Proof of DP - Bayesian Inference

Jiawen Liu

Tuesday 14th November, 2017

If we want the posterior distribution from the Bayesian inference is ϵ - differential privacy, this mechanism should satisfy:

$$\frac{Pr[BayesInfer_{DP}(d_1) \in S]}{Pr[BayesInfer_{DP}(d_2) \in S]} \leq e^{\epsilon},$$

where $BayesInfer_{DP}(d)$ is a differentially private Bayesian inference mechanism, and d_1, d_2 is a pair of adjacent observed data sets. Since in our model, this inference is based on a bias p with beta prior distribution: $p \sim Beta(\alpha_0, \beta_0)$ and an observed data set $d \sim B(n,p)$, which result in a posterior distribution on $p \sim Beta(\alpha_0 + k, \beta_0 + l)$ where k and l is the number of 1 and 0 in d. As a result, the requirement above can be rewrote as:

$$\frac{Pr[Beta(\alpha_0 + k_1^*, \beta_0 + l_1^*) \in S]}{Pr[Beta(\alpha_0 + k_2^*, \beta_0 + l_2^*) \in S]} \leq e^{\epsilon},$$

where k_1^* and l_1^* is the number of 1 and 0 in d_1 after protection, the same with k_2^* and l_2^*. The equation above is equivalent to:

$$\frac{Pr[\langle \alpha_0 + k_1^*, \beta_0 + l_1^* \rangle = S]}{Pr[\langle \alpha_0 + k_2^*, \beta_0 + l_2^* \rangle = S]} \leq e^{\epsilon}.$$

Under Laplace mechanism, the sensitivity of k and l is both 1 we have $k^* = k + Lap(\frac{\epsilon}{2})$, and $l^* = l + Lap(\frac{\epsilon}{2})$. Suppose $S = \langle S_1, S_2 \rangle$, where $S_1 - \alpha_0 - k \sim Lap(\frac{\epsilon}{2}), S_2 - \beta_0 - l \sim Lap(\frac{\epsilon}{2})$. Then,

$$Pr[\langle \alpha_0 + k_1^*, \beta_0 + l_1^* \rangle = S] = exp(-(S_1 - \alpha_0 - k_1)\frac{\epsilon}{2}))exp(-(S_2 - \beta_0 - l_1)\frac{\epsilon}{2})),$$

and

$$Pr[\langle \alpha_0 + k_2^*, \beta_0 + l_2^* \rangle = S] = exp(-(S_1 - \alpha_0 - k_2)\frac{\epsilon}{2})) * exp(-(S_2 - \beta_0 - l_2)\frac{\epsilon}{2})).$$

We can finally get:

$$\frac{Pr[\langle \alpha_0 + k_1^*, \beta_0 + l_1^* \rangle = S]}{Pr[\langle \alpha_0 + k_2^*, \beta_0 + l_2^* \rangle = S]} = exp(\epsilon),$$

i.e.

$$\frac{Pr[BayesInfer_{DP}(d_1) \in S]}{Pr[BayesInfer_{DP}(d_2) \in S]} \leq e^{\epsilon},$$