The Arbitrarily Varying Degraded Broadcast Channel with States Known at the Encoder

Amir Winshtok & Yossef Steinberg

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

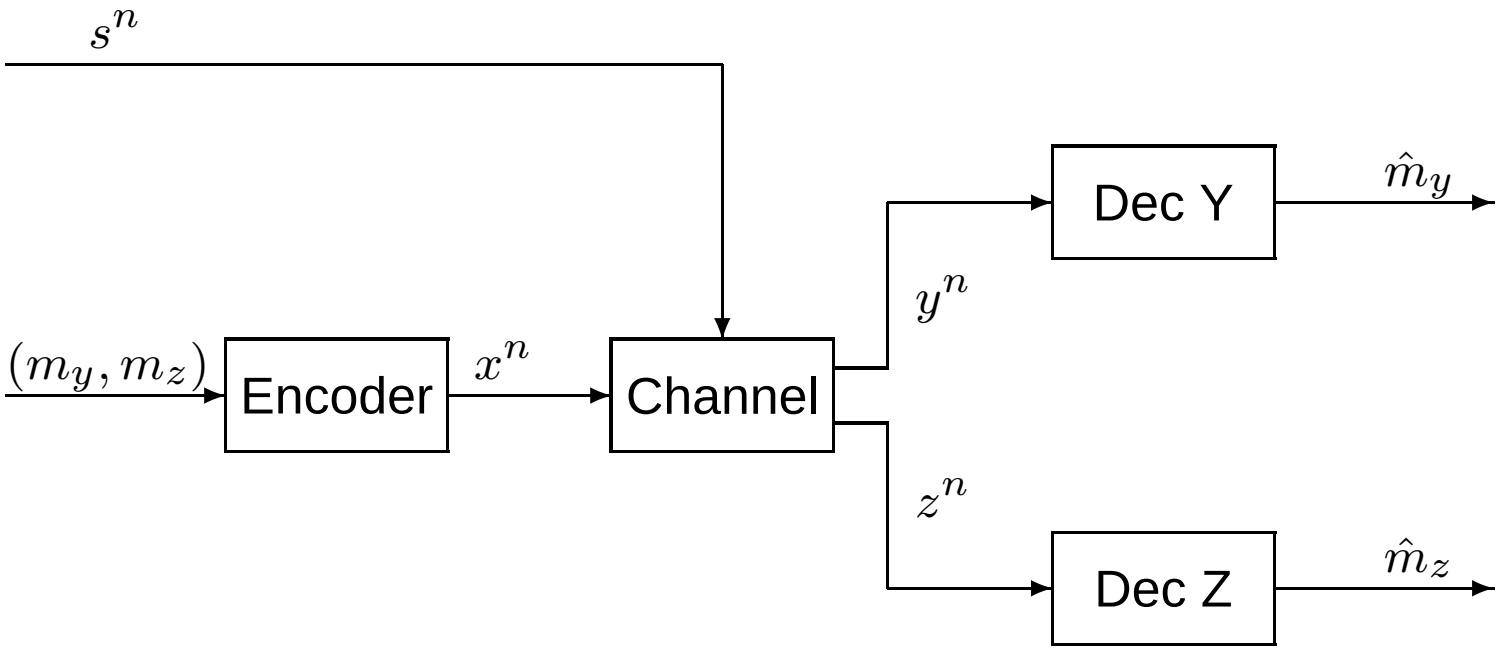
The 2006 International Symposium on Information Theory—ISIT '06:

Seattle, Washington, U.S.A, July 2006

Outline

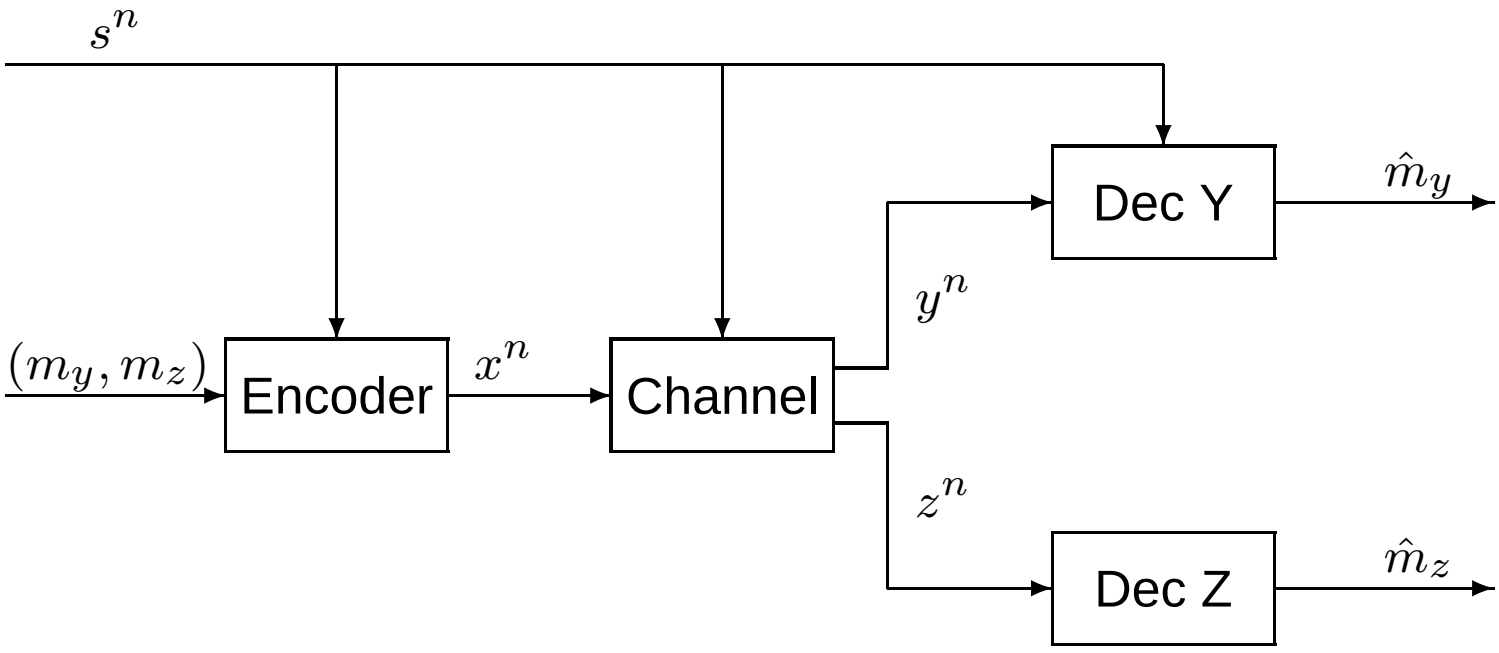
- Problem Formulation
- Motivation
- Previous Work
- Main Result
- Proof Idea
- Extension of Main Result
- Future Work

