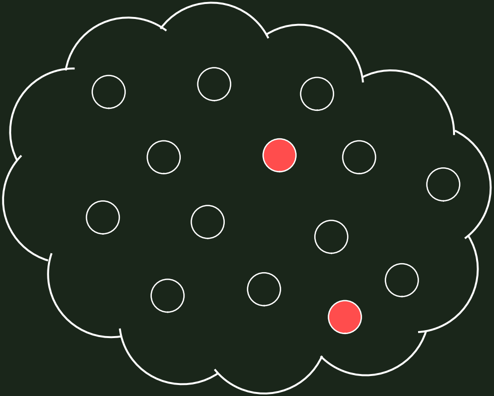
Network Equivalence in the Presence of Active Adversaries

Oliver Kosut

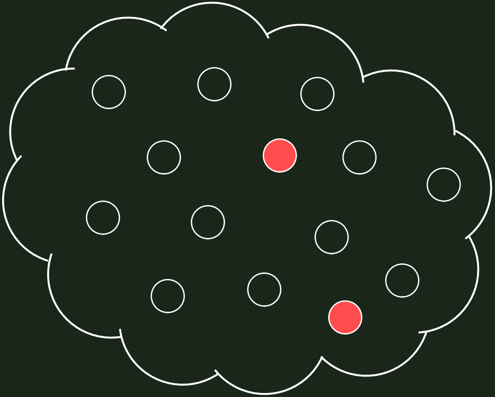
joint work with Jörg Kliewer

December 17, 2015

Networks with Active Adversaries



Networks with Active Adversaries



Two kinds of unknowns:

- Adversary's location — changes slowly
- Adversary's transmission — changes quickly

Joint Compound Channel / Arbitrarily Varying Channel

Network modeled by:

$$p\left(y_1, y_2, \ldots, y_m \,\middle|\, x_1, x_2, \ldots, x_m, s_{\mathsf{CC}}, s_{\mathsf{AVC}}\right)$$

- s_{CC} is a compound channel-type state
  — fixed across coding block
- s_{AVC} is an arbitrarily varying channel-type state
  — arbitrary across coding block

Joint Compound Channel / Arbitrarily Varying Channel

Network modeled by:

$$p\left(y_1, y_2, \ldots, y_m \,\middle|\, x_1, x_2, \ldots, x_m, s_{\mathsf{CC}}, s_{\mathsf{AVC}}\right)$$

- s_{CC} is a compound channel-type state
  — fixed across coding block
- s_{AVC} is an arbitrarily varying channel-type state
  — arbitrary across coding block

Difficulties:

- Multiple sources
- Complex noisy network
- Adversarial choices

Joint Compound Channel / Arbitrarily Varying Channel

Network modeled by:

$$p\left(y_1, y_2, \ldots, y_m \,\middle|\, x_1, x_2, \ldots, x_m, s_{\mathsf{CC}}, s_{\mathsf{AVC}}\right)$$

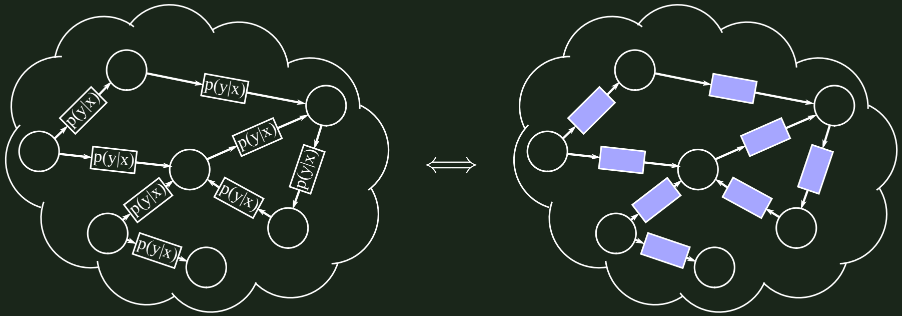
- s_{CC} is a compound channel-type state
  — fixed across coding block
- s_{AVC} is an arbitrarily varying channel-type state
  — arbitrary across coding block

Difficulties:

- Multiple sources
- Complex noisy network
- Adversarial choices $\Longleftarrow$ **Eliminate this!**

Network Equivalence

Koetter-Effros-Médard (2011):



