Communication Requirements for Generating Correlated Random Variables

Paul Cuff

Stanford University

International Symposium on Information Theory
Toronto - July 9, 2008
Overview

$X$ is random and specified by nature.
How much must be told about $X$ to generate $Y$ correlated with $X$?
What is the effect of common randomness?

Application:
- Game theory — mixed strategies among participants on a team.
  [Anantharam, Borkar 07]
Talk Outline

1. Correlation Encryption
2. Channel Simulation
3. Proof
   - Achievability
   - Converse
4. Examples
Correlation Encryption

\[ X^n \xrightarrow{\text{Public Channel}} M(X^n, Z) \xrightarrow{\text{Secret Key}} Y^n(M, Z) \xrightarrow{\text{Public Channel}} Y^n \]

\[ Z \in \{1, \ldots, 2^{nR_2} \} \]

\[ M \in \{1, \ldots, 2^{nR_1} \} \]

\( X \) is given by nature iid according to \( p_0(x) \).

Goal:

1. Construct \( Y \) correlated with \( X \) according to \( p_0(y|x) \).
2. Message doesn’t give away anything about \( X \) and \( Y \).
Correlation Encryption

Encoder: $p(m|x^n, z)$.
Decoder: $p(y^n|m, z)$.

Induced Distribution:

$$p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z)$$

Achievable if there exists a sequence of encoders and decoders such that

$$\lim_{n \to \infty} I(M; X^n, Y^n) = 0,$$

and

$$\lim_{n \to \infty} \left\| p(x^n, y^n) - \prod_{i=1}^n p_0(x_i)p_0(y_i|x_i) \right\|_{TV} = 0.$$
Correlation Encryption Rate Region

\[ S_1 \triangleq \text{Cl}\{ \text{encryption achievable} \ (R_1, R_2) \} \]

**Theorem: Encryption Rate Region**

\[ S_1 = \{(R_1, R_2) : R_1 \geq I(X; U), R_2 \geq I(X, Y; U), \text{for some } U \text{ such that } X - U - Y \text{ forms a Markov chain and } |U| \leq |X||Y| + 1.\} \]
Correlation Encryption Rate Region

\[ S_1 \triangleq Cl\{ \text{encryption achievable } (R_1, R_2) \} \]

Theorem: Encryption Rate Region

\[ S_1 = \{(R_1, R_2) : \]
\[ R_1 \geq I(X; U), \]
\[ R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1 \).}
Wyner’s Common Information

[Wyner 75]:

\[ C(X; Y) \triangleq \min_{X \rightarrow U \rightarrow Y} I(X, Y; U). \]
Wyner’s Common Information

[Wyner 75]:

\[ C(X; Y) \triangleq \min_{X \rightarrow U \rightarrow Y} I(X, Y; U). \]

How much common randomness is needed to generate \( X \) and \( Y \)?

\[ \text{Common Randomness} \quad (\text{Rate } R) \]

\[ \rightarrow \quad X \quad \rightarrow \quad Y \]

Result: \( R > C(X; Y) \).
Talk Outline

1. Correlation Encryption

2. Channel Simulation

3. Proof
   - Achievability
   - Converse

4. Examples
Channel Simulation

$X^n \rightarrow M(X^n, Z) \rightarrow Y^n(M, Z) \rightarrow Y^n$

$X$ is given by nature iid according to $p_0(x)$.

Goal:

1. Construct $Y$ correlated with $X$ according to $p_0(y|x)$. 

Common Randomness $Z \in \{1, ..., 2^{nR_2}\}$

Message $M \in \{1, ..., 2^{nR_1}\}$
Channel Simulation

Encoder: \( p(m|X^n, z) \).

Decoder: \( p(y^n|m, z) \).

