Differentially Private Markov Chain Monte Carlo

Mikko Heikkilä*¹, Joonas Jälkö*², Onur Dikmen³ and Antti Honkela¹

* Equal contribution
¹ University of Helsinki
² Aalto University
³ Halmstad University

NeurIPS, 12 December 2019
We propose a method for sampling from posterior distribution under DP guarantees.
We propose a method for sampling from posterior distribution under DP guarantees.
Three general purpose approaches for DP Bayesian inference:

1. Drawing single samples from the posterior with the exponential mechanism (Dimitrakakis et al., ALT 2014; Wang et al., ICML 2015; Geumlek et al., NIPS 2017)
   Privacy is conditional to sampling from the true posterior.
Three general purpose approaches for DP Bayesian inference:

1. Drawing single samples from the posterior with the exponential mechanism (Dimitrakis et al., ALT 2014; Wang et al., ICML 2015; Geumlek et al., NIPS 2017)

   Privacy is conditional to sampling from the true posterior.

2. Perturbation of gradients in SG-MCMC (Wang et al., ICML 2015, Li et al., AISTATS 2019) or variational inference (Jälkö et al., UAI 2017) with Gaussian mechanism, similar to DP stochastic gradient descent

   No guarantees where the algorithm converges, requires differentiability
DNA mechanisms for Bayesian inference

Three general purpose approaches for DP Bayesian inference:

1. Drawing single samples from the posterior with the exponential mechanism
   (Dimitrakakis et al., ALT 2014; Wang et al., ICML 2015; Geumlek et al., NIPS 2017)

   Privacy is conditional to sampling from the true posterior.

2. Perturbation of gradients in SG-MCMC (Wang et al., ICML 2015, Li et al., AISTATS 2019)
   or variational inference (Jälkö et al., UAI 2017) with Gaussian mechanism, similar to DP
   stochastic gradient descent

   No guarantees where the algorithm converges, requires differentiability

3. Computing the privacy cost of Metropolis–Hastings acceptances for the entire MCMC chain
   (Heikkilä et al., NeurIPS 2019; Yıldırım & Ermiş, Stat Comput 2019)
We employ the stochasticity of this decision to assure privacy
Acceptance test (Barker et al. 1965)

Accept $\theta'$ from proposal $q$ if $\Delta(\theta'; \mathcal{D}) + V_{\text{logistic}} > 0$
Outline of the method

**Acceptance test (Barker et al. 1965)**

Accept $\theta'$ from proposal $q$ if $\Delta(\theta'; D) + V_{\text{logistic}} > 0$

**Subsampled MCMC (Seita et al. 2017)**

Instead of using full data, evaluate above using $S \subset D$

Decompose the logistic noise: $V_{\text{logistic}} = V_{\text{normal}} + V_{\text{correction}}$

$\Rightarrow$ Accept $\theta'$ from proposal $q$ if $\Delta(\theta'; S) + \tilde{V}_{\text{normal}}(\sigma^2_\Delta) + V_{\text{correction}} > 0$
Outline of the method

Acceptance test (Barker et al. 1965)

Accept $\theta'$ from proposal $q$ if $\Delta(\theta'; D) + V_{\text{logistic}} > 0$

Subsampled MCMC (Seita et al. 2017)

Instead of using full data, evaluate above using $S \subset D$

Decompose the logistic noise: $V_{\text{logistic}} = V_{\text{normal}} + V_{\text{correction}}$

$\Rightarrow$ Accept $\theta'$ from proposal $q$ if $\Delta(\theta'; S) + \tilde{V}_{\text{normal}}(\sigma_\Delta^2) + V_{\text{correction}} > 0$

Analyse the privacy implications (This work)

We use Rényi DP to compute the privacy guarantees of the acceptance condition

Subsampling allows us to benefit from privacy amplification (Wang et al., AISTATS 2019)
Conclusions

• We have formulated a DP MCMC method for which privacy guarantees do not rely on the convergence of the chain.

Come see us at our poster #158 in East Exhibition Hall (B + C)