- Each channel replaced by a bit-pipe with the same capacity
- Networks are equivalent in that the capacity regions are the same, for arbitrary multicast requirements
- Separation between channel coding and network coding

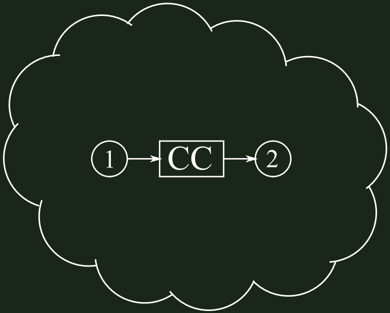
Most related work on network equivalence

- Koetter-Effros-Médard part II — multiterminal channels
- Dikaliotis-Yao-Ho-Effros-Kliewer (2012) — eavesdropper
- Bakshi-Effros-Ho (2011) — active adversary replaces the output of an unknown subset of channels

Outline

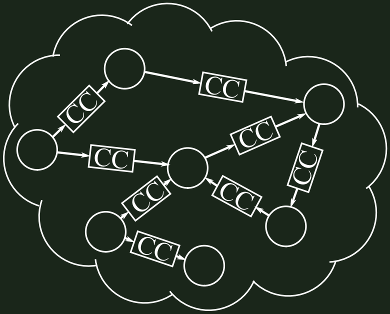
- Network equivalence results for compound channels
- Network equivalence results for arbitrarily varying channels
- Network equivalence results for joint CC/AVC model

Compound Channel Model



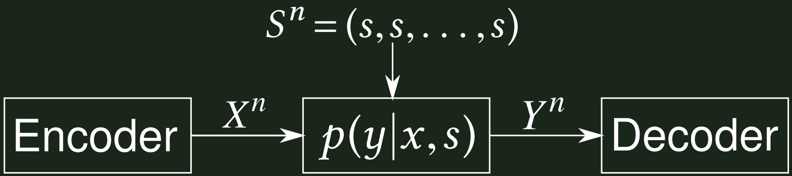
- Point-to-point compound channel, independent of the rest of the network, with independent state

Compound Channel Model

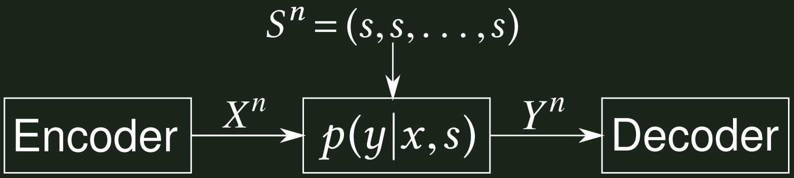


- Point-to-point compound channel, independent of the rest of the network, with independent state

