Resolvability on Continuous Alphabets

Matthias Frey, Igor Bjelaković and Sławomir Stańczak | Technische Universität Berlin | Supported by the German Research Foundation and the German Federal Ministry of Education and Research
Channel Model and Problem Statement

Symbols

$\mathcal{X}$: Polish channel input alphabet with Borel $\sigma$-algebra $\mathcal{F}$

$\mathcal{Y}$: Polish channel output alphabet with Borel $\sigma$-algebra $\mathcal{G}$

$K$: stochastic kernel from $(\mathcal{X}, \mathcal{F})$ to $(\mathcal{Y}, \mathcal{G})$ defining channel transition

$X \sim Q_X$ \hspace{2cm} $Y \sim Q_Y$

$C \quad X^n$ \hspace{2cm} $Y^n \sim P_{Y^n|C}$

$K \otimes^n$

$M$ distributed uniformly over $\{1, \ldots, \exp(nR)\}$
Channel Model and Problem Statement

Symbols

\( \mathcal{X} \): Polish channel input alphabet with Borel \( \sigma \)-algebra \( \mathcal{F} \)

\( \mathcal{Y} \): Polish channel output alphabet with Borel \( \sigma \)-algebra \( \mathcal{G} \)

\( K \): stochastic kernel from \((\mathcal{X}, \mathcal{F})\) to \((\mathcal{Y}, \mathcal{G})\) defining channel transition

Sequence of codebooks solves resolvability problem if

\[
\| P_{Y^n | C} - Q_{Y^n} \|_{TV} \xrightarrow{n \to \infty} 0
\]
Resolvability and the Wiretap Channel

Distinguishing Security: $\| P^n_{Y_{\text{tap} | M=m} - Q^n_{Y_{\text{tap} | M}} \|_{TV} \xrightarrow{n \to \infty} 0$

- implies both strong secrecy and semantic security
Resolvability and the Wiretap Channel

\[
\begin{array}{c}
X \\
\mathcal{W} \\
Y_{\text{tap}}|X \\
Y_{\text{legit}}
\end{array}
\]

channel resolvability problem

Decoding output

Distinguishing Security: \( \| P_{Y_{\text{tap}}^n|M=m} - Q_{Y_{\text{tap}}^n} \|_{\text{TV}} \xrightarrow{n \to \infty} 0 \)

- implies both strong secrecy and semantic security
Resolvability and the Wiretap Channel

Distinguishing Security: \[ \| P_{Y_{\text{tap}}^n | M = m} - Q_{Y_{\text{tap}}^n} \|_{TV} \xrightarrow{n \to \infty} 0 \]

- implies both **strong secrecy** and **semantic security**

Link observed and explored in:
I. Devetak. The private classical capacity and quantum capacity of a quantum channel. Trans. Inf. Theory, 2005

More references and discussion of semantic security and implications in MAC case:
Resolvability Region

Characterization of the resolvability region

Given \( Q \), suppose \( X \) is compact. For each \( A \subseteq Y \), \( x \mapsto K(x, A) \) is a continuous mapping. Then the achievable rates are

\[
\left\{ R \in \mathbb{R} : R \geq \inf_{Q \in G(Q,Y)} I(X;Y) \right\},
\]

where \( G(Q,Y) := \{ Q \in X : Q \text{ induces } Q \text{ through } K, I(X;Y) < \infty \} \).
Resolvability Region

Characterization of the resolvability region

Given $Q_Y$, suppose

- $\mathcal{X}$ is compact
- For each $A \subseteq \mathcal{Y}$, $x \mapsto K(x, A)$ is a continuous mapping.

