# Deterministic Identification

Mohammad J. Salariseddigh

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

Nov 11 2020

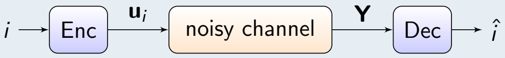
# Outline

# Outline

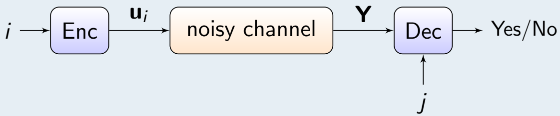
1. Motivation
2. Main Contributions
3. Definitions
   - Transmission
   - Deterministic Identification
   - Randomized Identification
4. Main Results
   - Deterministic Identification for DMC
   - Deterministic Identification for Gaussian Channel
5. Conclusions

# Transmission vs. Identification

- Shannon's setting: Bob recover the message




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




## Applications

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

# Randomized Identification [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 $n = 821 \rightarrow 2^{2^{8.21}} > \#$ atoms in universe

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

# Deterministic Identification [2]

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

## Why deterministic?

- Deterministic codes pros
  - Suitable for molecular communication
  - Suitable for Jamming scenarios
- Randomized identification cons
  - Process strings of exponential length
  - Enormous amount of randomness
  - Not easy to implement

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

# Outline

1. Motivation
2. Main Contributions
3. Definitions
   - Transmission
   - Deterministic Identification
   - Randomized Identification
4. Main Results
   - Deterministic Identification for DMC
   - Deterministic Identification for Gaussian Channel
5. Conclusions

# Main Contributions

- We established the deterministic identification capacity for channels with power constraints:
  - DMC
  - Fast Fading
  - Slow Fading
- We show that the code size scales as $\sim 2^{nR}$ for the DMC and as $\sim 2^{n\log(n)R} = n^{nR}$ for the Gaussian channel
- 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] 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. $L(n,R) = 2^{nR}$
2. $\boldsymbol{u_i} \in \mathcal{X}^n, \mathcal{D}_i \subset \mathcal{Y}^n$
3. $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$
4. $W^n(\mathcal{D}_i|\boldsymbol{u_i}) \geq 1-\varepsilon$
5. $\mathcal{D}_i \underset{i\neq j}{\cap} \mathcal{D}_j = \emptyset$

[a] Ahlswede, R. "General theory of information transfer", 2005

# Transmission

**Definition (Achievable Rate)**

Rate $R$ is said to be achievable if there exist an $(n, M_n, \varepsilon_n)$-code satisfying

$$\lim_{n\to\infty} \varepsilon_n = 0 \text{ and } \limsup_{n\to\infty} \frac{1}{n} \log(M_n) \geq R$$

**Definition (Channel Capacity)**

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

**Theorem (Shannon, 1948)**

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

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

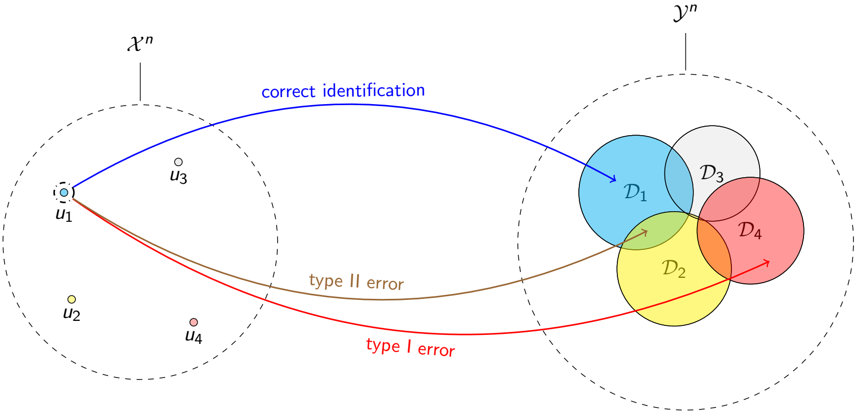
# Deterministic Identification Codes

**Definition (Ahlswede and Cai, 1999)**

A $(L(n,R), n, \lambda_1, \lambda_2)$-deterministic identification code for DMC $\mathcal{W}$ is a system $\{(\boldsymbol{u}, \mathcal{D}_{\boldsymbol{u}})\}_{\boldsymbol{u}\in\mathcal{U}}$ subject to