Point-to-Point Compound Channel

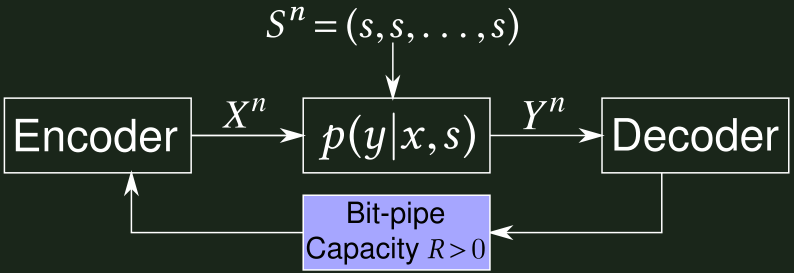


Point-to-Point Compound Channel



Capacity $= \max_{p(x)} \min_{s} I(X;Y|S=s)$

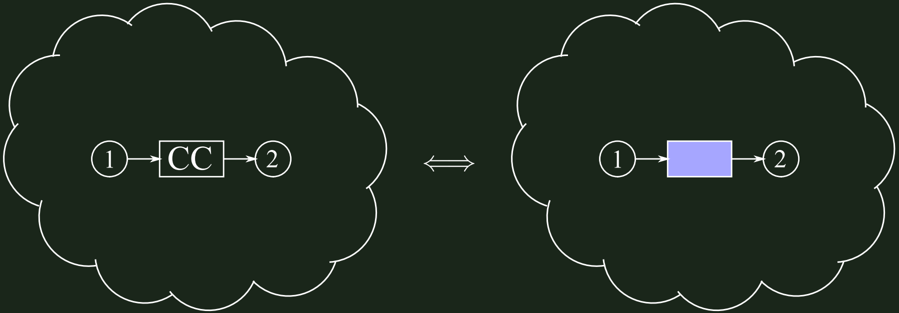
Point-to-Point Compound Channel



Capacity $= \max_{p(x)} \min_{s} I(X;Y|S=s)$

Feedback capacity $= \min_{s} \max_{p(x)} I(X;Y|S=s)$

Equivalence for Compound Channels

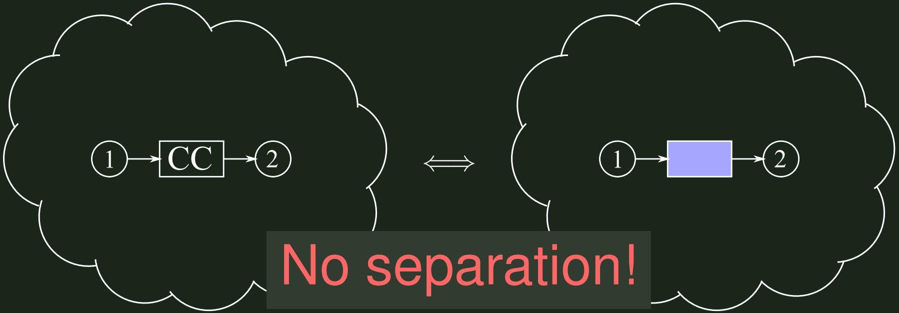


Theorem (KK-15)

Point-to-point compound channel between node 1 and 2 is equivalent to bit-pipe of capacity

$$\min_{s} \max_{p(x)} I(X;Y|S=s) \quad \textit{if the network allows feedback,}$$
$$\max_{p(x)} \min_{s} I(X;Y|S=s) \quad \textit{otherwise.}$$

Equivalence for Compound Channels



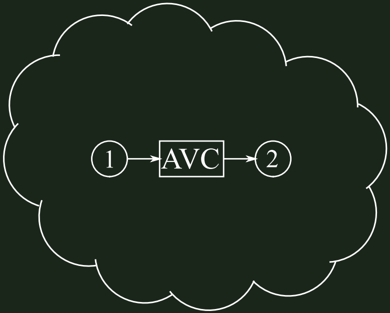
No separation!

Theorem (KK-15)

Point-to-point compound channel between node 1 and 2 is equivalent to bit-pipe of capacity

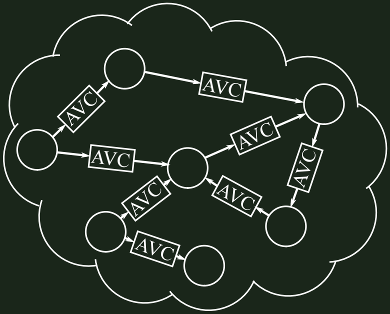
$$\min_{s} \max_{p(x)} I(X;Y|S=s) \quad \text{if the network allows feedback,}$$
$$\max_{p(x)} \min_{s} I(X;Y|S=s) \quad \text{otherwise.}$$

Arbitrarily Varying Channel Model



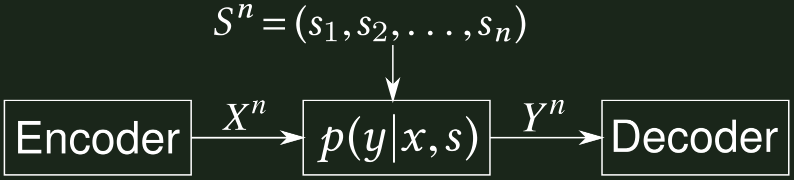
- Point-to-point AVC, independent of the rest of the network, with independent state

Arbitrarily Varying Channel Model

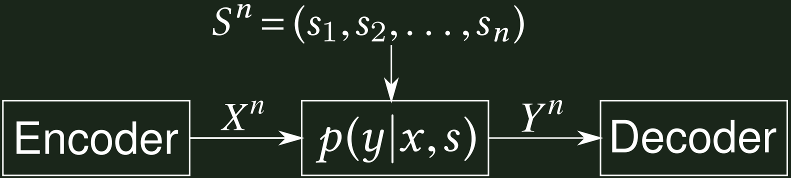


- Point-to-point AVC, independent of the rest of the network, with independent state

