Concavity, Core-concavity, Quasiconcavity: A Generalizing Framework for Entropy Measures.

Arthur Américo, Pasquale Malacaria

{a.passosderezende, p.malacaria}@qmul.ac.uk

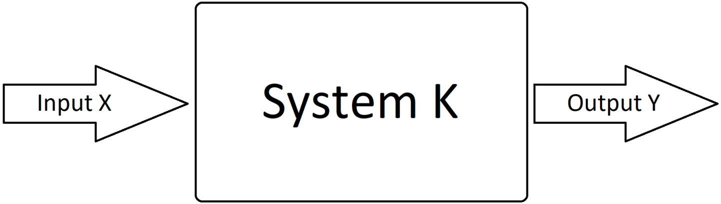
School of Electronic Engineering and Computer Science
Queen Mary University of London

34th IEEE Computer Security Foundations Symposium

23 June 2021

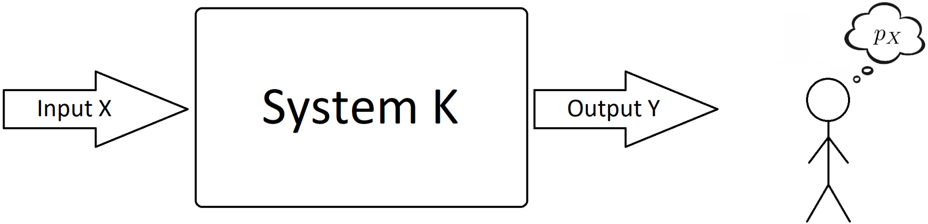
Introduction

Introduction: The Basic Setting



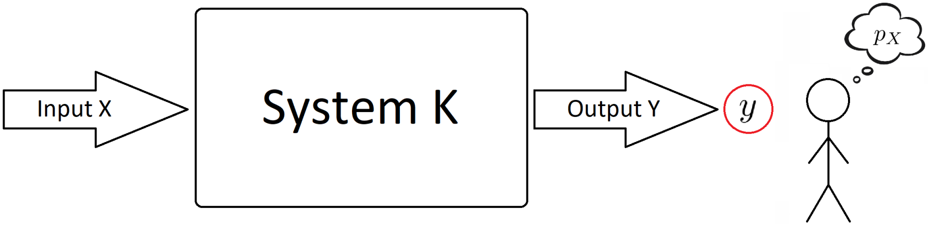
- A secret X (random variable) is fed to a System K

Introduction: The Basic Setting



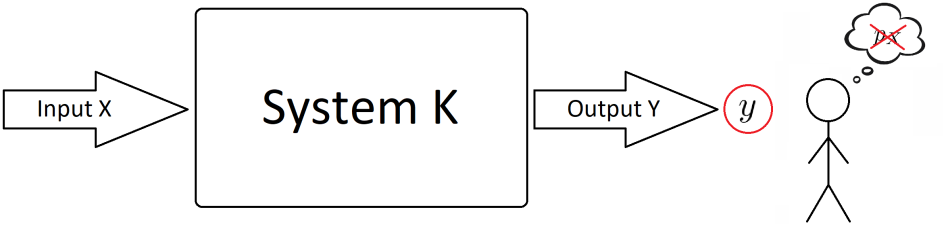
- A secret X (random variable) is fed to a System K
- There is an adversary that wishes to obtain information about X, and has some prior knowledge p_X

Introduction: The Basic Setting



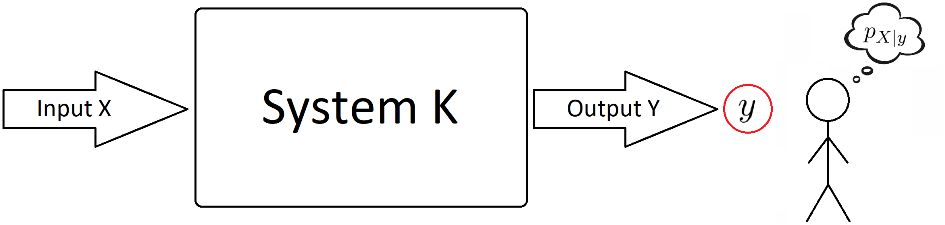
- A secret X (random variable) is fed to a System K
- There is an adversary that wishes to obtain information about X, and has some prior knowledge p_X
- K produces an output $Y = y$ according to the conditional probability: $K(y|x) = p(y|x)$.

