A Useful Analogy Between Wiretap and Gelfand-Pinsker Channels

Ziv Goldfeld and Haim Permuter

MIT and Ben Gurion University

The 2018 International Symposium on Information Theory
Vail, Colorado, US

Jun. 18th, 2018

Dualities and Analogies in Information Theory

- **Channel and Source Duality:**

Dualities and Analogies in Information Theory

- **Channel and Source Duality:**
  - Point-to-Point

    [Shannon 1959, Cover-Chiang 2002, Pradhan-Chou-Ramchandran 2003, Shirazi-Permuter 2010, Gupta-Verdú 2011]

Dualities and Analogies in Information Theory

- **Channel and Source Duality:**
  - Point-to-Point

    [Shannon 1959, Cover-Chiang 2002, Pradhan-Chou-Ramchandran 2003, Shirazi-Permuter 2010, Gupta-Verdú 2011]
  - Multiuser

    [Asnani-Permuter-Weissman 2013, Dikstein-Permuter-Shamai 2015, ZG-Permuter-Kramer 2016]

Dualities and Analogies in Information Theory

- **Channel and Source Duality:**
  - Point-to-Point
    [Shannon 1959, Cover-Chiang 2002, Pradhan-Chou-Ramchandran 2003, Shirazi-Permuter 2010, Gupta-Verdú 2011]
  - Multiuser
    [Asnani-Permuter-Weissman 2013, Dikstein-Permuter-Shamai 2015, ZG-Permuter-Kramer 2016]
- **Gaussian BC and MAC Duality**
  [Vishwanath-Tse 2003, Jindal-Vishwanath-Goldsmith 2004]

Dualities and Analogies in Information Theory

- **Channel and Source Duality:**
  - Point-to-Point
    [Shannon 1959, Cover-Chiang 2002, Pradhan-Chou-Ramchandran 2003, Shirazi-Permuter 2010, Gupta-Verdú 2011]
  - Multiuser
    [Asnani-Permuter-Weissman 2013, Dikstein-Permuter-Shamai 2015, ZG-Permuter-Kramer 2016]
- **Gaussian BC and MAC Duality**
  [Vishwanath-Tse 2003, Jindal-Vishwanath-Goldsmith 2004]
- **Kelly Gambling and Statistical Physics Analogy**
  [Vinkler-Permuter-Merhav 2016]

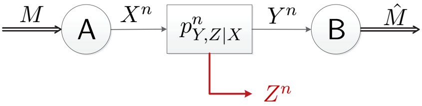
Dualities and Analogies in Information Theory

- **Channel and Source Duality:**
  - Point-to-Point
    [Shannon 1959, Cover-Chiang 2002, Pradhan-Chou-Ramchandran 2003, Shirazi-Permuter 2010, Gupta-Verdú 2011]
  - Multiuser
    [Asnani-Permuter-Weissman 2013, Dikstein-Permuter-Shamai 2015, ZG-Permuter-Kramer 2016]
- **Gaussian BC and MAC Duality**
  [Vishwanath-Tse 2003, Jindal-Vishwanath-Goldsmith 2004]
- **Kelly Gambling and Statistical Physics Analogy**
  [Vinkler-Permuter-Merhav 2016]
- **Gelfand-Pinsker and Wiretap Channel** [Liang-Poor-Shamai 2009]

The Wiretap Channel & The GP Channel

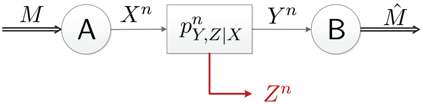
The Wiretap Channel & The GP Channel

The Wiretap Channel



The Wiretap Channel & The GP Channel

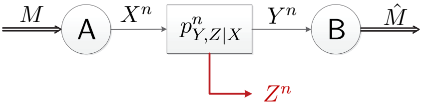
The Wiretap Channel



- Reliability

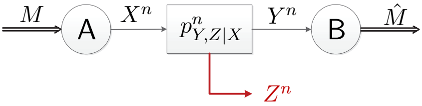
The Wiretap Channel & The GP Channel

The Wiretap Channel



- Reliability
- Security ($Z^n \perp M$ asymp.)

The Wiretap Channel



- Reliability
- Security ($Z^n \perp M$ asymp.)

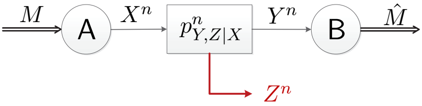
Theorem (Csiszár-Körner 1978)

$$\mathsf{C}_{\mathsf{WTC}} = \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$$

(Joint dist. $p_{U,X}\, p_{Y,Z|X}$*)*

The Wiretap Channel & The GP Channel

The Wiretap Channel



- Reliability
- Security ($Z^n \perp M$ asymp.)

Theorem (Csiszár-Körner 1978)

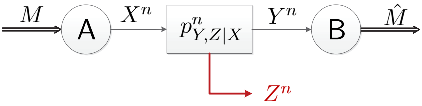
$$\mathsf{C}_{\mathsf{WTC}} = \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$$

(Joint dist. $p_{U,X} p_{Y,Z|X}$)

The Gelfand-Pinsker Channel

The Wiretap Channel & The GP Channel

The Wiretap Channel



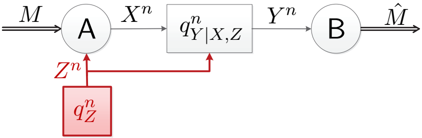
- Reliability
- Security ($Z^n \perp M$ asymp.)

Theorem (Csiszár-Körner 1978)

$$C_{\text{WTC}} = \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$$

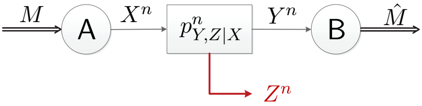
(Joint dist. $p_{U,X} p_{Y,Z|X}$*)*

The Gelfand-Pinsker Channel



The Wiretap Channel & The GP Channel

The Wiretap Channel



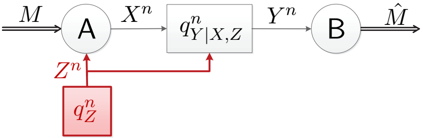
- Reliability
- Security ($Z^n \perp M$ asymp.)

