Secure Lossy Source Coding with Side Information at the Decoders

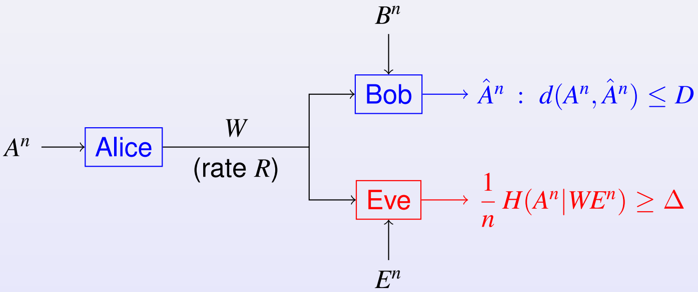
Joffrey Villard and Pablo Piantanida

SUPELEC, Telecom. Dpt., Gif-sur-Yvette, France.

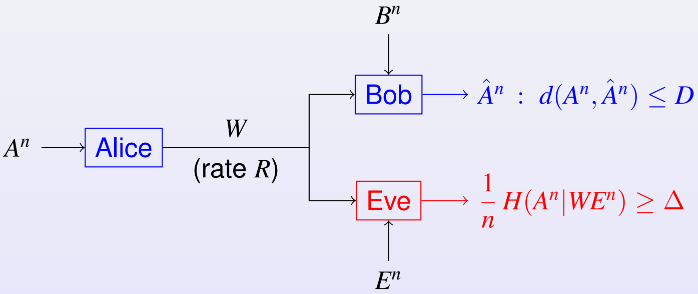
Email: {joffrey.villard, pablo.piantanida}@supelec.fr

Allerton 2010

Introduction

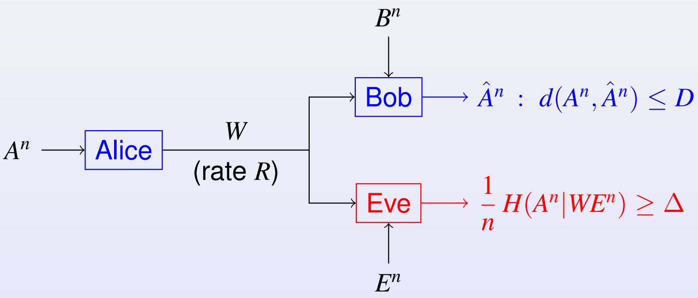


Introduction



Tradeoff: Min. R + Min. D + Max. Δ

Introduction



Tradeoff: Min. R + Min. D + Max. Δ

Our Aim: Find all *achievable* tuples (R, D, Δ)

References

Source coding with side-information.

D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. IT*, 19(4):471–480, 1973.

A.D. Wyner and J. Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. IT*, 22(1):1–10, 1976.

Information-theoretic secrecy/security.

C.E. Shannon. Communication theory of secrecy systems. *BSTJ*, 28:656–715, 1949.

A.D. Wyner. The wire-tap channel. *BSTJ*, 54(8):1355–1387, 1975.

I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. IT*, 24(3):339–348, 1978.

Y. Liang, H.V. Poor, and S. Shamai. *Information theoretic security*. Now Publishers, 2009.

R. Liu and W. Trappe. *Securing wireless communications at the physical layer*. Springer, 2010.

Secure source coding.

H. Yamamoto. Rate-distortion theory for the Shannon cipher system. *IEEE Trans. IT*, 43(3):827–835, 1997.

V. Prabhakaran and K. Ramchandran. On secure distributed source coding. In *Proc. ITW*, p. 442–447, 2007.

D. Gunduz, E. Erkip, and H.V. Poor. Lossless compression with security constraints. In *Proc. ISIT*, p. 111–115, 2008.

R. Tandon, S. Ulukus, and K. Ramchandran. Secure source coding with a helper. In *Proc. Allerton*, p. 1061–1068, 2009.

N. Merhav. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Trans. IT*, 54(6):2723–2734, 2008.

Outline

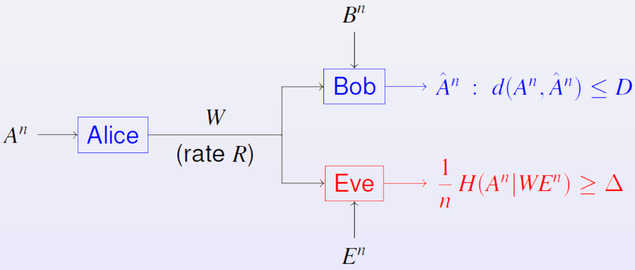
Definitions

- $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{E}$: three finite sets
- $(A_i, B_i, E_i)_{i \geq 1}$: i.i.d random variables on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$ with known joint distribution $p(a, b, e)$
- $d : \mathcal{A} \times \mathcal{A} \to [0\,; d_{max}]$: a finite distortion measure