Then the achievable rates are

$$\left\{ R \in \mathbb{R} : R \geq \inf_{Q_X \in G(Q_Y)} I(X; Y) \right\},$$

where

$$G(Q_Y) := \{ Q_X : Q_X \text{ induces } Q_Y \text{ through } K, \ I(X; Y) < \infty \}.$$
Direct Part

**Theorem**

Suppose

- $\mathbb{E}_{Q_{X,Y}} \exp(t \cdot i(X; Y)) < \infty$ for some $t > 0$
- $R > I(X; Y)$

Then there exist $\gamma_1 > 0$ and $\gamma_2 > 0$ such that

$$PC \left( \|P_{Y^n} - Q_Y^n\|_{TV} > \exp(-\gamma_1 n) \right) \leq \exp(-\exp(\gamma_2 n)).$$

for sufficiently large $n$. 
**Direct Part**

**Theorem**

Suppose

- $\mathbb{E}_{Q_X, Y} \exp(t \cdot i(X; Y)) < \infty$ for some $t > 0$
- $R > I(X; Y)$

Then there exist $\gamma_1 > 0$ and $\gamma_2 > 0$ such that

$$P_C \left( \| P_{Y^n} |_C - Q_Y^n \|_{TV} > \exp(-\gamma_1 n) \right) \leq \exp(-\exp(\gamma_2 n)),$$

for sufficiently large $n$.

- Codeword components drawn independently according to $Q_X$
- Probability of drawing “bad” codebook **doubly exponentially small**.
Direct Part: Proof Sketch (1)

- Typical set: \( \mathcal{T}_\varepsilon := \{(x^n, y^n) : \frac{1}{n} i(x^n; y^n) \leq I(X; Y) + \varepsilon\} \)
Direct Part: Proof Sketch (1)

- Typical set: $\mathcal{T}_\varepsilon := \{(x^n, y^n) : \frac{1}{n} i^n(x^n; y^n) \leq I(X; Y) + \varepsilon\}$

- Output distribution given codebook $C$: $P_{Y^n|C}(A) = \exp(-nR) \sum_{m=1}^{\exp(nR)} K^{\otimes n} (C(m), A)$

Chernoff-Hoeffding bound: Atypical part is exponentially small with doubly exponentially small error probability.
Direct Part: Proof Sketch (1)

- Typical set: $T_\varepsilon := \{(x^n, y^n) : \frac{1}{n} i(x^n; y^n) \leq I(X; Y) + \varepsilon\}$

- Output distribution given codebook $C$: $P_{Y^n | C}(A) = \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A)$

- Typical part: $P_{1,C}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A \cap \{y^n : (C(m), y^n) \in T_\varepsilon\})$

- Atypical part: $P_{2,C}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A \cap \{y^n : (C(m), y^n) \notin T_\varepsilon\})$
Direct Part: Proof Sketch (1)

- Typical set: $T_\varepsilon := \{(x^n, y^n) : \frac{1}{n} i(x^n; y^n) \leq I(X; Y) + \varepsilon\}$

- Output distribution given codebook $\mathcal{C}$: $P_{Y^n|\mathcal{C}}(A) = \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A)$

- Typical part: $P_{1,\mathcal{C}}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A \cap \{y^n : (C(m), y^n) \in T_\varepsilon\})$

- Atypical part: $P_{2,\mathcal{C}}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^\otimes n (C(m), A \cap \{y^n : (C(m), y^n) \notin T_\varepsilon\})$

$$\|P_{Y^n|\mathcal{C}} - Q_{Y^n}\|_{TV} = \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{Y^n|\mathcal{C}}}{dQ_{Y^n}} (Y^n) - 1 \right]^+ = \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{1,\mathcal{C}}}{dQ_{Y^n}} (Y^n) + \frac{dP_{2,\mathcal{C}}}{dQ_{Y^n}} (Y^n) - 1 \right]^+$$

$$\leq \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{1,\mathcal{C}}}{dQ_{Y^n}} (Y^n) - 1 \right]^+ + P_{2,\mathcal{C}}(Y^n)$$

\text{typical part} \quad \text{atypical part}
Direct Part: Proof Sketch (1)

- Typical set: \( T_{\varepsilon} := \left\{ (x^n, y^n) : \frac{1}{n} \log(x^n; y^n) \leq I(X; Y) + \varepsilon \right\} \)