Problem Formulation



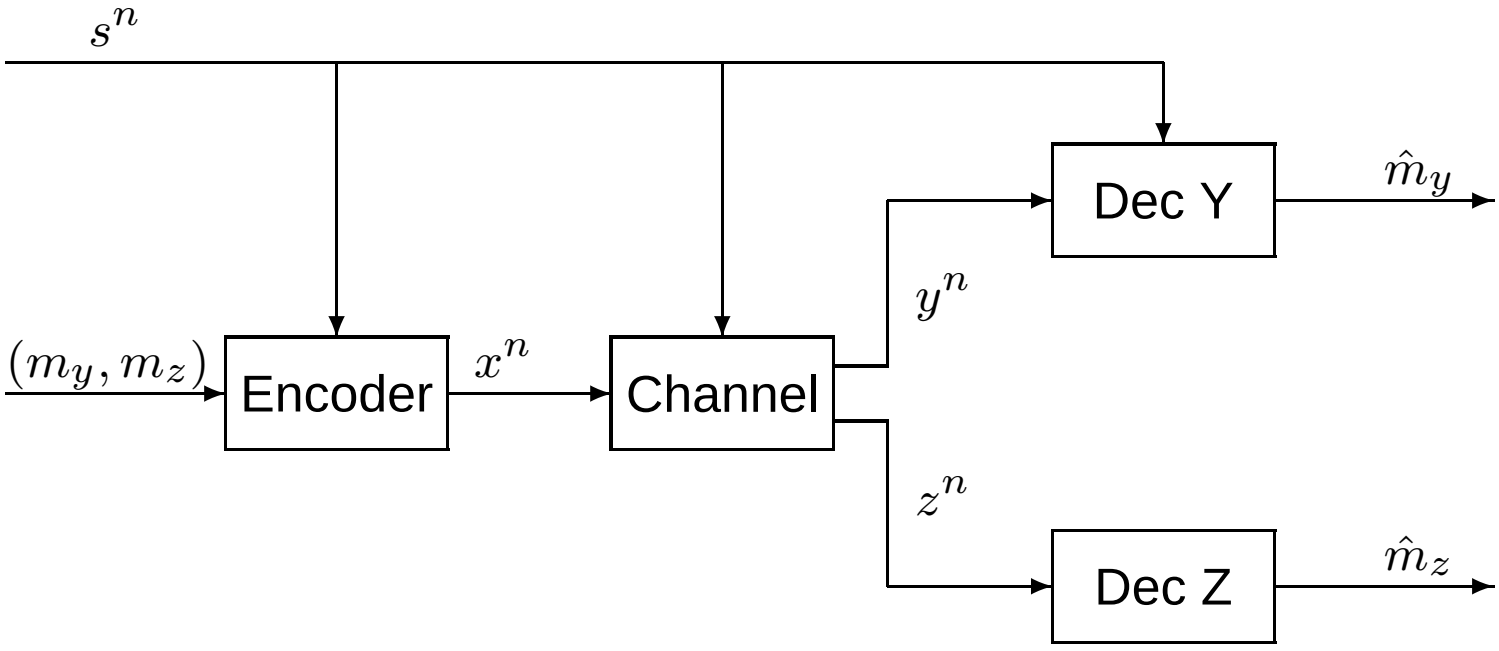
- $w(y, z|x, s)$ – Memoryless degraded broadcast channel (DBC) with arbitrarily varying (AV) state sequence s^n

Problem Formulation



- $w(y, z|x, s)$ – Memoryless degraded broadcast channel (DBC) with arbitrarily varying (AV) state sequence s^n
- State sequence is known a priori at the encoder (CSIT) and at the stronger decoder Y (CSIR).

Problem Formulation



- $w(y, z|x, s)$ – Memoryless degraded broadcast channel (DBC) with arbitrarily varying (AV) state sequence s^n
- State sequence is known a priori at the encoder (CSIT) and at the stronger decoder Y (CSIR).

We are interested in the deterministic code capacity region

$$R_Y = \frac{\log |\mathcal{M}_\mathcal{Y}|}{n}, \quad R_Z = \frac{\log |\mathcal{M}_\mathcal{Z}|}{n}.$$

Problem Formulation (cont'd)

Random, randomized-encoder and deterministic codes

- In a deterministic code the transmitted codeword is a deterministic function of the messages and the state sequence, $x^n = f(m_y, m_z, s^n)$. The decoding sets $\{D_Y, D_Z\}$ are fixed.
- For a fixed state sequence, the error probability of a deterministic code is given by

$$P_e(s^n) = 1 - \sum_{m_y, m_z} w(D_Y(m_y) \times D_Z(m_z) | f(m_y, m_z, s^n), s^n)$$