An (n, R)-code for source coding in this setup is defined by

- An encoding function at Alice $f : \mathcal{A}^n \to \{1, \ldots, 2^{nR}\}$
- A decoding function at Bob $g : \{1, \ldots, 2^{nR}\} \times \mathcal{B}^n \to \mathcal{A}^n$

Definitions (cont.)



A tuple $(R, D, \Delta) \in \mathbb{R}^3_+$ is achievable if,

for any $\varepsilon > 0$, there exists an $(n, R + \varepsilon)$-code (f, g) such that:

$$
\begin{aligned}
\mathbb{E}\left[d(A^n, g(f(A^n), B^n))\right] &\leq D + \varepsilon \\
\frac{1}{n} H(A^n | f(A^n), E^n) &\geq \Delta - \varepsilon
\end{aligned}
$$

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* *i.f.f.* *there exist*

- *sets* $\mathcal{U}$, $\mathcal{V}$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\ \Delta &\leq \left[H(A|VB) + I(A; B|U) - I(A; E|U)\right]_+ \end{aligned}$$

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* *i.f.f.* *there exist*

- *sets* $\mathcal{U}, \mathcal{V}$ $\quad \|\mathcal{U}\| \leq \|\mathcal{A}\| + 2, \ \|\mathcal{V}\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

$$
\begin{aligned}
R &\geq I(V; A|B) \\
D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\
\Delta &\leq \left[H(A|VB) + I(A; B|U) - I(A; E|U)\right]_+
\end{aligned}
$$

Outline

Lossless Secure Source Coding ($D = 0$)

Corollary (Prabhakaran2007,Gunduz2008)

$(R, 0, \Delta)$ *is achievable* *i.f.f.* *there exist*

- *a set* $\mathcal{U}$
- *a r.v.* U *on* $\mathcal{U}$

such that $U - A - (B, E)$ *form a Markov chain*

$$\begin{aligned} R &\geq H(A|B) \\ \Delta &\leq \Big[I(A;B|U) - I(A;E|U) \Big]_+ \end{aligned}$$

Set $V = A$ in the main theorem

Outline

B is Less Noisy Than E

Assumption

$I(U;B) \geq I(U;E)$ for each r.v. U s.t. $U - A - (B,E)$ form a MC

B is Less Noisy Than E

Assumption

$I(U;B) \geq I(U;E)$ for each r.v. U s.t. $U - A - (B,E)$ form a MC

Corollary

(R, D, Δ) is achievable i.f.f. there exist

- *a r.v. V on some set $\mathcal{V}$*
- *a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$*

such that $V - A - (B,E)$ *form a Markov chain*

$$
\begin{aligned}
R &\geq I(V;A|B) \\
D &\geq \mathbb{E}[d(A, \hat{A}(V,B))] \\
\Delta &\leq \Big[H(A|VB) + I(A;B) - I(A;E)\Big]_+
\end{aligned}
$$

B is Less Noisy Than E

Corollary

(R, D, Δ) is achievable i.f.f. there exist

- *a r.v. V on some set $\mathcal{V}$*
- *a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$*

such that $V - A - (B, E)$ form a Markov chain

$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] \\ \Delta &\leq \Big[H(A|VB) + I(A; B) - I(A; E)\Big]_+ \end{aligned}$$

- Set $U = cst$ in the main theorem
- Wyner-Ziv coding achieves the optimal performance