1. $L(n,R) = 2^{nR}$
2. $\mathcal{U} \subset \mathcal{X}^n, \ \mathcal{D}_{\boldsymbol{u}} \subset \mathcal{Y}^n, \ |\mathcal{U}| = 2^{nR}$
3. $\frac{1}{n}\sum_{t=1}^{n} \phi(u_{i,t}) \leq A$
4. $W^n(\mathcal{D}_{\boldsymbol{u}_i}|\boldsymbol{u}_i) > 1 - \lambda_1$
5. $W^n(\mathcal{D}_{\boldsymbol{u}_i}|\boldsymbol{u}_j) \underset{\boldsymbol{u}_i \neq \boldsymbol{u}_j}{<} \lambda_2$

# Geometry of Deterministic Identification Codes



# Randomized Identification Codes

**Definition (Ahlswede and Dueck, 1989)**

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

1. $L(n,R) = 2^{2^{nR}}$
2. $Q_i \in \mathcal{P}\left(\mathcal{X}^n\right), \mathcal{D}_i \subset \mathcal{Y}^n$
3. $Q_i W^n(\mathcal{D}_i) > 1 - \lambda_1$
4. $Q_j W^n(\mathcal{D}_i) \underset{i\neq j}{<} \lambda_2$

# Outline

# Deterministic Identification Capacity of DMC

## Theorem

[a] *Let $\mathcal{W}$ be a DMC with distinct rows in channel matrix. Then with constraint $\mathbb{E}[\phi(X)]$ and $L(n,R) = 2^{nR}$, deterministic identification capacity 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

# Deterministic Identification 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 $L(n, R) = 2^{nR}$, deterministic identification capacity is given by*

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

- A proof was not provided

# 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. $P_{e,1}(i) \leq e^{-\alpha_1(\delta)n}$ by standard type class argument
  2. $P_{e,2}(i,j) \leq e^{-n\alpha_2(\epsilon,\delta)}$ 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.,*

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

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

- $2^{nR} \leq \left| \{x^n : n^{-1} \sum_{t=1}^n \phi(x_t) \leq A\} \right|$
- $\left| \{x^n : n^{-1} \sum_{t=1}^n \phi(x_t) \leq A\} \right| \leq 2^{n(H(X)+\alpha_n)}$
  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 $\alpha_n \xrightarrow{n\to\infty} 0$

# Deterministic Identification 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* $L(n, R) = 2^{nR}$, *deterministic identification capacity is given by*

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

[a] arXiv:2010.04239

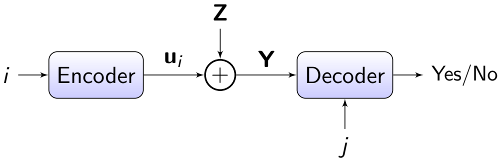



Figure 1: Deterministic identification over Gaussian channel

# Proof Sketch.

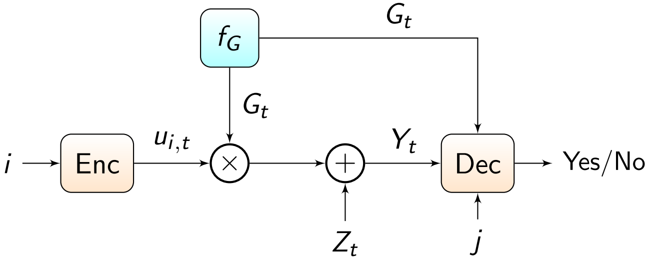
## Proof I

- 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 II

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

# Deterministic Identification for Fading Channel




## Definitions

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

# Deterministic Identification for Fast Fading Channel

**Theorem**

[a] *Let $\mathscr{G}_{fast}$ be fast fading Gaussian channel with positive fading coefficients. Then deterministic identification 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)**