Point-to-Point Arbitrarily Varying Channel



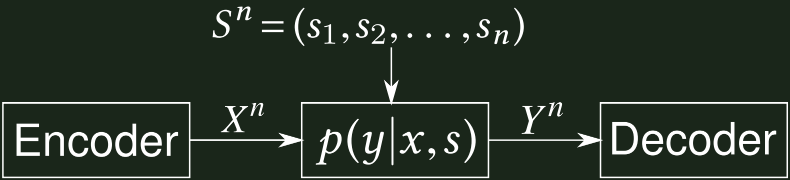
Point-to-Point Arbitrarily Varying Channel



- Random code capacity C_r is the capacity when the encoder/decoder have access to shared randomness

$$C_r = \max_{p(x)} \min_{p(s)} I(X;Y)$$

Point-to-Point Arbitrarily Varying Channel



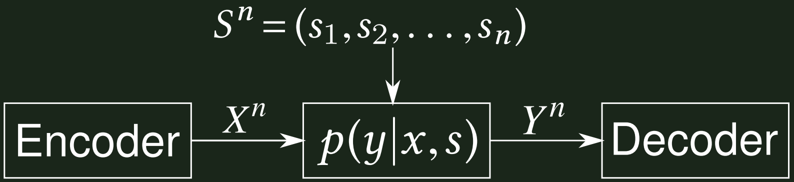
- Random code capacity C_r is the capacity when the encoder/decoder have access to shared randomness

$$C_r = \max_{p(x)} \min_{p(s)} I(X;Y)$$

- An AVC is symmetrizable if there exists $p(s|x)$ such that

$$\sum_s p(y|x,s)p(s|x') \text{ is symmetric in } x, x'$$

Point-to-Point Arbitrarily Varying Channel



- Random code capacity C_r is the capacity when the encoder/decoder have access to shared randomness

$$C_r = \max_{p(x)} \min_{p(s)} I(X;Y)$$

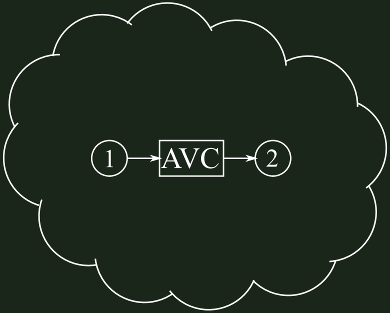
- An AVC is symmetrizable if there exists $p(s|x)$ such that

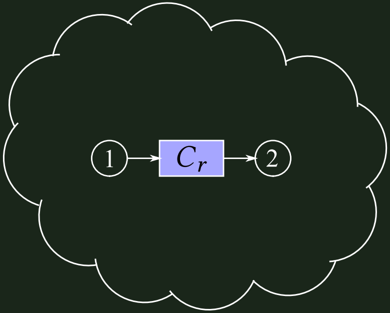
$$\sum_s p(y|x,s)p(s|x') \text{ is symmetric in } x, x'$$

- Csiszár-Narayan (1988):

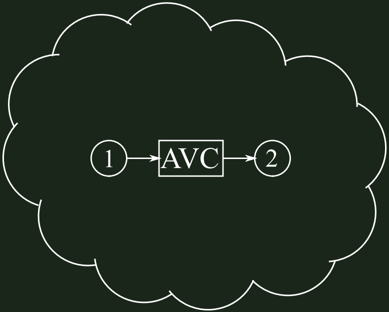
$$\text{AVC capacity} = \begin{cases} 0 & \text{if channel is symmetrizable} \\ C_r & \text{otherwise} \end{cases}$$