Theorem (Csiszár-Körner 1978)

$$C_{\text{WTC}} = \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$$

(Joint dist. $p_{U,X} p_{Y,Z|X}$)

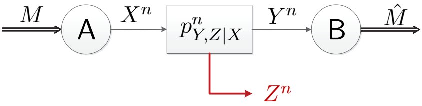
The Gelfand-Pinsker Channel



- Reliability (Corr. X^n w\ Z^n)

The Wiretap Channel & The GP Channel

The Wiretap Channel



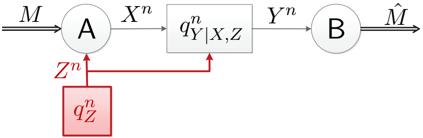
- Reliability
- Security ($Z^n \perp M$ asymp.)

Theorem (Csiszár-Körner 1978)

$$\mathsf{C}_{\mathsf{WTC}} = \max_{p_{U,X}} \big[I(U;Y) - I(U;Z) \big]$$

(Joint dist. $p_{U,X} p_{Y,Z|X}$)

The Gelfand-Pinsker Channel



- Reliability (Corr. X^n w\ Z^n)

Theorem (Gelfand-Pinsker 1980)

$$\mathsf{C}_{\mathsf{GP}} = \max_{q_{U,X|Z}} \big[I(U;Y) - I(U;Z) \big]$$

(Joint dist. $q_Z q_{U,X|Z} q_{Y|X,Z}$)

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.
- **Converse:** Csiszár sum \ Telescoping [Kramer, 2011]

  (Simpler for GP: Z^n is i.i.d. and independent of M).

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.
- **Converse:** Csiszár sum \ Telescoping [Kramer, 2011]

  (Simpler for GP: Z^n is i.i.d. and independent of M).

Unified Perspective:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.
- **Converse:** Csiszár sum \ Telescoping [Kramer, 2011]

  (Simpler for GP: Z^n is i.i.d. and independent of M).

Unified Perspective: Target asymptotic probabilistic relations:

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.
- **Converse:** Csiszár sum \ Telescoping [Kramer, 2011]

  (Simpler for GP: Z^n is i.i.d. and independent of M).

Unified Perspective: Target asymptotic probabilistic relations:

- **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of Z^n).

Gelfand-Pinsker Channel vs. Wiretap Channel

Similarities:

- Capacity expression.
- **Achievability:** Codebook + Encoding + Decoding.
- **Converse:** Csiszár sum \ Telescoping [Kramer, 2011]

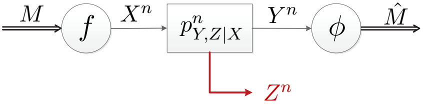
  (Simpler for GP: Z^n is i.i.d. and independent of M).

Unified Perspective: Target asymptotic probabilistic relations:

- **Gelfand-Pinsker Channel:** $\hat{M} = M$ (and M independent of Z^n).
- **Wiretap Channel:** $\hat{M} = M$ and M independent of Z^n.

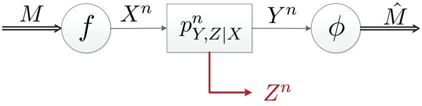
Unified Perspective - Quantification

The Wiretap Channel



Unified Perspective - Quantification

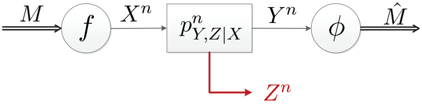
The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

Unified Perspective - Quantification

The Wiretap Channel



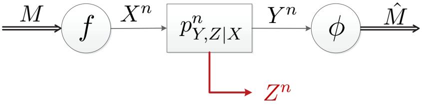
Code: Enc. (Stochastic) & Dec.

Induced Distribution:

$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Unified Perspective - Quantification

The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

Induced Distribution:

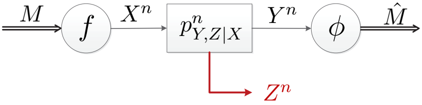
$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Achievability: $\exists\ q_Z$ s.t.

$$\left|\left| P_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\text{TV}} \to 0$$

Unified Perspective - Quantification

The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

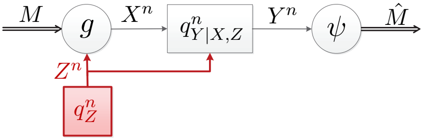
Induced Distribution:

$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Achievability: $\exists\ q_Z$ s.t.

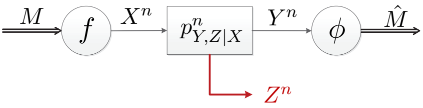
$$\left|\left| P_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\mathsf{TV}} \to 0$$

The Gelfand-Pinsker Channel



Unified Perspective - Quantification

The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

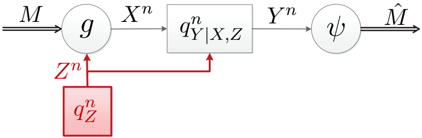
Induced Distribution:

$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Achievability: $\exists\ q_Z$ s.t.

$$\left|\left| P_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\text{TV}} \to 0$$

The Gelfand-Pinsker Channel

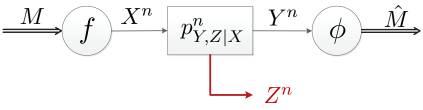


Induced Distribution:

$$Q \triangleq q^n_Z \frac{1}{|\mathcal{M}|} g_{X^n|M,Z^n} q^n_{Y|X,Z} \mathbb{1}_{\{\hat{M}=\psi(Y^n)\}}$$

Unified Perspective - Quantification

The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

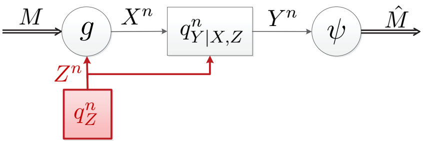
Induced Distribution:

$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Achievability: $\exists\ q_Z$ s.t.

$$\left|\left| P_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\text{TV}} \to 0$$

The Gelfand-Pinsker Channel



Induced Distribution:

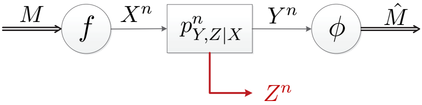
$$Q \triangleq q^n_Z \frac{1}{|\mathcal{M}|} g_{X^n|M,Z^n} q^n_{Y|X,Z} \mathbb{1}_{\{\hat{M}=\psi(Y^n)\}}$$

Achievability:

$$\left|\left| Q_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\text{TV}} \to 0$$

Unified Perspective - Quantification

The Wiretap Channel



Code: Enc. (Stochastic) & Dec.

