A Negative Result for Fuzzy Extractors

Luke Demarest
University of Connecticut
luke.h.demarest@gmail.com

Benjamin Fuller
University of Connecticut
benjamin.fuller@uconn.edu

Alexander Russell
University of Connecticut
acr@uconn.edu

April 11, 2022

Abstract

We show a negative result for efficient fuzzy extractors for all distributions with fuzzy min entropy even when given a (quasi) polynomial advice string from an unbounded collaborator.

1 Introduction

We show a negative result for efficient fuzzy extractors for all distributions with fuzzy min entropy even when given a (quasi) polynomial advice string from an unbounded collaborator.

We will compare to other works like [1].

2 Preliminaries

In this section we will introduce existing results to help clarify our place in the literature, provide necessary existing definitions to show what we are borrowing and what we build on, and we will provide new definitions in support of our novel results.

2.1 Existing Definitions

Definition (Entropy)**.** *Entropy*, denoted $H(X)$, for some random variable X is a measure of how stable the outcomes of the random variable are. It is calculated as

$$H(X) := \sum_{i=1}^{n} p(x_i) \operatorname{\mathsf{log}}(p(x_i))$$

where there are n values that X takes and we denote them as x_i.

Definition (Min Entropy)**.** *Min Entropy*, denoted $H_\infty(X)$, is a best case measure of the stability of the random variable X. It is calculated as

$$H_\infty(X) := -\mathsf{log}\left(\max_{x_i} p(x_i)\right)$$

.

Definition (Average Conditional Min Entropy)**.** *Average Conditional Min Entropy*, denoted $\widetilde{H}_\infty(X \,|\, Y)$ for two random variables X and Y is an average measure of the remaining entropy of the former given the outcome of the latter. It is calclulated as

$$\widetilde{H}_\infty(X \,|\, Y) := -\mathsf{log}\left(\mathop{\mathbb{E}}_{y \leftarrow Y}\left[\max_x \Pr[X = x \mid Y = y]\right]\right).$$

Definition (Hartley Entropy)**.** *Hartley Entropy* also called *Hartley's Function* measures the uncertainty of a random variable in a basic way, measuring the number of outcomes the random variable has with non-zero probability. It can be computed as

$$H_0(X) = |\{x \in X \mid \Pr[X = x] > 0\}\,|.$$

Definition (Markov's Inequality)**.** Markov's inequality is a tail bound for random variables that gives an upper bound on the probability of a random variable deviating from its mean. Let X be a non-negative valued random variable. Then the following inequality holds for any $\alpha > 0$:

$$\Pr[X \geq \alpha \cdot \mathbb{E}[X]] \leq 1/\alpha.$$

2.2 Previous Results

It has been shown that universal fuzzy extractors are impossible in the information theoretic setting.

2.2.1 Markov Bound for Predictability

Markov bounds are tail bounds that use Markov's Inequality to bound the probability that a random variable deviates significantly from its expected value. In Markov's inequality, we necessarily lose a multiplicative factor (here called *alpha*) in order to control the probability of the event occuring. When discussing entropy, we are dealing with a log scaled value which makes losing multiplicative factors costly. Instead, we can perform a Markov bound on the predictability scale. In this case, rather than lose a multiplicative factor in entropy, we lose a multiplicative factor in predictability which translates to a small number of bits of entropy lost for the controlled outcomes.

We present the proof here: Let $\vec{X} = (X_1, X_2, \ldots, X_k)$ be independent random variables. Let Y be a random variable arbitrarility correlated with $\vec{X}$.

Then we can bound the entropy loss of $\widetilde{H}_\infty\left(\vec{X}\,|\,Y\right)$ using a Markov bound on predictability.

$$\widetilde{H}_\infty\left(\vec{X}\,|\,Y\right) = \Delta \tag{1}$$

$$-\mathsf{log}\left(\mathop{\mathbb{E}}_{Y}\left[\max_{\vec{x}} \Pr\left[\vec{X} = \vec{x}\,|\,Y = y\right]\right]\right) = \Delta \tag{2}$$

$$\mathop{\mathbb{E}}_{Y}\left[\max_{\vec{x}} \Pr\left[\vec{X} = \vec{x}\,|\,Y = y\right]\right] = 2^{-\Delta} \tag{3}$$

$$\Pr_{Y}\left[\max_{\vec{x}} \Pr\left[\vec{X} = \vec{x}\,|\,Y = y\right] \geq \alpha \cdot 2^{-\Delta}\right] \leq \frac{1}{\alpha} \tag{4}$$

$$\Pr_{Y}\left[\mathsf{log}\left(\max_{\vec{x}} \Pr\left[\vec{X} = \vec{x}\,|\,Y = y\right]\right) \geq \mathsf{log}(\alpha) - \Delta\right] \leq \frac{1}{\alpha} \tag{5}$$

$$\Pr_{Y}\left[-\mathsf{log}\left(\max_{\vec{x}} \Pr\left[\vec{X} = \vec{x}\,|\,Y = y\right]\right) < \Delta - \mathsf{log}(\alpha)\right] \leq \frac{1}{\alpha} \tag{6}$$

$$\Pr_{Y}[H_\infty(X\,|\,Y) < \Delta - \mathsf{log}(\alpha)] \leq \frac{1}{\alpha} \tag{7}$$

2.3 New Definitions

Fuzzy extractors with quasipolynomial advice.

3 Sampling Proceedure

The sampling proceedure that we will use and discuss in this work is two fold. There is first, a family of distributions that we will call $\mathcal{W}$. There is some finite number of distributions in this family, we call $|\mathcal{W}| = \mathcal{R}$. We let Z be an index for the distributions in the family and we denote the Zth family W_Z. The distribution W_Z can then be sampled, and we denote a sample of W_Z as $w_Z \in \{0,1\}^n$. When Z is clear, we will omit the subscript.

To sample a uniform point in $\mathcal{W}$, we can uniformly select Z and then pick from W_Z unifromly. This two stage process gives us more tools to reason about the ability of an efficient adversary.

In general, we will assume that $\mathcal{W}$ is public to any adversary, algorithm, or party we may discuss. We will generally assume that the specific selection of Z is only shared with specific parties. We will also assume that the specific w sampled from W_Z is private and only known to parties who are given it explicity.

An interesting part of this work is how we share informtaion about W_Z. We will allow an inefficient adversary access to the entire description of W_Z and ask them to produce an advice string for an efficient adversary, that is that the advice string length is bound from above by a arbitrary polynomial function of our security parameter.

References

[1] Benjamin Fuller, Leonid Reyzin, and Adam Smith. When are fuzzy extractors possible? *IEEE Transactions on Information Theory*, 66(8):5282–5298, 2020.