- Output distribution given codebook \( \mathcal{C} \): \( P_{Y^n|C}(A) = \exp(-nR) \sum_{m=1}^{\exp(nR)} K^{\otimes n} (C(m), A) \)

- Typical part: \( P_{1,C}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^{\otimes n} (C(m), A \cap \{ y^n : (C(m), y^n) \in T_{\varepsilon} \}) \)

- Atypical part: \( P_{2,C}(A) := \exp(-nR) \sum_{m=1}^{\exp(nR)} K^{\otimes n} (C(m), A \cap \{ y^n : (C(m), y^n) \notin T_{\varepsilon} \}) \)

\[
\| P_{Y^n|C} - Q_{Y^n} \|_{TV} = \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{Y^n|C}}{dQ_{Y^n}} (Y^n) - 1 \right]^{+} = \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{1,C}}{dQ_{Y^n}} (Y^n) + \frac{dP_{2,C}}{dQ_{Y^n}} (Y^n) - 1 \right]^{+} \\
\leq \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{1,C}}{dQ_{Y^n}} (Y^n) - 1 \right]^{+} + P_{2,C}(Y^n)
\]

- Chernoff-Hoeffding bound: Atypical part is exponentially small with doubly exponentially small error probability
Direct Part: Proof Sketch (2)

How to bound the typical part $P_C \left( \mathbb{E}_{Q^n_{Y^n}} \left[ \frac{dP_{1,C}}{dQ^n_{Y^n}}(y^n) - 1 \right]^+ > \delta \right)$?

Finite $\mathcal{Y}$  

P. Cuff: Soft Covering with High Probability, ISIT 2016

Not necessarily finite $\mathcal{Y}$
Direct Part: Proof Sketch (2)

How to bound the typical part $P_C \left( \mathbb{E}_{Q^n} \left\{ \frac{dP_{1,C}}{dQ^n}(y^n) - 1 \right\}^+ > \delta \right) > \delta$ ?

Finite $\mathcal{Y}$

P. Cuff: Soft Covering with High Probability, ISIT 2016

Not necessarily finite $\mathcal{Y}$

Step 1: Eliminate $[\cdot]^+$ (since $\delta > 0$)

$P_C \left( f(C, y^n) > \delta \right) = P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)$
Direct Part: Proof Sketch (2)

How to bound the typical part $P_C \left( \underbrace{\mathbb{E}_{Q^n} \left[ \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) - 1 \right]}_{f(C, y^n)} > \delta \right)$?

Finite $\mathcal{Y}$: P. Cuff: Soft Covering with High Probability, ISIT 2016

Not necessarily finite $\mathcal{Y}$

Step 1: Eliminate $[\cdot]^+$ (since $\delta > 0$)

$$P_C \left( f(C, y^n) > \delta \right) = P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)$$

Step 2: Chernoff-Hoeffding (for any fixed $y^n$)

$$P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \leq \exp \left( - \frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right)$$
Direct Part: Proof Sketch (2)

How to bound the typical part $P_C \left( \sum_{y^n} \left( \mathbb{E}_{Q^n} \left( \frac{dP_{1,C}^n}{dQ^n}(y^n) \right) - 1 \right)^+ > \delta \right)$?

**Finite $\mathcal{Y}$**

Step 1: Eliminate $[\cdot]^+$ (since $\delta > 0$)

$$P_C \left( f(C, y^n) > \delta \right) = P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)$$

Step 2: Chernoff-Hoeffding (for any fixed $y^n$)

$$P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \leq \exp \left( -\frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right)$$

Step 3: Union bound

$$P_C \left( \exists y^n : \bar{f}(C, y^n) > 1 + \delta \right) \leq \sum_{y^n \in \mathcal{Y}^n} P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)$$
Direct Part: Proof Sketch (2)

How to bound the typical part $P_C \left( \mathbb{E}_{Q^n} \left[ \frac{dP_{1,C}}{dQ^n}(y^n) - 1 \right]^+ > \delta \right)$?

