# Two by Gel'fand and Pinsker

Amos Lapidoth
ETH Zurich

2012 IEEE European School of Information Theory, Antalya, Turkey

April 19, 2012

Joint work with Ligong Wang.

# Two Results of Gel'fand and Pinsker from 1980

*Problems of Control and Information Theory, Vol. 9 (1), pp. 19–31 (1980)*

## CODING FOR CHANNEL WITH RANDOM PARAMETERS

S. I. GEL'FAND, M. S. PINSKER

(Moscow)

(Received January 20, 1979)

## CAPACITY OF A BROADCAST CHANNEL WITH ONE DETERMINISTIC COMPONENT

S. I. Gel'fand and M. S. Pinsker

UDC 621.391.1

An internal bound is given for the capacity region of a two-output broadcast channel when there is common information. The capacity region for a broadcast channel with one deterministic component is computed. A noisy Blackwell channel is considered as an example.*

# A Channel with Random Parameters

- Channel law

$$W(y|x,s), \qquad \{S_k\} \sim \text{IID } P_S.$$

- The encoder knows the state sequence noncausally:

$$f\colon \mathcal{M} \times \mathcal{S}^n \to \mathcal{X}^n.$$

- $\mathcal{M}$ is the message set

$$\mathcal{M} = \{1, \ldots, 2^{nR}\}.$$

- $R$ is the rate, and $n$ is the blocklength.
- Decoder ignorant of state sequence:

$$\phi\colon \mathcal{Y}^n \to \mathcal{M}.$$

# The highest rate of reliably communication

Gel'fand and Pinsker:

$$C = \max I(U;Y) - I(U;S)$$

where the maximum is over all PMFs

$$P_S(s)\, P_{U|S}(u|s)\, P_{X|S,U}(x|s,u)\, W(y|x,s).$$

And there is NLG in choosing $P_{X|S,U}$ deterministic:

$$P_S(s)\, P_{U|S}(u|s)\, \mathrm{I}\{x = g(s,u)\}\, W(y|x,s)$$

$$C = \max_{P_{U|S},\ g:\, \mathcal{S}\times\mathcal{U}\to\mathcal{X}} I(U;Y) - I(U;S)$$

# Achievability

- Generate $2^{n(R+\tilde{R})}$ sequences IID $P_U$:

$$\mathbf{u}(m,\ell), \quad m \in \mathcal{M},\ \ell \in \left\{1,\ldots,2^{n\tilde{R}}\right\}.$$

- To send Message $m$ after observing $\mathbf{s}$, look for some $\ell$ such that $\big(u(m,\ell),\mathbf{s}\big)$ are j.t. w.r.t. $P_{S,U}$.
- If none found, "encoding failure."
- The probability of encoding failure vanishes if

$$\tilde{R} > I(U;S).$$

- Decoder searches for a unique pair $(m',\ell')$ such that $\big(u(m',\ell'),\mathbf{y}\big)$ is j.t. w.r.t. $P_{U,Y}$.
- The probability of success tends to one if

$$R + \tilde{R} < I(U;Y).$$

# The Converse

$$
\begin{aligned}
nR &\le I(M;Y^n) + n\epsilon_n \\
&= \sum_i I(M;Y_i|Y^{i-1}) + n\epsilon_n \\
&= \sum_i I\left(M, S_{i+1}^n; Y_i \middle| Y^{i-1}\right) - \sum_i I\left(S_{i+1}^n; Y_i \middle| M, Y^{i-1}\right) + n\epsilon_n \\
&= \sum_i I\left(M, S_{i+1}^n; Y_i \middle| Y^{i-1}\right) - \sum_i I\left(Y^{i-1}; S_i \middle| M, S_{i+1}^n\right) + n\epsilon_n \\
&= \sum_i I\left(M, S_{i+1}^n; Y_i \middle| Y^{i-1}\right) - \sum_i I\left(M, Y^{i-1}, S_{i+1}^n; S_i\right) + n\epsilon_n \\
&\le \sum_i I\left(M, Y^{i-1}, S_{i+1}^n; Y_i\right) - \sum_i I\left(M, Y^{i-1}, S_{i+1}^n; S_i\right) + n\epsilon_n \\
&= \sum_i I(U_i;Y_i) - I(U_i;S_i) + n\epsilon_n.
\end{aligned}
$$

It only remains to check that

$$(M, Y^{i-1}, S_{i+1}^n) -\!\!\circ\!\!- (X_i, S_i) -\!\!\circ\!\!- Y_i.$$

# What Is a Broadcast Channel?

- One transmitter and two receivers.
- Transmitted symbol: $X \in \mathcal{X}$.
- Received symbols: $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$.
- Message $m_y \in \mathcal{M}_y$ for Receiver $Y$, and $m_z \in \mathcal{M}_z$ for $Z$.
- Channel is used $n$ times ("the blocklength").
- The rates are

$$R_y = \frac{\log \# \mathcal{M}_y}{n}, \qquad R_z = \frac{\log \# \mathcal{M}_z}{n}.$$