Introduction: The Basic Setting



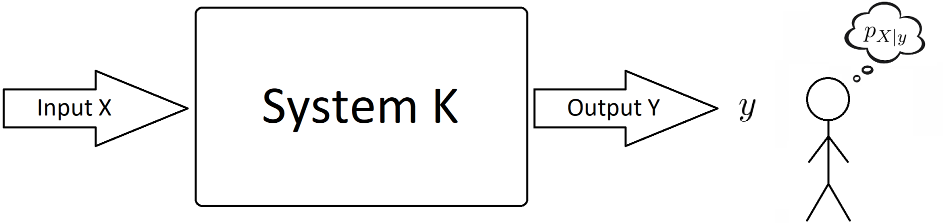
- A secret X (random variable) is fed to a System K
- There is an adversary that wishes to obtain information about X, and has some prior knowledge p_X
- K produces an output $Y = y$ according to the conditional probability: $K(y|x) = p(y|x)$.
- The knowledge of the adversary is updated to the conditional $p_{X|y}$

Introduction: The Basic Setting



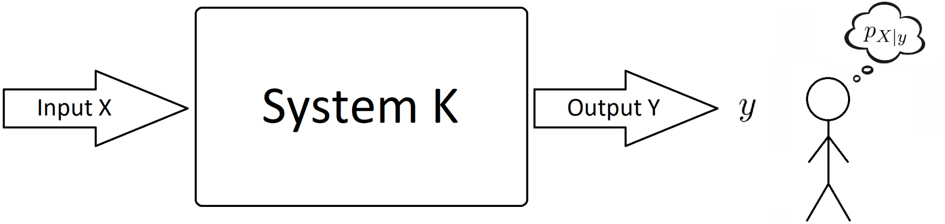
- A secret X (random variable) is fed to a System K
- There is an adversary that wishes to obtain information about X, and has some prior knowledge p_X
- K produces an output $Y = y$ according to the conditional probability: $K(y|x) = p(y|x)$.
- The knowledge of the adversary is updated to the conditional $p_{X|y}$

Introduction: Quantifying Information



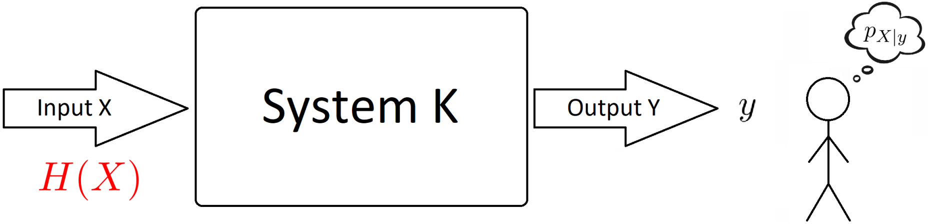
- Quantitative Information Flow (QIF): quantifying how much information systems leak

Introduction: Quantifying Information



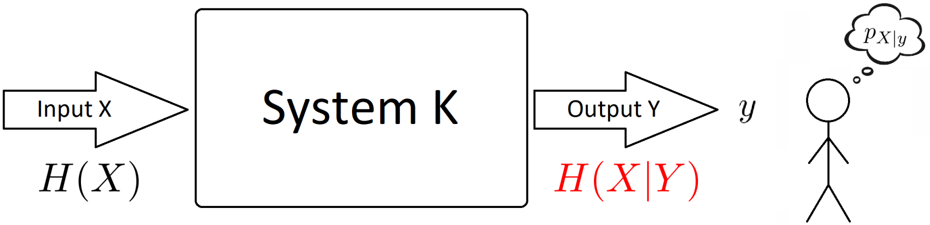
- Quantitative Information Flow (QIF): quantifying how much information systems leak
- Entropy: a quantity H, measuring uncertainty, that has two forms

Introduction: Quantifying Information



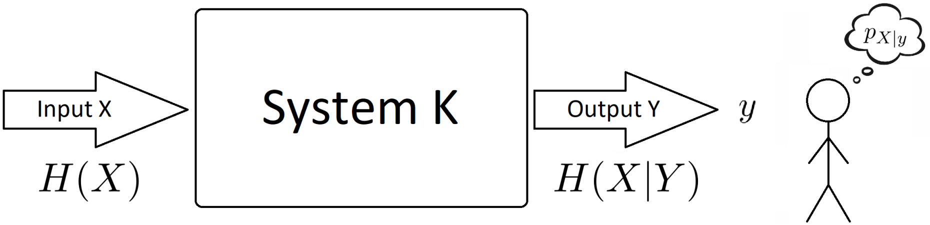
- Quantitative Information Flow (QIF): quantifying how much information systems leak
- Entropy: a quantity H, measuring uncertainty, that has two forms
  - Unconditional form: $H(X)$, a function of p_X

Introduction: Quantifying Information



- Quantitative Information Flow (QIF): quantifying how much information systems leak
- Entropy: a quantity H, measuring uncertainty, that has two forms
  - Unconditional form: $H(X)$, a function of p_X
  - Conditional form: $H(X|Y)$, a function of p_Y, $\{p_{X|y}\}_y$

Introduction: Quantifying Information



- Quantitative Information Flow (QIF): quantifying how much information systems leak
- Entropy: a quantity H, measuring uncertainty, that has two forms
  - Unconditional form: $H(X)$, a function of p_X
  - Conditional form: $H(X|Y)$, a function of p_Y, $\{p_{X|y}\}_y$
- Information Leakage: $I_H(X;Y) = H(X) - H(X|Y)$