*Deterministic identification capacity in traditional scales is given by*

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

# Deterministic Identification for Slow Fading Channel

## Theorem

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

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

[a] arXiv:2010.10010

## Corollary (Traditional Scales)

*Deterministic identification 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 Deterministic Identification Capacity

## Binary Symmetric Channel

- For $\epsilon$ arbitrary close to $\frac{1}{2}$:

  $W = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix} \Rightarrow \mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 2 = 1$

- Now let $\epsilon = \frac{1}{2}$, then

  $W = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix} \Rightarrow \mathbb{C}_{DI}(BSC) = \log\left(n_{row}[W]\right) = \log 1 = 0$

$$1 = \lim_{\epsilon \to \frac{1}{2}} \mathbb{C}_{DI}(BSC) \neq \mathbb{C}_{DI}(BSC)\Big|_{\epsilon = \frac{1}{2}} = 0$$

□

# Outline

# Conclusions

- Survey of deterministic and randomized identification results for DMC, Gaussian and Fading
- We have determined deterministic identification capacity for
  1. DMC $\rightarrow 2^{nC}$ behavior
  2. Fading $\rightarrow 2^{n\log(n)C} = n^{nC}$ behavior
- Future directions
  1. Multi-user scenarios
  2. Finite block-length regime
  3. Wiretap channel
  4. Molecular communication channel (with memory)

# Discussion

Thank you! Questions?

# Deterministic Identification Capacity of AVC I

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

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

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

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

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

# Deterministic Identification Capacity of AVC II

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

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

$\overline{\overline{\mathcal{A}}}$ 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 $\overline{A}(x)$

# Deterministic Identification 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:

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

# Deterministic Identification 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,*

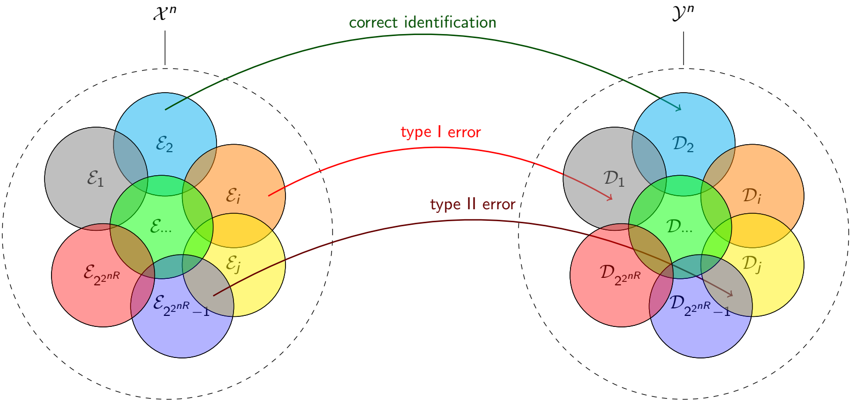
$$\mathbb{C}_{DI}(BSC) = 1$$

**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 Randomized Identification Codes



# Deterministic $\epsilon$-Identification Capacity for DMC

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

*For DMC $\mathcal{W}$, in the double exponential scale, $L(n,R) = 2^{2^{nR}}$, the deterministic $\epsilon$-Identification 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)**

*The deterministic and randomized $\epsilon$-identification achievable rate for $\epsilon \geq \frac{1}{2}$, in the double exponential scale, $L(n,R) = 2^{2^{nR}}$ can be made arbitrary large, i.e.,*

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

Proof $\rightarrow$ flip a **fair coin**

# Deterministic $\epsilon$-Identification Capacity for Gaussian Channel

## Theorem (Burnashev, 2000)

*For Gaussian chanel, in the double exponential scale, i.e., $L(n,R) = 2^{2^{nR}}$, the deterministic $\epsilon$-Identification 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 Gaussian chanel with power constraint $\|\mathbf{x}\|^2 \leq nA$ in the double exponential scale, i.e., $L(n,R) = 2^{2^{nR}}$, the deterministic $\epsilon$-Identification Capacity for $\epsilon \in [0, \frac{1}{2})$ is given by*

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