On Conditional Entropies
Advertising a “New” Notion of Conditional Collision Entropy

Serge Fehr
CWI Amsterdam
www.cwi.nl/~fehr

Based on:
Connection to Ivan

This work has its roots in:

- a line of work I had with
- discussions we had during EUROCRYPT 2005 (which took place in Aarhus, with
- as general chair).
Our Situation Back Then

We were trying to prove security of a 1-2 OT scheme needed to bound the adversary’s uncertainty in $X$ ended up with two bounds

$$H_2(X) \geq \log\left(\frac{4}{3}\right)n \approx 0.415n \quad \text{and} \quad H_\infty^\varepsilon(X) \geq \frac{1}{2}n$$

and no bound on $H_\infty$ (beyond $H_\infty \geq \frac{1}{2}H_2$)

had to use the bound in terms of $H_\infty^\varepsilon$, because $H_2$ did not (seem to) have the necessary properties to work with.

Advantage:

bound is asymptotically optimal

Disadvantages:

tedious to work with, ugly error term, worse non-asymptotically
Our Situation Back Then

We were trying to prove security of a 1-2 OT scheme needed to bound the adversary's uncertainty in $X$.

Can we or can we not use the collision entropy $H_2$
- in this specific example problem?
- very generally: as a working alternative for $H_\infty$?

Yes, we can! We had to use the bound in terms of $H_2$ because $H_2$ did not (seem to) have the necessary properties to work with.

Advantage:
- bound is asymptotically optimal

Disadvantages:
- tedious to work with, ugly error term, worse non-asymptotically
**Shannon Entropy**

**Shannon entropy** of random variables $X$ with distribution $P_X$

$$H(X) := -\sum_x P_X(x) \log P_X(x)$$

and the **conditional Shannon entropy** of $X$ given $Y$

$$H(X|Y) := \sum_y P_Y(y) H(X|Y=y)$$

Useful and intuitive properties:

- $0 \leq H(X), H(X|Y) \leq \log |\mathcal{X}|$
- $H(X) \leq H(XY) \leq H(X) + H(Y)$
- $H(X|Y) \leq H(X)$ (monotonicity)
- $H(X|Y) = H(XY) - H(Y)$ ("strong" chain rule)
- $H(X|Y) \geq H(XY) - \log |\mathcal{Y}| \geq H(X) - \log |\mathcal{Y}|$ (chain rule)
Some Other Entropies

**Min-entropy:**

\[ H_\infty(X) := - \log \text{Guess}(X) \quad \text{where} \quad \text{Guess}(X) := \max_x P_X(x) \]

and **conditional version:**

\[ H_\infty(X|Y) := - \log \text{Guess}(X|Y) \]

where

\[ \text{Guess}(X|Y) := \sum_y P_Y(y) \text{Guess}(X|Y = y) \]

Properties:

- \( H_\infty(X|Y) \leq H_\infty(X) \) (monotonicity)
- \( H_\infty(X|Y) \geq H_\infty(XY) - \log |Y| \geq H_\infty(X) - \log |Y| \) (chain rule)
Some Other Entropies

Collision entropy:

\[ H_2(X) := - \log \text{Col}(X) \quad \text{where} \quad \text{Col}(X) = \sum_x P_X(x)^2 = \| P_X \|_2^2 \]

Max-entropy:

\[ H_0(X) := \log |\text{supp}(P_X)| \]

No commonly accepted definition of conditional versions.
Conditional Collision Entropy?