Finite $\mathcal{Y}$

Step 1: Eliminate $[\cdot]^+$ (since $\delta > 0$)

$$P_C \left( f(C, y^n) > \delta \right) = P_C \left( \overline{f}(C, y^n) > 1 + \delta \right)$$

Step 2: Chernoff-Hoeffding (for any fixed $y^n$)

$$P_C \left( \overline{f}(C, y^n) > 1 + \delta \right) \leq \exp \left( - \frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right)$$

Step 3: Union bound

$$P_C \left( \exists y^n : \overline{f}(C, y^n) > 1 + \delta \right) \leq \sum_{y^n \in \mathcal{Y}} P_C \left( \overline{f}(C, y^n) > 1 + \delta \right)$$

Step 4: Infer bound on expectation

Not necessarily finite $\mathcal{Y}$

Finite $\mathcal{Y}$

P. Cuff: Soft Covering with High Probability, ISIT 2016

Not necessarily finite $\mathcal{Y}$
Direct Part: Proof Sketch (2)

How to bound the typical part \( P_C \left( \mathbb{E}_{Q_{Y^n}} \left[ \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) - 1 \right]^+ > \delta \right) \)?

Finite \( \mathcal{Y} \)  

Step 1: Eliminate \([\cdot]^+ \) (since \( \delta > 0 \))
\[
P_C \left( f(C, y^n) > \delta \right) = P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)
\]

Step 2: Chernoff-Hoeffding (for any fixed \( y^n \))
\[
P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \leq \exp \left( -\frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right)
\]

Step 3: Union bound
\[
P_C \left( \exists y^n : \bar{f}(C, y^n) > 1 + \delta \right) \leq \sum_{y^n \in \mathcal{Y}^n} P_C \left( \bar{f}(C, y^n) > 1 + \delta \right)
\]

Step 4: Infer bound on expectation

Not necessarily finite \( \mathcal{Y} \)

Step 1: As in finite case
Step 2: As in finite case
### Direct Part: Proof Sketch (2)

How to bound the typical part \( P_C \left( \mathbb{E}_{Q^n} \left[ \min \left\{ \frac{dP_1,C}{dQ^n}(y^n) - 1, 0 \right\}^+ > \delta \right] \right) ? \)

<table>
<thead>
<tr>
<th>Finite ( \mathcal{Y} )</th>
<th>Not necessarily finite ( \mathcal{Y} )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1:</strong> Eliminate ([\cdot]^+) (since ( \delta &gt; 0 ))</td>
<td><strong>Step 1:</strong> As in finite case</td>
</tr>
<tr>
<td>( P_C \left( f(C, y^n) &gt; \delta \right) = P_C \left( \bar{f}(C, y^n) &gt; 1 + \delta \right) )</td>
<td><strong>Step 2:</strong> As in finite case</td>
</tr>
<tr>
<td><strong>Step 2:</strong> Chernoff-Hoeffding (for any fixed ( y^n ))</td>
<td><strong>Step 3:</strong> For r.v. ( A \geq 0 ): ( \mathbb{E}A = \int_0^{\infty} P(A &gt; a)da )</td>
</tr>
<tr>
<td>( P_C \left( \bar{f}(C, y^n) &gt; 1 + \delta \right) \leq \exp \left( -\frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right) )</td>
<td><strong>Step 2:</strong> As in finite case</td>
</tr>
<tr>
<td><strong>Step 3:</strong> Union bound</td>
<td><strong>Step 3:</strong> For r.v. ( A \geq 0 ): ( \mathbb{E}A = \int_0^{\infty} P(A &gt; a)da )</td>
</tr>
<tr>
<td>( P_C \left( \exists y^n : \bar{f}(C, y^n) &gt; 1 + \delta \right) )</td>
<td><strong>Step 3:</strong> For r.v. ( A \geq 0 ): ( \mathbb{E}A = \int_0^{\infty} P(A &gt; a)da )</td>
</tr>
<tr>
<td>( \leq \sum_{y^n \in \mathcal{Y}^n} P_C \left( \bar{f}(C, y^n) &gt; 1 + \delta \right) )</td>
<td><strong>Step 4:</strong> Infer bound on expectation</td>
</tr>
</tbody>
</table>