Entropies: Unconditional Forms

- Different functions for the unconditional form reflect different attack scenarios:

Entropies: Unconditional Forms

- Different functions for the unconditional form reflect different attack scenarios:
  - Min-entropy: guessing secret in one try

$$H_\infty(X) = -\log \max_x p(x)$$

Entropies: Unconditional Forms

- Different functions for the unconditional form reflect different attack scenarios:
  - Min-entropy: guessing secret in one try

$$H_\infty(X) = -\log \max_x p(x)$$

  - Guessing entropy: brute-force scenarios

$$H_G(X) = \sum_i ip(x_{[i]}) \qquad \text{where } p(x_{[i]}) \geq p(x_{[2]}) \geq \dots$$

Entropies: Unconditional Forms

- Different functions for the unconditional form reflect different attack scenarios:
  - Min-entropy: guessing secret in one try

$$H_\infty(X) = -\log \max_x p(x)$$

  - Guessing entropy: brute-force scenarios

$$H_G(X) = \sum_i i p(x_{[i]}) \qquad \text{where } p(x_{[i]}) \geq p(x_{[2]}) \geq \dots$$

  - Shannon Entropy: expected number of “yes or no” questions

$$H_1(X) = -\sum_x p(x) \log p(x)$$

Entropies: Unconditional Forms

- Different functions for the unconditional form reflect different attack scenarios:
  - Min-entropy: guessing secret in one try

$$H_\infty(X) = -\log \max_x p(x)$$

  - Guessing entropy: brute-force scenarios

$$H_G(X) = \sum_i i p(x_{[i]}) \qquad \text{where } p(x_{[i]}) \geq p(x_{[2]}) \geq \dots$$

  - Shannon Entropy: expected number of "yes or no" questions

$$H_1(X) = -\sum_x p(x) \log p(x)$$

  - ... and many more

Entropies: Conditional Forms

- Moreover, given a unconditional form, there are different ways of obtaining a conditional form, depending on the scenario at hand

Entropies: Conditional Forms

- Moreover, given a unconditional form, there are different ways of obtaining a conditional form, depending on the scenario at hand
- Averaging (AVG):

$$H(X|Y) = \sum_y p(y) H(X|y)$$

  - Quantifies the expected leakage: large leakage is acceptable if it happens with low probability (e.g. password checker)

Entropies: Conditional Forms

- Moreover, given a unconditional form, there are different ways of obtaining a conditional form, depending on the scenario at hand
- Averaging (`AVG`):

$$H(X|Y) = \sum_y p(y)H(X|y)$$

  - Quantifies the expected leakage: large leakage is acceptable if it happens with low probability (e.g. password checker)
- Minimum (`MIN`):

$$H(X|Y) = \min_y H(X|y)$$

  - A worst-case scenario: useful when large leakage is unacceptable, even if unlikely (e.g. privacy)

Characterisation of Entropies

- What choices of unconditional and conditional forms are entropies that "make sense"?

Characterisation of Entropies

- What choices of unconditional and conditional forms are entropies that "make sense"?
- To solve this problem, Alvim et al[1] considered the following intuitively-reasonable properties

[1] M.S. Alvim et al, *Axioms for Information Leakage* (CSF 2016)

Characterisation of Entropies

- What choices of unconditional and conditional forms are entropies that "make sense"?
- To solve this problem, Alvim et al[1] considered the following intuitively-reasonable properties
  - Conditioning reduces entropy (CRE): $H(X|Y) \leq H(X)$ (observing Y does not increase uncertainty)

[1] M.S. Alvim et al, *Axioms for Information Leakage* (CSF 2016)

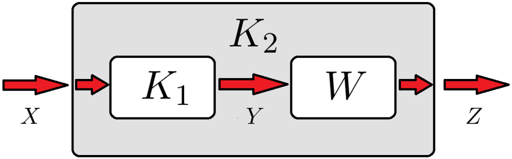
Characterisation of Entropies

- What choices of unconditional and conditional forms are entropies that "make sense"?
- To solve this problem, Alvim et al[1] considered the following intuitively-reasonable properties
  - Conditioning reduces entropy (`CRE`): $H(X|Y) \leq H(X)$ (observing Y does not increase uncertainty)
  - Data-Processing Inequality (`DPI`): If $X \to Y \to Z$, $H(X|Y) \leq H(X|Z)$ (postprocessing the output does not reduce uncertainty)

[1] M.S. Alvim et al, *Axioms for Information Leakage* (CSF 2016)