- The encoder:

$$(m_y, m_z) \mapsto \mathbf{x}(m_y, m_z) = \bigl(x_1(m_y, m_z), \ldots, x_n(m_y, m_z)\bigr) \in \mathcal{X}^n.$$

- The decoders:

$$\phi_y \colon \mathcal{Y}^n \to \mathcal{M}_y, \qquad \phi_z \colon \mathcal{Z}^n \to \mathcal{M}_z.$$

# The Probability of Error

A memoryless BC of law $W(y, z|x)$:

$$\Pr[\mathbf{Y} = \mathbf{y}, \mathbf{Z} = \mathbf{z} \,|\, \mathbf{X} = \mathbf{x}] = \prod_{k=1}^{n} W(y_k, z_k | x_k).$$

The probabilities of error:

$$\frac{1}{\# \mathcal{M}_y} \frac{1}{\# \mathcal{M}_z} \sum_{m_y \in \mathcal{M}_y} \sum_{m_z \in \mathcal{M}_z} \Pr[\phi_y(\mathbf{Y}) \neq m_y \,|\, M_y = m_y,\ M_z = m_z]$$

and

$$\frac{1}{\# \mathcal{M}_y} \frac{1}{\# \mathcal{M}_z} \sum_{m_y \in \mathcal{M}_y} \sum_{m_z \in \mathcal{M}_z} \Pr[\phi_z(\mathbf{Z}) \neq m_z \,|\, M_y = m_y,\ M_z = m_z].$$

# Capacity Region

- $(R_y, R_z)$ is achievable if for every $\epsilon > 0$ and $\delta > 0$ we are guaranteed that for all sufficiently large blocklengths $n$ we can find encoder/decoders of rates $(R_y - \delta, R_z - \delta)$ for which both error probabilities are smaller than $\epsilon$.
- Some special cases for which the capacity is known:
  - The degraded BC
  - Less Noisy
  - More capable
  - The deterministic BC
  - The semideterministic BC.

# The Deterministic Broadcast Channel

$$Y = f_y(X), \qquad Z = f_z(X)$$

for some

$$f_y \colon \mathcal{X} \to \mathcal{Y}, \qquad f_z \colon \mathcal{X} \to \mathcal{Z}.$$

Gel'fand, Marton, and Pinsker: The capacity region is the convex closure of the union over all PMFs $P_X$ of the (sets of) rate pairs

$$\begin{aligned} R_y &\leq H(Y) \\ R_z &\leq H(Z) \\ R_y + R_z &\leq H(Y, Z) \end{aligned}$$

where the entropies are computed for the joint PMF

$$P_{XYZ}(x, y, z) = P_X(x)\,\mathbf{1}\{y = f_y(x)\}\,\mathbf{1}\{z = f_z(x)\}.$$

# The Converse for the Deterministic BC

The converse is easy:

$$I(M_y; \mathbf{Y}) \leq \sum_{k=1}^{n} H(Y_k),$$

$$I(M_z; \mathbf{Z}) \leq \sum_{k=1}^{n} H(Z_k),$$

and

$$I(M_y, M_z) \leq \sum_{k=1}^{n} H(Y_k, Z_k).$$

To bound $R_y$ we ignore the fact that $H(\mathbf{Y}|M_y)$ is typically not zero (because of $M_z$). Likewise for $R_z$. And to bound $R_y + R_z$ we pretend that the receivers can cooperate.

# Deterministic BC—the Direct Part

- Choose $P_X$, inducing a joint $P_X P_{Y|X} P_{Z|X}$ of marginal $P_{Y,Z}$.
- In two independent assignments, assign to each $\mathbf{y} \in \mathcal{Y}^n$ a random index $I \in \{1, \ldots, 2^{nR_y}\}$ and to each $\mathbf{z} \in \mathcal{Z}^n$ a random index $J \in \{1, \ldots, 2^{nR_z}\}$.
- Let $B(i,j)$ comprise the pairs $(\mathbf{y}, \mathbf{z})$ that are mapped to $(i,j)$.
- If $(\mathbf{y}, \mathbf{z})$ are jointly typical w.r.t. $P_{Y,Z}$, then there must exist some $\mathbf{x} \in \mathcal{X}^n$ that produces the outputs $(\mathbf{y}, \mathbf{z})$, because joint typicality implies

$$\Pr[\mathbf{Y} = \mathbf{y}, \mathbf{Z} = \mathbf{z}] > 2^{-n\left(H(Y,Z)+\epsilon\right)} > 0,$$

  and the only way this probability can be positive is if some $\mathbf{x}$ induces these outputs.
- To send $(m_y, m_z)$ look for a pair $(\mathbf{y}, \mathbf{z})$ in $B(m_y, m_z)$ that is jointly typical, and transmit the sequence $\mathbf{x}$ that produces it.
- If there is no j.t. $(\mathbf{y}, \mathbf{z})$ in $B(m_y, m_z)$, $\Rightarrow$ "encoding failure."