**Step 4:** Infer bound on expectation
Direct Part: Proof Sketch (2)

How to bound the typical part \( P_C \left( \mathbb{E}_{Q^n} \left[ \frac{dP_1,C}{dQ^n}(y^n) - 1 \right]^+ > \delta \right) ? \)

\[
\begin{aligned}
&f(C, y^n) \\
&\bar{f}(C, y^n) \\
&\mathbb{E}_{Q^n} \left[ \frac{dP_1,C}{dQ^n}(y^n) - 1 \right]^+ > \delta
\end{aligned}
\]

Finite \( \mathcal{Y} \)  
P. Cuff: Soft Covering with High Probability, ISIT 2016

Not necessarily finite \( \mathcal{Y} \)

Step 1: Eliminate \([\cdot]^+ \) (since \( \delta > 0 \))

\[ P_C \left( f(C, y^n) > \delta \right) = P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \]

Step 2: Chernoff-Hoeffding (for any fixed \( y^n \))

\[ P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \leq \exp \left( -\frac{\delta^2}{2 \left( 1 + \frac{\delta}{3} \right)} \right) \]

Step 3: Union bound

\[ P_C \left( \exists y^n : \bar{f}(C, y^n) > 1 + \delta \right) \leq \sum_{y^n \in \mathcal{Y}^n} P_C \left( \bar{f}(C, y^n) > 1 + \delta \right) \]

Step 4: Infer bound on expectation

\[ \mathbb{E}_{Q^n} f(C, y^n) \leq \mathbb{E}_{Q^n} \mathbb{E}_{P_C} \left( \exp(\lambda f(C, y^n)) \right) \exp(-\delta \lambda) \]

Step 1: As in finite case

Step 2: As in finite case

Step 3: For r.v. \( A \geq 0 \):

\[ \mathbb{E}A = \int_0^\infty \mathbb{P}(A > a) \, da \]

Step 4: Apply Chernoff bound, Jensen, Fubini

\[ P_C \left( \mathbb{E}_{Q^n} f(C, y^n) > \delta \right) \leq \mathbb{E}_{Q^n} \mathbb{E}_{P_C} \left( \exp(\lambda f(C, y^n)) \right) \exp(-\delta \lambda) \]
Direct Part: Proof Sketch (3)

**Chernoff-Hoeffding bound:**

- For fixed, but arbitrary $y^n$, we have $P_C \left( \frac{dP_{1,C}}{dQ_{Y^n}} (y^n) > (1 + \xi) \right) \leq \exp \left( -\frac{\xi^2}{2(1 + \frac{\xi^3}{3})} \right)$

$$E_{P_C} \left( \exp \left( \lambda \left[ \frac{dP_{1,C}}{dQ_{Y^n}} (y^n) - 1 \right]^+ \right) \right) = \int_0^\infty P_C \left( \exp \left( \lambda \left[ \frac{dP_{1,C}}{dQ_{Y^n}} (y^n) - 1 \right]^+ \right) > a \right) da$$

$$\leq 1 + \int_1^\infty P_C \left( \frac{dP_{1,C}}{dQ_{Y^n}} (y^n) > 1 + \frac{\log(a)}{\lambda} \right) da$$
Direct Part: Proof Sketch (3)

Chernoff-Hoeffding bound:

- For fixed, but arbitrary \( y^n \), we have

\[
P_C \left( \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) > (1 + \xi) \right) \leq \exp \left( -\frac{\xi^2}{2(1 + \frac{\xi}{3})} \right)
\]

\[
\mathbb{E}_{P_C} \left( \exp \left( \lambda \left[ \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) - 1 \right]^+ \right) \right) = \int_0^\infty P_C \left( \exp \left( \lambda \left[ \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) - 1 \right]^+ \right) > a \right) \, da
\]

\[
\leq 1 + \int_1^\infty P_C \left( \frac{dP_{1,C}}{dQ_{Y^n}}(y^n) > 1 + \frac{\log(a)}{\lambda} \right) \, da
\]