Induced Distribution:

\[
p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z)
\]

Achievable if there exists a sequence of encoders and decoders such that

\[
\lim_{n \to \infty} \left\| p(x^n, y^n) - \prod_{i=1}^{n} p_0(x_i)p_0(y_i|x_i) \right\|_{TV} = 0.
\]
Correlation Encryption — Channel Simulation

Difference between Correlation Encryption and Channel Simulation:

- One-time pad needed for Correlation Encryption

**Theorem: Correlation Encryption relates to Channel Simulation**

Define,

\[ R_1' = R_1, \]
\[ R_2' = R_1 + R_2. \]

Then,

\[ (R_1', R_2') \in S_1 \iff (R_1, R_2) \in S_2. \]

Reminder: \( S_1 \) is encryption rate region; \( S_2 \) is simulation rate region.
Channel Simulation Rate Region

\[ S_2 \triangleq Cl\{ \text{simulation achievable } (R_1, R_2) \} \]

**Theorem: Simulation Rate Region**

\[ S_2 = \{(R_1, R_2) : \]
\[ R_1 \geq I(X;U), \]
\[ R_1 + R_2 \geq I(X,Y;U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \)
Channel Simulation Rate Region

\[ S_2 \triangleq \text{Cl}\{ \text{simulation achievable } (R_1, R_2) \} \]

**Theorem: Simulation Rate Region**

\[ S_2 = \{(R_1, R_2) : R_1 \geq I(X;U), \quad R_1 + R_2 \geq I(X, Y;U), \] 

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \)}
Channel Simulation Rate Region

\[ S_2 \triangleq Cl\{ \text{simulation achievable } (R_1, R_2) \} \]

**Theorem: Simulation Rate Region**

\[ S_2 = \{(R_1, R_2) : R_1 \geq I(X;U), \quad R_1 + R_2 \geq I(X,Y;U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \}

**Previous Results:**

[Bennett et al. 02]: Reverse Shannon Th.: \((I(X;Y), \infty) \in S_2.\)

[Wyner 75]: \((C(X;Y), 0) \in S_2.\)
Talk Outline

1. Correlation Encryption

2. Channel Simulation

3. Proof
   - Achievability
   - Converse

4. Examples
Achievability via Random Coding

Let \((R_1, R_2)\) satisfy

\[
R_1 > I(X; U), \\
R_1 + R_2 > I(X, Y; U),
\]

for some \(U\) such that \(X - U - Y\) form a Markov chain.
Achievability via Random Coding

Let \((R_1, R_2)\) satisfy

\[
R_1 > I(X; U), \\
R_1 + R_2 > I(X, Y; U),
\]

for some \(U\) such that \(X - U - Y\) form a Markov chain.

**Construct Codebook randomly:**

\[
C = \{U^n(m)\}_{m=1}^{2^{n(R_1+R_2)}} \quad \text{where} \quad U^n(m) \sim \prod_{i=1}^{n} p(u_i).
\]

**Binning:** Bin the codewords into \(2^{nR_2}\) bins.

Common randomness specifies the bin.

**Encoder:** Finds all jointly typical \(U^n\) in bin and randomly chooses one.

Sends index.

**Decoder:** Decodes \(U^n(m)\) and generates \(Y^n\) according to

\[
\prod_{i=1}^{n} p(y_i|u_i(m)).
\]
Achievability

Resolvability: [Wyner 75] [Han, Verdú 93]
Achievability

$X^n$ $Y^n$

Resolvability: [Wyner 75] [Han, Verdú 93]
Talk Outline

1. Correlation Encryption
2. Channel Simulation
3. Proof
   - Achievability
   - Converse
4. Examples
Converse

Assume \((R_1, R_2)\) is achievable.
Converse

Assume \((R_1, R_2)\) is achievable.