# The Semideterministic Broadcast Channel

Only $Y$ is deterministic given $x$:

$$Y = f_y(x), \qquad \Pr[Z = z \,|\, X = x] = W(z|x).$$

Gel'fand and Pinsker: The capacity is the convex hull of the union over all $P_X$ of the sets of rate pairs $(R_y, R_z)$

$$\begin{aligned} R_y &< H(Y) \\ R_z &< I(U;Z) \\ R_y + R_z &< H(Y) + I(U;Z) - I(U;Y) \end{aligned}$$

over all joint distribution on $(X, Y, Z, U)$ under which, conditional on $X$, the channel outputs $Y$ and $Z$ are drawn according to the channel law independently of $U$:

$$P_{XYZU}(x, y, z, u) = P_{X,U}(x, u)\, \mathbf{1}\{y = f_y(x)\} W(z|x).$$

Achievability follows from Marton's Inner Bound (More later).

# State-Dependence and Prescience

- A state sequence $S_1, \ldots, S_n$ is generated IID $\sim P_S$. The channel law is
$$W(y, z|s, x).$$
- A prescient encoder knows $S_1, \ldots, S_n$ before transmission begins:
$$\mathbf{x} = \mathbf{x}(m_y, m_z, \mathbf{s}).$$

# State-Dependence and Prescience

- A state sequence $S_1, \ldots, S_n$ is generated IID $\sim P_S$. The channel law is
$$W(y, z|s, x).$$
- A prescient encoder knows $S_1, \ldots, S_n$ before transmission begins:
$$\mathbf{x} = \mathbf{x}(m_y, m_z, \mathbf{s}).$$

At least as hard as the BC without a state. . . .

# The Steinberg-Shamai Inner Bound

Achievability of $(R_1, R_2)$ is guaranteed whenever

$$\begin{aligned} R_1 &\le I(U_0, U_1; Y) - I(U_0, U_1; S) \\ R_2 &\le I(U_0, U_2; Z) - I(U_0, U_2; S) \\ R_1 + R_2 &\le -\big[\max\{I(U_0; Y), I(U_0; Z)\} - I(U_0; S)\big]^+ \\ &\quad + I(U_0, U_1; Y) - I(U_0, U_1; S) \\ &\quad + I(U_0, U_2; Z) - I(U_0, U_2; S) - I(U_1; U_2 | U_0, S), \end{aligned}$$

for some PMF of marginal $P_S$; that satisfies

$$(U_0, U_1, U_2) \multimap\!\!- (X, S) \multimap\!\!- (Y, Z);$$

with the conditional of $(Y, Z)$ given $(X, S)$ being $W(y, z | x, s)$.

# The Semideterministic State-Dependent BC with a Prescient Transmitter

- $Y$ is a deterministic function of $(x, s)$ but $Z$ possibly not:

$$Y = f(s, x), \qquad \Pr[Z = z \,|\, X = x, S = s] = W(z|x, s).$$

- The transmitter has noncausal state-information:

$$\big(m_y, m_z, \mathbf{s}\big) \mapsto \mathbf{x}(m_y, m_z, \mathbf{s}) = \big(x_1(m_y, m_z, \mathbf{s}), \ldots, x_n(m_y, m_z, \mathbf{s})\big).$$

# Two Special Cases

- State is null $\Longrightarrow$ (classical) semideterministic BC.

  (Gel'fand and Pinsker'80b).

# Two Special Cases

- State is null $\Longrightarrow$ (classical) semideterministic BC. (Gel'fand and Pinsker'80b).
- $Y$ is null $\Longrightarrow$ the single-user "Gel'fand-Pinsker problem" (Gel'fand and Pinsker'80a):

$$C = \max_{U -\circ- (X,S) -\circ- Z} I(U;Z) - I(U;S)$$

where the maximization is over PMFs of the form

$$P_S(s)\, P_{U|S}(u|s)\, P_{X|S,U}(x|s,u)\, W(z|x,s),$$

and $P_{X|S,U}$ can be taken to be deterministic.

# Who Is S.I Gel'fand?

# Who Is S.I Gel'fand?

Sergey Israilevich Gel'fand.
Ph.D. 1968
Moscow State Univeristy

Supervisor: A. A. Kirillov.