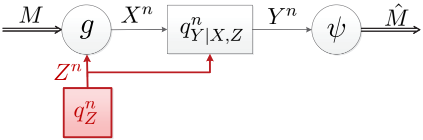
Induced Distribution:

$$P \triangleq \frac{1}{|\mathcal{M}|} f_{X^n|M} p^n_{Y,Z|X} \mathbb{1}_{\{\hat{M}=\phi(Y^n)\}}$$

Achievability: $\exists\ q_Z$ s.t.

$$\left|\left| P_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\mathsf{TV}} \to 0$$

The Gelfand-Pinsker Channel



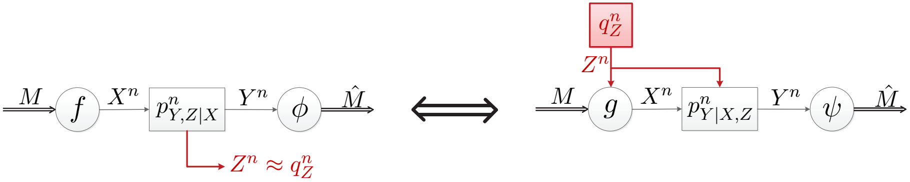
Induced Distribution:

$$Q \triangleq q^n_Z \frac{1}{|\mathcal{M}|} g_{X^n|M,Z^n} q^n_{Y|X,Z} \mathbb{1}_{\{\hat{M}=\psi(Y^n)\}}$$

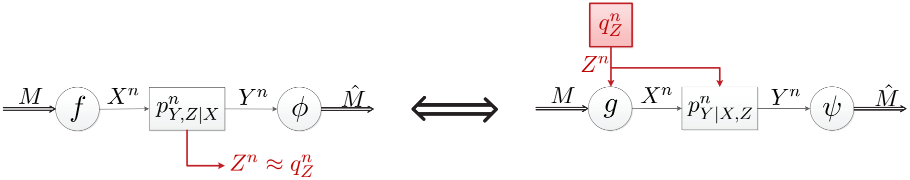
Achievability:

$$\left|\left| Q_{M,\hat{M},Z^n} - \frac{1}{|\mathcal{M}|} q^n_Z \mathbb{1}_{\{\hat{M}=M\}} \right|\right|_{\mathsf{TV}} \to 0$$

Analogy Transformation Principles

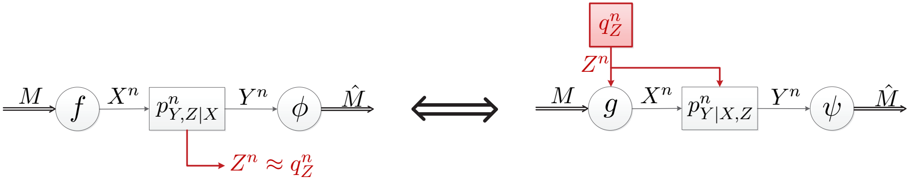


Analogy Transformation Principles



From Wiretap to Analogous GP Channel:

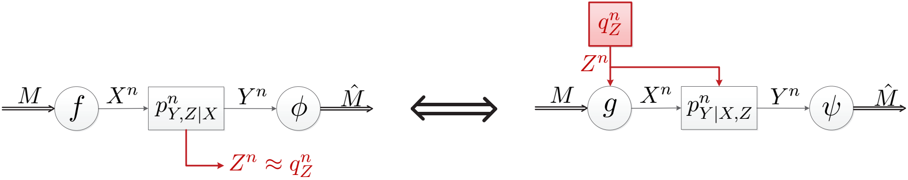
Analogy Transformation Principles



From Wiretap to Analogous GP Channel:

Given $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, p_{Y,Z|X})$ WTC with target q_Z:

Analogy Transformation Principles

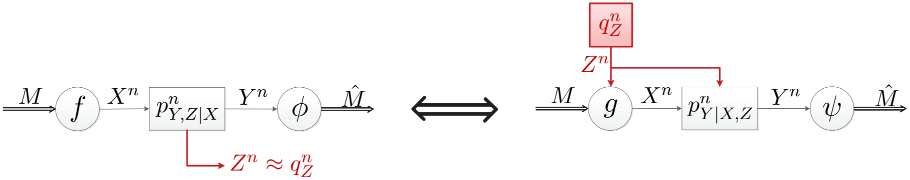


From Wiretap to Analogous GP Channel:

Given $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, p_{Y,Z|X})$ WTC with target q_Z:

1. Same alphabets for GPC as WTC.

Analogy Transformation Principles

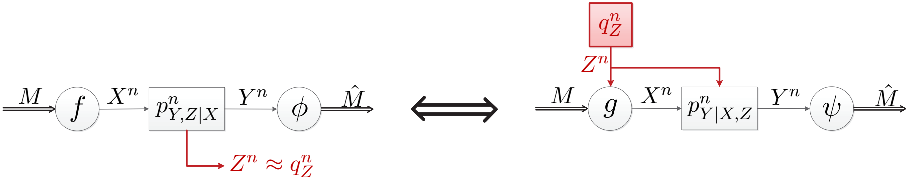


From Wiretap to Analogous GP Channel:

Given $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, p_{Y,Z|X})$ WTC with target q_Z:

1. Same alphabets for GPC as WTC.
2. Replace Eve's observation in WTC with i.i.d. state $Z^n \sim q^n_Z$.

Analogy Transformation Principles

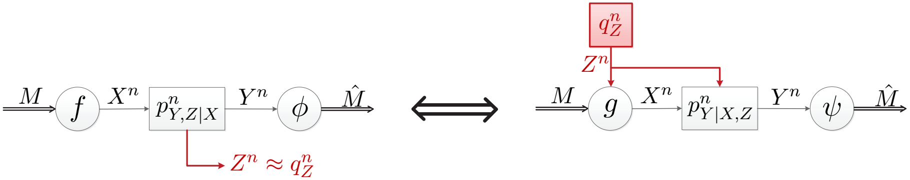


From Wiretap to Analogous GP Channel:

Given $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, p_{Y,Z|X})$ WTC with target q_Z:

1. Same alphabets for GPC as WTC.
2. Replace Eve's observation in WTC with i.i.d. state $Z^n \sim q^n_Z$.
3. Non-causally reveal Z^n to GP Enc. & Keep same Dec.

Analogy Transformation Principles

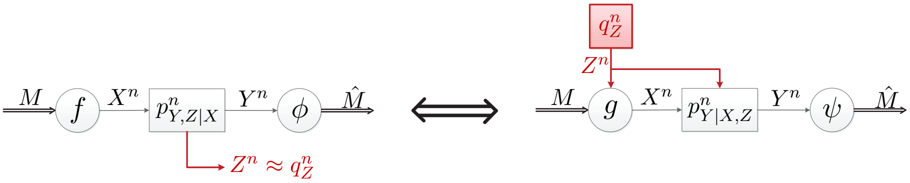


From Wiretap to Analogous GP Channel:

Given $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, p_{Y,Z|X})$ WTC with target q_Z:

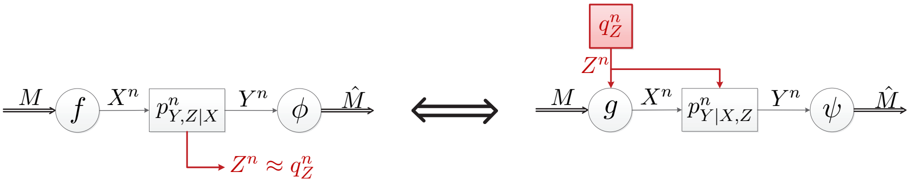
1. Same alphabets for GPC as WTC.
2. Replace Eve's observation in WTC with i.i.d. state $Z^n \sim q^n_Z$.
3. Non-causally reveal Z^n to GP Enc. & Keep same Dec.
4. Set GP channel transition prob. to $p_{Y|X,Z}$.

Main Analogy Result (Point-to-Point)



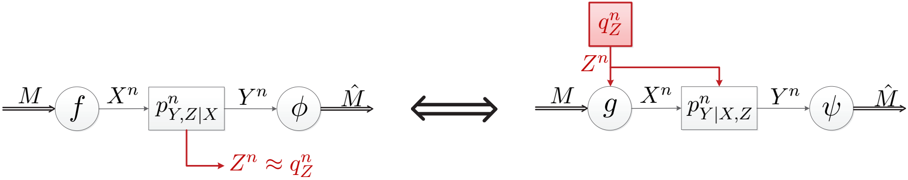
- Analogous WTC and GPC.

Main Analogy Result (Point-to-Point)



- Analogous WTC and GPC.
- $\{(f_n, \phi_n)\}_n$ 'good' (n, R) WTC codes for target q_Z.

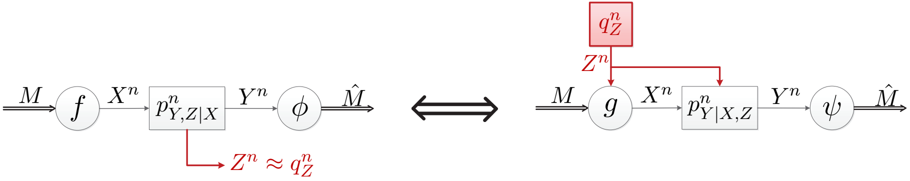
Main Analogy Result (Point-to-Point)



- Analogous WTC and GPC.
- $\{(f_n, \phi_n)\}_n$ 'good' (n, R) WTC codes for target q_Z.

  $\Longrightarrow$ Induced WTC distribution $P_n \triangleq P_{M,X^n,Y^n,Z^n,\hat{M}}$

Main Analogy Result (Point-to-Point)

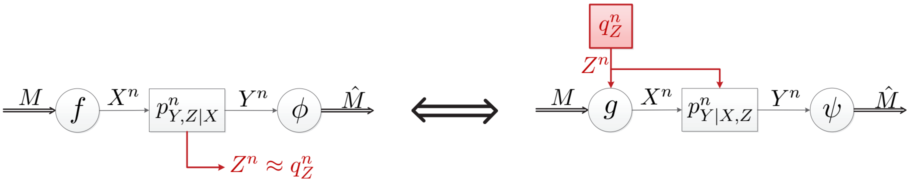


- Analogous WTC and GPC.
- $\{(f_n, \phi_n)\}_n$ 'good' (n, R) WTC codes for target q_Z.

  $\Longrightarrow$ Induced WTC distribution $P_n \triangleq P_{M,X^n,Y^n,Z^n,\hat{M}}$

  $\Longrightarrow$ Calculate $g_n \triangleq P_{X^n|M,Z^n}$ and set $\psi_n = \phi_n$.

Main Analogy Result (Point-to-Point)



- Analogous WTC and GPC.
- $\{(f_n, \phi_n)\}_n$ 'good' (n, R) WTC codes for target q_Z.