Markovity by construction:

\[
p(x^n, y^n, m, z) = p(x^n)p(z)p(m|x^n, z)p(y^n|m, z).
\]

Therefore,

\[
X^n - (M, Z) - Y^n,
\]

\[
X^n \perp Z.
\]
**Converse**

Assume \((R_1, R_2)\) is achievable.

\[ X^n - (M, Z) - Y^n, \]

\[ X^n \perp Z. \]
Converse

Assume \((R_1, R_2)\) is achievable.

\[
X^n - (M, Z) - Y^n,
X^n \perp Z.
\]

\[
n(R_1 + R_2) \quad \geq \quad H(M, Z)
\]

\[
\geq \quad I(X^n, Y^n; M, Z)
\]

\[
nR_1 \quad \geq \quad H(M)
\]

\[
\geq \quad H(M|Z)
\]

\[
\geq \quad I(X^n; M|Z)
\]

\[
= \quad I(X^n; M, Z)
\]
Converse

Assume \((R_1, R_2)\) is achievable.

\[ X^n - (M, Z) - Y^n, \]
\[ X^n \perp Z. \]

\[ n(R_1 + R_2) \geq H(M, Z) \]
\[ \geq I(X^n, Y^n; M, Z) \]
(\text{sequence of lemmas})
\[ \vdots \]
\[ \geq \approx \sum_{i=1}^{n} I(X_i, Y_i; M, Z) \]
\[ \approx n I(X_Q, Y_Q; M, Z, Q). \]

where \(Q \sim Unif(\{1, \ldots, n\}).\)
Converse

Assume \((R_1, R_2)\) is achievable.

\[
X^n - (M, Z) - Y^n, \quad X^n \perp Z.
\]

\[
R_1 \geq \approx I(X_Q; M, Z, Q), \quad R_1 + R_2 \geq \approx I(X_Q, Y_Q; M, Z, Q).
\]

where \(Q \sim Unif(\{1, ..., n\})\).
Converse

Assume \((R_1, R_2)\) is achievable.

\[ X^n - (M, Z) - Y^n, \]
\[ X^n \perp Z. \]

\[ R_1 \geq \approx I(X_Q; M, Z, Q), \]
\[ R_1 + R_2 \geq \approx I(X_Q, Y_Q; M, Z, Q). \]

where \(Q \sim Unif\{1, \ldots, n\}\).

Label \((M, Z, Q)\) as \(U\).
Talk Outline

1. Correlation Encryption

2. Channel Simulation

3. Proof
   - Achievability
   - Converse

4. Examples
Simulation Rate Region Examples

Simulation Rate Region

\[ S_2 = \{(R_1, R_2) : \]
\[ R_1 \geq I(X; U), \]
\[ R_1 + R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1 \).
Simulation Rate Region Examples

Simulation Rate Region

\[ S_2 = \{(R_1, R_2) : \]
\[ R_1 \geq I(X; U), \]
\[ R_1 + R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \}

Binary Symmetric Channel (\( X \sim Bern(\frac{1}{2}) \)):
Simulation Rate Region Examples

Simulation Rate Region

\[ S_2 = \{ (R_1, R_2) : \]
\[ R_1 \geq I(X; U), \]
\[ R_1 + R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \}

Binary Symmetric Channel \( (X \sim Bern(\frac{1}{2})) : \)

\[ p_1(1 - p_2) + p_2(1 - p_1) = P_e, \]
\[ p_1 \leq p_2 \leq P_e. \]
Simulation Rate Region Examples

**Simulation Rate Region**

\[ S_2 = \{ (R_1, R_2) : \]

\[ R_1 \geq I(X; U), \]

\[ R_1 + R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \(|U| \leq |X||Y| + 1.\}

**Binary Erasure Channel** \((X \sim \text{Bern}(\frac{1}{2}))\):

\[
\begin{array}{c}
X \quad \text{to} \quad Y \\
0 \quad \text{to} \quad 0 \\
\quad \text{Pe} \quad \text{to} \quad \text{e} \\
1 \quad \text{to} \quad 1
\end{array}
\]
Simulation Rate Region Examples

