# Communication & Compound-State Identification in Compound Arbitrarily Varying Channels

**Syomantak Chaudhuri**
Roll Number: 170070004

With Neha Sangwan, TIFR
Mayank Bakshi, Hong Kong
Guides: Prof. Bikash Dey, IITB & Prof. Vinod Prabhakaran, TIFR

May 9, 2021

Electrical Engineering Department
Indian Institute of Technology Bombay

# Introduction

# Arbitrarily Varying Channel

- Unknown parameter to capture changes in the channel
- Channel can be described using stochastic matrix $W : \mathcal{X} \times \mathcal{S} \to \mathcal{Y}$
- $W(y|x, s)$
- $n$-length transmission sequence described using stochastic matrix $W^n : \mathcal{X}^n \times \mathcal{S}^n \to \mathcal{Y}^n$
- Memoryless
- If the input sequence is $\boldsymbol{x}$ and the state sequence is $\boldsymbol{s}$, then probability of output sequence $\boldsymbol{y}$ is given by

$$W^n(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{s}) = \prod_{i=1}^{n} W(y_i|x_i, s_i)$$

# Diagram

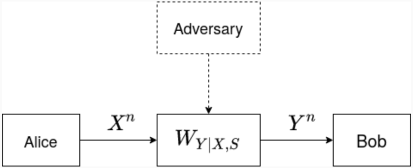


**Figure 1:** Classical AVC

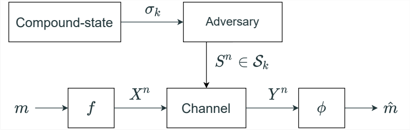


**Figure 2:** Proposed CAVC

# Compound Arbitrarily Varying Channel

- Two compound states, each has state symbols in the set $\mathcal{S}_i$
- Only one active during the transmission of a block
- Channel represented as $W : \mathcal{X} \times (\mathcal{S}_1 \cup \mathcal{S}_2) \to \mathcal{Y}$
- $\overline{\mathcal{W}}_i := \{\sum_s P(s) W_{Y|X,S=s} : P$ has support over $\mathcal{S}_i\})$
- Questions -
  - Communication
  - Compound state identification
  - Communication & compound state identification
  - Communication or compound state identification

# Random Coding Regime

# Communication (all proofs in BTP report)

- If compound-state can switch during transmission, then it is equivalent to an AVC with capacity

$$\max_{P_X} \underline{\min_{W \in \mathcal{W}_1 \cup \mathcal{W}_2}} I(X;Y)$$

**Theorem**

$$C^{\mathsf{r}}_{\mathsf{com}} = \max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cup \overline{\mathcal{W}}_2} I(X;Y).$$

- Choose $R, \delta > 0$ and $R + \delta < C^{\mathsf{r}}_{\mathsf{com}}$. Sample $2^{nR}$ codewords from $\tau_X$, $X \sim P_X$
- Decode message as $i$ if $I(X;Y) \geq R + \delta$ where $P_{XY} = P_{\boldsymbol{X}_i, \boldsymbol{y}}$

# Compound-State Identification

**Theorem**

*$\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$ is necessary and sufficient condition for compound-state identification.*

Achievability:

- send $\boldsymbol{x}$ i.i.d. $P_X$, w.h.p. $(\boldsymbol{f}, \boldsymbol{y}) \in \tau^{\epsilon}_{XY}$ where $P_{XY} = P_X \times Z_{Y|X}$

$$Z_{Y|X} = \frac{1}{n} \sum_{k \in \mathcal{S}_1} |\text{occurrences of } k \text{ in } \boldsymbol{s}| W_{Y|X,S=k} \in \overline{\mathcal{W}}_1$$

- Existence of another $\tilde{Z}_{Y|X} \in \overline{\mathcal{W}}_2$ for sufficiently small $\epsilon$ violates $\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$

# Communication and Compound-State Identification

**Theorem**

*If* $\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$*, then* $C^{\mathsf{r}}_{\mathsf{and}} = \max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cup \overline{\mathcal{W}}_2} I(X;Y)$.

