Deterministic Identification

Mohammad J. Salariseddigh

Joint work with:
Uzi Pereg, Holger Boche and Christian Deppe

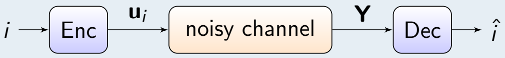
Nov 23, 2020

Outline

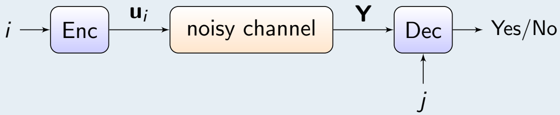
Outline

Transmission vs. Identification

- Shannon's setting: Bob recover the message



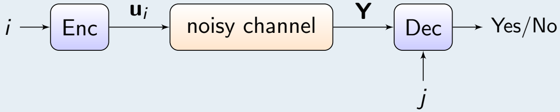
- Identification setting: Bob asks if a message was sent or not?



Transmission vs. Identification

- Shannon's setting: Bob recover the message

- Identification setting: Bob asks if a message was sent or not?



Apps → vehicle-to-X communications, health care, point to multi-point communication, molecular communication, online sales, communication complexity, and any event-triggered scenario

Randomized Identification (RI) [1]

- Originally introduced by Ahlswede and Dueck (1989)
- Capacity was established with randomness at encoder
- Encoder employs distribution to select codewords

Remarkable Property

- Reliable identification is possible with code size growth $\sim 2^{2^{nR}}$
- Sharp difference to transmission with code size growth $\sim 2^{nR}$

[1] Ahlswede, R. and Dueck, G. "Identification via channels", 1989

Randomized Identification (RI) [1]

- Originally introduced by Ahlswede and Dueck (1989)
- Capacity was established with randomness at encoder
- Encoder employs distribution to select codewords

Remarkable Property

- Reliable identification is possible with code size growth $\sim 2^{2^{nR}}$
- Sharp difference to transmission with code size growth $\sim 2^{nR}$

For $R = 0.01$ and $n = 821 \to 2^{2^{8.21}} >$ # of atoms in universe

[1] Ahlswede, R. and Dueck, G. "Identification via channels", 1989

Deterministic Identification (DI) [2]

- Encoder uses deterministic mapping for coding
- Code size $\sim 2^{nR}$ for DMC as in transmission paradigm
- Achievable rates **higher** than transmission

Why deterministic?

- Simpler implementation (random resource not required)
- Suitable for Jamming scenarios
- Suitable for molecular communication [a]

[a] Nakano, et. al, "Molecular communication and networking: Opportunities and challenges", 2012

[2] Ahlswede, R. and Cai, N. "Identification without randomization", 1999

Outline

Main Contributions

- We established the DI capacity for three channel models with power constraints:
  - DMC
  - Fast Fading
  - Slow Fading

Main Contributions

- We established the DI capacity for three channel models with power constraints:
  - DMC
  - Fast Fading
  - Slow Fading
- We show that the optimal code size scales as $\sim 2^{nR}$ for the DMC and as $\sim 2^{n \log(n) R} = n^{nR}$ for the fading channels

Main Contributions

- We established the DI capacity for three channel models with power constraints:
  - DMC
  - Fast Fading
  - Slow Fading
- We show that the optimal code size scales as $\sim 2^{nR}$ for the DMC and as $\sim 2^{n\log(n)R} = n^{nR}$ for the fading channels
- Our analysis combines techniques and ideas from both works, by JáJá [a] and Ahlswede [b]

[a] Ja, J.J., "Identification is easier than decoding", 1985

[b] Ahlswede, R. "A method of coding and its application to arbitrarily varying channels", 1980

Outline

Transmission

Definition (Transmission Code)

A $(L(n,R), n, \varepsilon)$-transmission code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

Transmission

Definition (Transmission Code)

A $(L(n,R), n, \varepsilon)$-transmission code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$

Transmission

Definition (Transmission Code)

A $(L(n,R), n, \varepsilon)$-transmission code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$
3. Input constraint: $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$ with $\phi : \mathcal{X} \to [0,\infty)$

Transmission

Definition (Transmission Code)

