Advanced Information Measures, and Quantification of Information Flow

Mário S. Alvim
(msalvim@dcc.ufmg.br)

Information Theory

DCC-UFMG
(2017/02)

Advanced Information Measures, and Quantification of Information Flow

- In this course we have focused on Shannon's original measures of information:

  - Shannon entropy,
  - conditional entropy,
  - mutual information,
  - relative entropy (a.k.a. Kullback-Liebler divergence).

  These measures formally capture the intuitive notion of "information" in the context of communication; and are extremely successful in doing so.

- However, these measures are not silver bullets: they may not be appropriate to capture all notions of "information" in every context.

- Here we discuss extensions of the classic information-theory framework to:

  1. capture **advanced information measures**;
  2. **quantify information flow** beyond the context of communication.

Advanced Information Measures, and Quantification of Information Flow

- The material contained in this lecture is a compilation of recent state-of-the-art results in the field of quantitative information flow.
- Be aware that this is a vibrant, evolving area, with many new results popping up all the time.
- Our goal in this lecture is to give an overview of recent developments.

  Do not feel distressed if you cannot get all details from this lecture alone!
- This material is based on drafts of a book on quantitative information flow that should be available in the Summer of 2018.
  - For this reason, the language used here will often use terms common to the security literature: "secret", "observable", "adversary", ...
  - This is, however, inessential: the principles of the theory developed can still be used in many different fields, such as machine learning, A.I., etc.

Modeling knowledge and quantifying information

Modeling knowledge: probability distributions

- We'll focus on **secrets**, which are something and **adversary** has some **partial knowledge** about.

  Typical secrets are a user's password, location within a city, RSA key, ...

- Given a set $\mathcal{X} = \{x_1, x_2, \ldots, x_n\}$ of secrets, the adversary can have probabilistic knowledge about the secret value.

  - Given a set $\mathcal{X}$, we denote by $\mathbb{D}\mathcal{X}$ the **set of all possible probability distributions** on $\mathcal{X}$.

  - **Prior knowledge** about the secret value can be modeled by a distribution $\pi \in \mathbb{D}\mathcal{X}$, usually called the **prior**.

- The prior π can come from:

  1. Knowledge about the probabilistic method by which the secret is generated.
  2. Knowledge about correlations in the real world.

Knowledge vs. information

- $\boxed{\text{Example 1}}$ Consider a secret set $\mathcal{X} = \{x_1, x_2, x_3, x_4\}$ consisting on 4 possible pincodes a user can pick for their bank account.

  Using information about the frequency according to which pincodes are chosen in a population, the adversary's knowledge about the secret can be modeled as a distribution $\pi \in \mathbb{D}\mathcal{X}$ below.

x_i	x_1	x_2	x_3	x_4
π_i	$1/4$	$1/8$	$1/2$	$1/8$

$\triangleleft$

- An important question is: given the adversary's knowledge π, what actual information do they have about the secret?

Quantifying information: information measures

- An information measure is a function that takes as input a state of knowledge and produces as output a real number representing the amount of information contained in that state of knowledge.

- Formally, a **(prior) information measure** is a function of type

$$\mathbb{D}\mathcal{X} \to \mathbb{R},$$

  which maps prior distributions to real numbers.

- An information measure can gauge:
  - **Uncertainty (or entropy)**: the higher its value, the less information the state of knowledge (the prior) carries.
  - **Vulnerability**: the higher its value, the more information the state of knowledge (the prior) carries.

Quantifying information: Shannon entropy

- A popular information measure is **Shannon entropy**, which is formally defined as:

  $$H(\pi) = \sum_{x} \pi_i \log {}^{1}\!/_{\pi_i},$$

  and measures the expected number of branches taken in an optimal binary search tree to figure out the value of the secret correctly.

  Shannon entropy is a measure of uncertainty: the higher its value, the less information the prior π carries.

- Example 2 For the prior

x_i	x_1	x_2	x_3	x_4
π_i	$1/4$	$1/8$	$1/2$	$1/8$

  ,

  the Shannon entropy is

  $$H(\pi) = {}^{1}\!/_{4} \log 4 + {}^{1}\!/_{8} \log 8 + {}^{1}\!/_{2} \log 2 + {}^{1}\!/_{8} \log 8 = {}^{7}\!/_{4} = 1.75.$$

Quantifying information: Bayes vulnerability

- A popular information measure is **Bayes vulnerability**, which is formally defined as:

  $$V(\pi) = \max_i \pi_i,$$

  and measures the probability of the adversary guessing the secret correctly in one try.