Outline

Rate

$U - V - A - (B, E)$ form a Markov chain

1. a simple binning operation to transmit U (message r_1)

$$R_1 > I(U; A|B)$$

2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob (message r_2)

$$R_2 > I(V; A|UB)$$

$\Rightarrow$ Sufficient condition:

$$R_1 + R_2 \; > \; I(V; A|B)$$

Details

Distortion at Bob

Bob can decode U^n and V^n from message (r_1, r_2) and SI B^n

$$\mathbb{E}\left[d(A^n, g(f(A^n), B^n))\right] \approx \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, g_i(V^n, B^n))\right]$$

$$= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}(V_i, B_i))\right]$$

$$= \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

Sufficient condition:

$$D \geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

Equivocation Rate at Eve

Eve receives messsage (r_1, r_2) and SI E^n

$$
\begin{aligned}
\frac{1}{n} H(A^n | f(A^n)\, E^n) &= \frac{1}{n} H(A^n | r_1 r_2 E^n) \\
&= \frac{1}{n}\Big[H(A^n) - I(A^n; r_1 E^n) - I(A^n; r_2 | r_1 E^n) \Big] \\
\big\{ I(\cdot;\cdot|\cdot) \le H(\cdot|\cdot) \le H(\cdot) \big\} \quad &\ge \frac{1}{n}\Big[H(A^n) - I(A^n; U^n E^n) - H(r_2) \Big] \\
\big\{ \text{i.i.d. r.v., } r_2 \in \{1, \ldots, 2^{nR_2}\} \big\} \quad &\ge H(A|UE) - R_2
\end{aligned}
$$

Sufficient condition:

$$
\Delta \le \Big[H(A|UE) - R_2 \Big]_+
$$

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* $\boxed{\Longleftarrow}$ *there exist*

- *sets* $\mathcal{U}, \mathcal{V}$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\ \Delta &\leq \left[H(A|VB) + I(A; B|U) - I(A; E|U)\right]_+ \end{aligned}$$

Outline

Definitions

- An achievable tuple: (R, D, Δ)
- Transmitted message: $W = f(A^n)$
- Auxiliary random variables:

$$\begin{aligned} U_i &= (W, \quad B_{i+1}^n, E^{i-1}) \\ V_i &= (W, A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1}) \end{aligned}$$

- $U_i - V_i - A_i - (B_i, E_i)$ form a Markov chain

Rate

$$
\begin{aligned}
nR &\geq H(W) \\
&= I(W;A^nB^nE^n) \\
&\geq I(W;A^nE^n|B^n) \\
\{\text{chain rule}\} &= \sum_{i=1}^{n} I(W;A_iE_i|A^{i-1}B^nE^{i-1}) \\
&= \sum_{i=1}^{n} I(WA^{i-1}B^{i-1}B_{i+1}^nE^{i-1};A_iE_i|B_i) \\
&\qquad -I(A^{i-1}B^{i-1}B_{i+1}^nE^{i-1};A_iE_i|B_i) \\
\{\text{indep. across time}\} &\geq \sum_{i=1}^{n} I(V_i;A_i|B_i)
\end{aligned}
$$

Distortion at Bob

- Bob reconstructs $g(W, B^n)$
- $V_i = (W, A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1})$

$$\hat{A}_i(V_i, B_i) \triangleq g_i(W, B^{i-1}, B_i, B_{i+1}^n)$$

Distortion at Bob

- Bob reconstructs $g(W, B^n)$
- $V_i = (W, A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1})$

$$\hat{A}_i(V_i, B_i) \triangleq g_i(W, B^{i-1}, B_i, B_{i+1}^n)$$

Component-wise mean distortion:

$$\begin{aligned} \mathbb{E}\Big[d(A^n, g(f(A^n), B^n))\Big] &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\Big[d(A_i, \hat{A}_i(V_i, B_i))\Big] \\ &\leq D \end{aligned}$$

Equivocation Rate at Eve

$$
\begin{aligned}
H(A^n|W\,E^n) &= H(A^n|W) - I(A^n;E^n|W) \\
\{W - A^n - (B^n, E^n)\} &= H(A^n|WB^n) + I(A^n;B^n) - I(W;B^n) - I(A^n;E^n) + I(W;E^n) \\
\{\text{chain rule}\} &= \sum_{i=1}^{n} H(A_i|WA^{i-1}B^n) + I(A_i;B_i) - I(A_i;E_i) \\
&\qquad - I(WB_{i+1}^n;B_i) + I(WE^{i-1};E_i) \\
\{\text{Csiszar–Körner}\} &= \sum_{i=1}^{n} H(A_i|WA^{i-1}B_{i-1}B_iB_{i+1}^nE^{i-1}) + I(A_i;B_i) - I(A_i;E_i) \\
&\qquad + I(E_i;WB_{i+1}^nE^{i-1}) - I(B_i;WB_{i+1}^nE^{i-1}) \\
\{U_i - A_i - (B_i, E_i)\} &= \sum_{i=1}^{n} H(A_i|V_iB_i) + I(A_i;B_i|U_i) - I(A_i;E_i|U_i)
\end{aligned}
$$