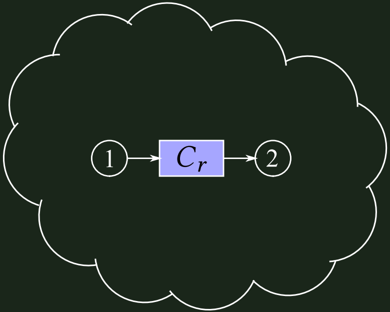
Towards Network Equivalence for AVC





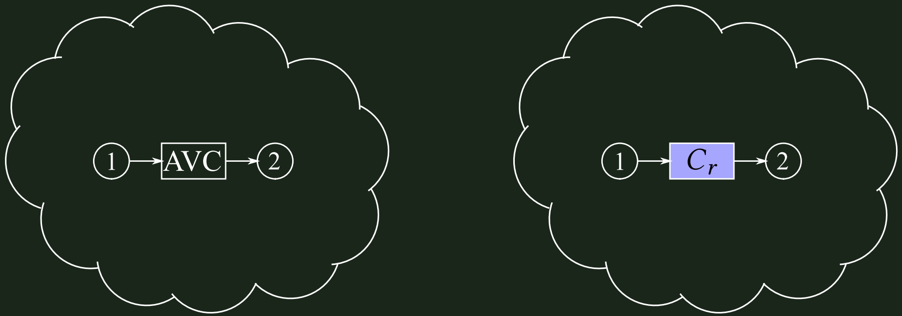
Towards Network Equivalence for AVC





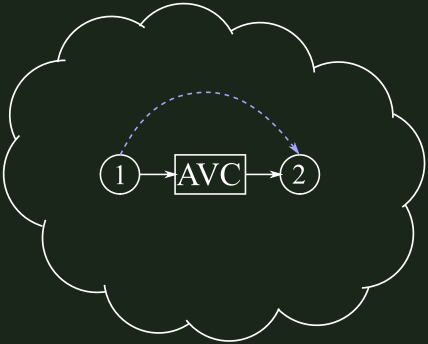
- Easy to show bit-pipe C_r is an outer bounding model

Towards Network Equivalence for AVC



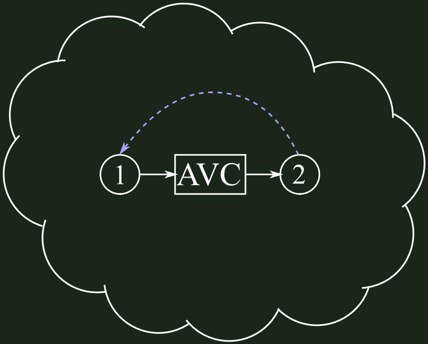
- Easy to show bit-pipe C_r is an outer bounding model
- Bit-pipe C_r is an inner bounding model if common randomness can be established between transmitter and receiver at any positive rate

When can common randomness be established?



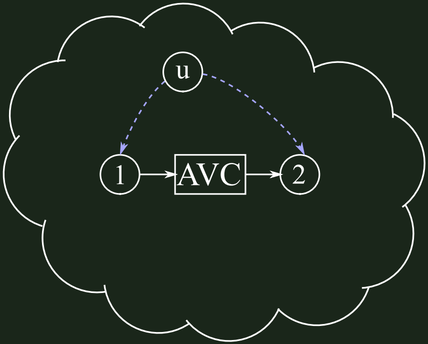
- parallel path from transmitter to receiver of any positive rate

When can common randomness be established?



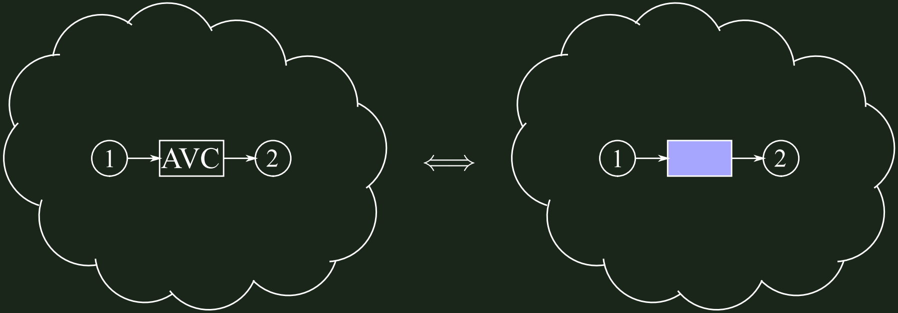
- parallel path from transmitter to receiver of any positive rate
- reverse path from receiver to transmitter of any positive rate

When can common randomness be established?