  Bayes vulnerability is a measure of vulnerability: the higher its value, the more information the prior π carries.

- $\boxed{\text{Example 3}}$ For the prior

x_i	x_1	x_2	x_3	x_4
π_i	$1/4$	$1/8$	$1/2$	$1/8$

  ,

  the Bayes vulnerability is

  $$V(\pi) = \max\left(1/4, 1/8, 1/2, 1/8\right) = 1/2 = 0.5.$$

◁

Quantifying information: Guessing entropy

- A popular information measure is **guessing entropy**, which is formally defined as:

  $$G(\pi) = \sum_{k} \pi_k \cdot k,$$

  where k is an non-increasing ordering of π_i.

  Guessing entropy measures the expected number of guesses needed in an optimal linear search for the correct secret value.

  Guessing entropy is a measure of uncertainty: the higher its value, the less information the prior π carries.

- Example 4 For the prior

x_i	x_1	x_2	x_3	x_4
π_i	$1/4$	$1/8$	$1/2$	$1/8$

  ,

  the guessing entropy is

  $$G(\pi) = 1/2 \cdot 1 + 1/4 \cdot 2 + 1/8 \cdot 3 + 1/8 \cdot 4 = 15/8 = 1.875$$

◁

Quantifying information: A more general view

- A same state of knowledge π can be considered as carrying different amounts of information, depending on what the interests of the adversary are.

- A measure of information should contain:

  - A **mathematical definition**, which is a formula telling how it's computed from the prior distribution.

  - An **operational interpretation**, which is the significance of the real value obtained in the real world.

    1. Shannon entropy's operational significance is tied to the efficiency of an optimal binary search on the space of secrets;

    2. Bayes vulnerability's operational significance is tied to the probability of success of a one-try guess; and

    3. Guessing entropy's operational significance is tied to the efficiency of an optimal linear search on the space of secrets.

- Can you think of yet other operational scenarios that would demand different definitions of information measures?

g-Vulnerability

g-Vulnerability: Motivation

- Bayes vulnerability measures the risk that the adversary could correctly guess it in one try.
- But of course there are many other operational scenarios that we could be worried about.

  What if the adversary can:

  - benefit from guessing only part of the secret;
  - benefit from guessing an approximate value of the secret;
  - benefit from a property of the secret;
  - benefit from guessing the secret within a fixed number of tries; or
  - be penalized for making an incorrect guess?

- Here we discuss the framework of g-**vulnerability**, a decision-theoretic approach to accommodate this multiplicity of possible operational scenarios.

g-Vulnerability: Definition

- The perspective of g-vulnerability is that knowledge about a secret is important only to the extent that it can be exploited by an adversary, enabling them to take some **action** that brings a reward.

- The operational scenario of g-leakage is specified by:

  - A (finite) set $\mathcal{X}$ of **secrets** the adversary can exploit.

  - A (finite) set $\mathcal{W}$ of possible **actions** that the adversary could make.

  - A **gain function** $g : \mathcal{W} \times \mathcal{X} \rightarrow \mathbb{R}$.

    The idea is that $g(w, x)$ represents the **gain** or **benefit** for the adversary when they take action $w \in \mathcal{W}$ and the secret takes value $x \in \mathcal{X}$.

- The **(prior)** g**-vulnerability** of a distribution π is an information measure defined as

$$V_g(\pi) = \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x g(w, x),$$

  and it represents the expected gain of a rational adversary taking a best action.

g-Vulnerability: A catalog of gain-functions

- The **identity gain-function** captures an adversary whose goal is to guess the secret in one try.

$$g_{id} = \begin{cases} 1, & \text{if } w = x, \\ 0, & \text{if } w \neq x. \end{cases}$$

In g_{id} we have that $\mathcal{W} = \mathcal{X}$, since an action is a guess of a secret value.

- **Theorem** Vulnerability under g_{id} coincides with Bayes vulnerability:

$$V_{g_{id}}(\pi) = V(\pi).$$

Proof.

Note that for any w, $\sum_x \pi_x g_{id}(w, x) = \pi_w$.

So $V_{id}(\pi) = \max_w \pi_w = V(\pi)$. □

g-Vulnerability: A catalog of gain-functions

- **Gain-functions induced from distances** can be used when we want the benefit of an action to reflect the similarity of the action to the actual secret value.

