Private Topic Modeling

Park, M.; Foulds, J.; Chaudhuri, K.; Welling, M.

Published in:
Private Multi-Party Machine Learning

Citation for published version (APA):
Abstract

We develop a privatized stochastic variational inference method for Latent Dirichlet Allocation (LDA). The iterative nature of stochastic variational inference presents challenges: multiple iterations are required to obtain accurate posterior distributions, yet each iteration increases the amount of noise that must be added to achieve a reasonable degree of privacy. We propose a practical algorithm that overcomes this challenge by combining: (1) A relaxed notion of the differential privacy, called concentrated differential privacy, which provides high probability bounds for cumulative privacy loss, which is well suited for iterative algorithms, rather than focusing on single-query loss; and (2) privacy amplification resulting from subsampling of large-scale data. Focusing on conjugate exponential family models, in our private variational inference, all the posterior distributions will be privatized by simply perturbing expected sufficient statistics. Using Wikipedia data, we illustrate the effectiveness of our algorithm for large-scale data.

1 Background

We start by providing background information on the definitions of algorithmic privacy that we use, as well as the general formulation of the variational inference algorithm.

Differential privacy. Differential privacy (DP) is a formal definition of the privacy properties of data analysis algorithms [1]. A randomized algorithm \( M(X) \) is said to be \((\epsilon, \delta)\)-differentially private if

\[
\Pr(M(X) \in S) \leq \exp(\epsilon) \Pr(M(X') \in S) + \delta
\]

for all measurable subsets \( S \) of the range of \( M \) and for all datasets \( X, X' \) differing by a single entry. If \( \delta = 0 \), the algorithm is said to be \( \epsilon \)-differentially private. Intuitively, the definition states that the output probabilities must not change very much when a single individual’s data is modified, thereby limiting the amount of information that the algorithm reveals about any one individual.

Concentrated differential privacy (CDP) [2] is a recently proposed relaxation of DP which aims to make privacy-preserving iterative algorithms more practical than for DP while still providing strong privacy guarantees. The CDP framework treats the privacy loss of an outcome, \( \log \frac{Pr(M(X) = o)}{Pr(M(X') = o)} \), as a random variable. An algorithm is \((\mu, \tau)\)-CDP if this privacy loss has mean \( \mu \), and after subtracting \( \mu \) the resulting random variable \( l \) is subgaussian with standard deviation \( \tau \), i.e. \( \forall \lambda \in \mathbb{R} : E[e^{\lambda l}] \leq \exp(\lambda^2 \tau^2 / 2) \). While \( \epsilon \)-DP guarantees bounded privacy loss, and \((\epsilon, \delta)\)-DP ensures bounded privacy loss with probability \( 1 - \delta \), \((\mu, \tau)\)-CDP requires the privacy loss to be near \( \mu \) w.h.p.

The general VI algorithm. Consider a generative model that produces a dataset \( D = \{D_n\}_{n=1}^{N} \) consisting of \( N \) independent identically distributed items, where \( D_n \) is an \( n \)th observation, generated using a set of latent variables \( l = \{l_n\}_{n=1}^{N} \). The generative model provides \( p(D_n | l_n, \mathbf{m}) \), where \( \mathbf{m} \) is the model parameters. We also consider the prior distribution over the model parameters \( p(\mathbf{m}) \) and the prior distribution over the latent variables \( p(l) \). Here, we focus on conjugate-exponential (CE) models[1] in which the variational updates are tractable. The CE fami-

---

[1] A large class of models falls in the CE family including linear dynamical systems and switching models; Gaussian mixtures; factor analysis and probabilistic PCA; hidden Markov models and factorial HMMs; discrete-variable belief networks; and latent Dirichlet allocation (LDA), which we will use in Sec 3.
ily models satisfy the two conditions [3]: (1) Complete-data likelihood is in exponential family:
\[ p(D_n, l_n | m) = q(m) f(D_n, l_n) \exp(n(m)^\top s(D_n, l_n)) \]
and (2) Prior over \( m \) is conjugate to the complete-data likelihood:
\[ p(m | \tau, \nu) = h(\tau, \nu) q(m)^\top \exp(\nu^\top m) \]
where natural parameters and sufficient statistics of the complete-data likelihood are denoted by \( n(m) \) and \( s(D_n, l_n) \), respectively. The hyperparameters are denoted by \( \tau \) (a scalar) and \( \nu \) (a vector).