A $(L(n,R), n, \varepsilon)$-transmission code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i \in [1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$
3. Input constraint: $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$ with $\phi : \mathcal{X} \to [0, \infty)$
4. Error requirement: $W^n(\mathcal{D}_i | \boldsymbol{u_i}) \geq 1 - \varepsilon$
5. Non-overlapping decoding regions: $\mathcal{D}_i \underset{i \neq j}{\cap} \mathcal{D}_j = \emptyset$

Transmission

Definition (Achievable Rate)

A rate R is called achievable if for every positive ε and sufficiently large n, there exists an $(L(n,R), n, \varepsilon)$-code

Definition (Channel Capacity)

$$\mathbb{C}_T(\mathcal{W}) = \sup\{R \,|\, \text{R is achievable}\}$$

Transmission

Definition (Achievable Rate)

A rate R is called achievable if for every positive ε and sufficiently large n, there exists an $(L(n,R), n, \varepsilon)$-code

Definition (Channel Capacity)

$$\mathbb{C}_T(\mathcal{W}) = \sup\{R \,|\, \text{R is achievable}\}$$

Theorem (Shannon, 1948)

Transmission capacity of a DMC $\mathcal{W}$ for $L(n,R) = 2^{nR}$ is given by

$$\mathbb{C}_T(\mathcal{W}, L) = \max_{p_X} I(X;Y)$$

DI Codes

Definition (Ahlswede and Cai, 1999)

A $(L(n,R),n,\lambda_1,\lambda_2)$-DI code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i},\mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

DI Codes

Definition (Ahlswede and Cai, 1999)

A $(L(n,R), n, \lambda_1, \lambda_2)$-DI code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$

DI Codes

Definition (Ahlswede and Cai, 1999)

A $(L(n,R), n, \lambda_1, \lambda_2)$-DI code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$
3. Input constraint: $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$ with $\phi : \mathcal{X} \to [0,\infty)$

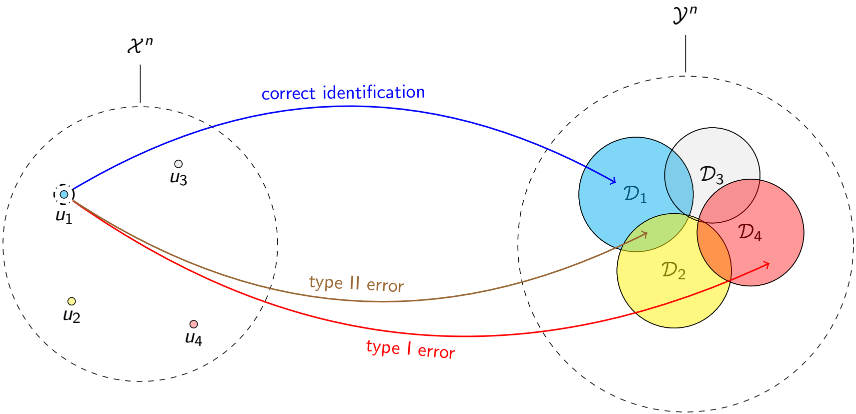
DI Codes

Definition (Ahlswede and Cai, 1999)

A $(L(n,R), n, \lambda_1, \lambda_2)$-DI code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u_i}, \mathcal{D}_i)\}_{i\in[1:L(n,R)]}$ subject to

1. Code size: $L(n,R) = 2^{nR}$
2. Code-word: $\boldsymbol{u_i} \in \mathcal{X}^n$, decoding regions: $\mathcal{D}_i \subset \mathcal{Y}^n$
3. Input constraint: $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$ with $\phi : \mathcal{X} \to [0,\infty)$
4. Error requirement type I: $W^n(\mathcal{D}_i|\boldsymbol{u}_i) > 1 - \lambda_1$
5. Error requirement type II: $W^n(\mathcal{D}_i|\boldsymbol{u}_j) \underset{i\neq j}{<} \lambda_2$

Geometry of DI Codes



RI Codes

Ahlswede and Dueck, 1989

Given local randomness at the transmitter, encoder send a random codeword $\boldsymbol{u}_i \sim Q_i$.