- parallel path from transmitter to receiver of any positive rate
- reverse path from receiver to transmitter of any positive rate
- paths of any positive rate from a node u to both transmitter and receiver

Equivalence for Arbitrary Varying Channels



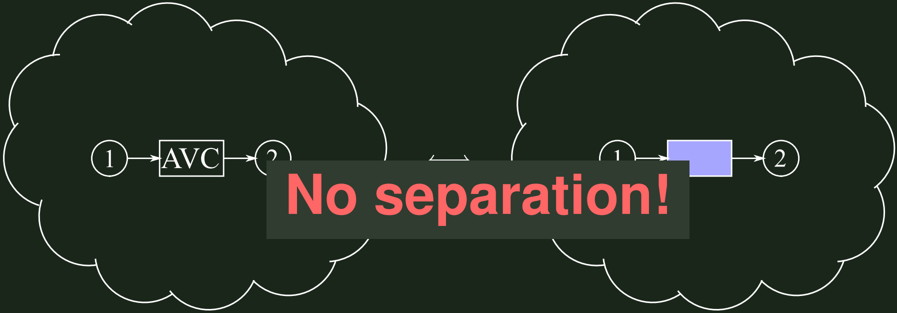
Theorem (KK-15)

AVC from node 1 to 2 is equivalent to bit-pipe of capacity C_r if

(i) *the channel is non-symmetrizable, or*

(ii) *there exists a node u that can send information at any positive rate to both nodes 1 and 2.*

Equivalence for Arbitrary Varying Channels



No separation!

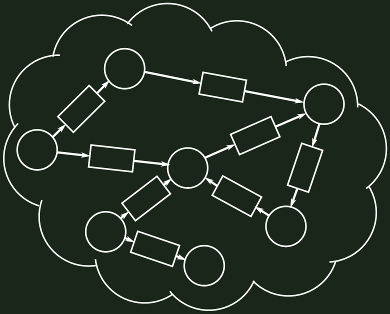
Theorem (KK-15)

AVC from node 1 to 2 is equivalent to bit-pipe of capacity C_r if

(i) *the channel is non-symmetrizable, or*

(ii) *there exists a node u that can send information at any positive rate to both nodes 1 and 2.*

Joint AVC/CC Model



- Each channel given by $p(y|x,s)$
- Adversary chooses k channels (CC-type state), and controls state s for each of those channels (AVC-type state)
- If channel is untouched by adversary, assume null state s_0

Simple Outer Bound

For each channel, two capacities:

- Ordinary capacity, with null state:

$$C = \max_{p(x)} I(X; Y|S = s_0)$$

- AVC random coding capacity:

$$C_r = \max_{p(x)} \min_{p(s)} I(X; Y)$$

Simple Outer Bound

For each channel, two capacities:

- Ordinary capacity, with null state:

$$C = \max_{p(x)} I(X;Y|S = s_0)$$

- AVC random coding capacity:

$$C_r = \max_{p(x)} \min_{p(s)} I(X;Y)$$

Given a set of channels $\mathcal{Z}$, let $\mathcal{N}_{\mathcal{Z}}$ be the noiseless network where:

- all channels in $\mathcal{Z}^c$ are replaced by bit-pipe of capacity C
- all channels in $\mathcal{Z}$ are replaced by bit-pipe of capacity C_r

Simple Outer Bound

For each channel, two capacities:

- Ordinary capacity, with null state:

$$C = \max_{p(x)} I(X;Y|S = s_0)$$

- AVC random coding capacity:

$$C_r = \max_{p(x)} \min_{p(s)} I(X;Y)$$

Given a set of channels $\mathcal{Z}$, let $\mathcal{N}_{\mathcal{Z}}$ be the noiseless network where:

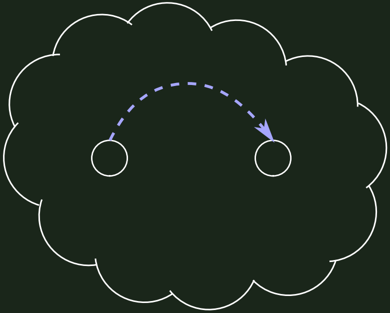
- all channels in $\mathcal{Z}^c$ are replaced by bit-pipe of capacity C
- all channels in $\mathcal{Z}$ are replaced by bit-pipe of capacity C_r

Theorem

For all $\mathcal{Z}$ with $|\mathcal{Z}| \leq k$, $\quad \mathscr{R}(\mathcal{N}) \subseteq \mathscr{R}(\mathcal{N}_{\mathcal{Z}})$