- In a randomized-encoder code the transmitted codeword is a random variable of the messages and the state sequence, $P(X^n | m_y, m_z, s^n)$. The decoding sets $\{D_Y, D_Z\}$ are fixed.
- For a fixed state sequence, the error probability of a randomized-encoder code is given by

$$P_e(s^n) = 1 - \sum_{x^n} P(x^n | m_y, m_z, s^n) \sum_{m_y, m_z} w(D_Y(m_y) \times D_Z(m_z) | x^n, s^n)$$

Problem Formulation (cont'd)

Random, randomized-encoder and deterministic codes (cont'd)

- A random code is a set of deterministic codes. The deterministic code in use is selected by an experiment result of a random variable μ, the encoder and both the decoders know.
- For a fixed state sequence, the error probability of a random code is the expectation of the error probabilities of the deterministic codes in the set, with respect to the random variable μ

$$P_e(s^n) = 1 - \sum_{\mu} p(\mu) \sum_{m_y, m_z} w(D_Y^{\mu}(m_y) \times D_Z^{\mu}(m_z) | f^{\mu}(m_y, m_z, s^n), s^n)$$

Motivation

Communication systems:

- AVC is a suitable model when the channel statistics is not fully known, or when a jammer is trying to disrupt the communication.
- Noncausal assumption is suitable when coding is not done along time, but across other dimension, like frequency or space. For example, an OFDM with coding for the broadcast channel, where coding is done across frequencies.

Motivation (cont'd)

Watermarking:

- In the context of watermarking, AVC models a situation where the cover text is an arbitrary sequence, not necessarily having a distribution.
- A broadcast channel can model two situations in watermarking:
  1. When the stegotext is subject to several stages of attack.
  2. When the state sequence is available at one of stronger users, broadcast channel can serve as a model to a single-user watermarking, where we do not know a priori whether the decoder has access to the cover text or not.

Previous Work

Channels with random parameters and noncausal CSIT (A very partial list):

- Gel'fand & Pinsker, 1980 – Capacity formula for the single user channel with random parameters and noncausal CSIT

$$C = \max_{P_{U,X|S}} I(U;Y) - I(U;S), \; U \multimap (X,S) \multimap Y.$$

- Steinberg, 2002 – Inner and outer bounds for the memoryless degraded broadcast channel with random parameters with noncausally CSIT. Let $w(y,z|x,s)$ be a (physically or stochastically) DBC with Z degraded user. Then for for every $P_{K,U,X|S}$ such that $(U,K) \multimap (S,X) \multimap (Y,Z)$

$$\begin{aligned} R_Z &\leq I(K;Z) - I(K;S) \\ R_Y &\leq I(U;Y|K) - I(U;S|K) \end{aligned}$$

is achieved. Tight for the case of informed stronger decoder Y.

Previous Work (cont'd)

If the stronger user Y is informed, then the capacity region is given by the collection of all pairs (R_Y, R_Z) such that

$$\begin{aligned} R_Z &\leq I(K;Z) - I(K;S) \\ R_Y &\leq I(X;Y|K,S) \end{aligned}$$

for some random variables (K, S, X, Y, Z) with joint probability holds the Markov rule $(U, K) \multimap (S, X) \multimap (Y, Z)$.

Previous Work (cont'd)

Arbitrarily varying channels (AVC) (A very partial list):

- Ahlswede's elimination technique ,1978 – An AVC deterministic-code capacity either equals its random-code capacity or else is zero (in the absence of side information and constraints).
  The randomness in the random code need not be too large: only polynomial large codes set with blocklength is needed.
- Ahlswede, 1986 – Positivity and capacity for an AVC with noncausal CSIT
  - Separation Lemma (SL) – The AVC deterministic-code capacity is positive iff for every given state s, the capacity of the DMC $w(y|x,s)$ is positive.
  - If the deterministic code capacity is positive then, $C = \inf_q C^q$.
  - The achievability of the capacity formula is shown in three steps
    1. Extension of Gel'fand & Pinsker capacity formula to a compound channel capacity formula
    2. Random-code capacity equals compound channel capacity
    3. Deterministic-code capacity equals random-code capacity

Main Result

- $w(y, z|x, s)$ – DBC with CSIT and CSIR at the stronger user Y.
- $q(\cdot)$ – An arbitrary probability on the state space $\mathcal{S}$.
- $\mathcal{R}^q$ – Capacity region of $w(y, z|x, s)$ with random parameters with probability q (Steinberg, 2002).
- $w_Z(z|x, s) \triangleq \sum_y w(y, z|x, s)$ is the single user channel to the degraded user Z with informed encoder.

