Differentially Private Fractional Frequency Moments Estimation with Polylogarithmic Space

PRESENTER:
Lun Wang

BACKGROUND: In the present work, we make the first customized effort towards DP estimation of fractional frequency moments, i.e. p ∈ (0, 1] with low space complexity. We show that a well-known streaming algorithm, namely Fp sketch [21], preserves differential privacy as is. With its small space complexity, Fp sketch elegantly solves the trilemma between efficiency, accuracy, and privacy.

Fp SKETCH REVIEW

Algorithm 1: $\mathbb{F}_p$ sketch.

Input : Data stream: $\mathcal{S} = \{(k_1, v_1), \cdots, (k_n, v_n)\}$

Construct:

  Initialize $\mathbf{a} = \{0\}^r$, $\mathbf{P} \sim \mathcal{D}_{p,1}^{r \times m}$;

Update:

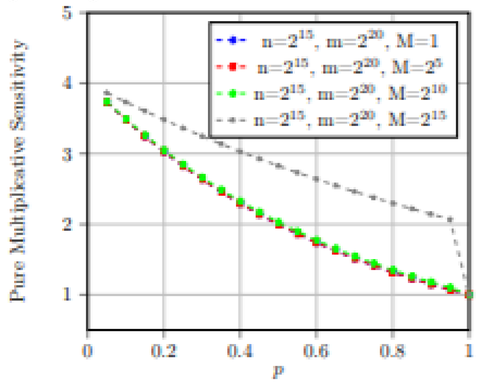
  for $i \in [n]$ **do** Let e_{k_i} be the one-hot encoder of k_i, $\mathbf{a} = \mathbf{a} + \mathbf{P} \times v_i \mathbf{e}_{k_i}$;

Query:

  return scale_estimator($\mathbf{a}$);

METHODOLOGY & RESULTS

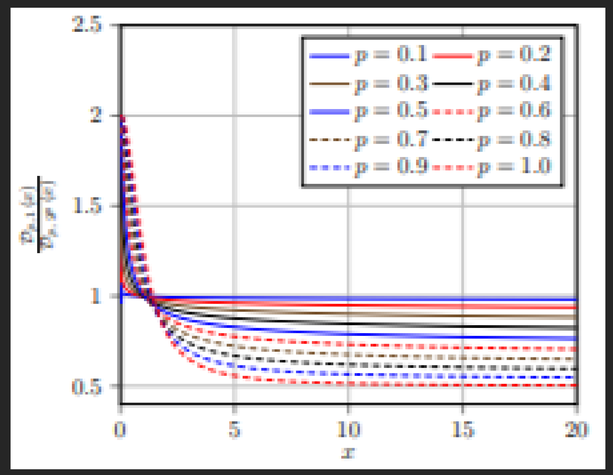
STEP 1: Bound the difference between scales of neighboring datasets



STEP 2: Bound the privacy loss

Theorem 3 (ϵ-DP for Algorithm 1). *Let ρ_p represent the multiplicative sensitivity of the p-th frequency moments. When $r = 1$ and $p \in (0, 1]$, moments. When $r = 1$ and $p \in (0, 1]$, $\mathbb{F}_p$ sketch is $\frac{1}{p} \ln \rho_p$-differentially private.*

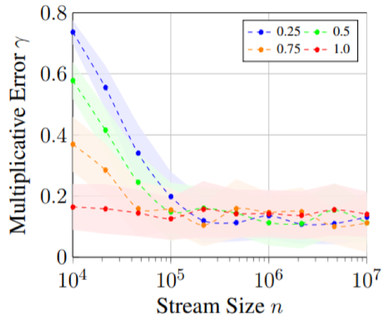
We prove that **Fp sketch**, a streaming algorithm for **frequency moments estimation**, is **differentially private** when **p ∈ (0, 1].**



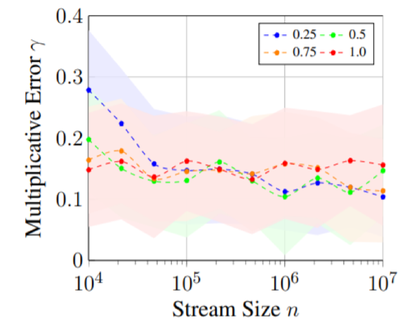
SCAN ME

Take a picture to download the full paper

EXPERIMENT



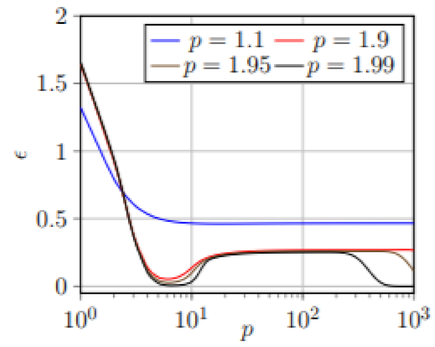
(a) Uniformly Distributed Stream.



(b) Binomially Distributed Stream.

OPEN PROBLEMS

The proof does not easily extend to p ∈ (1, 2).



Lun Wang, Iosif Pinelis, Dawn Song