- Constant vector $\tilde{\boldsymbol{x}}$ has $\log(n)$ repetitions of symbols of $\mathcal{X}$
- $\boldsymbol{X}_i = \Gamma(F_{\mathsf{com}}(i), \tilde{\boldsymbol{x}})$
- At decoder, use $\Gamma^{-1}$ to obtain $(\hat{\boldsymbol{y}}, \tilde{\boldsymbol{y}})$
- Random $\Gamma()$ ensures attack is identical in both parts of transmission

# Communication or Compound-State Identification

**Theorem**

$$C_{\mathsf{or}}^{\mathsf{r}} = \max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2} I(X;Y).$$

- Same encoding scheme as previous slide - communication encoder works at a different rate
- If attack sequence induces a channel in $\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2$, communication decoder works
- Else, communication decoder can not decode (but won't output wrong message)
- Use compound-state identification scheme for this case

# Deterministic Coding Regime

# Definitions

**Trans-symmetrizable**: if there exists some distributions $U(.|x)$ with support in $\mathcal{S}_1$ and $V(.|x)$ with support in $\mathcal{S}_2$ such that

$$\sum_s W(y|x,s)U(s|x') = \sum_s W(y|x',s)V(s|x) \qquad \forall y,x,x'$$

**Cis-symmetrizable** if there exists some distributions $U(.|x)$ and $V(.|x)$ both with support in $\mathcal{S}_i$ $(i \in \{1,2\})$ such that

$$\sum_s W(y|x,s)U(s|x') = \sum_s W(y|x',s)V(s|x) \qquad \forall y,x,x'$$

- any-symmetrizable

# Communication

**Theorem**

$C^{\mathsf{d}}_{\mathsf{com}} > 0$ *iff the CAVC is non-any-symmetrizable. If* $C^{\mathsf{d}}_{\mathsf{com}} > 0$, $C^{\mathsf{d}}_{\mathsf{com}} = C^{\mathsf{r}}_{\mathsf{com}}$.

- Existence of a 'nice' codebook $\boldsymbol{x}_1, \dots, \boldsymbol{x}_M$

Define

$$\mathcal{C}_\eta = \{P_{XSY} : D(P_{XSY} || P_X \times P_S \times W) \leq \eta,\ P_S \in \mathcal{P}_1 \cup \mathcal{P}_2\}.$$

Decoder: $\phi(\boldsymbol{y}) = i$ iff an $\boldsymbol{s} \in \mathcal{S}_1^n \cup \mathcal{S}_2^n$ exists such that:

1. the joint type $P_{\boldsymbol{x}_i, \boldsymbol{s}, \boldsymbol{y}}$ belongs to $\mathcal{C}_\eta$, and,
2. for each competitor $\boldsymbol{x}_j$ (and corresponding $\boldsymbol{s}'$), such that $P_{\boldsymbol{x}_j, \boldsymbol{s}', \boldsymbol{y}} \in \mathcal{C}_\eta$, we have $X' \longleftrightarrow S \longleftrightarrow XY$ $((I(X'; XY|S) \leq \eta)$.

# Compound-State Identification

**Theorem**

*Compound-State Identification is feasible iff* $\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$ *and the CAVC is non-trans-symmetrizable.*

- Existence of a 'nice' codebook $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M$
- Purpose of the messages if to only impart stochasticity to the system

Decoder: $\phi(\boldsymbol{y}) = \sigma_k$ iff an $\boldsymbol{s} \in \mathcal{S}_k^n$ and $\boldsymbol{x}_i$ exists such that:

1. the joint type $P_{\boldsymbol{x}_i, \boldsymbol{s}, \boldsymbol{y}}$ belongs to $\mathcal{C}_\eta$, and,
2. for each competitor $\boldsymbol{s}' \in \mathcal{S}_{3-k}^n$ and $\boldsymbol{x}_j$, such that $P_{\boldsymbol{x}_j, \boldsymbol{s}', \boldsymbol{y}} \in \mathcal{C}_\eta$, we have $X' \longleftrightarrow S \longleftrightarrow XY$.

# Communication and Compound-State Identification

**Theorem**

*$C^{\mathsf{d}}_{\mathsf{and}} > 0$ iff the $\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$ and the CAVC is non-any-symmetrizable. If $C^{\mathsf{d}}_{\mathsf{and}} > 0$, $C^{\mathsf{d}}_{\mathsf{and}} = C^{\mathsf{r}}_{\mathsf{and}}$.*

- Existence of a 'nice' codebook $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M$

Decoder: $\phi(\boldsymbol{y}) = (i, \sigma_k)$ iff an $\boldsymbol{s} \in \mathcal{S}_k^n$ exists such that:

1. the joint type $P_{\boldsymbol{x}_i, \boldsymbol{s}, \boldsymbol{y}}$ belongs to $\mathcal{C}_\eta$, and,
2. for each competitor $\boldsymbol{s}' \in \mathcal{S}_{3-k}^n$ and $\boldsymbol{x}_j$, such that $P_{\boldsymbol{x}', \boldsymbol{s}', \boldsymbol{y}} \in \mathcal{C}_\eta$, we have $X' \longleftrightarrow S \longleftrightarrow XY$.