Split integration domain into two parts to bound integral:

- \( a \in [1, \exp(\lambda)] \), i.e. \( \xi \in [0, 1] \)
- \( a \in [\exp(\lambda), \infty) \), i.e. \( \xi \in [1, \infty) \)

Integrals over upper bound can be calculated

Resulting bound independent of \( y^n \); i.e. is also a bound for the expectation
Direct Part

Second-order Theorem

Let $Q := 1 - \Phi$ with $\Phi$ the distribution function of the standard normal density and suppose

- $i(X; Y)$ has finite central second moment $V$ and finite absolute third moment $\rho$
- $\xi > 0$, $c > 1$ and a rate $R = I(X; Y) + \sqrt{V/n}Q^{-1}(\xi) + c \log n/n$ are given
- $d \in (0, c - 1)$ and a block length $n$ satisfying $n^{(c-d)/2} \geq 6$ are given

Then, we have

$$P_C \left( \| P_{Y^n|C} - Q_{Y^n} \|_{TV} > \mu \left( 1 + \frac{1}{\sqrt{n}} \right) + \frac{1}{\sqrt{n}} \right)$$

$$\leq \exp \left( -\frac{1}{3} n\mu \exp(nR) \right) + \left( \frac{7}{6} + \sqrt{3\pi/2} \exp \left( \frac{3}{4} \right) \right) \exp \left( -n^{1/(2(c-d-1))} \right),$$

where $\mu := Q \left( Q^{-1}(\xi) + d \log n/\sqrt{nV} \right) + \rho/(V^{3/2}\sqrt{n})$ tends to $\xi$ for $n \to \infty$. 

Resolvability on Continuous Alphabets | Matthias Frey, Igor Bjelaković and Sławomir Stańczak | Supported by the German Research Foundation and the German Federal Ministry of Education and Research
Page 9
Converse Part

Theorem

Let $Q_Y$ be an output distribution and $(C_\ell)_{\ell \geq 1}$ a sequence of codebooks with strictly increasing block lengths $n_\ell$ and fixed rate $R$ such that $\|P_{Y^n_{\ell}}|_{C_{\ell}} - Q_{Y^n_{\ell}}\|_{TV} = \delta_\ell \leq 1/4$ with $\delta_\ell \to 0$. Suppose

- $\mathcal{X}$ is compact
- for each $A \subseteq \mathcal{Y}$, $x \mapsto K(x, A)$ is a continuous mapping

Then there is $Q_{X,Y}$ compatible with $Q_Y$ and $K$ such that $I_{Q_{X,Y}}(X; Y) \leq R$. 

Resolvability on Continuous Alphabets | Matthias Frey, Igor Bjelaković and Sławomir Stańczak | Supported by the German Research Foundation and the German Federal Ministry of Education and Research
Page 10
Converse Part: Discrete Version

Lemma

Let $Q_Y$ be an output distribution and $(C_\ell)_{\ell \geq 1}$ a sequence of codebooks with strictly increasing block lengths $n_\ell$ and fixed rate $R$ such that $\| P_{Y^n|C_\ell} - Q_{Y^n} \|_{TV} = \delta_\ell \leq 1/4$ with $\delta_\ell \to 0$. Suppose

- $\mathcal{X}$ is compact, $\mathcal{Y}$ is finite and discrete
- $x \mapsto K(x, \cdot)$ is a continuous mapping from $\mathcal{X}$ to the probability measures on $\mathcal{Y}$

Then there is $Q_{X,Y}$ compatible with $Q_Y$ and $K$ such that $I_{Q_{X,Y}}(X; Y) \leq R$. 
Discrete Version of Converse Part: Proof Sketch

Define $Q_X^{(\ell)} := \frac{1}{n\ell} \sum_{k=1}^{n\ell} P_{X_k | C_{\ell}}$; consequently $Q_Y^{(\ell)} := \frac{1}{n\ell} \sum_{k=1}^{n\ell} P_{Y_k | C_{\ell}}$