Theorem (Ahlswede and Dueck, 1989)

RI capacity of a DMC $\mathcal{W}$ for $L(n,R) = 2^{2^{nR}}$ is given by

$$\mathbb{C}_{RI}(\mathcal{W}, L) = \max_{p_X} I(X;Y)$$

Outline

DI Capacity of DMC

Theorem

[a] *Let $\mathcal{W}$ be a DMC with distinct rows in channel matrix. Then for $L(n, R) = 2^{nR}$, the DI capacity under input constraint is given by*

$$\mathbb{C}_{DI}(\mathcal{W}, L) = \max_{p_X \,:\, \mathbb{E}\{\phi(X)\} \leq A} H(X)$$

[a] arXiv:2010.04239, 2020

DI Capacity of DMC

Theorem (Ahlswede and Dueck, 1989; Ahlswede and Cai, 1999)

For DMC $\mathcal{W}$ let $W : \mathcal{X} \to \mathcal{Y}$ be channel matrix with distinct rows. Then for $L(n,R) = 2^{nR}$, the DI capacity is given by

$$\mathbb{C}_{DI}(\mathcal{W}, L) = \log|\mathcal{X}|$$

- A proof was not provided
- Consequence of our result with $A = \phi_{max}$
- $\mathbb{C}_{DI}(\mathcal{W}, L) = \max_{p_X : \mathbb{E}\{\phi(X)\} \leq \phi_{max}} H(X) = H(X) \Big|_{p_X \sim \mathcal{U}(\{1:|\mathcal{X}|\})} = \log|\mathcal{X}|$

Proof Sketch (Achievability)

Lemma

Let $R < H(X)$ *and* $\epsilon > 0$. *Then,* $\exists\, \mathcal{U}^* = \{\boldsymbol{v}_i\}_{i \in \mathcal{M}}$ *such that*

1. $\boldsymbol{v}_i \in \mathcal{T}(p_X) \quad \forall i \in \mathcal{M}$
2. $d_H(\boldsymbol{v}_i, \boldsymbol{v}_j) \geq n\epsilon \quad \forall i \neq j$
3. $|\mathcal{M}| \geq 2^{n(R-\theta)}$

Coding Scheme

- **Enc**: given message $i \in \mathcal{M}$ transmit $x^n = \boldsymbol{v}_i$
- **Dec**: $\mathcal{D}_j = \{y^n \,:\, (\boldsymbol{v}_j, y^n) \in \mathcal{T}_\delta(p_X W)\}$
- **Error Analysis**
  1. $P_{e,1}(i) \leq 2^{-\alpha_1(\delta)n}$ by standard type class argument
  2. $P_{e,2}(i,j) \leq 2^{-n\alpha_2(\epsilon,\delta)}$ by conditional type intersection lemma

Proof Sketch (Achievability)

Lemma (Ahlswede, 1980)

Let $W : \mathcal{X} \to \mathcal{Y}$ be a channel matrix of a DMC $\mathcal{W}$ with distinct rows. Then, for every $x^n, x'^n \in \mathcal{T}_\delta(p_X)$ with $d(x^n, x'^n) \geq n\epsilon$,

$$\frac{|\mathcal{T}_\delta(p_{Y|X}|x^n) \cap \mathcal{T}_\delta(p_{Y|X}|x'^n)|}{|\mathcal{T}_\delta(p_{Y|X}|x^n)|} \leq e^{-ng(\epsilon)}$$

with $p_{Y|X} \equiv W$, for sufficiently large n and some positive function $g(\epsilon) > 0$ which is independent of n.

Proof Sketch (Converse)

Lemma

Distinct messages have distinct codewords, i.e.,

$$i_1 \neq i_2 \;\Rightarrow\; \quad \boldsymbol{u}_{i_1} \neq \boldsymbol{u}_{i_2}$$

Proof. If $\boldsymbol{u}_{i_1} = \boldsymbol{u}_{i_2} = x^n$, then

$$P_{e,1}(i_1) + P_{e,2}(i_2, i_1) = W^n(\mathcal{D}_{i_1}^c | x^n) + W^n(\mathcal{D}_{i_1} | x^n) = 1$$

Proof Sketch (Converse)