Israil Moiseevich Gel'fand (father)

# The Main Result

The capacity region is convex closure of the union of rate-pairs $(R_y, R_z)$ satisfying

$$\begin{aligned} R_y &< H(Y|S) \\ R_z &< I(U;Z) - I(U;S) \\ R_y + R_z &< H(Y|S) + I(U;Z) - I(U;S,Y) \end{aligned}$$

over all joint distribution on $(X, Y, Z, S, U)$ whose marginal $P_S$ is the given state distribution and under which, conditional on $X$ and $S$, the channel outputs $Y$ and $Z$ are drawn according to the channel law independently of $U$:

$$P_{XYZSU}(x, y, z, s, u) = P_S(s) P_{XU|S}(x, u|s) \mathbf{1}\{y = f(x, s)\} W(z|x, s).$$

Moreover, the capacity region is unchanged if the state sequence is revealed to the deterministic receiver.

# If the State Is Null

$$R_y < H(Y|\cancel{S})$$

$$R_z < I(U;Z) - \cancelto{0}{I(U;S)}$$

$$R_y + R_z < H(Y|\cancel{S}) + I(U;Z) - \cancelto{I(U;Y)}{I(U;S,Y)}$$

$$P_{XYZ\cancel{S}U}(x,y,z,\cancel{s},u) = \cancel{P_S(s)}P_{XU|\cancel{S}}(x,u|\cancel{s})\mathbf{1}\{y = f(x,\cancel{s})\}W(z|x,\cancel{s}).$$

That is,

$$R_y < H(Y)$$

$$R_z < I(U;Z)$$

$$R_y + R_z < H(Y) + I(U;Z) - I(U;Y)$$

$$P_{XYZU}(x,y,z,u) = P_{XU}(x,u)\mathbf{1}\{y = f(x)\}W(z|x).$$

# If the Deterministic Receiver Is Null

$$\cancel{R_y} \cancel{<} \cancel{H(Y|S)}$$

$$R_z < I(U;Z) - I(U;S)$$

$$\cancel{R_y +} R_z < \cancel{H(Y|S)} \xrightarrow{} 0 + I(U;Z) - \cancel{I(U;S,Y)} \xrightarrow{} I(U;S)$$

$$P_{X\cancel{Y}ZSU}(x,\cancel{y},z,s,u) = P_S(s)P_{XU|S}(x,u|s)\cancel{\mathbf{1}\{y = f(x,s)\}}W(z|x,s).$$

# If the Deterministic Receiver Is Null

$$\cancel{R_y < H(Y|S)}$$
$$R_z < I(U;Z) - I(U;S)$$

$$\cancel{R_y} + R_z < \cancel{H(Y|S)}^{\,0} + I(U;Z) - \cancel{I(U;S,Y)}^{\,I(U;S)}$$

$$P_{X\cancel{Y}ZSU}(x,\cancel{y},z,s,u) = P_S(s)P_{XU|S}(x,u|s)\cancel{\mathbf{1}\{y = f(x,s)\}}W(z|x,s).$$

Third and second constraints are identical and

$$R_z < I(U;Z) - I(U;S)$$

$$P_{XZSU}(x,z,s,u) = P_S(s)\,P_{XU|S}(x,u|s)\,W(z|x,s).$$

# Previous Work

- On the degraded BC, see

  Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2867–2877, Aug. 2005.

# Previous Work

- On the degraded BC, see

  Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2867–2877, Aug. 2005.

- Reza Khosravi and Farokh Marvasti solved the following special cases of our setting:
  - The deterministic case.
  - The case where $S$ is also known to the nondeterministc receiver $Z$.
  - The degraded case, from the deterministic to the noisy:

$$W(z|x,s) = \tilde{W}(z|y).$$

  "Capacity Bounds for Multiuser Channels with Non-Causal Channel State Information at the Transmitters," arXiv:1102.3410v2 (Feb. and May 2011).

# The Achievability—the Proof for Yossi and Shlomo

Substitute in the Steinberg-Shamai inner bound

$$U_0 = 0, \quad U_1 = Y, \quad U_2 = U.$$

$$\begin{aligned} R_1 &\le I(\cancel{U_0}, \cancelto{Y}{U_1}; Y) - I(\cancel{U_0}, \cancelto{Y}{U_1}; S) \\ R_2 &\le I(\cancel{U_0}, U_2; Z) - I(\cancel{U_0}, U_2; S) \end{aligned}$$

$$\begin{aligned} R_1 + R_2 \le & \cancelto{0}{-\big[\max\{I(U_0; Y), I(U_0; Z)\} - I(U_0; S)\big]^+} \\ & + I(\cancel{U_0}, \cancelto{Y}{U_1}; Y) - I(\cancel{U_0}, \cancelto{Y}{U_1}; S) \\ & + I(\cancel{U_0}, U_2; Z) - I(\cancel{U_0}, U_2; S) - I(\cancelto{Y}{U_1}; U_2 | \cancel{U_0}, S), \end{aligned}$$