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* $\boxed{\Longrightarrow}$ *there exist*

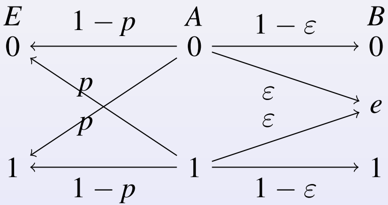
- *sets* $\mathcal{U}, \mathcal{V}$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

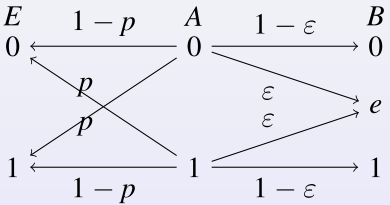
$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\ \Delta &\leq \left[H(A|VB) + I(A; B|U) - I(A; E|U)\right]_+ \end{aligned}$$

Outline

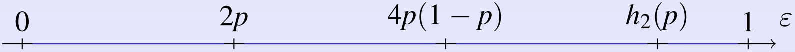
Binary Source with BEC and BSC Side Informations



Binary Source with BEC and BSC Side Informations

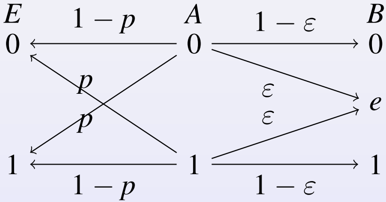


Neither Bob nor Eve is a lessnoisy decoder for all values of (p, ε):

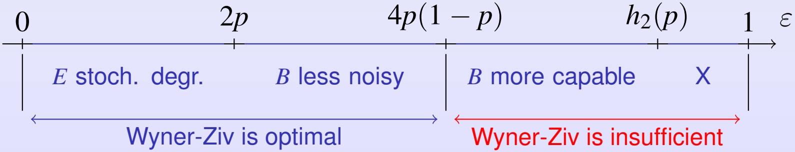


E stoch. degr.	B less noisy	B more capable	X
$A - B - \tilde{E}$	$U - A - (B,E) \Rightarrow I(U;B) \geq I(U;E)$	$I(A;B) \geq I(A;E)$	

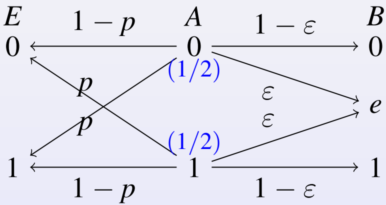
Binary Source with BEC and BSC Side Informations



Neither Bob nor Eve is a lessnoisy decoder for all values of (p, ε):



Binary Source with BEC and BSC Side Informations



- distortion d: Hamming distance
- source A: uniformly distributed

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* *i.f.f.* *there exist*

- *sets* $\mathcal{U}, \mathcal{V}$ $\quad \|\mathcal{U}\| \leq \|\mathcal{A}\| + 2, \ \|\mathcal{V}\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\ \Delta &\leq \left[H(A|VB) + I(A; B|U) - I(A; E|U)\right]_+ \end{aligned}$$

Main Result

Theorem (Rate-Distortion-Equivocation Region)

(R, D, Δ) *is achievable* *i.f.f.* *there exist*

- *sets* $\mathcal{U}, \mathcal{V}$ $\|\mathcal{U}\| \leq 4,\ \|\mathcal{V}\| \leq 12$
- *r.v.* U *on* $\mathcal{U}$, V *on* $\mathcal{V}$
- *a function* $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$

such that $U - V - A - (B, E)$ *form a Markov chain*

$$\begin{aligned} R &\geq I(V; A|B) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\ \Delta &\leq \Big[H(A|VB) + I(A; B|U) - I(A; E|U)\Big]_+ \end{aligned}$$

Rate-Distortion-Equivocation Region

Proposition

(R, D, Δ) *is achievable* *i.f.f.*

there exist $\alpha, \beta \in [0, 1/2]$ *such that*

$$\begin{aligned} R &\geq \varepsilon\,(1 - h_2(\alpha))\ , \\ D &\geq \varepsilon\,\alpha\ , \\ \Delta &\leq \Big[\varepsilon\, h_2(\alpha) + (1-\varepsilon)\, h_2(\alpha \star \beta) - h_2(p \star \alpha \star \beta) + h_2(p)\Big]_+ . \end{aligned}$$