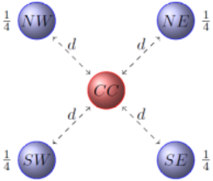
  In general, given a distance function $d : \mathcal{W} \times \mathcal{X} \rightarrow \mathbb{R}$, a gain function based on this distance is

  $$g_d = 1 - \overline{d}(w,x),$$

  where

  $$\overline{d}(w,x) = \frac{d(w,x)}{\max_{w,x} d(w,x)}.$$

- $\boxed{\text{Example 5}}$ **Distance gain-function.**



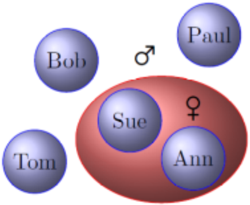
g-Vulnerability: A catalog of gain-functions

- **Binary gain-functions.** Given a set $\mathcal{W} \subseteq \mathcal{P}(\mathcal{X})$, with $\mathcal{W}$ nonempty, the binary gain function $g_{\mathcal{W}}$ is

$$g_{\mathcal{W}}(W,x) = \begin{cases} 1, & \text{if } x \in W, \\ 0, & \text{otherwise.} \end{cases}$$

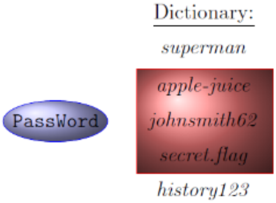
- Example 6

  Property gain-function.



- Example 7

  ***k*-tries gain-functions.**



g-Vulnerability: A catalog of gain-functions

- **Gain-functions that penalize bad actions.**

- $\boxed{\text{Example 8}}$ Consider a scenario where the adversary tries to input an access code X into a keypad outside a locked door.

  Inputting the correct code unlocks the door, but inputting the wrong code triggers a penalty (say, opening a trap door to a pit of tigers).

  This scenario can be modeled with a gain function g_{tiger} using $\mathcal{W} = \mathcal{X} \cup \{\perp\}$ where the special action $\perp$ is used to opt not to input a guess, and

$$g_{tiger}(w, x) = \begin{cases} 1, & \text{if } w = x, \\ 0, & \text{if } w = \perp, \\ -1, & \text{otherwise.} \end{cases}$$

◁

g-Vulnerability: A catalog of gain-functions

- **Gain-functions for medical diagnosis.**

- $\boxed{\text{Example 9}}$ Consider that we are trying to diagnose a certain disease.

  Here the set of possible values of the secret is $\mathcal{X} = \{\textit{disease}, \textit{no disease}\}$.

  Of course we would like to correctly guess whether or not the disease is present, but we are more interested in what action to take.

  The set of action may be $\mathcal{W} = \{\textit{treat}, \textit{don't treat}\}$.

  Or we might have a set of possible treatments, some aggressive and some conservative.

  Different errors would bring different penalties.

  Thus we might want a gain function something like the following:

$g_{\textit{diagnosis}}$	*treat*	*don't treat*
disease	5	−5
no disease	−2	0

The dual of g-vulnerabilities: ℓ-uncertainties

- As it turns out, Shannon entropy and guessing entropy can be captured in a decision-theoretic approach to information measures.

  To do so, however, we need a dual concept of vulnerability, as follows.

- The dual of a gain-function is a **loss function** $\ell : \mathcal{W} \times \mathcal{X} \rightarrow \mathbb{R}$.

  The idea is that $\ell(w, x)$ represents the **loss** for the adversary when they take action $w \in \mathcal{W}$ and the secret takes value $x \in \mathcal{X}$.

- The **(prior)** ℓ**-uncertainty** of a distribution π is an entropy measure defined as

$$U_\ell(\pi) = \inf_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \ell(w, x).$$

  and it represents the expected loss of a rational adversary taking a best action.

  (A technical detail: here we use inf instead of min because we will allow the set $\mathcal{W}$ of actions to be uncountable.)

A loss function for Shannon entropy

- Shannon entropy can be captured as follows.
  - Let the action set be $\mathcal{W} = \mathbb{D}\mathcal{X}$, i.e., the adversary must choose a probability distribution on secrets to bet on.
  - Let the loss function be

    $$\ell_{Shannon}(w, x) = -\log_2 w_x,$$

    i.e., the loss for picking action w when the secret is x is the Shannon information content of secret x according to distribution w.