$$R_1 \le \cancel{H(Y) - I(Y;S)} \to H(Y|S)$$

$$R_2 \le I(U_2;Z) - I(U_2;S)$$

$$R_1 + R_2 \le \cancel{H(Y) - I(Y;S)} \to H(Y|S) + I(U_2;Z)$$

$$\cancel{-I(U_2;S) - I(Y;U_2|S)} \to -I(U_2;S,Y).$$

The condition

$$(\cancel{U_0}, \cancel{U_1} \to Y, U_2) -\!\circ\!- (X,S) -\!\circ\!- (Y,Z)$$

becomes

$$(Y, U_2) -\!\circ\!- (X,S) -\!\circ\!- (Y,Z),$$

which, because $Y$ is a deterministic function of $(X,S)$, holds whenever

$$U_2 -\!\circ\!- (X,S) -\!\circ\!- Z.$$

# Achievability for Mortals

Fix some $P_{XYZSU}$ of the form

$$P_{XYZSU}(x, y, z, s, u) = P_S(s) P_{XU|S}(x, u|s) \mathbf{1}\{y = f(x, s)\} W(z|x, s).$$

# Achievability for Mortals

Fix some $P_{XYZSU}$ of the form

$$P_{XYZSU}(x, y, z, s, u) = P_S(s) P_{XU|S}(x, u|s) \mathbf{1}\{y = f(x, s)\} W(z|x, s).$$

Sum over $z$ to obtain $P_{SUYX}$ and write it as

$$P_{SUY}(s, u, y)\, P_{X|S,U,Y}(x|s, u, y).$$

# Achievability for Mortals

Fix some $P_{XYZSU}$ of the form

$$P_{XYZSU}(x, y, z, s, u) = P_S(s) P_{XU|S}(x, u|s) \mathbf{1}\{y = f(x, s)\} W(z|x, s).$$

Sum over $z$ to obtain $P_{SUYX}$ and write it as

$$P_{SUY}(s, u, y)\, P_{X|S,U,Y}(x|s, u, y).$$

For fixed $P_{SUY}$, only the terms in red depend on $P_{X|S,U,Y}$:

$$\begin{aligned} R_y &< H(Y|S) \\ R_z &< I(U;Z) - I(U;S) \\ R_y + R_z &< H(Y|S) + I(U;Z) - I(U;S,Y) \end{aligned}$$

# Achievability for Mortals

Fix some $P_{XYZSU}$ of the form

$$P_{XYZSU}(x, y, z, s, u) = P_S(s) P_{XU|S}(x, u|s) \mathbf{1}\{y = f(x, s)\} W(z|x, s).$$

Sum over $z$ to obtain $P_{SUYX}$ and write it as

$$P_{SUY}(s, u, y)\, P_{X|S,U,Y}(x|s, u, y).$$

For fixed $P_{SUY}$, only the terms in red depend on $P_{X|S,U,Y}$:

$$\begin{aligned} R_y &< H(Y|S) \\ R_z &< I(U; Z) - I(U; S) \\ R_y + R_z &< H(Y|S) + I(U; Z) - I(U; S, Y) \end{aligned}$$

so, by convexity, we can assume that $P_{X|S,U,Y}$ is zero-one-valued:

$$g \colon (y, u, s) \mapsto x.$$

# The Reduction

Henceforth we only consider joint PMFs satisfying

$$P_{XYZSU}(x, y, z, s, u) = P_S(s)P_{YU|S}(y, u|s)\mathbf{1}\{x = g(y, u, s)\}W(z|x, s)$$

and

$$Y = f(S, X).$$

# Codebook and Encoder

Generate $2^{nR_y}$ $y$-bins, each containing $2^{n\tilde{R}_y}$ $y$-tuples IID $\sim P_Y$

$$\mathbf{y}(m_y, l_y), \quad m_y \in \{1, \ldots, 2^{nR_y}\},\ l_y \in \{1, \ldots, 2^{n\tilde{R}_y}\}.$$

# Codebook and Encoder

Generate $2^{nR_y}$ $y$-bins, each containing $2^{n\tilde{R}_y}$ $y$-tuples IID $\sim P_Y$

$$\mathbf{y}(m_y, l_y), \quad m_y \in \{1, \ldots, 2^{nR_y}\},\ l_y \in \{1, \ldots, 2^{n\tilde{R}_y}\}.$$

Independently of that, generate $2^{nR_z}$ $u$-bins, each containing $2^{n\tilde{R}_z}$ $u$-tuples IID $\sim P_U$

$$\mathbf{u}(m_z, l_z), \quad m_z \in \{1, \ldots, 2^{nR_z}\},\ l_z \in \{1, \ldots, 2^{n\tilde{R}_z}\}.$$