- $a \star b = a(1-b) + (1-a)b$
- $h_2(x) = -x \log_2(x) - (1-x)\log_2(1-x)$

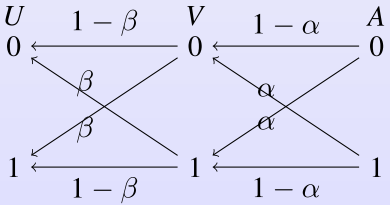
Rate-Distortion-Equivocation Region

Proposition

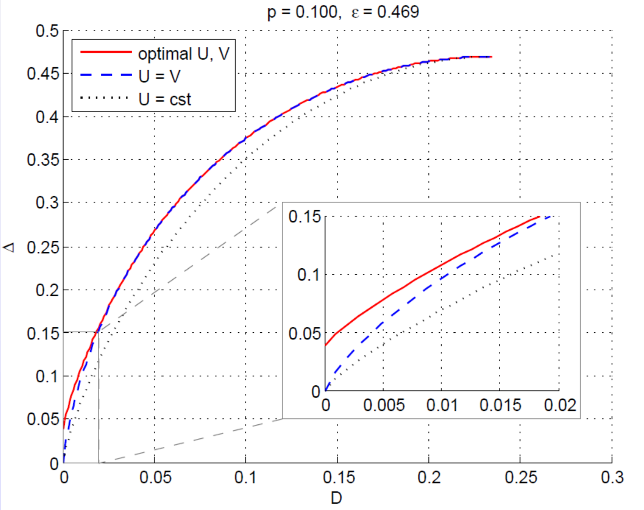
(R, D, Δ) *is achievable* *i.f.f.*

there exist $\alpha, \beta \in [0, 1/2]$ *such that*

$$\begin{aligned} R &\geq \varepsilon\,(1 - h_2(\alpha))\;, \\ D &\geq \varepsilon\,\alpha\;, \\ \Delta &\leq \Big[\varepsilon\, h_2(\alpha) + (1-\varepsilon)\, h_2(\alpha \star \beta) - h_2(p \star \alpha \star \beta) + h_2(p)\Big]_+ \;. \end{aligned}$$



Illustration



Equivocation rate at Eve Δ as a function of the distortion at Bob D

Summary and Discussion

- Complete single-letter characterization of the rate-distortion-equivocation region
- Binary sources with BEC and BSC Side Informations

Future work:

- Vector Gaussian sources and side informations
- Rate-distortion-distortion region

Thank you for your attention.

Appendix

Outline

E is Less Noisy Than B

Corollary

(R, D, Δ) is achievable i.f.f. there exist

- *a r.v. V on some set $\mathcal{V}$*
- *a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$*

such that $V - A - (B, E)$ form a Markov chain

$$
\begin{aligned}
R &\geq I(V; A|B) \\
D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] \\
\Delta &\leq H(A|VE)
\end{aligned}
$$

E is Less Noisy Than B

Corollary

(R, D, Δ) is achievable i.f.f. there exist

- *a r.v. V on some set $\mathcal{V}$*
- *a function $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$*

such that $V - A - (B, E)$ form a Markov chain

$$
\begin{aligned}
R &\geq I(V; A|B) \\
D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] \\
\Delta &\leq H(A|VE)
\end{aligned}
$$

- Set $U = V$ in the main theorem
- Wyner-Ziv coding achieves the optimal performance

Outline

Codebook generation

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

Codebook generation

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

- randomly pick 2^{nS_1} sequences $u^n(s_1)$ from $T_\epsilon^n(U)$
- divide them into 2^{nR_1} equal-size bins $\{B_1(r_1)\}_{r_1 \in \{1,\dots,2^{nR_1}\}}$

Then, for each codeword $u^n(s_1)$,

- randomly pick 2^{nS_2} sequences $v^n(s_1, s_2)$ from $T_\epsilon^n(V|u^n(s_1))$
- divide them into 2^{nR_2} equal-size bins $\{B_2(s_1, r_2)\}_{r_2 \in \{1,\dots,2^{nR_2}\}}$