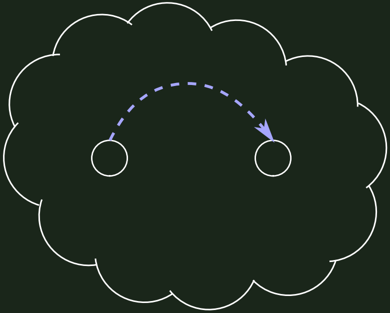
Full Connectivitiy

Assume any pair of nodes can communicate at some positive rate



Full Connectivitiy

Assume any pair of nodes can communicate at some positive rate

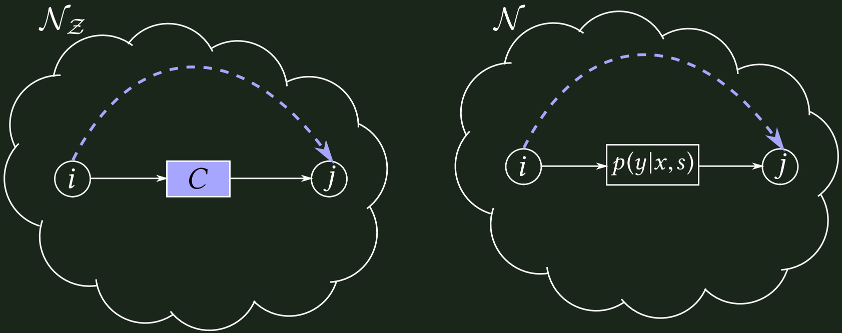


Theorem

Assuming full connectivity,

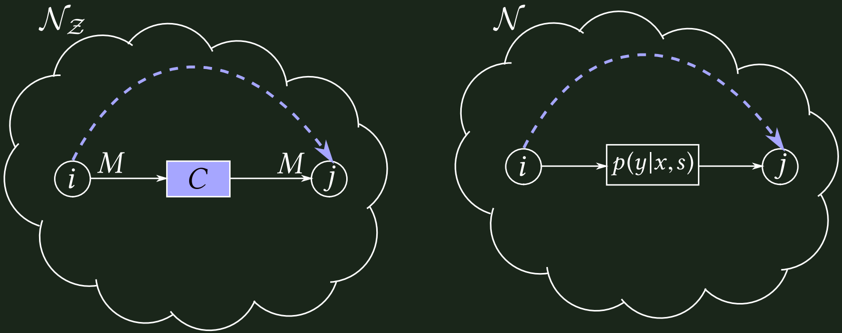
$$\mathscr{R}(\mathcal{N}) = \bigcap_{\mathcal{Z}:\ |\mathcal{Z}|\leq k} \mathscr{R}(\mathcal{N}_{\mathcal{Z}})$$

Achievability Proof



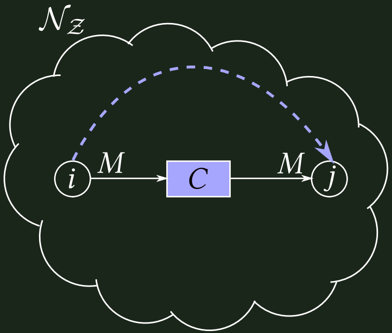
- Maintain global list $\mathcal{Z}$ of suspected adversarial channels