Theorem:

A. The interior of the deterministic code capacity region is not empty iff $w_Z(z|x, s)$ fulfills Ahlswede's separation lemma, that is for every s, the DMC $w_Z(z|x, s)$ has a positive capacity.

B. If the interior of the deterministic code capacity region is nonempty, then the capacity region is given by the intersection of all $\mathcal{R}^q$, for every possible probability q, i.e.,

$$C = \bigcap_q \mathcal{R}^q$$

Proof Idea

A. Nonempty of the capacity region

If the channel $w_Z(z|x,s)$ has a positive AVC capacity, by degraded structure of the channel so does $w_Y(y|x,s)$. Time sharing achieves positive rate in the interior of the capacity region.

B. Converse

Assume that $(r_y, r_z) \notin \bigcap_q \mathcal{R}^q$ is an achievable rate pair. Then there exists q' such that $(r_y, r_z) \notin \mathcal{R}^{q'}$. There exists a deterministic code with rate (r_y, r_z) and small error probability for every state sequence. Averaging the error probability with respect to q' , results in a contradiction to Steinberg's formula.

B. Achievability

Achievability of the Capacity region following Ahlswede 1986 ideas, applied to the broadcast setting. Proof in three steps

Proof Idea (cont'd)

First step: Compound DBC

- In a compound DBC the state sequence is chosen in an i.i.d manner with unknown probability.
- Key Idea: preassign for every possible type t of state sequence a code for state-dependent DBC, with state distribution t', and good error performance

$$\frac{1}{M_Y M_Z} \sum_{m_y, m_z} \sum_{s^n} w([D_Y^{t'}(m_y) \times D_Z^{t'}(m_z)]^c | s^n, f^{t'}(m_y, m_z, s^n)) \leq$$

$$\inf_q \frac{1}{M_Y M_Z} \sum_{m_y, m_z} \sum_{s^n} w([D_Y^{q}(m_y) \times D_Z^{q}(m_z)]^c | s^n, f^{q}(m_y, m_z, s^n)) + e^{-\epsilon n}$$

- Given a state sequence, the encoder concatenates a type preamble to the preassigned-code codeword in order to inform the decoders.

Proof Idea (cont'd)

First step: Compound DBC (cont'd)

- The decoders use the preamble to choose the appropriate decoding sets
- The number of different types of states sequence is only polynomial in blocklength. The preamble does not affects the overall rate.
- The concatenated code has an exponentially small error probability. Deterministic-code for known state probability (can be shown to) have exponentially small error probability.
  The preamble has exponentially small error probability.

Proof Idea (cont'd)

Second step: Construction of a random-code for an AV-DBC using the RT

Robustification Technique (Ahlswede, 1986)

- $g : s^n \to [0, 1]$
- π – a permutation function on $\mathcal{S}^n$

if the expectation of g is bounded by α for every memoryless probability p^n on the state sequence, i.e.,

$$\sum_{s^n} p^n(s^n) g(s^n) > \alpha$$

then, for every sequence s^n

$$\frac{1}{n!} \sum_{\pi} g(\pi s^n) > \alpha (n+1)^{|\mathcal{S}|}$$

Proof Idea (cont'd)

Second step: Construction of a random-code for an AV-DBC using the RT (cont'd)

- Applying the RT on the compound DBC

$$\frac{1}{M_Y M_Z} \sum_{m_y, m_z} \sum_{\pi} \frac{1}{n!}$$

$$w(\pi^{-1} D_Y(m_y) \times \pi^{-1} D_Z(m_z) \big| \pi^{-1} f(m_y, m_z, \pi s^n), s^n)$$

$$> 1 - \alpha(n+1)^{|\mathcal{S}|}$$

- 'Random-permutation code' achieves exponentially small error probability for every state sequence. Random coding achieves the capacity region.