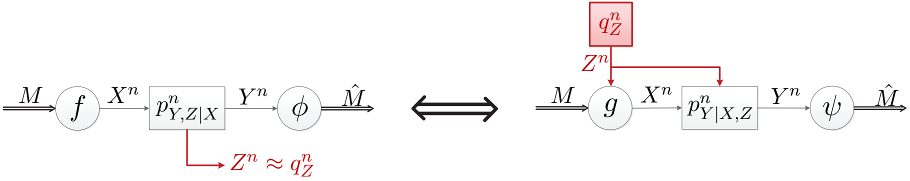
  $\Longrightarrow$ Induced WTC distribution $P_n \triangleq P_{M,X^n,Y^n,Z^n,\hat{M}}$

  $\Longrightarrow$ Calculate $g_n \triangleq P_{X^n|M,Z^n}$ and set $\psi_n = \phi_n$.

Theorem

1. $\{(g_n, \psi_n)\}_n$ *'good' (n, R) codes for analogous GPC:* $\mathbb{P}(\textit{error}) \to 0$.

Main Analogy Result (Point-to-Point)



- Analogous WTC and GPC.
- $\{(f_n, \phi_n)\}_n$ 'good' (n, R) WTC codes for target q_Z.

  $\Longrightarrow$ Induced WTC distribution $P_n \triangleq P_{M,X^n,Y^n,Z^n,\hat{M}}$

  $\Longrightarrow$ Calculate $g_n \triangleq P_{X^n|M,Z^n}$ and set $\psi_n = \phi_n$.

Theorem

1. $\{(g_n, \psi_n)\}_n$ *'good'* (n, R) *codes for analogous GPC:* $\mathbb{P}($*error*$) \to 0$.
2. Q_n *is induced by* $(g_n, \psi_n) \Longrightarrow ||P_n - Q_n||_{\text{TV}} \to 0$ *(superlinearly)*.

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \big[I(U;Y) - I(U;Z)\big].$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right].$ **Converse..?**

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \big[I(U;Y) - I(U;Z) \big].$ **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \big[I(U;Y) - I(U;Z) \big].$ **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$:

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right].$ **Converse..?**

1. $\left\{(f_n, \phi_n)\right\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\left\{(g_n, \phi_n)\right\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\left\{(f_n, \phi_n)\right\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\left\{(g_n, \phi_n)\right\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1)**

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\implies$ good GPC (n, R) codes (Q_n induced dist.)**

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \big[I(U;Y) - I(U;Z)\big]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n,R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\implies$ good GPC (n,R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\Big[I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Y_i) - I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Z_i)\Big] + \epsilon_n$$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\Longrightarrow$ good GPC (n, R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Y_i) - I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Z_i) \right] + \epsilon_n$$

⊛ **Thm. Part (2)**

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\implies$ good GPC (n, R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Y_i) - I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Z_i) \right] + \epsilon_n$$

⊛ **Thm. Part (2) $\implies$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right].$ **Converse..?**

1. $\{(f_n,\phi_n)\}_n$ - good (n,R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n,\phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\implies$ good GPC (n,R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\left[I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Y_i) - I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Z_i)\right] + \epsilon_n$$

⊛ **Thm. Part (2) $\implies$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\left[I_{P_n}(M,Y^{i-1},Z_{i+1}^n;Y_i) - I_{P_n}(M,Y^{i-1},Z_{i+1}^n;Z_i)\right] + \epsilon_n + \delta_n$$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \big[I(U;Y) - I(U;Z)\big]$. **Converse..?**

1. $\{(f_n,\phi_n)\}_n$ - good (n,R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n,\phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\Longrightarrow$ good GPC (n,R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\Big[I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Y_i) - I_{Q_n}(M,Y^{i-1},Z_{i+1}^n;Z_i)\Big] + \epsilon_n$$

⊛ **Thm. Part (2) $\Longrightarrow$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\Big[I_{P_n}(\underbrace{M,Y^{i-1},Z_{i+1}^n}_{\triangleq U_i};Y_i) - I_{P_n}(\underbrace{M,Y^{i-1},Z_{i+1}^n}_{\triangleq U_i};Z_i)\Big] + \epsilon_n + \delta_n$$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\Longrightarrow$ good GPC (n, R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Y_i) - I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Z_i) \right] + \epsilon_n$$

⊛ **Thm. Part (2) $\Longrightarrow$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{P_n}(U_i; Y_i) - I_{P_n}(U_i; Z_i) \right] + \epsilon_n + \delta_n$$

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z)\right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\Longrightarrow$ good GPC (n, R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\left[I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Y_i) - I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Z_i)\right] + \epsilon_n$$

⊛ **Thm. Part (2) $\Longrightarrow$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

$$R \leq \frac{1}{n}\sum_{i=1}^{n}\left[I_{P_n}(U_i; Y_i) - I_{P_n}(U_i; Z_i)\right] + \epsilon_n + \delta_n$$

4. Single-letterize + Verify Markov relations (hold under P_n)

Simple Application - New WTC Converse Proof

We know: $\mathsf{C}_{\mathsf{WTC}}(p_{Y,Z|X}) \geq \max_{p_{U,X}} \left[I(U;Y) - I(U;Z) \right]$. **Converse..?**

1. $\{(f_n, \phi_n)\}_n$ - good (n, R) WTC codes for q_Z (P_n induced dist.)
2. Analogous GPC $(q_Z, p_{Y|X,Z})$: Construct $\{(g_n, \phi_n)\}_n$, $g_n \triangleq P_{X^n|M,Z^n}$

⊛ **Thm. Part (1) $\implies$ good GPC (n, R) codes (Q_n induced dist.)**

3. 'Borrow' steps from GP converse ($H_{P_n}(M) = H_{Q_n}(M) = nR$):

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Y_i) - I_{Q_n}(M, Y^{i-1}, Z_{i+1}^n; Z_i) \right] + \epsilon_n$$

⊛ **Thm. Part (2) $\implies$ $||P_n - Q_n||_{\mathsf{TV}} \to 0$ + MI domination:**

$$R \leq \frac{1}{n} \sum_{i=1}^{n} \left[I_{P_n}(U_i; Y_i) - I_{P_n}(U_i; Z_i) \right] + \epsilon_n + \delta_n$$