Elementary manipulations, triangle inequality: $\|Q_Y^{(\ell)} - Q_Y\|_{TV} \leq \|P_{Y^{n\ell} | C_{\ell}} - Q_{Y^{n\ell}}\|_{TV} = \delta_{\ell}$
Discrete Version of Converse Part: Proof Sketch

Define $Q_X^{(\ell)} := \frac{1}{n} \sum_{k=1}^{n} P_{X_k | C_\ell}$; consequently $Q_Y^{(\ell)} := \frac{1}{n} \sum_{k=1}^{n} P_{Y_k | C_\ell}$

Elementary manipulations, triangle inequality: $\|Q_Y^{(\ell)} - Q_Y\|_{TV} \leq \|P_{Y^n | C_\ell} - Q_{Y^n}\|_{TV} = \delta_{\ell}$

$n_{\ell} R \geq H_{P_{X^n_{\ell} | C_\ell}} (X) \geq I_{P_{X^n_{\ell}, Y^n_{\ell} | C_\ell}} (X^n_{\ell}; Y^n_{\ell})$

$= n_{\ell} I_{Q_X^{(\ell)}, Y} (X; Y) - n_{\ell} H_{Q_Y^{(\ell)}} (Y) + H_{P_{Y^n_{\ell} | C_\ell}} (Y^n_{\ell})$
Discrete Version of Converse Part: Proof Sketch

Define \( Q_X^{(\ell)} := \frac{1}{n\ell} \sum_{k=1}^{n\ell} P_{X_k|C_\ell} \); consequently \( Q_Y^{(\ell)} := \frac{1}{n\ell} \sum_{k=1}^{n\ell} P_{Y_k|C_\ell} \).

Elementary manipulations, triangle inequality:
\[
\| Q_Y^{(\ell)} - Q_Y \|_{TV} \leq \| P_{Y^{n\ell}|C_\ell} - Q_{Y^{n\ell}} \|_{TV} = \delta\ell
\]

Lemma: Continuity of entropy with respect to variational distance

Let \( A \) and \( B \) be random variables on a finite alphabet \( \mathcal{A} \), distributed according to \( Q_A \) and \( Q_B \). Then, if \( \| Q_A - Q_B \|_{TV} = \delta \leq 1/4 \), we have
\[
|H(A) - H(B)| \leq -\frac{1}{2} \delta \log \frac{\delta}{2|\mathcal{A}|}.
\]
From discrete to continuous version: Sketch

\[ Q^{(1,1)}_{X,Y} \cdots Q^{(\ell,1)}_{X,Y} \cdots \rightarrow Q^{(1)}_{X,Y} \text{ compatible with } K^{(1)} \text{ on } G^{(1)} \]

\[ \vdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \]

\[ Q^{(1,k)}_{X,Y} \cdots Q^{(\ell,k)}_{X,Y} \cdots \rightarrow Q^{(k)}_{X,Y} \text{ compatible with } K^{(k)} \text{ on } G^{(k)} \]

\[ \vdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \]
From discrete to continuous version: Sketch

\[ Q^{(1,1)}_{X,Y} \cdots Q^{(\ell,1)}_{X,Y} \cdots \rightarrow Q^{(1)}_{X,Y} \text{ compatible with } K^{(1)} \text{ on } G^{(1)} \]

\[ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \]

\[ Q^{(1,k)}_{X,Y} \cdots Q^{(\ell,k)}_{X,Y} \cdots \rightarrow Q^{(k)}_{X,Y} \text{ compatible with } K^{(k)} \text{ on } G^{(k)} \]

\[ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \]

\[ Q_{X,Y} \text{ compatible with } K \text{ on } G \]
Conclusion

- Extended resolvability results from finite alphabets to Polish spaces
  - First-order direct part, random codebooks with doubly exponentially small error probability
  - Second-order direct part
  - Converse part via discrete approximations
  - Compact input alphabet needed for converse part only

- Outlook
  - Resolvability schemes that can be practically implemented
  - Extension to MACs with continuous alphabets
  - Remove compactness assumption in converse case