definition

For each $x \in \mathcal{X}$, let

$$D_\epsilon(x) = \left\{ D \subset \mathcal{Y} : \sum_{y \in D} \mathcal{P}(Y = y | X = x) \geq 1 - \epsilon \right\}$$

Definition

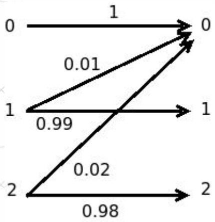
For each $x \in \mathcal{X}$, let

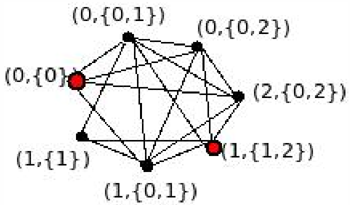
$$D_\epsilon(x) = \left\{ D \subset \mathcal{Y} : \sum_{y \in D} \mathcal{P}(Y = y | X = x) \geq 1 - \epsilon \right\}$$

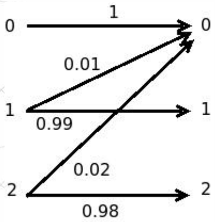
Definition (Maximum-One-Shot Graph)

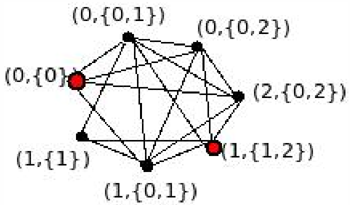
- Nodes: (x, D) with $x \in \mathcal{X}$ and $D \in D_\epsilon(x)$
- (x, D) and (x', D') are connected $\Leftrightarrow x = x'$ or $D \cap D' \neq \emptyset$

instituto de telecomunicações


0
1
0
0.01
1
1
0.99
0.02
2
2
0.98


(0,{0,1})
(0,{0,2})
(0,{0})
(2,{0,2})
(1,{1})
(1,{1,2})
(1,{0,1})





- Independent Set: no two nodes are connected.
- Independence Number: size of the largest independent set; denoted by $\alpha(G)$.

Main Result

Theorem

Consider a channel described by $P_{Y|X}$ and the corresponding one-shot graph $G_\epsilon = (V, E_\epsilon)$, with $\epsilon \in [0, 1)$. The ϵ-maximum one-shot capacity satisfies

$$C_\epsilon = \log(\alpha(G_\epsilon)).$$

Main Argument in the Proof:

- **Decoding Function** $\leftrightarrow$ **Independent Set** in the maximum one-shot graph

Complexity

- The one-shot capacity is directly related to an independent set problem
- The independent set problem in 3-regular graphs (NP-Hard) can be reduced to an instance of the ϵ-maximum one-shot capacity problem, for $\epsilon < 1/3$

Theorem

The computation of the ϵ-maximum one-shot capacity is NP-Hard, for $\epsilon < 1/3$.

Average One-Shot Capacity

- Similar techniques are used to analyze the case of Average Error Probability:

$$\bar{\epsilon}_{\underline{\mathcal{X}},\gamma} = \frac{1}{|\underline{\mathcal{X}}|} \sum_{x \in \underline{\mathcal{X}}} \mathcal{P}(\gamma(Y) \neq x | X = x)$$

- The main result is again combinatorial, based on sparse sets in a graph.

instituto de telecomunicações

Conclusions

- We formalize the notion of ϵ-**one-shot capacity**, both for the maximum and average error cases
- We present a family of channels for which the zero-error capacity is null, but by allowing a small error probability, we can transmit a significant number of bits
- In contrast with previous work, we provide a precise characterization of one-shot capacity, using combinatorial techniques
- We prove that computing the one-shot capacity is NP-Hard

Future Steps

- We are aiming at an extension of our techniques to the n-shot case
- Using the n-shot framework, we will analyze classic channels and compare results with the standard capacity notions
- We are also considering the case where security constrains are present: how can we describe the **one-shot secrecy capacity**?