Plan of the course

Quantitative Information Flow
- Motivation, application examples
- Secrets and vulnerability
- Channels and leakage
- Multiplicative Bayes-Capacity
- Comparing systems, the lattice of information
- Applications and exercises
Expressiveness of $V_g$

Bayes-vulnerability

\[ W = \mathcal{X} \]

\[ g_{id}(w, x) = \begin{cases} 
1, & \text{if } w = x, \\
0, & \text{if } w \neq x. 
\end{cases} \]

Guessing-entropy

\[ W = \text{permutations of } \mathcal{X} \]

\[ l_G(w, x) = \text{index of } w \text{ in } x \]

Shannon-entropy

\[ W = \mathcal{P}\mathcal{X} \]

\[ l_S(w, x) = -\log_2 w_x \]
Expressiveness of $V_g$

What other measures can we express as $V_g, U_l$?

What is a reasonable uncertainly measure $f$?

Let’s fix some desired properties of $f$
Desired prop. of uncertainty measures

Domain and range: $f : \mathcal{P}(\mathcal{X}) \to [0, \infty)$

Continuity: a small change in $\pi$ should have a small effect in $f(\pi)$

Concavity

We flip a coin give to the adversary the prior $\pi^1$ with pb $c$ and prior $\pi^2$ with pb $1 - c$

His uncertainty on average is $cf(\pi^1) + (1 - c)f(\pi^1)$

If we give him a single prior $\pi = c\pi^1 + (1 - c)\pi^2$ his uncertainly should be at least as big

$$f(\sum_i c_i \pi^i) \geq \sum_i c_i f(\pi^i) \quad \text{where } \sum_i c_i = 1$$
Desired prop. of uncertainty measures

Implies continuity everywhere except on the boundary

Shannon-entropy, Bayes-vulnerability and Guessing-entropy satisfy these properties
Let $\mathcal{U}_X$ denote the set of all uncertainty measures (i.e. non-negative continuous concave functions of $\mathcal{P}_X$).

Let $\mathcal{L}_X$ denote the set of $l$-uncertainty functions $U_l$.

What’s the relationship between $\mathcal{U}_X$ and $\mathcal{L}_X$?
We might have an infinite number of guess vectors $w$

$$U_l(\pi) = \inf_w l_w(\pi) \quad \text{where} \quad l_w(\pi) = \sum_x \pi_x l(w, x)$$

Is $U_l(\pi)$ concave?
- Yes as inf of concave functions

Is $U_l(\pi)$ continuous?
- Upper semi-continuous as inf of continuous functions
- Lower semi-continuous due to the Gale-Klee-Rockafellar theorem

So $L\mathcal{X} \subseteq U\mathcal{X}$

what about the converse?
Geometric view of $U_i$

A guess $w$ can be thought as a vector in $\mathbb{R}^n$ containing the loss for each secret $x$:

$$(l(w, x_1), \ldots, l(w, x_n))$$

Loss for a fixed $w$:

$$l_w(\pi) = \sum_x \pi_x w_x = \pi \cdot w$$

The graph of $l_w$ is a hyperplane with parameters $a = (-w, 1)$, $b = 0$.

Any hyperplane $(a, 1) \cdot (\pi, y) = b$ is the graph of $l_w$ for a guess vector $w = b\mathbf{1} - a$. 
Direction $Ux \subseteq Lx$

Supporting hyperplane theorem
If $S$ is a convex set and $x$ is a point on the boundary of $S$, then there is a supporting hyperplane that contains $x$ (i.e. all points lie on one side of the hyperplane and $x$ lies on the hyperplane)
Direction $\mathbb{U}\mathcal{X} \subseteq \mathbb{L}\mathcal{X}$

**Theorem**
Let $f \in \mathbb{U}\mathcal{X}$. There exist a loss function $l$ with a countable number of guesses s.t. $f = U_l$. Hence $\mathbb{U}\mathcal{X} = \mathbb{L}\mathcal{X}$.

