Explicit Rényi Entropy for Hidden Markov Chains

Joachim Breitner, *Maciej Skorski*

ISIT, June 2020

Plan

Rényi Entropy

- Renyi Entropy [Rén61] is *popular measure of randomness*, with lots of applications
- Formally, the Renyi entropy of a discrete random variable Z is

$$\mathbf{H}_\alpha(Z) = \frac{1}{1-\alpha} \log \left(\sum_i \Pr[Z = i]^\alpha \right)$$

- For a stochastic process $\mathbf{Z} = (Z_i)_i$ of interest are the *limiting entropy* and the *rate*

$$\mathbf{H}_\alpha(\mathbf{Z}) = \lim_{n \to +\infty} \frac{1}{n} \mathbf{H}_\alpha(Z_1, \ldots, Z_n)$$

Think of it as limiting entropy per sample. Well defined under mild assumptions.

Stochastic Models

- IID: z_i are independent
- Markov Model: $\mathbf{P}(z_i \mid z_{i-1})$ given by *transition matrix*
- Hidden Markov Model: *transitions* $\mathbf{P}(x_i \mid x_{i-1})$, *emissions* $\mathbf{P}(z_i \mid x_i)$, observed are z_i
- ... more complicated models possible, in this work we focus on HMM

Renyi Entropy Rate

- Finding the limit $\mathbf{H}_\alpha(\mathbf{Z})$ is generally hard, we know formulas only for certain cases
- IID model has explicit formulas (entropy rate is entropy of sampled symbol)
- Markov Model has explicit formulas [RAC01] (depending on transitions)
- Don't seem to generalize to Hidden Markov Model ...
- Related Work: certain approximation proposed in [WXH17] but no formulas

Issue: Factorization Difficulties

- IID and MM factorize: $\mathbf{P}(z_1, \ldots, z_n)$ can be written as a power of *known matrix*.
- Factors of HMM would depend on hidden states, e.g. are *random*, harder to analyze.

Problem: Determine Entropy Rate for Hidden Markov Model

Can we have an explicit formula for the entropy rate of *Hidden Markov Chains*?
Motivation: HMM are reach models with important applications, e.g. in linguistic.

Plan

Our Result

- We work under Hidden Markov Model, observed are $Z_i \in \mathcal{Z}$, unobserved $X_i \in \mathcal{X}$
- We assume the entropy order $\alpha > 1$ is integer
- We give a formula which depends on the (Markov!) transition matrix M of (X_i, Z_i)
- To state the formula we need the set of z-collisions

$$\mathcal{C} = \{(x_1, z_1, \ldots, x_\alpha, z_\alpha) \mid z_1 = \ldots = z_\alpha\}$$

Below $M^{\otimes\alpha}$ is α-fold Kronecker product, $M_{\mathcal{C}}^{\otimes\alpha}$ the submatrix matching restrictions $\mathcal{C}$

Theorem (Renyi Entropy of Sample Paths for HMM)

$$\mathbf{H}_\alpha(Z_1, \ldots, Z_n) = \frac{1}{1-\alpha} \log\left(\mathbf{P}_{X_1,Z_1}^T \cdot \left(M_{\mathcal{C}}^{\otimes\alpha}\right)^{n-1} \cdot \mathbf{1}\right)$$

Theorem (Renyi Entropy Rate of HMM)

Let I^+ be reachable irreducible components of $M_{\mathcal{C}}^{\otimes\alpha}$ with largest eigenvalues ρ_i

$$\mathbf{H}_\alpha(\mathbf{Z}) = \frac{1}{1-\alpha} \log\left(\max_{i \in I^+} \rho_i\right), \quad \mathbf{Z} = \{Z_i\}_i$$

Techniques / Proof Sketch (I)

- Collision/Parallelization Trick: α is integer so Renyi entropy of $Z = (Z_1, \ldots, Z_n)$ relates to collision probability of α parallel copies of Z.
- Bringing hidden states: Let $x_1^n = (x_1, \ldots, x_n)$ and $z_1^n = (z_1, \ldots, z_n)$. We can write

$$2^{(\alpha-1)\mathbf{H}_\alpha(Z)} = \sum_{x_1^n, z_1^n \in \mathcal{C}} \mathbf{P}(x_1^n, z_1^n)$$

- Chain with revealed hidden states is Markov: we can factor (X_i, Z_i)

$$\sum_{x_1^n, z_1^n \in \mathcal{C}} \mathbf{P}(x_1^n, z_1^n) = \sum_{x_1^n, z_1^n \in \mathcal{C}} \mathbf{P}(x_i, z_i \mid x_{i-1}, z_{i-1})$$

- Since M is the matrix of the parallelized Markov chain (X_i, Z_i), Thm 1 follows.

Techniques / Proof Sketch (II)

- For the second theorem we develop a growth lemma for non-negative matrix powers
- Specifically, let $A \geqslant \mathbf{0}$ be a matrix, $u \geqslant \mathbf{0}$ be vector, and A^+ the submatrix of rows and cols i s.t. $u^T A^n \mathbf{e}_i > 0$ for some k. Then we have $u^T A^n \mathbf{1} = (\rho(A^+) + o(1))^n$.
- The lemma utilizes Gelfand's formula, applied to pseudonorm $A \to u^T A \mathbf{1}$.
- Result of independent interest, can replace applications of Perron-Frobenius theory

Application: Modelling side-channel leakage [BBG+17]

- Attacked algorithm: Modular exponentation with sliding window
  - Hidden: The bits of the secret exponent
  - Observed: When we square and when we multiply.

  This can be modeled as an Hidden Markov Chain!
- Attack effective if > 0.5 bits of Rényi entropy leaked per input bit
  Why Rényi entropy? Intuitively:
  Attacker learns more when the observed output of fewer hidden states *collide*
  Theorem 3 in [BBG+17], proof in [Bre18]
- The present work now explains why attack is effective
  (against 1024 bit RSA, window width $w = 4$))

More applications (see our paper)

- Relaxing regularity conditions for Markov Chain rates
- Algebraic characterization of Rényi Rates under HMM
- Renyi rates for HMM with certain noise structure
- Evaluating Security of TRNG

Plan

Summary

- Explicit characterization of Renyi Entropy under HMM for integer α. For non-integer α one can do entropy smoothing or sandwiching
- Result on growth of matrix powers, of independent interest.
- Applications, including an analysis of a cryptography attack!
- For mode details, please see the paper and slides (available online)

Thank you for your attention!


Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, and Yuval Yarom, *Sliding right into disaster: Left-to-right sliding windows leak*, Cryptology ePrint Archive, Report 2017/627, 2017, `https://eprint.iacr.org/2017/627`.


Joachim Breitner, *More on sliding right*, Cryptology ePrint Archive, Report 2018/1163, 2018, `https://eprint.iacr.org/2018/1163`.


Ziad Rached, Fady Alajaji, and L. Lorne Campbell, *Rényi's divergence and entropy rates for finite alphabet markov sources*, IEEE Trans. Information Theory **47** (2001), no. 4, 1553–1561.


Alfréd Rényi, *On measures of information and entropy*, Proceedings of the 4th Berkeley symposium on mathematics, statistics and probability, vol. 1, 1961.


Chengyu Wu, Easton Li Xu, and Guangyue Han, *Rényi entropy rate of hidden markov processes*, 2017 IEEE International Symposium on Information Theory (ISIT), IEEE, 2017, pp. 2970–2974.