4. Single-letterize + Verify Markov relations (hold under P_n) ■

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

Analogy - Extensions to Multiuser

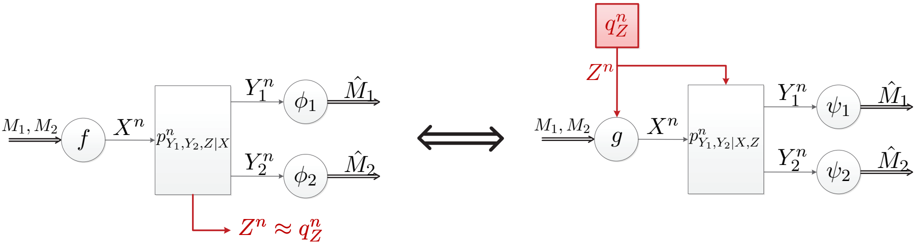
Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

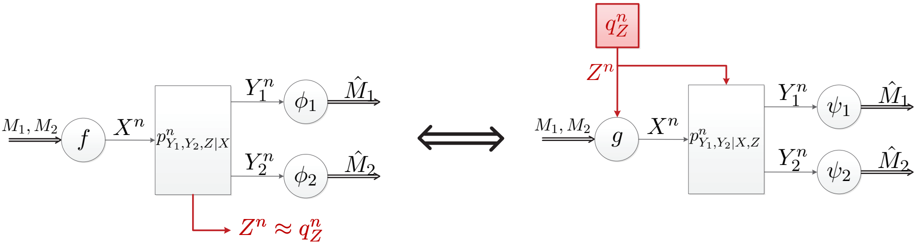
From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC



Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC

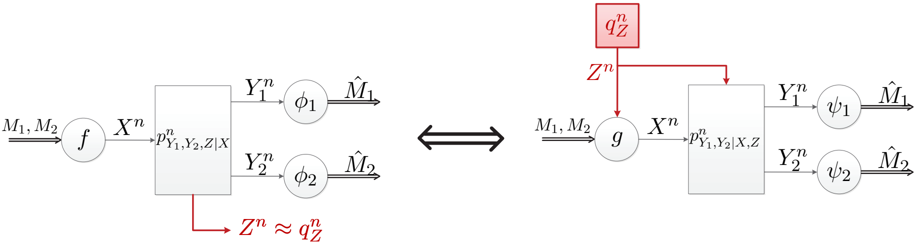


⊛ **Point-to-point theorem extends:**

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC



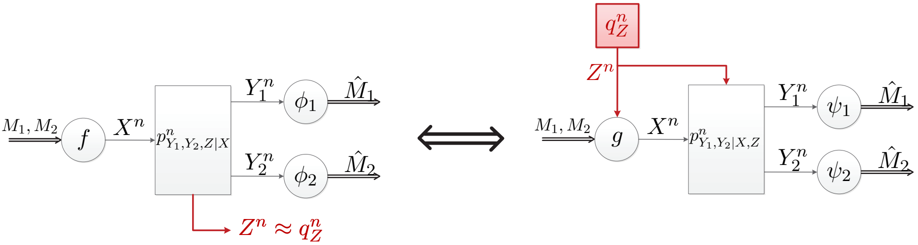
⊛ **Point-to-point theorem extends:**

$\Longrightarrow$ Good WT-BC codes induce good GP-BC codes.

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC



⊛ **Point-to-point theorem extends:**

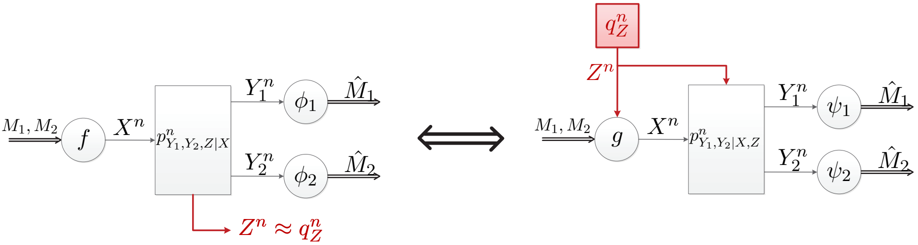
$\Longrightarrow$ Good WT-BC codes induce good GP-BC codes.

$\Longrightarrow$ Induced distributions are close in TV.

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC

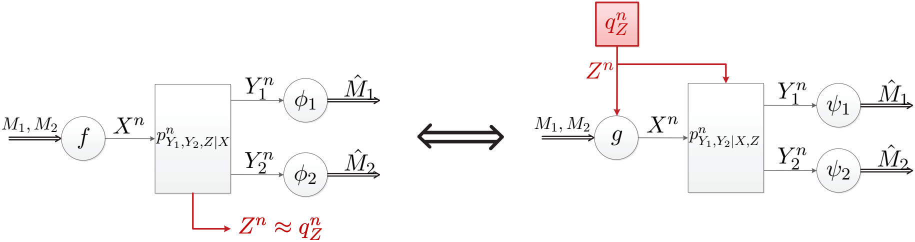


- **Point-to-point theorem extends:**
  - $\Longrightarrow$ Good WT-BC codes induce good GP-BC codes.
  - $\Longrightarrow$ Induced distributions are close in TV.
- **Includes:** Semi-Det. BC / Degraded BC / Rx. Cooperation / Rx. CSI.

Analogy - Extensions to Multiuser

Analogy naturally extends to wiretap and GP BCs with the same 4 steps:

From $p_{Y_1,Y_2,Z|X}$ WT-BC with target q_Z construct $(q_Z, p_{Y_1,Y_2|X,Z})$ GP-BC

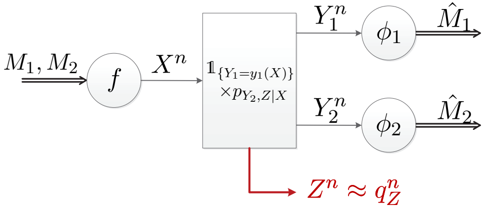


- **Point-to-point theorem extends:**
  - $\Longrightarrow$ Good WT-BC codes induce good GP-BC codes.
  - $\Longrightarrow$ Induced distributions are close in TV.
- **Includes:** Semi-Det. BC / Degraded BC / Rx. Cooperation / Rx. CSI.
- Exploit existing outer bounds for GP-BCs to progress WT-BC study.