Characterisation of Entropies

- What choices of unconditional and conditional forms are entropies that "make sense"?
- To solve this problem, Alvim et al[1] considered the following intuitively-reasonable properties
  - Conditioning reduces entropy (CRE): $H(X|Y) \leq H(X)$ (observing Y does not increase uncertainty)
  - Data-Processing Inequality (DPI): If $X \to Y \to Z$, $H(X|Y) \leq H(X|Z)$ (postprocessing the output does not reduce uncertainty)



[1] M.S. Alvim et al, *Axioms for Information Leakage* (CSF 2016)

Alvim et al's Characterisation of Entropies

- They proved the following:

Alvim et al's Characterisation of Entropies

- They proved the following:
  - If the conditional form of H is averaging, then H satisfies `DPI` and `CRE` iff $H(X)$ is concave (`CV`) over p_X

Alvim et al's Characterisation of Entropies

- They proved the following:
  - If the conditional form of H is averaging, then H satisfies `DPI` and `CRE` iff $H(X)$ is concave (`CV`) over p_X
  - If the conditional form of H is minimum, then H satisfies `DPI` and `CRE` iff $H(X)$ is quasiconcave (`QCV`) over p_X

Alvim et al's Characterisation of Entropies

- They proved the following:
  - If the conditional form of H is averaging, then H satisfies `DPI` and `CRE` iff $H(X)$ is concave (`CV`) over p_X
  - If the conditional form of H is minimum, then H satisfies `DPI` and `CRE` iff $H(X)$ is quasiconcave (`QCV`) over p_X
- This characterises two important families of entropy

Alvim et al's Characterisation of Entropies

- They proved the following:
  - If the conditional form of H is averaging, then H satisfies DPI and CRE iff $H(X)$ is concave (CV) over p_X
  - If the conditional form of H is minimum, then H satisfies DPI and CRE iff $H(X)$ is quasiconcave (QCV) over p_X
- This characterises two important families of entropy
  - The ones that satisfy averaging and concavity: $\mathcal{C}_{\mathtt{AVG}}$

Alvim et al's Characterisation of Entropies

- They proved the following:
  - If the conditional form of H is averaging, then H satisfies $\texttt{DPI}$ and $\texttt{CRE}$ iff $H(X)$ is concave ($\texttt{CV}$) over p_X
  - If the conditional form of H is minimum, then H satisfies $\texttt{DPI}$ and $\texttt{CRE}$ iff $H(X)$ is quasiconcave ($\texttt{QCV}$) over p_X
- This characterises two important families of entropy
  - The ones that satisfy averaging and concavity: $\mathcal{C}_{\texttt{AVG}}$
  - The ones that satisfy minimum and quasiconcavity: $\mathcal{Q}_{\texttt{MIN}}$

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\mathtt{AVG}}$ or $\mathcal{Q}_{\mathtt{MIN}}$

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\texttt{AVG}}$ or $\mathcal{Q}_{\texttt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\texttt{AVG}}$ or $\mathcal{Q}_{\texttt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

- In a recent work[2] in collaboration with MHR Khouzani, we extended the results from Alvim et al

[2] Arthur Américo, MHR Khouzani and Pasquale Malacaria, *Conditional Entropy and Data Processing: an Axiomatic Approach Based on Core-Concavity* (2020)

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\mathtt{AVG}}$ or $\mathcal{Q}_{\mathtt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

- In a recent work[2] in collaboration with MHR Khouzani, we extended the results from Alvim et al
- Entropies are pairs $H = (\eta, F)$ such that η is increasing and $H(X) = \eta(F(X))$

[2] Arthur Américo, MHR Khouzani and Pasquale Malacaria, *Conditional Entropy and Data Processing: an Axiomatic Approach Based on Core-Concavity* (2020)

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\texttt{AVG}}$ or $\mathcal{Q}_{\texttt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

- In a recent work[2] in collaboration with MHR Khouzani, we extended the results from Alvim et al
- Entropies are pairs $H = (\eta, F)$ such that η is increasing and $H(X) = \eta(F(X))$ (**note:** any unconditional H can be described this way, by the pair (id, H))

[2] Arthur Américo, MHR Khouzani and Pasquale Malacaria, *Conditional Entropy and Data Processing: an Axiomatic Approach Based on Core-Concavity* (2020)

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\texttt{AVG}}$ or $\mathcal{Q}_{\texttt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

- In a recent work[2] in collaboration with MHR Khouzani, we extended the results from Alvim et al
- Entropies are pairs $H = (\eta, F)$ such that η is increasing and $H(X) = \eta(F(X))$ (**note:** any unconditional H can be described this way, by the pair (id, H))
- Core-concavity ($\texttt{CCV}$): $H = (\eta, F)$ satisfies $\texttt{CCV}$ if F is concave over p_X

[2] Arthur Américo, MHR Khouzani and Pasquale Malacaria, *Conditional Entropy and Data Processing: an Axiomatic Approach Based on Core-Concavity* (2020)