Encoding

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

Sequence A^n is produced at Alice

- look for a codeword $u^n(s_1)$ s.t. $(u^n(s_1), A^n) \in T_\epsilon^n(U, A)$

$\rightarrow$ bin $B_1(r_1)$

- look for a codeword $v^n(s_1, s_2)$ s.t. $(v^n(s_2), A^n) \in T_\epsilon^n(V, A|u^n(s_1))$

$\rightarrow$ bin $B_2(s_1, r_2)$

- send the message $f(A^n) \triangleq (r_1, r_2)$

Encoding

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

Sequence A^n is produced at Alice

- look for a codeword $u^n(s_1)$ s.t. $(u^n(s_1), A^n) \in T_\epsilon^n(U, A)$

$\rightarrow$ bin $B_1(r_1)$ $\boxed{S_1 > I(U;A)}$

- look for a codeword $v^n(s_1, s_2)$ s.t. $(v^n(s_2), A^n) \in T_\epsilon^n(V, A|u^n(s_1))$

$\rightarrow$ bin $B_2(s_1, r_2)$ $\boxed{S_2 > I(V;A|U)}$

- send the message $f(A^n) \triangleq (r_1, r_2)$

Decoding

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

Bob receives (r_1, r_2) from Alice and his SI sequence B^n

- look for the unique codeword $u^n(s_1) \in B_1(r_1)$ s.t.

  $(u^n(s_1), B^n) \in T_\epsilon^n(U, B)$

- look for the unique codeword $v^n(s_1, s_2) \in B_2(s_1, r_2)$ s.t.

  $(v^n(s_1, s_2), B^n) \in T_\epsilon^n(V, B|u^n(s_1))$

Decoding

1. a simple binning operation to transmit U
2. a Wyner–Ziv coding to transmit A with SI (U, B) at Bob

Bob receives (r_1, r_2) from Alice and his SI sequence B^n

- look for the unique codeword $u^n(s_1) \in B_1(r_1)$ s.t.

  $(u^n(s_1), B^n) \in T_\epsilon^n(U, B)$ $\boxed{S_1 - R_1 < I(U;B)}$

- look for the unique codeword $v^n(s_1, s_2) \in B_2(s_1, r_2)$ s.t.

  $(v^n(s_1, s_2), B^n) \in T_\epsilon^n(V, B|u^n(s_1))$ $\boxed{S_2 - R_2 < I(V;B|U)}$

Rate

Markov Chain $U - V - A - (B, E)$

Encoding and decoding constraints:

$$\begin{aligned} S_1 &> I(U;A) \\ S_2 &> I(V;A|U) \\ S_1 - R_1 &< I(U;B) \\ S_2 - R_2 &< I(V;B|U) \end{aligned}$$

Rate

Markov Chain $U - V - A - (B, E)$

Encoding and decoding constraints:

$$
\begin{aligned}
R_1 &> I(U;A|B) \\
R_2 &> I(V;A|UB)
\end{aligned}
$$

Rate

Markov Chain $U - V - A - (B, E)$

Encoding and decoding constraints:

$$\begin{aligned} R_1 &> I(U;A|B) \\ R_2 &> I(V;A|UB) \end{aligned}$$

Sufficient condition:

$$R_1 + R_2 > I(V;A|B)$$

Return

Outline

Definition of New Random Variables

$$
\begin{aligned}
R &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_i; A_i|B_i) \\
D &\geq \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i, B_i))\right] \\
\Delta &\leq \frac{1}{n}\sum_{i=1}^{n} H(A_i|V_iB_i) + I(A_i; B_i|U_i) - I(A_i; E_i|U_i)
\end{aligned}
$$

Definition of New Random Variables

$$\begin{aligned} R &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_i; A_i|B_i) \\ D &\geq \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i, B_i))\right] \\ \Delta &\leq \frac{1}{n}\sum_{i=1}^{n} H(A_i|V_iB_i) + I(A_i; B_i|U_i) - I(A_i; E_i|U_i) \end{aligned}$$

Define:

- an independent r.v. Q unif. distributed over $\{1, \ldots, n\}$
- $A = A_Q, \quad B = B_Q, \quad E = E_Q, \quad U = (Q, U_Q), \quad V = (Q, V_Q)$