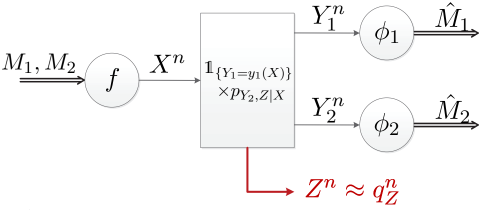
Semi-Deterministic Wiretap BCs

Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$



Semi-Deterministic Wiretap BCs



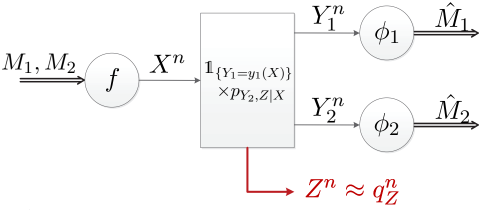
Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

Semi-Deterministic Wiretap BCs



Semi-Deterministic:

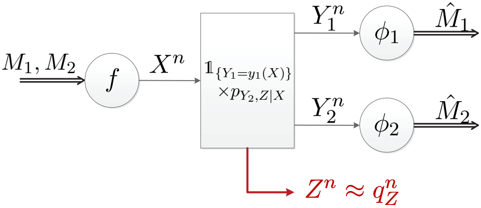
$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

Recent Work: [Benammar-Piantanida 2015]

Semi-Deterministic Wiretap BCs



Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

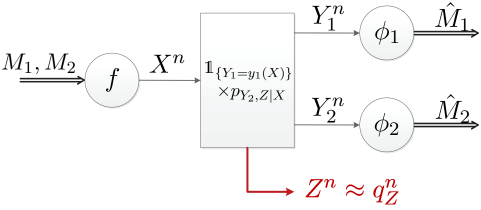
Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

Recent Work: [Benammar-Piantanida 2015]

- **Extra Assumption:** Stochastic Rx. less-noisy than Eve.

Semi-Deterministic Wiretap BCs



Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

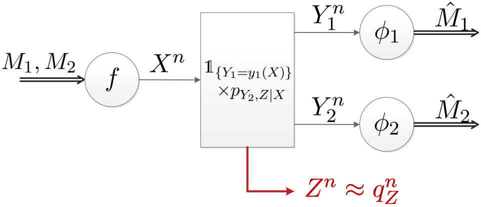
Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

Recent Work: [Benammar-Piantanida 2015]

- **Extra Assumption:** Stochastic Rx. less-noisy than Eve.
- **Result:** Secrecy-capacity region (2 auxiliaries)

Semi-Deterministic Wiretap BCs



Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

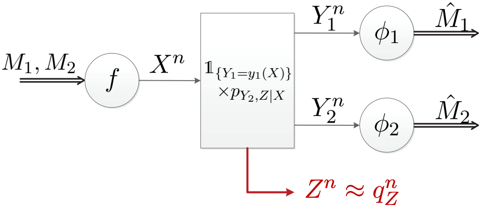
Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

Recent Work: [Benammar-Piantanida 2015]

- **Extra Assumption:** Stochastic Rx. less-noisy than Eve.
- **Result:** Secrecy-capacity region (2 auxiliaries)
  - **Achievability:** One auxiliary & Doesn't rely on less-noisy assumption.

Semi-Deterministic Wiretap BCs



Semi-Deterministic:

$$p_{Y_1,Y_2,Z|X} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$$

Achievability: $\exists\ q_Z$ s.t.

$$P_{M_1,M_2,Z^n,\hat{M}_1,\hat{M}_2} \approx \frac{1}{|\mathcal{M}_1||\mathcal{M}_2|} q_Z^n \mathbb{1}_{\{(\hat{M}_1,\hat{M}_2)=(M_1,M_2)\}}$$

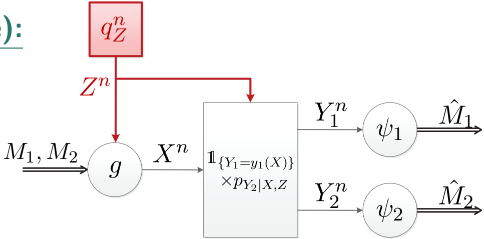
Recent Work: [Benammar-Piantanida 2015]

- **Extra Assumption:** Stochastic Rx. less-noisy than Eve.
- **Result:** Secrecy-capacity region (2 auxiliaries)
  - **Achievability:** One auxiliary & Doesn't rely on less-noisy assumption.
  - **Converse:** Needs both - memory in Z^n & correlation with (M_1, M_2).

Analogous Semi-Deterministic Gelfand-Pinsker BCs
[Lapidoth-Wang 2013]

Semi-Deterministic (Special Case):

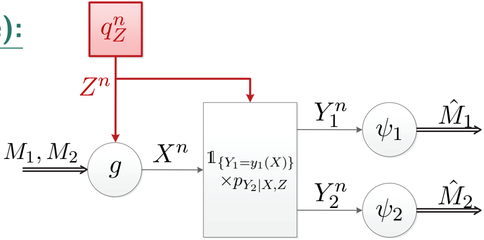
$$q_{Y_1,Y_2|X,Z} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2|X,Z}$$



Analogous Semi-Deterministic Gelfand-Pinsker BCs
[Lapidoth-Wang 2013]

Semi-Deterministic (Special Case):

$$q_{Y_1,Y_2|X,Z} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2|X,Z} = p_{Y_1,Y_2|X,Z}$$