Some (previous) suggestions:

- $H_2(X|Y) := \sum_y P_Y(y) \, H_2(X|Y = y)$  \[ \times \]  \[ \times \]
- $H_2(X|Y) := -\log \sum_y P_Y(y) \, \text{Col}(X|Y = y)$  \[ \checkmark \]  \[ \times \]
- $H_2(X|Y) := H_2(XY) - H_2(Y)$  \[ \times \]  \[ \checkmark \]

Our new definition:

$H_2(X|Y) := -\log \text{Col}(X|Y)$

where

$$\text{Col}(X|Y) := \left( \sum_y P_Y(y) \sqrt{\text{Col}(X|Y = y)} \right)^2 = \left( \sum_y P_Y(y) \left\| P_{X|Y}(\cdot|y) \right\|_2 \right)^2$$

Recall:

$$\text{Col}(X) = \|P_X\|_2^2$$
Monotonicity, and Chain Rule

Theorem (Monotonicity): \( H_2(X|Y) \leq H_2(X) \)

Proof. To show: \( \text{Col}(X|Y) \geq \text{Col}(X) \).

\[
\text{Col}(X|Y) = \left( \sum_y P_Y(y) \left\| P_{X|Y}(\cdot|y) \right\|_2 \right)^2
\]

\[
= \left( \sum_y \left\| P_Y(y) P_{X|Y}(\cdot|y) \right\|_2 \right)^2
= \left( \sum_y \left\| P_{XY}(\cdot,y) \right\|_2 \right)^2
\]

\[
\geq \left\| \sum_y P_{XY}(\cdot,y) \right\|_2^2 = \left\| P_X \right\|_2^2 = \text{Col}(X)
\]

\( \triangle \text{-inequality} \)

QED
Monotonicity, and Chain Rule

Theorem (Chain Rule): \( H_2(X|Y) \geq H_2(XY) - \log|\mathcal{Y}| \)

Proof. To show: \( \text{Col}(X|Y) \leq \text{Col}(XY) \cdot |\mathcal{Y}| \).

\[
\text{Col}(X|Y) = \left( \sum_y P_Y(y) \| P_{X|Y}(\cdot|y) \|_2 \right)^2 = \left( \sum_y \| P_{XY}(\cdot,y) \|_2 \right)^2
\]

\[
= \left( \sum_y \sqrt{\sum_x P_{XY}(x,y)^2} \right)^2 = \left( |\mathcal{Y}| \cdot \frac{1}{|\mathcal{Y}|} \sum_y \sqrt{\sum_x P_{XY}(x,y)^2} \right)^2
\]

\[
\leq \left( |\mathcal{Y}| \cdot \sqrt{\frac{1}{|\mathcal{Y}|} \sum_{x,y} P_{XY}(x,y)^2} \right)^2 = |\mathcal{Y}| \cdot \sum_{x,y} P_{XY}(x,y)^2
\]

Jensen’s inequality

\[
= |\mathcal{Y}| \cdot \text{Col}(XY)
\]

QED
Privacy Amplification

The standard leftover hash lemma

$$\delta(F(X), \text{UNIF}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_2(X)-\ell)}$$

extends to a leftover hash lemma with side information:

$$\delta(F(X), \text{UNIF} | Y) = \sum_y P_Y(y) \delta(F(X), \text{UNIF} | Y = y)$$

$$\leq \frac{1}{2} \sum_y P_Y(y) 2^{-\frac{1}{2}(H_2(X|Y=y)-\ell)}$$

$$= \frac{1}{2} \sum_y P_Y(y) \sqrt{\text{Col}(X|Y=y)} \cdot 2^{\ell/2}$$

$$= \frac{1}{2} \sqrt{\text{Col}(X|Y)} \cdot 2^{\ell/2}$$

$$= \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_2(X|Y)-\ell)}$$
In Summary

Our notion of (condition) collision entropy satisfies the properties upon which security proofs using the min-entropy usually rely.

=> may serve well as an alternative to the min-entropy.