Core-concave Entropies

- However, many entropies in the literature are not in $\mathcal{C}_{\texttt{AVG}}$ or $\mathcal{Q}_{\texttt{MIN}}$

$$H_\infty(X) = -\log \max_x p_X(x) \quad H_\infty(X|Y) = -\log \sum_y p(y) \max_x p(x|y)$$

- In a recent work[2] in collaboration with MHR Khouzani, we extended the results from Alvim et al
- Entropies are pairs $H = (\eta, F)$ such that η is increasing and $H(X) = \eta(F(X))$ (**note:** any unconditional H can be described this way, by the pair (id, H))
- Core-concavity ($\texttt{CCV}$): $H = (\eta, F)$ satisfies $\texttt{CCV}$ if F is concave over p_X
- η-Averaging ($\texttt{EAVG}$): $H = (\eta, F)$ satisfies $\texttt{EAVG}$ if

$$H(X|Y) = \eta\left(\sum_y p(y) F(X|y)\right)$$

[2] Arthur Américo, MHR Khouzani and Pasquale Malacaria, *Conditional Entropy and Data Processing: an Axiomatic Approach Based on Core-Concavity* (2020)

Extension to Core-concave

- Core-concavity (`CCV`): $H = (\eta, F)$ satisfies `CCV` if F is concave over p_X
- η-Averaging (`EAVG`): The pair $H = (\eta, F)$ satisfies `EAVG` if

$$H(X|Y) = \eta\left(\sum_y p(y)F(X|y)\right)$$

Theorem (Alvim et al, 2016)

If the conditional form of H is averaging, then H satisfies DPI and CRE iff $H(X)$ is concave
If the conditional form of H is minimum, then H satisfies DPI and CRE iff $H(X)$ is quasiconcave

Extension to Core-concave

- Core-concavity (`CCV`): $H = (\eta, F)$ satisfies `CCV` if F is concave over p_X
- η-Averaging (`EAVG`): The pair $H = (\eta, F)$ satisfies `EAVG` if

$$H(X|Y) = \eta\left(\sum_{y} p(y)F(X|y)\right)$$

Theorem (Alvim et al, 2016 and Américo et al, 2020)

If the conditional form of $H = (\eta, F)$ is $\eta-$averaging, then H satisfies DPI and CRE iff $H = (\eta, F)$ is core-concave
If the conditional form of H is minimum, then H satisfies DPI and CRE iff $H(X)$ is quasiconcave

Extension to Core-concave

- Core-concavity (`CCV`): $H = (\eta, F)$ satisfies `CCV` if F is concave over p_X
- η-Averaging (`EAVG`): The pair $H = (\eta, F)$ satisfies `EAVG` if

$$H(X|Y) = \eta\left(\sum_y p(y)F(X|y)\right)$$

Theorem (Alvim et al, 2016 and Américo et al, 2020)

If the conditional form of $H = (\eta, F)$ is $\eta-$averaging, then H satisfies DPI and CRE iff $H = (\eta, F)$ is core-concave
If the conditional form of H is minimum, then H satisfies DPI and CRE iff $H(X)$ is quasiconcave

- We denote the family of entropies satisfying `EAVG` and `CCV` by $\mathcal{H}_{\texttt{EAVG}}$.

Extension to Core-concave

- Core-concavity ($\texttt{CCV}$): $H = (\eta, F)$ satisfies $\texttt{CCV}$ if F is concave over p_X
- η-Averaging ($\texttt{EAVG}$): The pair $H = (\eta, F)$ satisfies $\texttt{EAVG}$ if

$$H(X|Y) = \eta\left(\sum_y p(y) F(X|y)\right)$$

Theorem (Alvim et al, 2016 and Américo et al, 2020)

If the conditional form of $H = (\eta, F)$ is $\eta-$averaging, then H satisfies DPI and CRE iff $H = (\eta, F)$ is core-concave
If the conditional form of H is minimum, then H satisfies DPI and CRE iff $H(X)$ is quasiconcave

- We denote the family of entropies satisfying $\texttt{EAVG}$ and $\texttt{CCV}$ by $\mathcal{H}_{\texttt{EAVG}}$.
- Notice that $\mathcal{C}_{\texttt{AVG}} \subset \mathcal{H}_{\texttt{EAVG}}$, by taking $\eta = \mathrm{id}$.

Limit Entropies

Limit Entropies

- Entropies in QIF are thus divided into two distinct families

Limit Entropies

- Entropies in QIF are thus divided into two distinct families
  - The ones in $\mathcal{H}_{\texttt{EAVG}}$, defined by a core-concave (η, F) and η-averaging. We refer to them as core-concave entropies

Limit Entropies

- Entropies in QIF are thus divided into two distinct families
  - The ones in $\mathcal{H}_{\texttt{EAVG}}$, defined by a core-concave (η, F) and η-averaging. We refer to them as core-concave entropies
  - And the ones in $\mathcal{Q}_{\texttt{MIN}}$, defined by a quasiconcave $H(X)$ and minimum, which represents the worst-case leakage ones. We refer to them as worst-case entropies

Limit Entropies

- Entropies in QIF are thus divided into two distinct families
  - The ones in $\mathcal{H}_{\texttt{EAVG}}$, defined by a core-concave (η, F) and η-averaging. We refer to them as core-concave entropies
  - And the ones in $\mathcal{Q}_{\texttt{MIN}}$, defined by a quasiconcave $H(X)$ and minimum, which represents the worst-case leakage ones. We refer to them as worst-case entropies
- Can we find some generalising definition that includes both families?