Hence we have

$$\begin{aligned}
U_{\ell_{Shannon}} &= \inf_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \ell(w, x) && \text{(def. of } U_\ell\text{)} \\
&= \inf_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x (-\log_2 w_x) && \text{(def of } \ell_{Shannon}\text{)} \\
&= \sum_{x \in \mathcal{X}} \pi_x (-\log_2 \pi_x) && \text{(By Gibb's inequality)} \\
&= H(\pi) && \text{(by def. of entropy)}
\end{aligned}$$

A loss function for guessing entropy

- Guessing entropy can be captured as follows.
  - Let the action set $\mathcal{W}$ be the set of all permutations w of the secrets in $\mathcal{X}$.
  - Let the loss function be
  $$\ell_{guessing}(w, x) = i,$$
  where i is the index of element x within permutation w. (Note that $1 \leq i \leq |\mathcal{X}|$.)

Hence we have

$$\begin{aligned}
U_{\ell_{guessing}} &= \inf_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi_x \ell(w, x) && \text{(def. of } U_\ell\text{)} \\
&= \inf_{w \in \mathcal{W}} \sum_{i=1}^{|\mathcal{X}|} \pi_{w_i} i && \text{(def of } \ell_{guessing}\text{)} \\
&= G(\pi) && \text{(minimized when } w \text{ is non-increasing)}
\end{aligned}$$

Channels

Channel matrices

- Channels are ways of processing information.

  They can be represented in a variety of ways, such as in a programming language:

  ```
  if X mod 8 = 0
        Y := X
     else
        Y := 1
  ```

- Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets, intuitively representing **secret input** values and **observable output** values.

  A **channel matrix** C from $\mathcal{X}$ to $\mathcal{Y}$ is a matrix, indexed by $\mathcal{X} \times \mathcal{Y}$, whose rows give the distribution on outputs corresponding to each possible input.

  That is, entry $C_{x,y}$ denotes $p(y \mid x)$, the conditional probability of getting output y given input x.

The effect of channel matrices on knowledge update

- As we have seen, the adversary's prior knowledge is represented by a distribution $\pi \in \mathbb{D}\mathcal{X}$.
- The effect of a channel is to update this knowledge to a posterior knowledge.
- Example 10 Consider the prior knowledge

$$\pi = (1/3, 1/3, 0, 1/3)$$

and channel C

C	y_1	y_2	y_3	y_4
x_1	$1/2$	$1/6$	$1/3$	0
x_2	0	$1/3$	$2/3$	0
x_3	0	$1/2$	0	$1/2$
x_4	$1/4$	$1/4$	$1/2$	0

.

The effect of channel matrices on knowledge update

- $\boxed{\text{Example 10}}$ (Continued)

Here we find that the joint matrix is

J	y_1	y_2	y_3	y_4
x_1	$1/6$	$1/18$	$1/9$	0
x_2	0	$1/9$	$2/9$	0
x_3	0	0	0	0
x_4	$1/12$	$1/12$	$1/6$	0

.

Hence $p_Y = (1/4, 1/4, 1/2, 0)$, making $p_{X|y_4}$ undefined.

The posterior distributions that we do get are

	$p_{X\|y_1}$	$p_{X\|y_2}$	$p_{X\|y_3}$
x_1	$2/3$	$2/9$	$2/9$
x_2	0	$4/9$	$4/9$
x_3	0	0	0
x_4	$1/3$	$1/3$	$1/3$

.

◁

The effect of channel matrices on knowledge update

- But note that in the previous example:
  - $p_{X|y_2} = p_{X|y_3}$, so there are really only two possible adversary "worlds", rather than three.
  - The probability of the second "world" is actually $p(y_2) + p(y_3) = {}^1/_4 + {}^1/_2 = {}^3/_4$, since it makes no difference to the adversary whether the output is y_2 or y_3.
- It is useful to forget about particular output values and to model the effect of channel C on prior π simply as a $\underline{\text{distribution on posterior distributions}}$, which we call a **hyper-distribution** and denote by $[\pi\rangle C]$.
- $\boxed{\text{Example 11}}$ The combination of prior π and channel C of the previous example produces the hyper-distribution

$[\pi\rangle C]$	$^1/_4$	$^3/_4$
x_1	$^2/_3$	$^2/_9$
x_2	0	$^4/_9$
x_3	0	0
x_4	$^1/_3$	$^1/_3$

In this hyper the posterior distributions corresponding to y_2 and y_3, which were identical, were grouped in one single column, and the probability of this new merged column is the sum $p(y_2) + p(y_3)$.