Additional bonus:

\[ H_2 \geq H_\infty \]

i.e., we may get more entropy and thus better parameters
Extension to the Rényi Entropy

For $\alpha \in \mathbb{R}_{\geq 0}$, $\alpha \neq 1$:

$$H_\alpha(X) := \frac{1}{1 - \alpha} \log \sum_x P_X(x)^\alpha$$

Equivalent formulation:

$$H_\alpha(X) = - \log \text{Ren}_\alpha(X)$$

where

$$\text{Ren}_\alpha(X) := \left( \sum_x P_X(x)^{\alpha} \right)^{\frac{1}{\alpha-1}} = \left( \sum_x P_X(x)^{\alpha} \right)^{\frac{1}{\alpha}} \cdot \frac{\alpha}{\alpha-1} = \| P_X \|_\alpha^{\frac{\alpha}{\alpha-1}}$$

Then, rather naturally:

$$H_\alpha(X|Y) := - \log \text{Ren}_\alpha(X|Y)$$

where

$$\text{Ren}_\alpha(X|Y) := \left( \sum_y P_Y(y)\| P_{X|Y=y} \|_\alpha \right)^{\frac{\alpha}{\alpha-1}}$$

[Arimoto77]
Rényi divergence or relative Rényi entropy (of order $\alpha$):
For distributions $P$ and $Q$ on $\mathcal{X}$

$$D_\alpha(P\|Q) := \frac{1}{\alpha - 1} \log \sum_x P(x)^\alpha Q(x)^{1-\alpha}$$

For $\alpha = 1$ : known as Kullback–Leibler divergence

Should be understood as measure of distance – but is no metric

Easy to see (recall that $H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha$):

$$H_\alpha(X) = -D_\alpha(P_X\|1) = \log |\mathcal{X}| - D_\alpha(P_X\|\text{UNIF}_X)$$

I.e., $H_\alpha(X) = (\text{entropy of unif}) - (\text{distance to unif})$. 
Another View on (Conditional) Rényi Entropy

Easy to see (recall that $H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha$):

$$H_\alpha(X) = -D_\alpha(P_X\|1) = \log |\mathcal{X}| - D_\alpha(P_X\|\text{UNIF}_X)$$

I.e., $H_\alpha(X) = (\text{entropy of unif}) - (\text{distance to unif})$.

For the conditional version:

$$H_\alpha(X|Y) = \log |\mathcal{X}| - \min_{Q_Y} D_\alpha(P_{X|Y}\|\text{UNIF}_X \cdot Q_Y)$$

I.e., $H_\alpha(X|Y) = (\text{entropy of indep. unif}) - (\text{distance to indep. unif})$.

Proof: Solving the optimization problem using Lagrange multipliers.
Natural extension of Rényi divergence $D_{\alpha}$ to quantum states:

$$D_{\alpha}(\rho \| \sigma) := \frac{1}{\alpha - 1} \log \text{tr}(\rho^\alpha \sigma^{1-\alpha})$$

called Petz quasi entropy [Petz84].

Define $H_{\alpha}(\rho_{XY} \| Y)$ by means of the connection the divergence:

$$H_{\alpha}(\rho_{XY} \| Y) := \log d_X - \min_{\sigma_Y} D_{\alpha}(\rho_{XY} \| \frac{1}{d_X} I_X \otimes \sigma_Y)$$

Does not give us the properties we want/expect!

Mainly because $D_{\alpha}$ does not behave very well.
Natural extension of Rényi divergence $D_\alpha$ to quantum states:

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha - 1} \log \text{tr}(\rho^\alpha \sigma^{1-\alpha})$$

called Petz quasi entropy [Petz84].

A different extension:

$$\tilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha - 1} \log \text{tr}
\left((\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha\right)$$

called “sandwiched” Rényi divergence [Müller-Lennert,Dupuis,Szehr,Fehr,Tomamichel2013]
[Wilde,Winter,Yang2013]

Define $H_\alpha(\rho_{XY}|Y)$ by means of the connection the divergence:

$$H_\alpha(\rho_{XY}|Y) := \log d_X - \min_{\sigma_Y} \tilde{D}_\alpha(\rho_{XY}\|\frac{1}{d_X} I_X \otimes \sigma_Y)$$
Next time you do a security proof using min-entropy, privacy amplification and co., check if you could use collision entropy as well, and get more entropy this way.