Limit Entropies

- Entropies in QIF are thus divided into two distinct families
  - The ones in $\mathcal{H}_{\texttt{EAVG}}$, defined by a core-concave (η, F) and η-averaging. We refer to them as core-concave entropies
  - And the ones in $\mathcal{Q}_{\texttt{MIN}}$, defined by a quasiconcave $H(X)$ and minimum, which represents the worst-case leakage ones. We refer to them as worst-case entropies
- Can we find some generalising definition that includes both families?
- Yes, we can!

Limit Entropies: A Unifying Family

- Let $\{H^i = (\eta_i, F_i)\}_i$ be a sequence in $\mathcal{H}_{\texttt{EAVG}}$, such that $\eta_i \circ F_i$ converges uniformly. We define the limit of $\{H^i\}$ to be the entropy H defined as

Limit Entropies: A Unifying Family

- Let $\{H^i = (\eta_i, F_i)\}_i$ be a sequence in $\mathcal{H}_{\texttt{EAVG}}$, such that $\eta_i \circ F_i$ converges uniformly. We define the limit of $\{H^i\}$ to be the entropy H defined as
  - $H(X) = \lim_{i\to\infty} \eta_i(F_i(X))$

Limit Entropies: A Unifying Family

- Let $\{H^i = (\eta_i, F_i)\}_i$ be a sequence in $\mathcal{H}_{\texttt{EAVG}}$, such that $\eta_i \circ F_i$ converges uniformly. We define the limit of $\{H^i\}$ to be the entropy H defined as
  - $H(X) = \lim_{i\to\infty} \eta_i(F_i(X))$
  - $H(X|Y) = \limsup_{i\to\infty} \eta_i \left(\sum_y p(y)F_i(X|y)\right)$.

Limit Entropies: A Unifying Family

- Let $\{H^i = (\eta_i, F_i)\}_i$ be a sequence in $\mathcal{H}_{\texttt{EAVG}}$, such that $\eta_i \circ F_i$ converges uniformly. We define the limit of $\{H^i\}$ to be the entropy H defined as
  - $H(X) = \lim_{i\to\infty} \eta_i(F_i(X))$
  - $H(X|Y) = \limsup_{i\to\infty} \eta_i \left(\sum_y p(y) F_i(X|y)\right)$.
- We denote by $\mathcal{Q}$ the set of all limits of sequences of entropies in $\mathcal{H}_{\texttt{EAVG}}$. We call these entropies limit entropies

Limit Entropies: A Unifying Family

- Let $\{H^i = (\eta_i, F_i)\}_i$ be a sequence in $\mathcal{H}_{\texttt{EAVG}}$, such that $\eta_i \circ F_i$ converges uniformly. We define the limit of $\{H^i\}$ to be the entropy H defined as
  - $H(X) = \lim_{i\to\infty} \eta_i(F_i(X))$
  - $H(X|Y) = \limsup_{i\to\infty} \eta_i \left(\sum_y p(y)F_i(X|y)\right)$.
- We denote by $\mathcal{Q}$ the set of all limits of sequences of entropies in $\mathcal{H}_{\texttt{EAVG}}$. We call these entropies limit entropies

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

- That $\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ is immediate, by taking constant sequences in $\mathcal{H}_{\texttt{EAVG}}$.

$\mathcal{H}_{\mathtt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\mathtt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

- That $\mathcal{H}_{\mathtt{EAVG}} \subset \mathcal{Q}$ is immediate, by taking constant sequences in $\mathcal{H}_{\mathtt{EAVG}}$.
- Proving $\mathcal{Q}_{\mathtt{MIN}} \subset \mathcal{Q}$ is a bit more tricky

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

- That $\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ is immediate, by taking constant sequences in $\mathcal{H}_{\texttt{EAVG}}$.
- Proving $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$ is a bit more tricky
- A first obstacle is that, in general, for a quasiconcave $H(X)$, there is no $(\eta, F) \in \mathcal{H}_{\texttt{EAVG}}$ such that $H(X) = \eta(F(X))$

$\mathcal{H}_{\mathtt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\mathtt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{\mathtt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\mathtt{MIN}} \subset \mathcal{Q}$