The effect of channel matrices on knowledge update

- The abstraction afforded by the hyper-distribution perspective is particularly important when we are interested in comparing two channels to try to decide whether one is more secure than the other.

- Example 12 Given $\mathcal{X} = \{x_1, x_2, x_3\}$, consider channel matrices C and D:

C	y_1	y_2	y_3
x_1	1	0	0
x_2	$1/4$	$1/2$	$1/4$
x_3	$1/2$	$1/3$	$1/6$

D	z_1	z_2	z_3
x_1	$2/5$	0	$3/5$
x_2	$1/10$	$3/4$	$3/20$
x_3	$1/5$	$1/2$	$3/10$

.

While C and D look completely different, it turns out that they are actually identical with respect to the leakage of X that they cause.

Both map an arbitrary prior distribution $\pi = (p_1, p_2, p_3)$ to the very same hyper-distribution:

	$\frac{4p_1+p_2+2p_3}{4}$	$\frac{3p_2+2p_3}{4}$
x_1	$\frac{4p_1}{4p_1+p_2+2p_3}$	0
x_2	$\frac{p_2}{4p_1+p_2+2p_3}$	$\frac{3p_2}{3p_2+2p_3}$
x_3	$\frac{2p_3}{4p_1+p_2+2p_3}$	$\frac{2p_3}{3p_2+2p_3}$

Hyper-distributions

- We will now formally define a hyper-distribution.
- If $\mathcal{X}$ is a finite set (of possible secret values), a **hyper-distribution** Δ is a distribution on distributions on $\mathcal{X}$, so that Δ has type

  $$\mathbb{D}(\mathbb{D}\mathcal{X}) = \mathbb{D}^2\mathcal{X}.$$

  The **support** of Δ is $\{\delta \in \mathbb{D}\mathcal{X} \mid \Delta_\delta > 0\}$, the set of distributions to which Δ gives positive probability.

  These are the set of possible "worlds" under Δ and we call them the **inner distributions**, or just the **inners**, of Δ.

  We refer to the distribution on the inners as the **outer distribution** of Δ.

- The **information-theoretic essence** of a channel matrix C is a mapping from priors π to hyper-distributions $[\pi\rangle C]$.

Posterior vulnerability and leakage

Posterior g-vulnerability

- Given prior π, gain function g, and channel C, let $\delta^1, \delta^2, \ldots, \delta^m$ denote the inner distributions in the support of $[\pi\rangle C]$ and let $a_1, a_2, \ldots, a_m$ denote their respective outer probabilities.

  Then the **posterior g-vulnerability** $V_g\,[\pi\rangle C]$ is defined as the expected value of V_g over $[\pi\rangle C]$:

  $$V_g\,[\pi\rangle C] = \sum_{i=1}^{m} a_i V_g(\delta^i).$$

  Note that posterior V_g is a function of type $\mathbb{D}^2\mathcal{X} \to \mathbb{R}$, as it maps a posterior state of knowledge to a real number.

- The following results characterizes posterior V_g's operational significance as a rational adversary's expected optimal gain over all possible channel outputs.

- **Theorem** Given prior π, gain function g, and channel matrix C from $\mathcal{X}$ to $\mathcal{Y}$, we have

  $$V_g\,[\pi\rangle C] = \sum_{\substack{y\in\mathcal{Y}\\ p(y)\neq 0}} p(y) V_g(p_{X|y}).$$

Leakage of information

- Now we are ready to define the concept of the leakage of information of a channel for a prior.
- Intuitively, the leakage of information of a channel for prior π is the amount by which the observation of the channel output increases the adversary's information about the secret value.
- It seems just natural to quantify leakage in terms of the prior and posterior g-vulnerabilities, $V_g(\pi)$ and $V_g\left[\pi\rangle C\right]$.
- The following result states that by observing the output of a channel the adversary is never expected to have less information about the secret than he had before observing the channel.
- **Theorem (Monotonicity)** For any prior π, channel C, and gain function g:

$$V_g\left[\pi\rangle C\right] \geq V_g(\pi).$$

Multiplicative and additive g-leakage

- Now we are ready to define g-leakage.

