Lecture 4:

Today

- Talk more about Maximal Leakage
  - Criticisms of Mutual Information
  - Extensions of Maximal Leakage
- Functional Representation Lemma
  - Motivation
  - Proof

Motivation:

$$U - X - \boxed{Enc} - Y$$

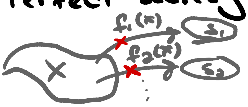
Maximal leakage:
- control a measure of leakage from X to Y, $\mathcal{L}(X \to Y)$

Alternative Approach:
- Require perfect secrecy for U.

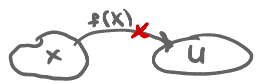
Write $I(U;Y) = 0$

"Secrecy by design"

Perfect Secrecy

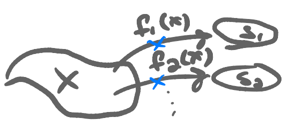


No information leakage for <u>any</u> function of X



No information leakage for one specific function

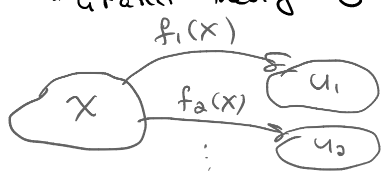
Maximal Leakage



some information leakage is OK, but lets control it.

for every function U

"Grand theory" :)



Given a family of functions, Could we control the leakage?

could you have zero leakage?

Feasibility (Mechanism design)

Lemma: (Functional Representation Lemma)

$|\mathcal{X}|$ & $|\mathcal{U}|$ are finite

Given P_{XU}, there exist Y on $\mathcal{Y}$ ← finite alphabet

such that

(i) $I(U;Y)=0$

$X = g(U,Y)$

(ii) $H(X \mid U,Y) = 0$

(iii) $|\mathcal{Y}| \leq |\mathcal{U}|(|\mathcal{X}|-1)+1$

Comments:

- Could also study $U - X - Y$ then it may be infeasible to construct Y s.t. $I(U;Y)=0$ and $I(X;Y)>0$
- Strong FRL where we bound $I(X;Y)$ & also constructions for continuous R.V.
- My work w/ FRL we bound $H(Y)$ for compression

Proof: (By example) $\mathcal{X} = \{\overset{1}{x_1}, \overset{2}{x_2}\}$

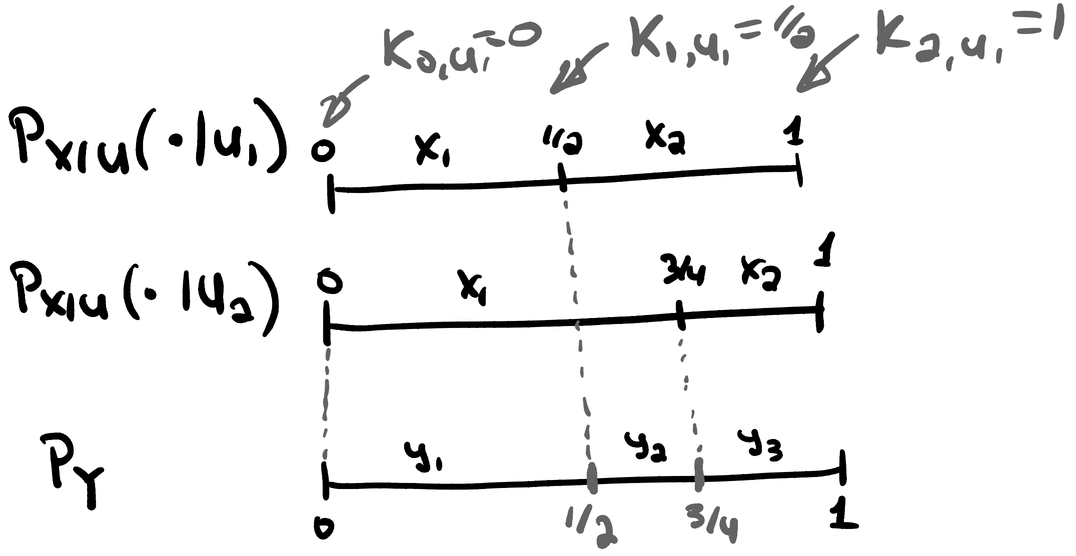
$\mathcal{U} = \{u_1, u_2\}$

P_{XU}

$U - X \rightarrow Y$

	x_1	x_2
u_1	$1/4$	$1/4$
u_2	$3/8$	$1/8$

then
$$P_{X|U}(x|u) = \begin{cases} 1/2, & u = u_1 \\ 3/4, & (u,x) = (u_1, x_1) \\ 1/4, & (u,x) = (u_2, x_2) \end{cases}$$