Lemma

Distinct messages have distinct codewords, i.e.,

$$i_1 \neq i_2 \;\Rightarrow\; \boldsymbol{u}_{i_1} \neq \boldsymbol{u}_{i_2}$$

Proof. If $\boldsymbol{u}_{i_1} = \boldsymbol{u}_{i_2} = x^n$, then

$$P_{e,1}(i_1) + P_{e,2}(i_2, i_1) = W^n(\mathcal{D}_{i_1}^c | x^n) + W^n(\mathcal{D}_{i_1} | x^n) = 1$$

Further Steps

- $2^{nR} \leq \left| \{x^n : n^{-1} \sum_{t=1}^n \phi(x_t) \leq A\} \right|$
- $\left| \{x^n : n^{-1} \sum_{t=1}^n \phi(x_t) \leq A\} \right| \leq 2^{n(\max_{p_X : \mathbb{E}\{\phi(X)\} \leq A} H(X) + \alpha_n)}$
  since input subspace is a union of type classes
- $R \leq \max_{p_X : \mathbb{E}\{\phi(X)\} \leq A} H(X) + \alpha_n$ for $\alpha_n \xrightarrow{n\to\infty} 0$

DI for Gaussian Channel

Theorem

[a] *Let* $\mathscr{G}$; $\mathbf{Y} = \mathbf{x} + \mathbf{Z}$ *be Gaussian channel with power constraint* $\|\mathbf{x}\|^2 \leq nA$ *and* $\mathbf{Z} \overset{iid}{\sim} \mathcal{N}(0, \sigma_Z^2)$. *Then for* $L(n, R) = 2^{nR}$, *DI capacity is given by*

$$\mathbb{C}_{DI}(\mathscr{G}, L) = \infty$$

[a] arXiv:2010.04239

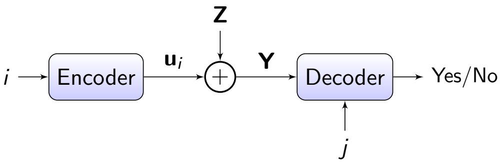


Figure 1: DI over Gaussian channel

Proof Sketch.

Proof I

- Dense sphere packing arrangement with radius $\sqrt{\epsilon}$
- *Minkowski-Hlawka Theorem* guarantees a density $\Delta \geq 2^{-n}$
- $2^{nR} = \frac{\text{Vol}\left(\bigcup_{i=1}^{2^{nR}} \mathcal{S}_{\mathbf{u}_i}(n,\sqrt{\epsilon})\right)}{\text{Vol}(\mathcal{S}_{\mathbf{u}_1}(n,\sqrt{\epsilon}))} = \Delta \cdot \frac{\text{Vol}(\mathcal{S}_{\mathbf{0}}(n,\sqrt{A}))}{\text{Vol}(\mathcal{S}_{\mathbf{u}_1}(n,\sqrt{\epsilon}))} \geq 2^{-n} \cdot \left(\frac{A}{\epsilon}\right)^{\frac{n}{2}}$
- $R \geq \frac{1}{2} \log\left(\frac{A}{\epsilon}\right) - 1 \xrightarrow{\epsilon \to 0} \infty$

Proof Sketch.

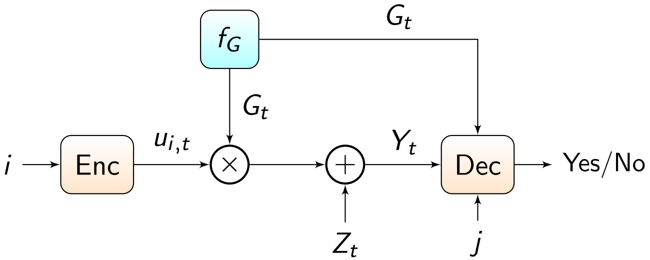
Proof I

- Dense sphere packing arrangement with radius $\sqrt{\epsilon}$
- *Minkowski-Hlawka Theorem* guarantees a density $\Delta \geq 2^{-n}$
- $2^{nR} = \frac{\text{Vol}\left(\bigcup_{i=1}^{2^{nR}} \mathcal{S}_{\mathbf{u}_i}(n,\sqrt{\epsilon})\right)}{\text{Vol}(\mathcal{S}_{\mathbf{u}_1}(n,\sqrt{\epsilon}))} = \Delta \cdot \frac{\text{Vol}(\mathcal{S}_{\mathbf{0}}(n,\sqrt{A}))}{\text{Vol}(\mathcal{S}_{\mathbf{u}_1}(n,\sqrt{\epsilon}))} \geq 2^{-n} \cdot \left(\frac{A}{\epsilon}\right)^{\frac{n}{2}}$
- $R \geq \frac{1}{2}\log\left(\frac{A}{\epsilon}\right) - 1 \xrightarrow{\epsilon \to 0} \infty$