# Codebook and Encoder

Generate $2^{nR_y}$ $y$-bins, each containing $2^{n\tilde{R}_y}$ $y$-tuples IID $\sim P_Y$

$$\mathbf{y}(m_y, l_y), \quad m_y \in \{1, \ldots, 2^{nR_y}\},\ l_y \in \{1, \ldots, 2^{n\tilde{R}_y}\}.$$

Independently of that, generate $2^{nR_z}$ $u$-bins, each containing $2^{n\tilde{R}_z}$ $u$-tuples IID $\sim P_U$

$$\mathbf{u}(m_z, l_z), \quad m_z \in \{1, \ldots, 2^{nR_z}\},\ l_z \in \{1, \ldots, 2^{n\tilde{R}_z}\}.$$

To send $(m_y, m_z)$ look for a $y$-tuple $\mathbf{y}(m_y, l_y)$ in $y$-bin $m_y$ and a $u$-tuple $\mathbf{u}(m_z, l_z)$ in $u$-bin $m_z$ such that

$$\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big) \text{ are jointly typical } P_{YUS}.$$

If such a pair can be found, send (componentwise)

$$\mathbf{x} = g\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big).$$

# Analysis: The Deterministic Decoder Errs:

- The deterministic receiver observes $\mathbf{y}(m_y, l_y)$.
- It errs only if

$$\mathbf{y}(m_y, l_y) = \mathbf{y}(m_y', l_y'), \quad \text{for } m_y' \neq m_y.$$

- This probability of error tends to zero whenever

$$R_y + \tilde{R}_y < H(Y).$$

# Analysis: The Nondeterministic Decoder Errs:

- The nondeterministic decoder searches for a unique pair $(m_z, l_z)$ such that $u(m_z, l_z)$ & $\mathbf{z}$ are jointly typical.
- The probability of error tends to zero if

$$R_z + \tilde{R}_z < I(U; Z).$$

## Analysis: An Encoding Error

- Encoding error: We cannot find a pair $(l_y, l_z)$ such that
$$\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big) \text{ are jointly typical } P_{YUS}.$$

# Analysis: An Encoding Error

- Encoding error: We cannot find a pair $(l_y, l_z)$ such that

$$\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big) \text{ are jointly typical } P_{YUS}.$$

- For the probability of this event to tend to zero it suffices that:
  - For every fixed j.t. $(\mathbf{u}, \mathbf{s})$, the expected number of $\mathbf{y}$'s in $y$-Bin$(m_y)$ that are j.t. with $(\mathbf{u}, \mathbf{s})$ be exponentially large.
  - For every fixed j.t. $(\mathbf{y}, \mathbf{s})$, the expected number of $\mathbf{u}$'s in $u$-Bin$(m_z)$ that are j.t. with $(\mathbf{y}, \mathbf{s})$ be exponentially large.
  - For every fixed typical $\mathbf{s}$, the expected number of $(l_y, l_z)$ pairs such that $\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big)$ are joinly typical be exponentially large.

# Analysis: An Encoding Error

- Encoding error: We cannot find a pair $(l_y, l_z)$ such that
$$\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big) \text{ are jointly typical } P_{YUS}.$$

- For the probability of this event to tend to zero it suffices that:
  - For every fixed j.t. $(\mathbf{u}, \mathbf{s})$, the expected number of $\mathbf{y}$'s in $y$-Bin$(m_y)$ that are j.t. with $(\mathbf{u}, \mathbf{s})$ be exponentially large.
  - For every fixed j.t. $(\mathbf{y}, \mathbf{s})$, the expected number of $\mathbf{u}$'s in $u$-Bin$(m_z)$ that are j.t. with $(\mathbf{y}, \mathbf{s})$ be exponentially large.
  - For every fixed typical $\mathbf{s}$, the expected number of $(l_y, l_z)$ pairs such that $\big(\mathbf{y}(m_y, l_y), \mathbf{u}(m_z, l_z), \mathbf{s}\big)$ are joinly typical be exponentially large.
- Hence, it suffices that
$$\begin{aligned} \tilde{R}_y &> I(Y;S) \\ \tilde{R}_z &> I(U;S) \\ \tilde{R}_y + \tilde{R}_z &> H(Y) + H(U) + H(S) - H(Y,U,S). \end{aligned}$$

# Concluding the Achievability Proof

The constraints

$$\begin{aligned} R_y + \tilde{R}_y &< H(Y) && \text{(a)} \\ R_z + \tilde{R}_z &< I(U;Z) && \text{(b)} \\ \tilde{R}_y &> I(Y;S) && \text{(c)} \\ \tilde{R}_z &> I(U;S) && \text{(d)} \\ \tilde{R}_y + \tilde{R}_z &> H(Y) + H(U) + H(S) - H(Y,U,S). && \text{(e)} \end{aligned}$$