- That $\mathcal{H}_{\mathtt{EAVG}} \subset \mathcal{Q}$ is immediate, by taking constant sequences in $\mathcal{H}_{\mathtt{EAVG}}$.
- Proving $\mathcal{Q}_{\mathtt{MIN}} \subset \mathcal{Q}$ is a bit more tricky
- A first obstacle is that, in general, for a quasiconcave $H(X)$, there is no $(\eta, F) \in \mathcal{H}_{\mathtt{EAVG}}$ such that $H(X) = \eta(F(X))$
- This has been first discovered by Bruno de Finetti in the paper *Sulle stratificazioni convesse* (1949), motivated by the study of utility functions in microeconomics

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

- Thankfully, in the more recent paper *Concavifying the Quasiconcave* (2012), Connell and Rasmussen proved that any quasiconcave function is the limit of a uniformly convergent sequence of core-concaves.

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

- Thankfully, in the more recent paper *Concavifying the Quasiconcave* (2012), Connell and Rasmussen proved that any quasiconcave function is the limit of a uniformly convergent sequence of core-concaves.
- Moreover, in the work in which we extended Alvim et al's results, we also proved that for all $(\eta, F) \in \mathcal{H}_{\texttt{EAVG}}$, there is a sequence (η_i, F_i) in $\mathcal{H}_{\texttt{EAVG}}$ such that

$$\lim_{i \to \infty} \eta_i \left(\sum_y p(y) F_i(X|y) \right) = \min_y \eta(F(X|y))$$

$\mathcal{H}_{\texttt{EAVG}} \subset \mathcal{Q}$ and $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Theorem

$\mathcal{H}_{EAVG} \subset \mathcal{Q}$ and $\mathcal{Q}_{MIN} \subset \mathcal{Q}$

- Thankfully, in the more recent paper *Concavifying the Quasiconcave* (2012), Connell and Rasmussen proved that any quasiconcave function is the limit of a uniformly convergent sequence of core-concaves.
- Moreover, in the work in which we extended Alvim et al's results, we also proved that for all $(\eta, F) \in \mathcal{H}_{\texttt{EAVG}}$, there is a sequence (η_i, F_i) in $\mathcal{H}_{\texttt{EAVG}}$ such that

$$\lim_{i \to \infty} \eta_i \left(\sum_y p(y) F_i(X|y) \right) = \min_y \eta(F(X|y))$$

- By combining these results, we were able to prove that $\mathcal{Q}_{\texttt{MIN}} \subset \mathcal{Q}$

Applications

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy $\texttt{CRE}$ and $\texttt{DPI}$

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy `CRE` and `DPI`
- All symmetric and expansible $H \in \mathcal{Q}$ satisfy some interesting information-theoretical properties:

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy `CRE` and `DPI`
- All symmetric and expansible $H \in \mathcal{Q}$ satisfy some interesting information-theoretical properties:
  - Additional information increases entropy: $H(X,Y) \geq H(X)$, $H(X,Y|Z) \geq H(X|Z)$

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy `CRE` and `DPI`
- All symmetric and expansible $H \in \mathcal{Q}$ satisfy some interesting information-theoretical properties:
  - Additional information increases entropy: $H(X,Y) \geq H(X)$, $H(X,Y|Z) \geq H(X|Z)$
  - A weaker form of subadditivity: $H(X,Y) \leq H(\tilde{p})$ where $\tilde{p}(x,y) = p_X(x)/|\mathcal{Y}|$

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy `CRE` and `DPI`
- All symmetric and expansible $H \in \mathcal{Q}$ satisfy some interesting information-theoretical properties:
  - Additional information increases entropy: $H(X,Y) \geq H(X)$, $H(X,Y|Z) \geq H(X|Z)$
  - A weaker form of subadditivity: $H(X,Y) \leq H(\tilde{p})$ where $\tilde{p}(x,y) = p_X(x)/|\mathcal{Y}|$
  - Shannon's perfect secrecy: a symmetric encryption scheme in which a message M is encrypted using a key K can only be perfectly secret and correct if $H(M) \leq H(K)$

Properties of Limit Entropies

- Many properties of core-concave entropies can be straightforwardly generalised to limit entropies:
- All entropies in $\mathcal{Q}$ satisfy `CRE` and `DPI`
- All symmetric and expansible $H \in \mathcal{Q}$ satisfy some interesting information-theoretical properties:
  - Additional information increases entropy: $H(X,Y) \geq H(X)$, $H(X,Y|Z) \geq H(X|Z)$
  - A weaker form of subadditivity: $H(X,Y) \leq H(\tilde{p})$ where $\tilde{p}(x,y) = p_X(x)/|\mathcal{Y}|$
  - Shannon's perfect secrecy: a symmetric encryption scheme in which a message M is encrypted using a key K can only be perfectly secret and correct if $H(M) \leq H(K)$
  - A bound in terms of probability of error, that generalises Fano's inequality:

$$H(X|Y) \leq H\left(1-\hat{e}, \frac{\hat{e}}{n-1}, \ldots, \frac{\hat{e}}{n-1}\right)$$

where $\hat{e} = \sum_y p(y)(1 - \max_x p(x|y))$

New Conditional Forms: η-Geometric Mean

- Besides generalising entropies that satisfy `MIN` or `EAVG`, $\mathcal{Q}$ also subsumes other conditional forms