  Both definitions use the fact that the adversary's information about the secret is never smaller after observing the channel than before.

- Given prior distribution π, gain function g, and channel C:

  - **multiplicative g-leakage** is given by

    $$\mathcal{L}_g^{\times}(\pi, C) = \frac{V_g\left[\pi\rangle C\right]}{V_g(\pi)},$$

    and

  - **additive g-leakage** is given by

    $$\mathcal{L}_g^{+}(\pi, C) = V_g\left[\pi\rangle C\right] - V_g(\pi).$$

Robustness and Capacity

The need for robustness

- Both multiplicative and additive g-leakages represent useful quantities.
- However, to properly compute them one needs to know not only the channel C representing the system, but also the prior π and the gain-function g.

  The problem is that both π and g can vary depending on the adversary's knowledge and interests.
- For **robustness**, we can consider **capacities**, which are leakage measures that universally quantify:
  - over the prior π (acknowledging that, in many situations, it is unknown and the assumption that it is uniform is not reasonable);
  - over the gain function g (acknowledging that we might not know the value to the adversary of different sorts of partial information about the secret, neither now nor even in the future); or
  - over both.

  Capacities make the measurements less dependent on the particular context in which the system will run.

g-capacities and the state-of-the-art

- Combining all ways of quantifying over π and g (one, other, or both), and the two versions of leakage (multiplicative and additive), we arrive at a total of six types of capacities.

Quantification	Multiplicative Leakage	Additive Leakage
For all π, fixed g	$\mathcal{L}_g\,[\forall\rangle C] = \max_{\pi} \mathcal{L}_g\,[\pi\rangle C]$	$\mathcal{L}^+_g\,[\forall\rangle C] = \max_{\pi} \mathcal{L}^+_g\,[\pi\rangle C]$
Fixed π, for all g	$\mathcal{L}_\forall\,[\pi\rangle C] = \max_{g} \mathcal{L}_g\,[\pi\rangle C]$	$\mathcal{L}^+_\forall\,[\pi\rangle C] = \max_{g} \mathcal{L}^+_g\,[\pi\rangle C]$
For all π, for all g	$\mathcal{L}_\forall\,[\forall\rangle C] = \max_{\pi,g} \mathcal{L}_g\,[\pi\rangle C]$	$\mathcal{L}^+_\forall\,[\forall\rangle C] = \max_{\pi,g} \mathcal{L}^+_g\,[\pi\rangle C]$

- 3rd NSA Annual Best Scientific Cybersecurity Paper Competition:

  `https://cps-vo.org/node/21539`

Axiomatization of information measures

The need for axiomatization

- There are so many options to measure leakage:
  - Choice of prior vulnerabilities: Shannon-entropy? Guessing-entropy? g-vulnerability?
  - Choice of posterior vulnerabilities: Average case? Worst-case?
  - Choice of comparison between prior and posterior vulnerabilities: Additively? Multiplicatively?

  Can we organize this zoo?

- Axiomatic study of leakage reveals:
  - Important dependencies among axioms.
  - The completeness of g-vulnerabilities w.r.t. intuitively-reasonable properties.

Approach to axiomatization

- So far we have derived vulnerability measures by quantifying the adversary's success in specific operational scenarios.
- After introducing channels whose effect is to map prior distributions to hypers, we have extended vulnerability measures on priors to vulnerability measures on posteriors by averaging each prior vulnerability over the hyper.
- Here we take an alternative approach.

  Instead of constructing specific vulnerability measures for particular operational scenarios, we shall consider generic vulnerability functions of type

  $$\begin{aligned} &\textbf{prior vulnerability:} && \mathbb{V} : \mathbb{D}\mathcal{X} \to \mathbb{R}^+, \qquad \text{and} \\ &\textbf{posterior vulnerability:} && \widehat{\mathbb{V}} : \mathbb{D}^2\mathcal{X} \to \mathbb{R}^+. \end{aligned}$$

  We then consider a variety of properties that "reasonable" vulnerability functions might be expected to have in terms of *axioms*, and study their consequences.

Axioms for prior vulnerability

- **Axiom of continuity (`CNTY`)**: A vulnerability $\mathbb{V}$ is a continuous function of π (w.r.t. the standard topology on $\mathbb{D}\mathcal{X}$).

