Objectives

- Design a differentially private Bayesian inference mechanism.
- Improve accuracy by calibrating noise to the sensitivity of a metric over distributions (e.g. Hellinger distance ($\mathcal{H}$), f-divergences, etc.).

An example of Bayesian inference: the Beta-Binomial model

- Prior on $\theta : P_\theta = \text{beta}(\alpha, \beta)$, $\alpha, \beta \in \mathbb{R}^+$, observed data $x = (x_1, \ldots, x_n) \in \{0, 1\}^n$, $n \in \mathbb{N}$.
- Likelihood function: $L_{\theta|x} = \theta^{n-\Delta \alpha}(1-\theta)^{\Delta \alpha}$, where $\Delta \alpha = \sum_{i=1}^n x_i$.
- Posterior on $\theta : BI(x) \equiv P_{\theta|x} = \text{beta}(\alpha + \Delta \alpha, \beta + n - \Delta \alpha) \propto L_{\theta|x} \cdot P_{\theta}$.

Differentially private Bayesian inference

- Baseline approach: $\Delta BI \equiv \max_{x,x' \in \{0,1\}^n, ||x-x'|| \leq 1} ||BI(x) - BI(x')||_1$.
- Measure accuracy with a metric over distributions. E.g. $\mathcal{H}(f,g)^2 \equiv 1 - \int (\sqrt{T(x)g(x)}dx) (f,g \text{ densities})$.

But $\Delta BI$ grows linearly with the dimension: too noisy when we generalize to Dirichlet-Multinomial (DL-) model.

- Another approach:
  - Calibrate noise w.r.t global sensitivity of $\mathcal{H}$: but global sensitivity is still too big.
  - Fig. 1 shows that there is a gap between global and local sensitivity of $\mathcal{H}$.
- A different approach:
  - Calibrate noise w.r.t. the smooth sensitivity of $\mathcal{H}$.

Our approach: smoothed Hellinger distance based exponential mechanism

We define the mechanism $\mathcal{M}_H$ which produces an element $r$ in $\mathcal{R}_{post}$ with probability:

$$P_{r \sim \mathcal{M}_H} = \frac{\exp \left( -\frac{\epsilon \cdot \mathcal{H}(BI(x), r)}{2S(x)} \right)}{\sum_{r \in \mathcal{R}_{post}} \exp \left( -\frac{\epsilon \cdot \mathcal{H}(BI(x), r)}{2S(x)} \right)}$$

- $\mathcal{R}_{post} \equiv \{\text{beta}(\alpha', \beta') \mid \alpha' = \alpha + \Delta \alpha, \beta' = \beta + n - \Delta \alpha\}$. With prior distribution $\beta_{post} = \text{beta}(\alpha, \beta)$.
- $-\mathcal{H}(BI(x), r)$ denotes the scoring function.
- $S(x) \equiv \max_{x' \in \{0,1\}^n} \{LS(x') \cdot e^{-\gamma d(x,x')}\}$: smooth sensitivity[1], $d$ is the Hamming distance.
- $LS(x') \equiv \max_{y \in \mathcal{X}^n \setminus \{adj(x,x')\}, r \in \mathcal{R}} [\mathcal{H}(BI(y), r) - \mathcal{H}(BI(x'), r)]$ is the local sensitivity of $x'$, $\gamma = \ln(1 - \frac{\epsilon}{2S(x)})$.

Preliminary experimental results

Experiments are about three mechanisms and plotted as follows:

- **Green**: Baseline approach.
- **Red**: Improved approach by using sensitivity 1 in 2 dimensions and 2 in higher dimensions. Indeed: we can see the output of the Bayesian inference as a histogram, and $||BI(x) - BI(x')||_1 \leq 2$.
- **Blue**: $\mathcal{M}_H$. The fact that there is only one candidate distribution which achieves the highest score and different distributions which achieve a sub-optimal score explains the (highest) peaks in Fig. 2(a) (and Fig. 2(b)).

Conclusion

- $\mathcal{M}_H$ outperforms the baseline approach but not the improved one, for priors with small parameters.
- When the prior parameters increase $\mathcal{M}_H$ is comparable with the improved baseline approach.

References