New Conditional Forms: η-Geometric Mean

- Besides generalising entropies that satisfy `MIN` or `EAVG`, $\mathcal{Q}$ also subsumes other conditional forms
- An entropy $H = (\eta, F)$ satisfies η-geometric mean (`EGM`), if $H(X|Y) = \eta\left(\prod_y (F(X|y))^{p(y)}\right)$.

New Conditional Forms: η-Geometric Mean

- Besides generalising entropies that satisfy `MIN` or `EAVG`, $\mathcal{Q}$ also subsumes other conditional forms
- An entropy $H = (\eta, F)$ satisfies η-geometric mean (`EGM`), if $H(X|Y) = \eta\left(\prod_y (F(X|y))^{p(y)}\right)$.

Proposition

If $H = (\eta, F)$ satisfies EGM, CCV and if F is nonegative, $H \in \mathcal{Q}$

New Conditional Forms: η-Geometric Mean

- Besides generalising entropies that satisfy MIN or EAVG, $\mathcal{Q}$ also subsumes other conditional forms
- An entropy $H = (\eta, F)$ satisfies η-geometric mean (EGM), if $H(X|Y) = \eta\left(\prod_y (F(X|y))^{p(y)}\right)$.

Proposition

If $H = (\eta, F)$ satisfies EGM, CCV and if F is nonegative, $H \in \mathcal{Q}$

- These CCV+EGM entropies have never been considered in QIF.

New Conditional Forms: η-Geometric Mean

- Besides generalising entropies that satisfy `MIN` or `EAVG`, $\mathcal{Q}$ also subsumes other conditional forms
- An entropy $H = (\eta, F)$ satisfies η-geometric mean (`EGM`), if $H(X|Y) = \eta\left(\prod_y (F(X|y))^{p(y)}\right)$.

Proposition

If $H = (\eta, F)$ satisfies EGM, CCV and if F is nonegative, $H \in \mathcal{Q}$

- These `CCV`+`EGM` entropies have never been considered in QIF.
- However, our results guarantee that they satisfy `CRE`, `DPI`, and the other aforementioned information-theoretical inequalities.

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy `CRE`, `DPI` and other important information-theoretic properties

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy CRE, DPI and other important information-theoretic properties
  - derived a new subfamily inspired on the geometric mean

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy `CRE`, `DPI` and other important information-theoretic properties
  - derived a new subfamily inspired on the geometric mean
  - investigated some applications of limit entropies on channel orderings, making connections with some recent results from Chatzikokolakis et al[3]

[3] Comparing Systems: Max-case Refinement Orders and Application to Differential Privacy (CSF 2019)

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy CRE, DPI and other important information-theoretic properties
  - derived a new subfamily inspired on the geometric mean
  - investigated some applications of limit entropies on channel orderings, making connections with some recent results from Chatzikokolakis et al[3]
- Future work:

[3] Comparing Systems: Max-case Refinement Orders and Application to Differential Privacy (CSF 2019)

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy $\texttt{CRE}$, $\texttt{DPI}$ and other important information-theoretic properties
  - derived a new subfamily inspired on the geometric mean
  - investigated some applications of limit entropies on channel orderings, making connections with some recent results from Chatzikokolakis et al[3]
- Future work:
  - Most QIF results concern entropies in $\mathcal{C}_{\texttt{AVG}}$. Is it possible to generalise these to $\mathcal{Q}$, which will as a consequence have $\mathcal{Q}_{\texttt{MIN}}$ as a particular case?

[3] Comparing Systems: Max-case Refinement Orders and Application to Differential Privacy (CSF 2019)

Conclusion and Future Work

- In this work, we
  - introduced a new generalizing family $\mathcal{Q}$, subsuming the core-concave and worst-case-scenario entropies used so far in the QIF literature
  - established that limit entropies satisfy `CRE`, `DPI` and other important information-theoretic properties
  - derived a new subfamily inspired on the geometric mean
  - investigated some applications of limit entropies on channel orderings, making connections with some recent results from Chatzikokolakis et al[3]
- Future work:
  - Most QIF results concern entropies in $\mathcal{C}_{\mathtt{AVG}}$. Is it possible to generalise these to $\mathcal{Q}$, which will as a consequence have $\mathcal{Q}_{\mathtt{MIN}}$ as a particular case?
  - Are there other families with interesting conditional forms to be derived from $\mathcal{Q}$?

[3] Comparing Systems: Max-case Refinement Orders and Application to Differential Privacy (CSF 2019)