One guess for each $\pi$ in the interior of $\mathcal{P}\mathcal{X}$

Apply the separating hyperplane thm on the hypo-graph of $f$

From the hyperplane construct a guess vector $w_\pi$ s.t.

\[ w_\pi \cdot \pi = f(\pi) \quad \text{for } \pi \text{ in particular, and} \]
\[ w_\pi \cdot \pi' \geq f(\pi') \quad \text{for all (other) } \pi' \]

Conclude that $U_l = f$

Restrict to $\pi$ with rational coordinates
Plan of the course

Quantitative Information Flow
- Motivation, application examples
- Secrets and vulnerability
- Channels and leakage
- Multiplicative Bayes-Capacity
- Comparing systems, the lattice of information
- Applications and exercises
Channels

Basic model from information theory to capture the behaviour of a system

Inputs $\mathcal{X}$: secret events

Outputs $\mathcal{Y}$: observable events
Probabilistic systems are **noisy** channels: an output can correspond to different inputs, and an input can generate different outputs, according to a prob. distribution

\[
p(o_j|s_i): \text{ the conditional probability to observe } o_j \text{ given the secret } s_i
\]
Channel Matrix

\[
\begin{bmatrix}
  x_1 & C_{11} & \cdots & C_{1n} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_m & C_{m1} & \cdots & C_{mn}
\end{bmatrix}
\]

Rows are probability distributions over the observations \( \mathcal{Y} \)

Prior \( \pi \): distribution over the secrets \( \mathcal{X} \)

Given \( \pi, C \) we can construct a joint distribution over \( \mathcal{X} \times \mathcal{Y} \):

\[
p(x, y) = \pi_x C_{xy}
\]

For this distribution we have:

\[
p(x) = \sum_y p(x, y) = \pi_x
\]

\[
p(y|x) = \frac{p(x, y)}{p(x)} = C_{xy}
\]
Particular case: **Deterministic systems**

In these systems an input generates only one output

Still interesting: the problem is how to retrieve the input from the output

The entries of the channel matrix can be only 0 or 1
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, $b=1$)
Example: DC nets (ring of 3 nodes, b=1)
Example: DC nets (ring of 3 nodes, b=1)

<table>
<thead>
<tr>
<th></th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>n₀</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
<tr>
<td>n₁</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
<tr>
<td>n₂</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
<td>¼</td>
</tr>
</tbody>
</table>

fair coins: \( \Pr(0) = \Pr(1) = \frac{1}{2} \)
strong anonymity

biased coins: \( \Pr(0) = \frac{2}{3} , \Pr(1) = \frac{1}{3} \)

The source is more likely to declare 1 than 0
Let us construct the channel matrix

Note: The string $x_1x_2x_3$ typed by the user is a parameter, and $K_1K_2K_3$ is the channel input

The standard view is that the input represents the secret. Hence we should take $K_1K_2K_3$ as the channel input
Let us construct the channel matrix

Input: \( K_1 K_2 K_3 \in \{000, 001, \ldots, 111\} \)
Output: \( out \in \{\text{OK, FAIL}\} \)

Assume the user string is \( x_1 x_2 x_3 = 110 \)

Different values of \( x_1 x_2 x_3 \) give different channel matrices, but they all have this kind of shape (seven inputs map to Fail, one maps to OK)
Let us construct the channel matrix

Input: \( K_1 K_2 K_3 \in \{000, 001, \ldots, 111\} \)
Output: \( out \in \{\text{OK}, (\text{FAIL}, 1), (\text{FAIL}, 2), (\text{FAIL}, 3)\} \)
Posterior distributions

\[
\begin{bmatrix}
  y_1 & y_2 \\
  2/4 & 2/4 \\
  1/4 & 3/4 \\
\end{bmatrix}
\]

Each observation \( y \) provides evidence for some secret(s)

Starting from \( \pi \), it gives a posterior dist. \( \sigma^y \in \mathcal{PX} \):

\[
\sigma^y_x = p(x|y) = \frac{p(x, y)}{p(y)} \quad \text{Bayes thm}
\]

Eg. from \( \pi = (1/2, 1/2) \) we get:

\[
\sigma^{y_1} = (2/3, 1/3) \\
\sigma^{y_2} = (2/5, 3/5)
\]
Observables: prior $\Rightarrow$ posterior
Observables: prior $\Rightarrow$ posterior

<table>
<thead>
<tr>
<th>$p(n)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
</tr>
</tbody>
</table>

$p(o|n)$
conditional prob

prior secret prob
Observables: prior $\Rightarrow$ posterior

<table>
<thead>
<tr>
<th>$p(n)$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
</tr>
<tr>
<td>$\frac{1}{4}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{2}{9}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{2}{9}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n_0$</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{6}$</td>
<td>$\frac{1}{9}$</td>
<td>$\frac{1}{9}$</td>
<td>$\frac{1}{9}$</td>
<td></td>
</tr>
<tr>
<td>$\frac{1}{18}$</td>
<td>$\frac{1}{12}$</td>
<td>$\frac{1}{18}$</td>
<td>$\frac{1}{18}$</td>
<td></td>
</tr>
<tr>
<td>$\frac{1}{18}$</td>
<td>$\frac{1}{18}$</td>
<td>$\frac{1}{12}$</td>
<td>$\frac{1}{18}$</td>
<td></td>
</tr>
</tbody>
</table>