# Concluding the Achievability Proof

The constraints

$$
\begin{aligned}
R_y + \tilde{R}_y &< H(Y) && \text{(a)}\\
R_z + \tilde{R}_z &< I(U;Z) && \text{(b)}\\
\tilde{R}_y &> I(Y;S) && \text{(c)}\\
\tilde{R}_z &> I(U;S) && \text{(d)}\\
\tilde{R}_y + \tilde{R}_z &> H(Y) + H(U) + H(S) - H(Y,U,S). && \text{(e)}
\end{aligned}
$$

allow the achievability of

$$
\begin{aligned}
R_y &< H(Y|S) && \text{from (a) and (c)}\\
R_z &< I(U;Z) - I(U;S) && \text{from (b) and (d)}\\
R_y + R_z &< H(Y|S) + I(U;Z) - I(U;S,Y) && \text{from (a)+(b) and (e)}
\end{aligned}
$$

(Constraint (e) pinches more than (c) + (d).)

# The Converse I

Upper-bounding $R_y$ is straightforward:

$$\begin{aligned} nR_y &= H(M_y) \\ &\le I(M_y; Y^n, S^n) + n\epsilon_n \\ &= I(M_y; Y^n | S^n) + n\epsilon_n \\ &= \sum_{i=1}^{n} I(M_y; Y_i | Y^{i-1}, S^n) + n\epsilon_n \\ &\le \sum_{i=1}^{n} H(Y_i | Y^{i-1}, S^n) + n\epsilon_n \\ &\le \sum_{i=1}^{n} H(Y_i | S_i) + n\epsilon_n, \end{aligned}$$

where $\epsilon_n$ decays to zero as $n$ tends to infinity.

# The Converse II

Upper-bounding $R_z$ à-la-Gelf'and-Pinsker (first approach):

$$\begin{aligned}
nR_2 &\leq I(M_z; Z^n) + n\epsilon_n \\
&= \sum_i I(M_z; Z_i | Z^{i-1}) + n\epsilon_n \\
&= \sum_i I\left( M_z, S_{i+1}^n; Z_i \middle| Z^{i-1} \right) - \sum_i I\left( S_{i+1}^n; Z_i \middle| M_z, Z^{i-1} \right) + n\epsilon_n \\
&= \sum_i I\left( M_z, S_{i+1}^n; Z_i \middle| Z^{i-1} \right) - \sum_i I\left( Z^{i-1}; S_i \middle| M_z, S_{i+1}^n \right) + n\epsilon_n \\
&= \sum_i I\left( M_z, S_{i+1}^n; Z_i \middle| Z^{i-1} \right) - \sum_i I\left( M_z, Z^{i-1}, S_{i+1}^n; S_i \right) + n\epsilon_n \\
&\leq \sum_i I\left( M_z, Z^{i-1}, S_{i+1}^n; Z_i \right) - \sum_i I\left( M_z, Z^{i-1}, S_{i+1}^n; S_i \right) + n\epsilon_n \\
&= \sum_i I(V_i; Z_i) - I(V_i; S_i) + n\epsilon_n.
\end{aligned}$$

# The Converse III

Upper-bounding the sum-rate:

$$\begin{aligned} n(R_y + R_z) &= H(M_y, M_z) \\ &= H(M_z) + H(M_y|M_z) \\ &\leq I(M_z; Z^n) + I(M_y; Y^n, S^n|M_z) + n\epsilon_n. \end{aligned}$$

# The Converse IV

Another bound on $I(M_2; Z^n)$:

$$
\begin{aligned}
& I(M_z; Z^n) \\
&= \sum_i I(M_z; Z_i | Z^{i-1}) \\
&\leq \sum_i I(M_z, Z^{i-1}; Z_i) \\
&= \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; Z_i\right) - \sum_i I\left(S_{i+1}^n, Y_{i+1}^n; Z_i \middle| M_z, Z^{i-1}\right) \\
&= \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; Z_i\right) - \sum_i I\left(Z^{i-1}; S_i, Y_i \middle| M_z, S_{i+1}^n, Y_{i+1}^n\right) \\
&= \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; Z_i\right) - \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; S_i, Y_i\right) \\
&\quad + \sum_i I\left(M_z, S_{i+1}^n, Y_{i+1}^n; S_i, Y_i\right).
\end{aligned}
$$

# The Converse V

The last term and $I(M_y; Y^n, S^n|M_z)$ add to

$$\sum_{i=1}^{n} I\left(M_z, S_{i+1}^n, Y_{i+1}^n; S_i, Y_i\right) + I(M_y; Y^n, S^n|M_z) = \sum_{i=1}^{n} H(Y_i|S_i).$$

(After lots of identities).