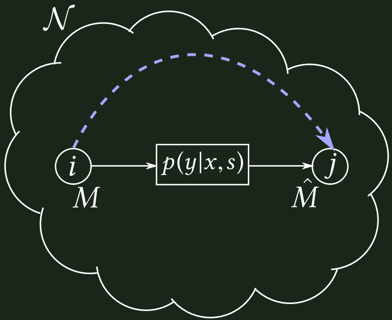
Achievability Proof



- Maintain global list $\mathcal{Z}$ of suspected adversarial channels

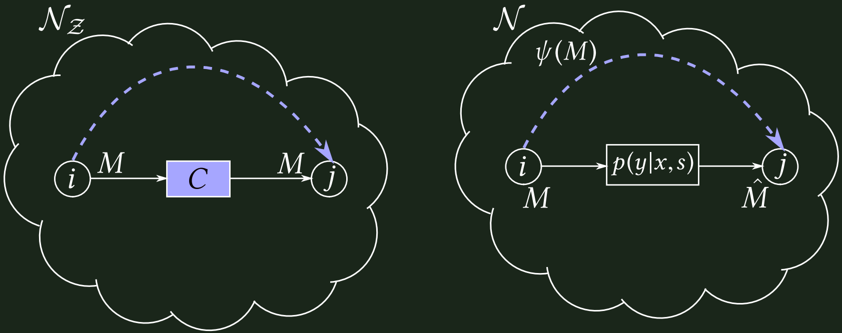
Achievability Proof





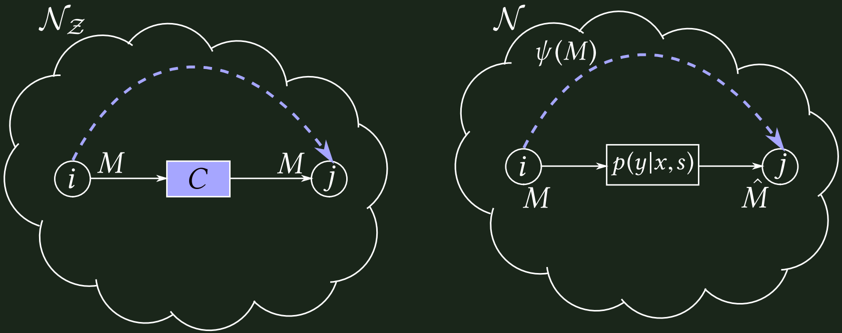
- Maintain global list $\mathcal{Z}$ of suspected adversarial channels
- If M sent in noiseless network, encode M on noisy channel, assuming null state

Achievability Proof



- Maintain global list $\mathcal{Z}$ of suspected adversarial channels
- If M sent in noiseless network, encode M on noisy channel, assuming null state
- Transmit hash $\psi(M)$ on parallel, low-rate path

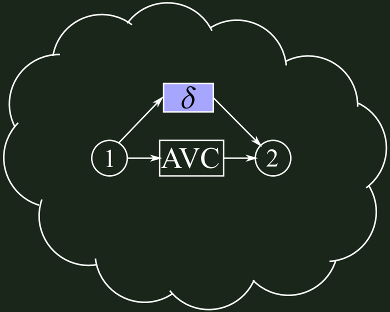
Achievability Proof



- Maintain global list $\mathcal{Z}$ of suspected adversarial channels
- If M sent in noiseless network, encode M on noisy channel, assuming null state
- Transmit hash $\psi(M)$ on parallel, low-rate path
- If mismatch, drop to AVC code at rate C_r, and add channel (i, j) to global list $\mathcal{Z}$

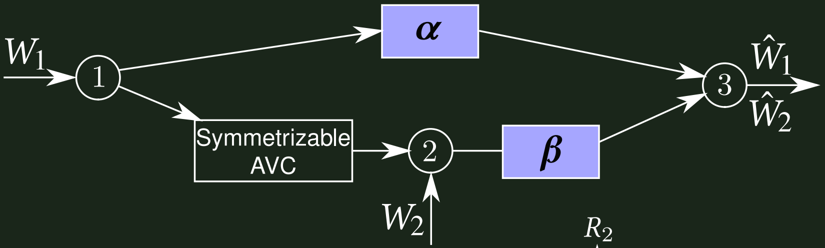
Edge Removal

The edge removal property does **NOT** hold with adversarial channels:



Deleting bit-pipe δ significantly effects capacity region

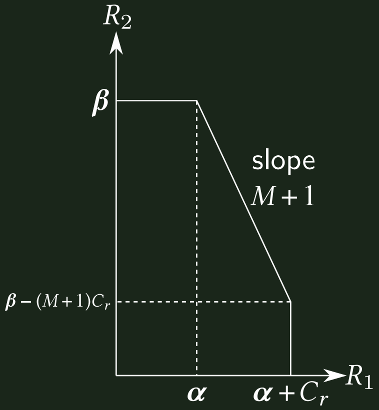
Example Network Without Full Connectivity



Capacity region consists of pairs (R_1, R_2) such that

$$R_2 \leq \boldsymbol{\beta}$$

$$R_1 \leq \boldsymbol{\alpha} + \min\left\{C_r, \frac{\boldsymbol{\beta} - R_2}{M+1}\right\}$$



This region cannot occur with any fixed-capacity bit-pipe

Conclusions

- Network equivalence results for:
  - Compound channels
  - Arbitrarily varying channels
  - Joint CC/AVC model
- All results become simpler under full connectivity assumption

Conclusions

- Network equivalence results for:
  - Compound channels
  - Arbitrarily varying channels
  - Joint CC/AVC model
- All results become simpler under full connectivity assumption

Open problems:

- What if full connectivity assumption does not hold?
- Joint CC/AVC model beyond network of point-to-point links