Proof II

- Apply quantization to approximate $\mathscr{G}$ with a DMC
- $H(X^{\Delta}) \approx \frac{1}{2}\log(2\pi e A) - \frac{2}{\sqrt{2\pi A}}\Delta + \log\frac{1}{\Delta}$
- $R \xrightarrow{\Delta \to 0^+} \infty$

DI for Fading Channel



Definitions

- Fast fading → $\mathbf{Y} = \mathbf{G} \circ \mathbf{x} + \mathbf{Z}$ where $\mathbf{G} = (G_t)_{t=1}^{\infty} \overset{iid}{\sim} f_G$
- Slow fading → $Y_t = Gx_t + Z_t$ where $G \sim f_G$
- Power const. → $\|\mathbf{x}\| \leq \sqrt{nA}$, Noise → $\mathbf{Z} \overset{iid}{\sim} \mathcal{N}(0, \sigma_Z^2)$
- $\mathcal{G} \triangleq$ set of fading coefficient values

DI for Fast Fading Channel

Theorem

[a] *Let $\mathscr{G}_{fast}$ be fast fading channel with positive fading coefficients. Then the DI capacity for $L(n,R) = 2^{n\log(n)R}$ is given by*

$$\frac{1}{4} \leq \mathbb{C}_{DI}(\mathscr{G}_{fast}, L) \leq 1$$

[a] arXiv:2010.10010

DI for Fast Fading Channel

Theorem

[a] *Let $\mathscr{G}_{fast}$ be fast fading channel with positive fading coefficients. Then the DI capacity for $L(n,R) = 2^{n\log(n)R}$ is given by*

$$\frac{1}{4} \leq \mathbb{C}_{DI}(\mathscr{G}_{fast}, L) \leq 1$$

[a] arXiv:2010.10010

Corollary (Traditional Scales)

DI capacity in traditional scales is given by

$$\mathbb{C}_{DI}(\mathscr{G}_{fast}, L) = \begin{cases} \infty & \text{for } L(n,R) = 2^{nR} \\ 0 & \text{for } L(n,R) = 2^{2^{nR}} \end{cases}$$

- Standard Gaussian channel is a special case
- To prove lower-bound, we pack sphere of radius $\sqrt{n\epsilon_n} \sim n^{\frac{1}{4}}$, which results in $\sim 2^{\frac{1}{4}n\log(n)}$ codewords

DI for Slow Fading Channel

Theorem

[a] *Let $\mathscr{G}_{slow}$ be slow fading Gaussian channel. Then DI capacity for $L(n,R) = 2^{n\log(n)R}$ is given by*

$$\begin{array}{ll} \frac{1}{4} \leq \mathbb{C}_{DI}(\mathscr{G}_{slow}, L) \leq 1 & \text{if } 0 \notin cl(\mathcal{G}) \\ \mathbb{C}_{DI}(\mathscr{G}_{slow}, L) = 0 & \text{if } 0 \in cl(\mathcal{G}) \end{array}$$

[a] arXiv:2010.10010

DI for Slow Fading Channel

Theorem

[a] *Let $\mathscr{G}_{slow}$ be slow fading Gaussian channel. Then DI capacity for $L(n,R) = 2^{n\log(n)R}$ is given by*

$$\begin{aligned} &\tfrac{1}{4} \le \mathbb{C}_{DI}(\mathscr{G}_{slow}, L) \le 1 && \text{if } 0 \notin cl(\mathcal{G}) \\ &\mathbb{C}_{DI}(\mathscr{G}_{slow}, L) = 0 && \text{if } 0 \in cl(\mathcal{G}) \end{aligned}$$

[a] arXiv:2010.10010

Corollary (Traditional Scales)

