Quantifying Correlation

- Shannon’s Mutual Information:
  \[ I(X; Y) = H(X) - H(X|Y) \]
- Wyner’s Common Information:
  How much common randomness needed to generate correlated \( \{X^n, Y^n\} \)?

\[ F \rightarrow X^n \]
\[ G \rightarrow Y^n \]

Common Randomness (Rate \( R \))

Ans: \( R > C(X, Y) = m \min_{V} H(X, Y|U) \)

- Reverse Shannon Theorem [Bennett et al. 02]: How much communication needed to synthesize \( Y^n \sim \prod P_{Y|X} \) using a noiseless link and \( X^n \sim \prod P_X \)?

Ans: Need communication rate \( R > I(X; Y) \)
(needed shared randomness)

An Operational Viewpoint: Strong Coordination [Cuff 08, Bennett et al. 09]

\[ X^n \xleftarrow{F} X^n \]
\[ Y^n \xleftarrow{G} Y^n \]
\[ K \in [2^m R_1] \]
\[ J \in [2^m R_2] \]
\[ G(J, K) \]

Fix \( P_{Y|X} \) and consider \( X^n \sim \prod P_X \) given by nature, independent of \( K \)

- Want \( \lim_{m \rightarrow \infty} \left| Q_{X^n Y^n} \right| - \prod P_X P_Y X \right|_1 = 0 \)
- What are optimal rates of communication and shared randomness?

Ans: Need \( R > I(U; X, Y) \)

with \( X \rightarrow U \rightarrow Y \)

Cloud-Mixing Lemma 1

Fix \( P_{Y|X} \). Want to synthesize \( Y^n \sim \prod P_Y \) given a codebook \( B^G \) of \( 2^{m R} U^n \) sequences. How small can this codebook be?

\[ J \sim \text{Unif} \{ B^G \} \]
\[ U^n(J) \]
\[ P_{Y^n|U^n} \]

Ans: \( R > I(U; V) \) is sufficient[1].

Secure Cascade Channel Synthesis

\[ X^n \sim \prod P_X \]
\[ nR_1 \text{ bits} \]
\[ F_n \]
\[ J_1 \]
\[ G_n \]
\[ J_2 \]
\[ H_n \]
\[ nR_0 \text{ bits} \]
\[ Y^n \]
\[ Z^n \]

Want \( \lim_{m \rightarrow \infty} \left| Q_{X^n Y^n Z^n} \right| - \prod P_X P_Y Z X Y \right|_1 = 0 \)
- Security constraint: \( (J_1, J_2) \perp (X^n, Y^n, Z^n) \)
- Ans: Need \( R_2 > I(V, X, Y) \)
  \( R_1 > I(U, V, X, Y) \)
  \( R_0 > I(U, V, X, Y, Z) \)

with \( X \rightarrow (U, V) \rightarrow Y \)
(\( X, Y, U \rightarrow V \rightarrow Z \)) and \( H(Y|U) = 0 \).

Strong Coordination: Achievability

Pick \( U : X \rightarrow U \rightarrow Y \) and fold the problem.

\[ U^n \]
\[ P_{U^n} \]
\[ X^n \]
\[ Y^n \]

\[ R + R_0 \geq I(U; X, Y) \Rightarrow \lim_{m \rightarrow \infty} \left| Q_{X^n Y^n} - \prod P_X P_Y X \right|_1 = 0 \]
- Still need \( X^n \) to be i.i.d. and independent of \( K \)
- \( R > I(U; X) \Rightarrow \lim_{m \rightarrow \infty} \left| Q_{X^n | K = k} - \prod P_X \right|_1 = 0 \)

Strong Coordination with Eavesdropper [Cuff 08]

\[ X^n \]
\[ F_J X^n \]
\[ J \in [2^m R_1] \]
\[ F(J, K) \]
\[ \rightarrow Y^n \]

\[ K \in [2^m R_0] \]

Same as before, but want \( J \perp (X^n, Y^n) \) as well
- Ans: With \( X \rightarrow U \rightarrow Y \), need \( R > I(U, X) \)
\( R_0 > I(U, X, Y) \).

Cloud-Mixing Lemma 2

Fix \( P_{Y|X} \). Want to synthesize \( Y^n \sim \prod P_Y \) given a codebook \( B^{G^R} \) of \( 2^{m R} U^n \) sequences. How small can this codebook be?

\[ V^n \sim P_Y \]
\[ R \]
\[ U^n \]
\[ F_{X^n V^n} \]
\[ J \]
\[ G^n \]
\[ H \]
\[ Z^n \]

Ans: \( R > I(U; X, Y) \) is sufficient[1].

Example: Task Assignment

Let \( X \rightarrow [u(m)] \) for \( m \geq 3 \). Consider \( P_{Y|Z|X} \) that produces a pair \( Y \neq Z \) uniformly distributed over all distinct pairs in \( [m] \setminus \{X\} \). The optimal rate region is

\[ \text{Convex Hull} \left\{ (R_0, R_1, R_2) \in R^3 : \begin{aligned} &3a \in [m - 1] \setminus \{1\}, b \in [a - 1] \setminus \{0\} \setminus \{1\}, \text{s.t.} \quad R_2 \geq \log \left( \frac{a+b}{2} \right) \quad R_1 \geq \log \left( \frac{a}{b+1} \right) \quad R_0 \geq \log \left( \frac{a(m-1)(m-2)}{(a-b)(a+b)(a+1)} \right) \end{aligned} \right\} \]

Open Problems/Applications

- Cascade Channel Synthesis (without Eavesdropper)[2]
- Strong Coordination with Private Channel [3]
- Strong Coordination through a Noisy Channel[4]
- Strong Coordination with Side Information at Decoder
- Rate-Distortion Theory for Secrecy Systems[5]

Acknowledgement

The authors would like to thank Carl Schuler for helpful discussions. This work is supported by the National Science Foundation (grant CCF-1116013) and the Air Force Office of Scientific Research (grant FA9550-12-1-0196).

References