Simulation Rate Region

\[ S_2 = \{(R_1, R_2) : \]
\[ R_1 \geq I(X; U), \]
\[ R_1 + R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) forms a Markov chain and \( |U| \leq |X||Y| + 1. \)

Binary Erasure Channel \((X \sim Bern(\frac{1}{2})):\)

\[(1 - p_1)(1 - p_2) = 1 - P_e, \]
\[0 \leq p_2 \leq \min\{P_e, 1/2\}.\]
Example: Binary Erasure Channel

Simulation Rate Region for BEC with $P_e = 0.75$

Figure: Boundary of the simulation rate region for a binary erasure channel with erasure probability $P_e = 0.75$ and a Bernoulli-half input.
Correlation Encryption (Public Channel)

\[ R_1 \geq I(X; U), \]
\[ R_2 \geq I(X, Y; U), \]

for some \( U \) such that \( X - U - Y \) and \( |U| \leq |X||Y| + 1 \).

Fundamental quantities discovered as extreme points
Erasure Challenge

Person A

0 1 0 0 1 1 1 1 1
### Erasure Challenge

<table>
<thead>
<tr>
<th>Person A</th>
<th>Person B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 0 0 1 1 1 1</td>
<td>0 e e e e e e e e</td>
</tr>
</tbody>
</table>

Paul Cuff (Stanford University)
Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Person B

0 e e e e e e e

How much must Person A tell Person B?
### Erasure Challenge

<table>
<thead>
<tr>
<th>Person A</th>
<th>Person B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 0 0 1 1 1 1 1 1</td>
<td>0 e e e e e 1 e e</td>
</tr>
</tbody>
</table>

How much must Person A tell Person B?

- Tell all the bits
- 8 bits
Erasure Challenge

<table>
<thead>
<tr>
<th>Person A</th>
<th>Person B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 0 0 1 1 1 1</td>
<td>0 e e e e e 1 e e</td>
</tr>
</tbody>
</table>

How much must Person A tell Person B?

- Tell all the bits
  - 8 bits

- Choose the sequence for B and tell it
  - $\log_2 \binom{8}{2} + 2$ bits
## Erasure Challenge

<table>
<thead>
<tr>
<th>Person A</th>
<th>Person B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 0 0 1 1 1 1</td>
<td>0 e e e e e e e e</td>
</tr>
</tbody>
</table>

How much must Person A tell Person B?

- **Tell all the bits**
  - 8 bits
- **Choose the sequence for B and tell it**
  \[
  \log_2 \left( \binom{8}{2} \right) + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits}
  \]
Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Person B

0 e e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  \( \log_2 \left( \binom{8}{2} \right) + 2 \) bits = \( \log_2 112 \) = 6.81 bits
- Split the randomization
Erasure Challenge

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  \[ \log_2 \binom{8}{2} + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits} \]
- Split the randomization
Erasure Challenge

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  \( \log_2 \left( \frac{8}{2} \right) + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits} \)
- Split the randomization
Erasure Challenge

Person A

0 1 0 0 1 1 1 1

Person B

0 e e e e 1 e e

How much must Person A tell Person B?

- Tell all the bits
  - 8 bits
- Choose the sequence for B and tell it
  \[ \log_2 \left( \frac{8}{2} \right) + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits} \]
- Split the randomization
Erasure Challenge

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  \[ \log_2 \left( \frac{8}{2} \right) + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits} \]
- Split the randomization
  \[ \log_2 \left( \frac{4}{2} \right) + 4 \text{ bits} \]
Erasure Challenge

How much must Person A tell Person B?

- Tell all the bits
  8 bits
- Choose the sequence for B and tell it
  \[ \log_2 \binom{8}{2} + 2 \text{ bits} = \log_2 112 = 6.81 \text{ bits} \]
- Split the randomization
  \[ \log_2 \binom{4}{2} + 4 \text{ bits} = \log_2 96 = 6.58 \text{ bits} \]