Definition of New Random Variables

$$
\begin{aligned}
R &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_i; A_i|B_i) \\
D &\geq \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i, B_i))\right] \\
\Delta &\leq \frac{1}{n}\sum_{i=1}^{n} H(A_i|V_iB_i) + I(A_i; B_i|U_i) - I(A_i; E_i|U_i)
\end{aligned}
$$

Define:

- an independent r.v. Q unif. distributed over $\{1, \dots, n\}$
- $A = A_Q, \quad B = B_Q, \quad E = E_Q, \quad U = (Q, U_Q), \quad V = (Q, V_Q)$

Then:

- $U - V - A - (B, E)$ form a Markov chain
- $(A, B, E) \sim p(a, b, e)$

Rate

$$\begin{aligned} R &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_i;A_i|B_i) \\ &= \frac{1}{n}\sum_{i=1}^{n} I(V_Q;A_Q|B_Q,Q=i) \\ &= I(V_Q;A_Q|B_Q,Q) \\ &= I(QV_Q;A_Q|B_Q) \\ &= I(V;A|B) \end{aligned}$$

Distortion at Bob

$$\begin{aligned} D &\geq \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[d(A_i,\hat{A}_i(V_i,B_i))\Big] \\ &= \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[d(A_Q,\hat{A}_Q(V_Q,B_Q))\,\Big|\,Q=i\Big] \\ &= \mathbb{E}\Big[d(A_Q,\hat{A}_Q(V_Q,B_Q))\Big] \\ &= \mathbb{E}\Big[d(A,\hat{A}(V,B))\Big] \end{aligned}$$

where

$$\hat{A}(V,B)=\hat{A}(Q,V_Q,B_Q)\triangleq\hat{A}_Q(V_Q,B_Q)$$

Equivocation Level at Eve

$$
\begin{aligned}
\Delta &\leq \frac{1}{n}\sum_{i=1}^{n} H(A_i|V_iB_i) + I(A_i;B_i|U_i) - I(A_i;E_i|U_i) \\
&= \frac{1}{n}\sum_{i=1}^{n} H(A_Q|V_QB_Q, Q=i) \\
&\qquad\qquad + I(A_Q;B_Q|U_Q, Q=i) - I(A_Q;E_Q|U_Q, Q=i) \\
&= H(A_Q|V_QB_Q, Q) + I(A_Q;B_Q|U_Q, Q) - I(A_Q;E_Q|U_Q, Q) \\
&= H(A|VB) + I(A;B|U) - I(A;E|U)
\end{aligned}
$$

Return

Outline

Cardinality Bounds

$$
\begin{aligned}
R &\geq H(A|B) - H(AB|V) + H(B|V) \\
D &\geq \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \\
\Delta &\leq \Big[H(AB|V) - H(B|V) + I(A;B|U) - I(A;E|U)\Big]_{+}
\end{aligned}
$$

Follow standard arguments[1]:

- identify continuous functions of prob. distributions
- use Fenchel-Eggleston-Carathéodory's theorem to define new admissible random variables

[1] [A. El Gamal and Y.-H. Kim. Lecture Notes on Netw IT. arXiv:1001.3404]

Cardinality Bounds (cont.)

$\|\mathcal{A}\| + 2$ continuous functions of $p(v|u)$:

$$\begin{cases} p(a|u) = \mathbb{E}[p(a|V)|U = u] \\ H(AB|V, U = u) - H(B|V, U = u) = H(VAB|U = u) - H(VB|U = u) \\ \mathbb{E}\left[d(A, \hat{A}(V, B))|U = u\right] \\ I(A; B|U = u) - I(A; E|U = u) \end{cases}$$

Cardinality Bounds (cont.)

$\|\mathcal{A}\| + 2$ continuous functions of $p(v|u)$:

$$\begin{cases} p(a|u) = \mathbb{E}[p(a|V)|U = u] \\ H(AB|V, U = u) - H(B|V, U = u) = H(VAB|U = u) - H(VB|U = u) \\ \mathbb{E}\left[d(A, \hat{A}(V, B))|U = u\right] \\ I(A; B|U = u) - I(A; E|U = u) \end{cases}$$

Fenchel-Eggleston-Carathéodory's theorem $\Rightarrow$ there exist:

- a set $\mathcal{U}'$ with $\|\mathcal{U}'\| \leq \|\mathcal{A}\| + 2$
- a r.v. U' on $\mathcal{U}'$ s.t. $p(a)$, $H(AB|V) - H(B|V)$, $\mathbb{E}[d(A, \hat{A}(V, B))]$ and $I(A; B|U) - I(A; E|U)$ are preserved

Cardinality Bounds (cont.)