DI capacity in traditional scales is given by

$$\mathbb{C}_{DI}(\mathscr{G}_{slow}, L) = \begin{cases} 0 & \text{if } 0 \in cl(\mathcal{G}) \\ \infty & \text{if } 0 \notin cl(\mathcal{G}) \end{cases}, \quad \text{for } L(n,R) = 2^{nR}$$

$$\mathbb{C}_{DI}(\mathscr{G}_{slow}, L) = 0\,, \quad \text{for } L(n,R) = 2^{2^{nR}}$$

Discontinuity of DI Capacity

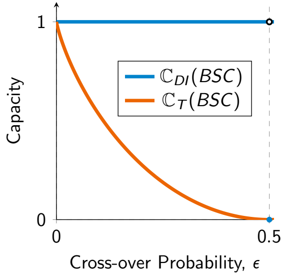
Binary Symmetric Channel

- For $\epsilon < \frac{1}{2}$ (arbitrary close to $\frac{1}{2}$): $W = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix} \Rightarrow$
  $\mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 2 = 1$
- For $\epsilon = \frac{1}{2}$, it is a pure noise channel, and $W = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix} \Rightarrow$
  $\mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 1 = 0$

Discontinuity of DI Capacity

Binary Symmetric Channel

- For $\epsilon < \frac{1}{2}$ (arbitrary close to $\frac{1}{2}$): $W = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix} \Rightarrow$
  $\mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 2 = 1$
- For $\epsilon = \frac{1}{2}$, it is a pure noise channel, and $W = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix} \Rightarrow$
  $\mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 1 = 0$



Outline

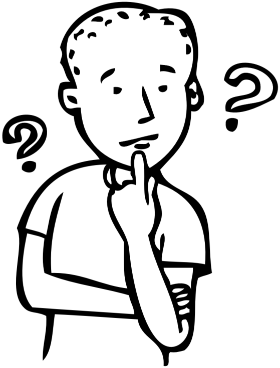
Conclusions

- We have determined DI capacity for
  1. DMC $\rightarrow 2^{nC}$ behavior
  2. Fading $\rightarrow 2^{n\log(n)C} = n^{nC}$ behavior

  As opposed to $2^{2^{nR}}$ for random identification
- Future directions
  1. Multi-user scenarios
  2. Molecular communication channel (with memory)
  3. Finite block-length regime

Discussion

Thank You!



ϵ-DI Capacity for DMC

Theorem (Ahlswede et al, 1989 ; Burnashev, 2000)

For a DMC $\mathcal{W}$ with $L(n,R) = 2^{2^{nR}}$, the ϵ-DI Capacity for $\epsilon \in [0, \frac{1}{2})$ are given by

$$\mathbb{C}^{\epsilon}_{RI}(\mathcal{W}, L) = \mathbb{C}_{RI}(\mathcal{W}, L) = \max_{p_X} I(X;Y)$$

$$\mathbb{C}^{\epsilon}_{DI}(\mathcal{W}, L) = \mathbb{C}_{DI}(\mathcal{W}, L) = 0$$

Theorem (Ahlswede et al, 1989)

ϵ-DI and ϵ-RI achievable rate with $L(n,R) = 2^{2^{nR}}$ for $\epsilon \geq \frac{1}{2}$ can be made arbitrary large, i.e.,

$$\mathbb{C}^{\epsilon}_{DI}(\mathcal{W}, L) = \mathbb{C}^{\epsilon}_{RI}(\mathcal{W}, L) = \infty$$

Proof $\rightarrow$ Decoder flips a **fair coin**

ϵ-DI Capacity for Gaussian Channel

Theorem (Burnashev, 2000)

For a Gaussian channel with $L(n, R) = 2^{2^{nR}}$, the ϵ-DI capacity for $\epsilon \geq \frac{1}{2}$ is given by

$$\mathbb{C}^{\epsilon}_{DI}(\mathscr{G}, L) = \mathbb{C}^{\epsilon}_{RI}(\mathscr{G}, L) = \infty$$

Theorem (Labidi et al, 2020)