# The Converse VI

$$
\begin{aligned}
&n(R_y + R_z) \\
&\quad \leq \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; Z_i\right) \\
&\qquad - \sum_i I\left(M_z, Z^{i-1}, S_{i+1}^n, Y_{i+1}^n; S_i, Y_i\right) \\
&\qquad + \sum_{i=1}^n H(Y_i|S_i) + n\epsilon_n \\
&\quad = \sum_{i=1}^n I(V_i, T_i; Z_i) - \sum_{i=1}^n I(V_i, T_i; S_i, Y_i) + \sum_{i=1}^n H(Y_i|S_i) + n\epsilon_n.
\end{aligned}
$$

# The Converse VII

We have:

$$
\begin{aligned}
R_y &< H(Y|S) \\
R_z &< I(V;Z) - I(V;S) \\
R_y + R_z &< H(Y|S) + I(V,T;Z) - I(V,T;S,Y).
\end{aligned}
$$

$$(V,T) -\!\!\circ\!\!- (X,S) -\!\!\circ\!\!- (Y,Z).$$

# The Converse VII

We have:

$$\begin{aligned} R_y &< H(Y|S) \\ R_z &< I(V;Z) - I(V;S) \\ R_y + R_z &< H(Y|S) + I(V,T;Z) - I(V,T;S,Y). \end{aligned}$$

$$(V,T) -\!\circ\!- (X,S) -\!\circ\!- (Y,Z).$$

We want:

$$\begin{aligned} R_y &< H(Y|S) \\ R_z &< I(U;Z) - I(U;S) \\ R_y + R_z &< H(Y|S) + I(U;Z) - I(U;S,Y) \end{aligned}$$

$$U -\!\circ\!- (X,S) -\!\circ\!- (Y,Z).$$

# The Converse IIX

We are looking for an auxiliary r.v. $U$ such that

$$U \multimap\!\!- (X, S) \multimap\!\!- (Y, Z).$$

for which

$$I(V; Z) - I(V; S) \leq I(U; Z) - I(U; S)$$

and

$$\cancel{H(Y|S)} + I(V, T; Z) - I(V, T; S, Y) \leq \cancel{H(Y|S)} + I(U; Z) - I(U; S, Y)$$

# The Converse IIX

We are looking for an auxiliary r.v. $U$ such that

$$U -\!\circ\!- (X,S) -\!\circ\!- (Y,Z).$$

for which

$$I(V;Z) - I(V;S) \leq I(U;Z) - I(U;S)$$

and

$$\cancel{H(Y|S)} + I(V,T;Z) - I(V,T;S,Y) \leq \cancel{H(Y|S)} + I(U;Z) - I(U;S,Y)$$

Choosing $U$ as $V$ will work if

$$I(T;Z|V) - I(T;S,Y|V) \leq 0.$$

# The Converse IIX

We are looking for an auxiliary r.v. $U$ such that

$$U -\!\!\circ\!\!- (X,S) -\!\!\circ\!\!- (Y,Z).$$

for which

$$I(V;Z) - I(V;S) \le I(U;Z) - I(U;S)$$

and

$$\cancel{H(Y|S)} + I(V,T;Z) - I(V,T;S,Y) \le \cancel{H(Y|S)} + I(U;Z) - I(U;S,Y)$$

Choosing $U$ as $V$ will work if

$$I(T;Z|V) - I(T;S,Y|V) \le 0.$$

Choosing $U$ as $(V,T)$ will work if

$$I(T;Z|V) - I(T;S|V) \ge 0.$$

# The Converse IX

At least one of the conditions

$$I(T;Z|V) - I(T;S,Y|V) \leq 0$$

and

$$I(T;Z|V) - I(T;S|V) \geq 0$$

must hold:

# The Converse IX

At least one of the conditions

$$I(T;Z|V) - I(T;S,Y|V) \leq 0$$

and

$$I(T;Z|V) - I(T;S|V) \geq 0$$

must hold: having the first be positive and the second negative violates

$$I(T;Z|V) - I(T;S,Y|V) \leq I(T;Z|V) - I(T;S|V).$$

# The Converse IX

At least one of the conditions

$$I(T;Z|V) - I(T;S,Y|V) \leq 0$$

and

$$I(T;Z|V) - I(T;S|V) \geq 0$$

must hold: having the first be positive and the second negative violates

$$I(T;Z|V) - I(T;S,Y|V) \leq I(T;Z|V) - I(T;S|V).$$

The latter holds because

$$\cancel{I(T;Z|V)} - I(T;S|V) - \big(\cancel{I(T;Z|V)} - I(T;S,Y|V)\big) = I(T;Y|S,V)$$

and is thus nonnegative.

Thank you.

# Cardinality Bounds

$$\#\,\mathcal{U} \leq (\#\,\mathcal{S})(\#\,\mathcal{X}) + 2.$$