Proof Idea (cont'd)

Second step: Construction of a random-code for an AV-DBC using the RT (cont'd)

- Applying the RT on the compound DBC

$$\frac{1}{M_Y M_Z} \sum_{m_y, m_z} \sum_{\pi} \frac{1}{n!}$$

$$w(\pi^{-1} D_Y(m_y) \times \pi^{-1} D_Z(m_z) \big| \pi^{-1} f(m_y, m_z, \pi s^n), s^n)$$

$$> 1 - \alpha(n+1)^{|\mathcal{S}|}$$

- 'Random-permutation code' achieves exponentially small error probability for every state sequence. Random coding achieves the capacity region.
- Problem: The number of codes in a random-permutation code is exponential with blocklength. Can not be transmitted to the decoder without affecting the code rate!

Proof Idea (cont'd)

Third step: Extension of the elimination technique to BC

- The randomness in the random code should not be exponentially large – 'only' polynomial number with block length of codes is needed.
- Key idea: A random average of an independent experiments of a random variable, will excises the mean with exponentially small probability, with the number of experiments.
- Create a new random-code by selecting at random only n^2 codes out of the whole family. The new random-code exceeds a fixed error probability with a super-exponentially small probability,

$$\max_{s^n} P\left\{\frac{1}{n^2}\sum_{1}^{n^2} P_e(\text{randomly selected code}) \geq \lambda\right\}$$

$$\leq |\mathcal{S}|^n M_Y M_Z e^{-\lambda n^2}$$

Proof Idea (cont'd)

Third step: Extension of the elimination technique to BC (cont'd)

- Random selection argument guarantees the existence of a random-code with 'only' n^2 codes, with a fixed error probability.
- Create a randomized-encoder code by adding a code index preamble (positivity).
  A randomized encoder code achieves the capacity region.
- A randomized encoder code can not out perform a deterministic code in a DBC with CSIT.
  A deterministic code achieves the capacity region.
- The error probability of the deterministic code is arbitrary small for sufficiently large blocklength, rather then exponential with blocklength.

Extension of Main Result

- $w(y, z|x, s)$ – discrete memoryless BC with state set $\mathcal{S}$. CSIT assumed.
- $\mathcal{R}^q$ – Capacity region inner bound to $w(y, z|x, s)$ with random parameters with probability q
- $\tilde{\mathcal{R}}^q$ – Capacity region outer bound to $w(y, z|x, s)$ with random parameters with probability q
- $w_Z(z|x, s) \triangleq \sum_y w(y, z|x, s)$ is the single user channel to user Z with informed encoder. Similarly define $w_Y(y|x, s)$.

Theorem:

A. The interior of the deterministic code capacity region is not empty iff $w_Z(z|x, s)$ and $w_Y(y|x, s)$ fulfill Ahlswede's separation lemma.

B. If the interior of the deterministic code capacity region is nonempty, then an inner bound to the capacity region is given by the intersection of all $\mathcal{R}^q$, for every possible probability q, i.e., $C \supset \bigcap_q \mathcal{R}^q$.

C. An outer bound to the capacity region is given by the intersection of all $\tilde{\mathcal{R}}^q$, for every possible probability q, i.e., $C \subset \bigcap_q \tilde{\mathcal{R}}^q$.

Future Work

Applying states constrains

- $l : s \to [0, \infty)$ is a state constrain function. $l(s^n) = \frac{1}{n} \sum_n l(s_i)$.
- Single-user AVC with constrain was solved by Csiszar & Narayan.
- How to extend Csiszar & Narayan technique to AV-DBC with informed encoder (or to simplify, a single-user AVC with informed encoder)