# Communication or Compound-State Identification

**Theorem**

$C^{\mathsf{d}}_{\mathsf{or}} > 0$ *iff the CAVC is non-trans-symmetrizable.*

- Existence of a 'nice' codebook $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M$

Decoder used to show $C^{\mathsf{d}}_{\mathsf{or}} > 0$: Let $B_k, k = 1, 2$ be sets of messages. $m \in B_k$ if:

1. $\exists \boldsymbol{s}\ in \mathcal{S}_k^n$, $P_{\boldsymbol{x}_m, \boldsymbol{s}, \boldsymbol{y}}$ belongs to $\mathcal{C}_\eta$, and
2. for every $m' \neq m$ such that $\exists \boldsymbol{s}' \in \mathcal{S}_{3-k}^n$, $P_{\boldsymbol{x}_{m'}, \boldsymbol{s}', \boldsymbol{y}} \in \mathcal{C}_\eta$, we have $X' \longleftrightarrow S \longleftrightarrow XY$.

- If $B_1 = B_2 = \{m\}$, $\phi(\boldsymbol{y}) = m$
- If $|B_k| = 0 < |B_{3-k}|$, $\phi(\boldsymbol{y}) = \sigma_{3-k}$

# Conclusions

# Results Summarized (Published Work - ISIT 2021)

| **Task** | **Conditions for positive deterministic capacity** | **Capacity expression** |
|---|---|---|
| Communication | Non-any-sym. | $\max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cup \overline{\mathcal{W}}_2} I(X;Y)$ |
| Compound-State Identification | Non-trans-sym.<br>$\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$ | - |
| Communication<br>and<br>Compound-State Identification | Non-any-sym.<br>$\overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2 = \emptyset$ | $\max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cup \overline{\mathcal{W}}_2} I(X;Y)$ |
| Communication<br>or<br>Compound-State Identification | Non-trans-sym. | $\max_{P_X} \min_{W \in \overline{\mathcal{W}}_1 \cap \overline{\mathcal{W}}_2} I(X;Y)$ |

# Generalization: $k > 2$ Compound States (Unpublished)

- $C^{\mathsf{r}}_{\mathsf{com}} = \max_{P_X} \min_{W \in \bigcup_k \overline{\mathcal{W}}_k} I(X;Y)$
- Compound-State identification feasible if $\bigcup_{i \neq j} \overline{\mathcal{W}}_i \cap \overline{\mathcal{W}}_j = \emptyset$
- $C^{\mathsf{r}}_{\mathsf{or}} = \max_{P_X} \min_{W \in \bigcup_{i \neq j} \overline{\mathcal{W}}_i \cap \overline{\mathcal{W}}_j} I(X;Y)$
- Define $i, j$-symmetrizability
- $C^{\mathsf{d}}_{\mathsf{com}} > 0$ iff CAVC is non-$i, j$-symmetrizable $\forall i, j$ (any)
- Compound-State identification feasible if $\bigcup_{i \neq j} \overline{\mathcal{W}}_i \cap \overline{\mathcal{W}}_j = \emptyset$ and non-$i, j$-symmetrizable $\forall i \neq j$ (trans)
- $C^{\mathsf{d}}_{\mathsf{and}} > 0$ iff non-any-symmetrizable and $\bigcup_{i \neq j} \overline{\mathcal{W}}_i \cap \overline{\mathcal{W}}_j = \emptyset$
- $C^{\mathsf{d}}_{\mathsf{or}}$ - not yet worked out (doable!)

# Error Exponent Analysis

- Given rate $R$ of communication, what's the best possible error exponent for compound-state identification?
- We give a lower bound based on an achievability scheme
- Converse - upper bound on the error exponent for compound-state identification (no communication required)
- If the input to the channel is i.i.d. $P_X$, the pair $(X,Y)_i \sim P_X W^{(i)}_{Y|X}$
- Non-stationary composite hypothesis testing problem - can take adversary to be operating with i.i.d. attack
- If input vector $\boldsymbol{x}$ is not i.i.d., then non-independent samples - complicated!

# Thank You!