$P_{Y|XU}(y|x,u)$

$$P_{Y|XU}(y_1 \mid x_1, u_1) = 1$$

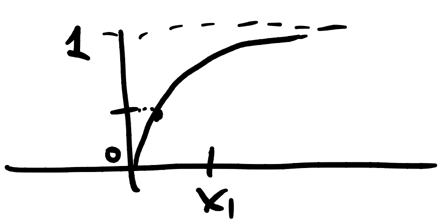
$$P_{Y|XU}(y_2 \mid x_2, u_1) = P_{Y|XU}(y_3 \mid x_2, u_1) = 1/2$$

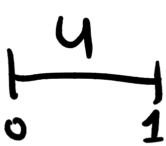
$$P_{Y|XU}(y_1 \mid x_1, u_2) = 2/3$$

$$P_{Y|XU}(y_2 \mid x_1, u_2) = 1/3$$

$$P_{Y|XU}(y_3 \mid x_2, u_2) = 1$$

CDF





$$\Phi^{(-1)}(u)$$

Proof (FRL):

$$(X, U) - V - Y$$

quantization of V

uniform on $(0,1)$ and independent of U

- Assum w.l.o.g. $\mathcal{X} = \{1, \ldots, |\mathcal{X}|\}$ and let $\mathcal{X}_u = \{x : P_{X|U}(x|u) > 0\}$
- For each $u \in \mathcal{U}$, $x \in \mathcal{X}_u$ define

$$K_{x,u} = F_{X|U}(x|u) = \mathbb{P}[X \leq x | U = u]$$

CDF of X given $U = u$

and $K_{0,u} = 0 \quad \forall \quad u \in \mathcal{U}$.

- $$V = V[K_{\tilde{x},u}, K_{x,u})$$

$V[a, \tilde{a})$ uniform R.V. on $[a, \tilde{a})$

R.V.

$$\tilde{x} = \max\{x \in \mathcal{X}_u \cup \{0\} : x < x\}$$

- $$F_{V|U}(v|u) = F_V(v) = \begin{cases} v, & v \in [0,1) \\ 0, & \text{o.w.} \end{cases}$$

and so V & U are independent

• Next $\mathcal{Y} = \bigcup_{u \in \mathcal{U}} \bigcup_{x \in \mathcal{X}} \{K_{x,s}\}$

$$Y = \min\{y \in \mathcal{Y} : V \le y\}$$

so condition (1) holds by DPI

& (3) holds

• $g(u,y) = \underset{x \in \mathcal{X}_u}{\arg\min}\{K_{x,u} : Y \le K_{x,u}\}$

this shows (2)

$\blacksquare$

Properties:

(1) Sequential Composition

$$(X, U) \to T \to \tilde{Y}$$

$$I(U; Y) = 0 \Rightarrow I(U; \tilde{Y}) = 0$$

Holds by DPI

(2) Parallel Composition

$$(X, U) \to Y_1 \qquad I(U; Y_1) = 0$$

$$\to Y_2 \qquad I(U; Y_2) = 0$$

$$\cdots \qquad \cdots$$

$$\to Y_K \qquad I(U; Y_K) = 0$$

then $\cancel{I(U; Y^K) \stackrel{?}{=} 0}$

Instead

$$(X, U) \to Y_1 \qquad I(U; Y_1) = 0$$

$$\to Y_2 \qquad I(U; Y_2 \mid Y_1) = 0$$

$$\cdots$$

$$\to Y_K \qquad I(U; Y_K \mid Y^{K-1}) = 0$$

then $I(U; Y^K) = 0$