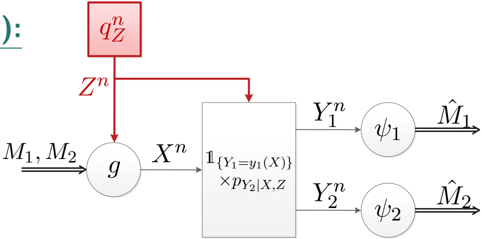


Analogous Semi-Deterministic Gelfand-Pinsker BCs

[Lapidoth-Wang 2013]

Semi-Deterministic (Special Case):

$$q_{Y_1,Y_2|X,Z} = \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2|X,Z}$$
$$= p_{Y_1,Y_2|X,Z}$$



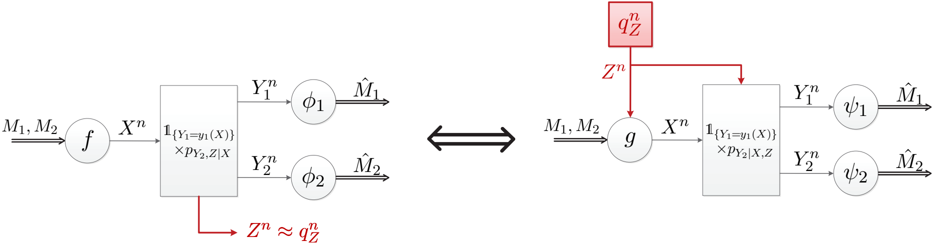
Theorem (Lapidoth-Wang 2013)

The capacity region of $(q_Z, \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2|X,Z})$ *GP-BC is union of*

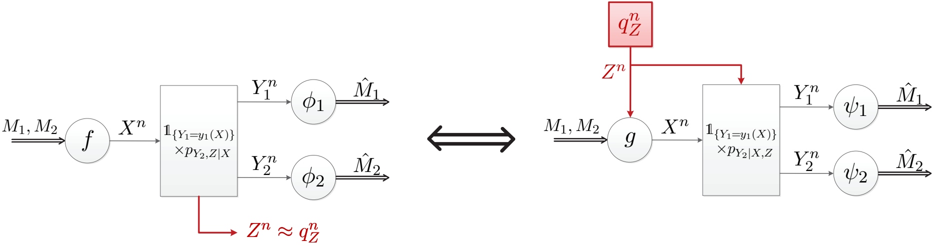
$$R_1 \le H(Y_1|Z)$$
$$R_2 \le I(U;Y_2) - I(U;Z)$$
$$R_1 + R_2 \le H(Y_1|Z) + I(U;Y_2) - I(U;Y_1,Z)$$

over all $q_Z q_{U,X|Z} \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2|X,Z}$.

Semi-Deterministic WT-BC - Capacity via Analogy



Semi-Deterministic WT-BC - Capacity via Analogy



Theorem

The secrecy-capacity region of $\mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$ *WT-BC is union of*

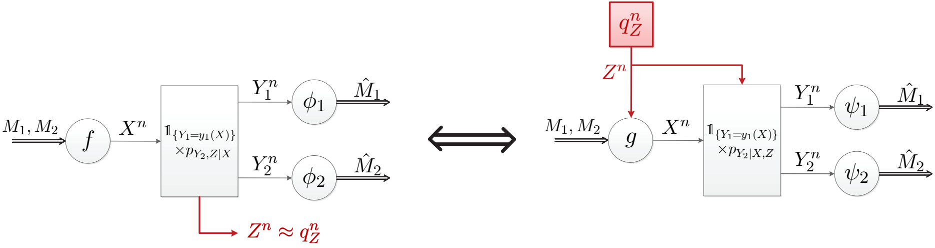
$$R_1 \leq H(Y_1|Z)$$

$$R_2 \leq I(U;Y_2) - I(U;Z)$$

$$R_1 + R_2 \leq H(Y_1|Z) + I(U;Y_2) - I(U;Y_1,Z)$$

over all $p_{U,X} \mathbb{1}_{\{Y_1=y_1(X)\}} p_{Y_2,Z|X}$.

Semi-Deterministic WT-BC - Capacity via Analogy



Theorem

The secrecy-capacity region of $\mathbb{1}_{\{Y_1=y_1(X)\}}p_{Y_2,Z|X}$ *WT-BC is union of*

$$R_1 \leq H(Y_1|Z)$$

$$R_2 \leq I(U;Y_2) - I(U;Z)$$

$$R_1 + R_2 \leq H(Y_1|Z) + I(U;Y_2) - I(U;Y_1,Z)$$

over all $p_{U,X}\mathbb{1}_{\{Y_1=y_1(X)\}}p_{Y_2,Z|X}$.

⊛ Single auxiliary & no less-noisy assumption.

Summary

- New analogy framework between wiretap and GP channels

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)
- 'Good' wiretap codes $\Longrightarrow$ 'Good' GP codes.

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)
- ‘Good’ wiretap codes $\Longrightarrow$ ‘Good’ GP codes.
- Exploit existing GP (converse) results to progress wiretap study.

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)
- 'Good' wiretap codes $\Longrightarrow$ 'Good' GP codes.
- Exploit existing GP (converse) results to progress wiretap study.
- **Application:** Secrecy-capacity of semi-det. WT-BC.

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)
- 'Good' wiretap codes $\Longrightarrow$ 'Good' GP codes.
- Exploit existing GP (converse) results to progress wiretap study.
- **Application:** Secrecy-capacity of semi-det. WT-BC.
- **Available on arXiv**: `https://arxiv.org/abs/1712.10299`.

Summary

- New analogy framework between wiretap and GP channels
  - Point-to-Point
  - Multiuser broadcasting (semi-det./degraded/cooperation/CSI)
- 'Good' wiretap codes $\Longrightarrow$ 'Good' GP codes.
- Exploit existing GP (converse) results to progress wiretap study.
- **Application:** Secrecy-capacity of semi-det. WT-BC.
- **Available on arXiv**: `https://arxiv.org/abs/1712.10299`.

Thank you!