For each $u' \in \mathcal{U}'$, $\|\mathcal{A}\| + 1$ continuous functions of $p(a|u', v)$:

$$\begin{cases} p(a|u', v) \\ H(AB|U' = u', V = v) - H(B|U' = u', V = v) \\ \mathbb{E}\left[d(A, \hat{A}(V, B))|U' = u', V = v\right] \end{cases}$$

Cardinality Bounds (cont.)

For each $u' \in \mathcal{U}'$, $\|\mathcal{A}\| + 1$ continuous functions of $p(a|u', v)$:

$$\begin{cases} p(a|u', v) \\ H(AB|U' = u', V = v) - H(B|U' = u', V = v) \\ \mathbb{E}\big[d(A, \hat{A}(V, B))|U' = u', V = v\big] \end{cases}$$

Fenchel-Eggleston-Carathéodory's theorem $\Rightarrow$ there exist:

- a set $\mathcal{V}'$ with $\|\mathcal{V}'\| \leq \|\mathcal{A}\| + 1$
- for each $u' \in \mathcal{U}'$, a r.v. $V'|\{U' = u'\}$ on $\mathcal{V}'$
  a function $\hat{A}'_{u'} : \mathcal{V}' \times \mathcal{B} \to \mathcal{A}$

s.t. $p(a|u')$, $H(AB|U' = u', V) - H(B|U' = u', V)$ and $\mathbb{E}[d(A, \hat{A}(V, B))|U' = u']$ are preserved.

Cardinality Bounds (cont.)

- set $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$
- random variable $V'' = (U', V')$
- fun. $\hat{A}'' : \mathcal{V}'' \times \mathcal{B} \to \mathcal{A}$ by $\hat{A}''(v'', b) = \hat{A}''(u', v', b) \triangleq \hat{A}'_{u'}(v', b)$

$U' - V'' - A - (B, E)$ form a Markov chain

Cardinality Bounds (cont.)

- set $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$
- random variable $V'' = (U', V')$
- fun. $\hat{A}'' : \mathcal{V}'' \times \mathcal{B} \to \mathcal{A}$ by $\hat{A}''(v'', b) = \hat{A}''(u', v', b) \triangleq \hat{A}'_{u'}(v', b)$

$U' - V'' - A - (B, E)$ form a Markov chain

$$\begin{aligned} H(AB|V'') - H(B|V'') &= H(AB|U', V') - H(B|U', V') \\ &= H(AB|U', V) - H(B|U', V) \\ &= H(AB|V) - H(B|V) \end{aligned}$$

Cardinality Bounds (cont.)

- set $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$
- random variable $V'' = (U', V')$
- fun. $\hat{A}'' : \mathcal{V}'' \times \mathcal{B} \to \mathcal{A}$ by $\hat{A}''(v'', b) = \hat{A}''(u', v', b) \triangleq \hat{A}'_{u'}(v', b)$

$U' - V'' - A - (B, E)$ form a Markov chain

$$H(AB|V'') - H(B|V'') = H(AB|V) - H(B|V)$$

$$\begin{aligned}
\mathbb{E}[d(A, \hat{A}''(V'', B))] &= \mathbb{E}[d(A, \hat{A}'_{U'}(V', B))] \\
&= \mathbb{E}\Big[\mathbb{E}\big[d(A, \hat{A}'_{U'}(V', B))|U'\big]\Big] \\
&= \mathbb{E}\Big[\mathbb{E}\big[d(A, \hat{A}(V, B))|U'\big]\Big] \\
&= \mathbb{E}\big[d(A, \hat{A}(V, B))\big]
\end{aligned}$$

Cardinality Bounds (cont.)

- set $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$ $\quad \|\mathcal{V}''\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$
- random variable $V'' = (U', V')$
- fun. $\hat{A}'' : \mathcal{V}'' \times \mathcal{B} \to \mathcal{A}$ by $\hat{A}''(v'', b) = \hat{A}''(u', v', b) \triangleq \hat{A}'_{u'}(v', b)$

$U' - V'' - A - (B, E)$ form a Markov chain

$$H(AB|V'') - H(B|V'') = H(AB|V) - H(B|V)$$

$$\mathbb{E}[d(A, \hat{A}''(V'', B))] = \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

Return