For a Gaussian channel under input constraint $\|\mathbf{x}\|^2 \leq nA$ with $L(n, R) = 2^{2^{nR}}$, the ϵ-DI capacity for $\epsilon \in [0, \frac{1}{2})$ is given by

$$\mathbb{C}^{\epsilon}_{RI}(\mathscr{G}, L) = \mathbb{C}_{RI}(\mathscr{G}, L) = \frac{1}{2} \log\left(1 + \frac{A}{\sigma_Z^2}\right)$$

DI for Compound Channel

1. Let $\mathcal{V} = \{V(.|.,s) \ : \ s \in \mathcal{S}\}_{|\mathcal{S}|<\infty}$ be a compound channel
2. Each $V(.|.,s)$ induces a partition $\{\mathcal{X}(1|s),\ldots,\mathcal{X}(j_s|s)\}$ of $\mathcal{X}$ with

$$x, x' \in \mathcal{X}(.|s) \iff V(.|x,s) = V(.|x',s)$$

3. Any RV X taking values in $\mathcal{X}$ induces a RV $\hat{X}(s)$ s.t.

$$\hat{X}(s) = k \iff X \in \mathcal{X}(k|s) \text{ for } k \in [1:j_s]$$

Theorem (Ahlswede and Cai, 1999)

$$C_{DI}(\mathcal{V}, L) = \max_X \min_s H(\hat{X}(s)) \quad \textit{for } L(n,R) = 2^{nR}$$

DI for AVC

Theorem (Ahlswede and Cai, 1999)

1. *Let* $P \in \mathcal{P}(\mathcal{X})$ *and* $\overline{\overline{\mathcal{A}}}$ *be the row-convex closure of* $\mathcal{A}$
2. *Set* $\mathcal{Q}(P, \mathcal{A}) = \{(X, X', Y) : P_{Y|X}, P_{Y|X'} \in \overline{\overline{\mathcal{A}}}, P_X = P_{X'} = P, X \to X' \to Y\}$

then

$$C_{DI}(\mathcal{A}) \geq \max_{P} \min_{(X,X',Y) \in \mathcal{Q}(\mathcal{P},\mathcal{A})} I(X' \wedge XY)$$

DI Capacity of AVC I

- For every fixed $x \in \mathcal{X}$ define

$$\mathcal{A}_1(x) = \{A(.|x, s) : s \in \mathcal{S}\}$$

as set of PDs on $\mathcal{Y}$ where $\mathcal{A}_1 = \{A(.|., \ s) : s \in \mathcal{S}\}$

- Define $\overline{A}(x)$ as **convex closure** of $\mathcal{A}_1(x)$ i.e. of entries in form

$$\sum_{s \in \tilde{\mathcal{S}}} P(s) A(y|x, s)$$

DI Capacity of AVC II

- Define **row-convex closure** of $\mathcal{A}$ denote by $\overline{\overline{\mathcal{A}}}$ as follows:

$$\overline{\overline{\mathcal{A}}} = \{(A(y|x))_{x\in\mathcal{X},y\in\mathcal{Y}} : A(.|x) \in \overline{A}(x)\}$$

$\overline{\overline{\mathcal{A}}}$ has entries of form:

$$\sum_{s\in\tilde{\mathcal{S}}} P(s|x)A(y|x,s)$$

$P(s|x)$ means that coefficient are conditioned on choice of x, i.e., for every different x there would be in general a complete different set of coefficients than that of required for defining entries of $\overline{A}(x)$

DI Codes for Gaussian Channel

Cost Constraints

1. Average power constraint:

$$\frac{1}{n}\sum_{1}^{n}|x_t|^2 \leq P \iff \|x^n\|_2 \leq \sqrt{nP}$$

2. Peak power constraint:

$$\max_{1\leq t\leq n}|x_t| \leq A \iff \|x^n\|_\infty \leq A$$

DI Capacity Results

Theorem (JáJá, 1985)

For Binary Symmetric Channel (BSC) with $\epsilon \neq 0.5$, the DI with rate arbitrarily close to 1 is possible, i.e,

$$\mathbb{C}_{DI}(BSC) = 1$$

Theorem (Ahlswede, 1989)

For DMC $\mathcal{W}$ with stochastic matrix W, let n_{row} be # of distinct rows in W, then the DI capacity is given by

$$\mathbb{C}_{DI}(\mathcal{W}) = \log \left(n_{row}[W] \right)$$

Geometry of RI Codes