$p(o|n)$
conditional prob

$p(n,o)$
joint prob
Observables: prior ⇒ posterior

<table>
<thead>
<tr>
<th>p(n)</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>½</td>
<td>⅓</td>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
</tr>
<tr>
<td>¼</td>
<td>⅑</td>
<td>⅓</td>
<td>⅑</td>
<td>⅑</td>
</tr>
<tr>
<td>¼</td>
<td>⅑</td>
<td>⅑</td>
<td>⅓</td>
<td>⅑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>p(o)</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
</tr>
<tr>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
</tr>
<tr>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
<td>⅛</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>p(o)</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
</tr>
<tr>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
</tr>
<tr>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
<td>⅕</td>
</tr>
</tbody>
</table>

| p(o|n) | 001 | 010 | 100 | 111 |
|------|-----|-----|-----|-----|
| ⅓   | ⅑  | ⅑  | ⅑  | ⅑  |
| ⅑   | ⅓  | ⅑  | ⅑  | ⅑  |
| ⅑   | ⅑  | ⅓  | ⅑  | ⅑  |

<table>
<thead>
<tr>
<th>p(n,o)</th>
<th>001</th>
<th>010</th>
<th>100</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
<td>⅙</td>
</tr>
<tr>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
</tr>
<tr>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
<td>⅑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>p(n)</th>
<th>p(o)</th>
<th>p(n,o)</th>
</tr>
</thead>
<tbody>
<tr>
<td>⅓</td>
<td>⅕</td>
<td>⅕</td>
</tr>
<tr>
<td>⅑</td>
<td>⅕</td>
<td>⅕</td>
</tr>
<tr>
<td>⅑</td>
<td>⅕</td>
<td>⅕</td>
</tr>
</tbody>
</table>
\[ p(n|o) = \frac{p(n, o)}{p(o)} \]

**Bayes theorem**

- **Post secret prob**
  - \( p(n|001) \)
    - \( \frac{3}{5} \) (n₀)
    - \( \frac{1}{5} \) (n₁)
    - \( \frac{1}{5} \) (n₂)

- **Conditional prob**
  - \( p(o|n) \)
    - \( p(n, o) \)
      - \( \frac{5}{18} \) (001)
      - \( \frac{1}{4} \)
      - \( \frac{1}{4} \)
      - \( \frac{2}{9} \)

- **Joint prob**
  - \( p(o) \)
    - \( 001 \)
    - \( 010 \)
    - \( 100 \)
    - \( 111 \)
Hyper distributions

\[
\begin{align*}
\pi & \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 1/2 \\
C & \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 2/4 \\ 2/4 \end{bmatrix} \\
\text{Joint} & \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2/8 \\ 2/8 \end{bmatrix} \\
\end{align*}
\]

\[
\begin{align*}
\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} & = \frac{1}{2} \begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix} \\
\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} & = \frac{1}{2} \begin{bmatrix} 2/4 \\ 3/4 \end{bmatrix} \\
\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} & = \frac{1}{4} \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} \\
\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} & = \frac{1}{4} \begin{bmatrix} 1/4 \\ 3/4 \end{bmatrix}
\end{align*}
\]

Posteriors: \( \sigma^{y_1} = (2/3, 1/3) \), \( \sigma^{y_2} = (2/5, 3/5) \)

Output distribution \( \delta \in \mathcal{P} \mathcal{Y} \):

\[
\delta_y = p(y) = \sum_x p(x, y) = \sum_x \pi_x c_{xy}
\]

\[
\delta = \pi c = (3/8, 5/8)
\]

Hyper distribution \( \delta \in \mathcal{P}^2 \mathcal{X} \):

\[
\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3/8 \\ 1/8 \end{bmatrix} \quad \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 2/8 \\ 1/8 \end{bmatrix} \]

\[
\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2/3 \\ 1/3 \end{bmatrix} \quad \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 2/5 \\ 3/5 \end{bmatrix}
\]
Hyper distributions

$[\pi, C]$: hyper distribution obtained from $\pi, C$

$\delta \in \mathcal{PY}$: outer distribution (output)

$\sigma^y \in \mathcal{PX}$: inner distributions (posteriors)

$\pi$ can be obtained by averaging the inners

$$\pi = \sum_y \delta_y \sigma^y$$

Abstract channel $C$: mapping $\mathcal{PX} \rightarrow \mathcal{P}^2\mathcal{X}$:

$$C(\pi) = [\pi, C]$$