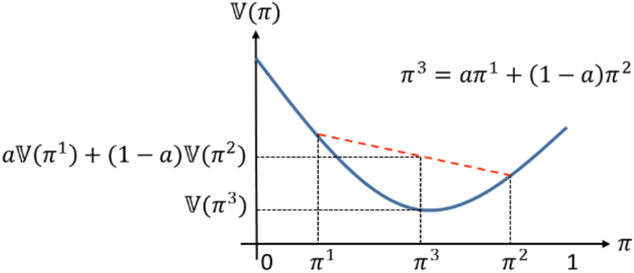
  Intuition: the adversary is not infinitely risk-averse.

Axioms for prior vulnerability

- **Axiom of convexity (CVX)**: A vulnerability $\mathbb{V}$ is a convex function of π — that is, for all convex combinations $\sum_i a_i \pi^i$ we have

$$\mathbb{V}\left(\sum_i a_i \pi^i\right) \leq \sum_i a_i \mathbb{V}(\pi^i).$$

Intuition:


$\mathbb{V}(\pi)$
$\pi^3 = a\pi^1 + (1-a)\pi^2$
$a\mathbb{V}(\pi^1) + (1-a)\mathbb{V}(\pi^2)$
$\mathbb{V}(\pi^3)$
π
0
π^1
π^3
π^2
1

Expressiveness of g-vulnerabilities

- The next results characterizes the expressiveness of g-vulnerabilities.

- **Theorem** The class of g-vulnerabilities is exactly the class of continuous and convex functions of type $\mathbb{D}\mathcal{X} \rightarrow \mathbb{R}^+$:

  1. Any g-vulnerability V_g satisfies CNTY, CVX.
  2. If $\mathbb{V} : \mathbb{D}\mathcal{X} \rightarrow \mathbb{R}^+$ is a vulnerability function satisfying CNTY, CVX, then there exists a gain function g with a countable number of guesses such that $\mathbb{V} = V_g$.

Axioms for posterior vulnerability

- **Axiom of non-interference (`NI`)**: The vulnerability of a point-hyper equals the vulnerability of the unique inner of this hyper:

$$\forall \pi : \quad \widehat{\mathbb{V}}[\pi] = \mathbb{V}(\pi).$$

Intuition: an adversary observing the output of a non-interfering channel does not gain or lose any information about the secret.

Axioms for posterior vulnerability

- **Axiom of data-processing inequality (DPI)**: Post-processing does not increase vulnerability:

  $$\forall \pi, C, R: \quad \widehat{\mathbb{V}}\,[\pi\rangle C] \geq [\pi\rangle CR]\,,$$

  where the number of columns in matrix C is the same as the number of rows in matrix R.

  Intuition: from the output of C it is possible to compute the output of CR, but the opposite is not true in general.

Axioms for posterior vulnerability

- **Axiom of monotonicity (`MONO`)**: Pushing a prior through a channel does not decrease vulnerability:

$$\forall \pi, C : \quad \widehat{\mathbb{V}}\,[\pi\rangle C] \geq \mathbb{V}(\pi).$$

Intuition: equivalent to stating the **non-negativity** of additive and multiplicative leakage.

Axioms for posterior vulnerability

- **Axiom of averaging (AVG)**: The vulnerability of a hyper is the expected value, w.r.t. the outer distribution, of the vulnerabilities of its inners:

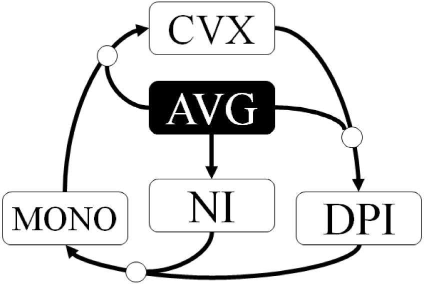
  $$\forall \Delta \quad \widehat{\mathbb{V}}\Delta = \mathsf{Exp}_{\Delta}\,\mathbb{V},$$

  where the hyper $\Delta \in \mathbb{D}^2\mathcal{X}$ typically results from $\Delta = [\pi\rangle C]$ for some π, C.

  Intuition: equivalent to stating the **non-negativity** of additive and multiplicative leakage.

Relationship among axioms

- **Theorem** By imposing AVG on a prior/posterior pair $(\mathbb{V}, \widehat{\mathbb{V}})$ of vulnerabilities:
  1. the axiom of NI must hold; and
  2. the axioms of CVX, DPI and MONO become equivalent to each other.


CVX
AVG
MONO
NI
DPI