Variational inference for a CE family model iterates the following two steps in order to optimise the lower bound to the log marginal likelihood,
\[ \mathcal{L}(q(l), q(m)) = \int d\theta q(l) q(m) \log \frac{p(l, D_n, m)}{q(l) q(m)} \]
\[ \approx \sum_{n=1}^{N} \left[ \sum_{l=1}^{L} \log \frac{p(l_n, D_n, m_n)}{q(l_n) q(m_n)} \right] \]
\[ \approx Q \left[ \sum_{n=1}^{N} \left( \sum_{l=1}^{L} \log \frac{p(l_n, D_n, m_n)}{q(l_n) q(m_n)} \right) \right] \]

(a) given expected natural parameters \( \bar{n} \), the first step computes the approximate posterior over latent variables:
\[ q(l) = \prod_{n=1}^{N} q(l_n) \propto \prod_{n=1}^{N} f(D_n, l_n) \exp(\bar{n}^\top s(D_n, l_n)) = \prod_{n=1}^{N} p(l_n | D_n, \bar{n}) \]
Using \( q(l) \), the first step outputs expected sufficient statistics \( \bar{s}(D) = \frac{1}{N} \sum_{n=1}^{N} s(D_n, l_n) | q(l_n) \).

(b) given expected sufficient statistics \( \bar{s}(D) \), the second step computes the approximate posterior over parameters:
\[ q(m) = h(\bar{\tau}, \bar{\nu}) q(m)^\top \exp(\bar{\nu}^\top m) \]
Using \( q(m) \), the second step outputs expected natural parameters \( \bar{n} = (n(m)) | q(m) \).

2 Privacy Preserving VI algorithm for CE family

The only place where the algorithm looks at the data is when computing the expected sufficient statistics \( \bar{s}(D) \) in the first step. The expected sufficient statistics then dictates the expected natural parameters in the second step. So, perturbing the sufficient statistics leads to perturbing both posterior distributions \( q(l) \) and \( q(m) \). Perturbing sufficient statistics in exponential families is also used in [4]. Existing work focuses on privatising posterior distributions in the context of posterior sampling [5][6][7][8], while our work focuses on privatising approximate posterior distributions for optimisation-based approximate Bayesian inference.

Suppose there are two neighbouring datasets \( D \) and \( \bar{D} \), where there is only one datapoint difference among them. We also assume that the dataset is pre-processed such that the \( L_2 \) norm of any datapoint is less than 1. The maximum difference in the expected sufficient statistics given the datasets, e.g., the \( L_1 \) sensitivity of the expected sufficient statistics is given by (assuming \( s \) is a vector of length \( L \))
\[ \Delta s = \max_{D_n, \bar{D}_n, q(l_n), q(\bar{l}_n)} \sum_{l=1}^{L} | \frac{1}{N} \sum_{n=1}^{N} s(D_n, l_n) - \frac{1}{N} \sum_{n=1}^{N} s(\bar{D}_n, l_n) | \]
Under some models like LDA below, the expected sufficient statistic has a limited sensitivity, in which case we add noise to each coordinate of the expected sufficient statistics to compensate the maximum change.

3 Privacy preserving Latent Dirichlet Allocation (LDA)

The most successful topic modeling is based on LDA, where the generative process is given by [9].

- Draw topics \( \beta_k \sim \text{Dirichlet} (\eta 1_K) \)

- For each document \( d \in \{1, \ldots, D\} \)
  - Draw topic proportions \( \theta_d \sim \text{Dirichlet} (\alpha 1_K) \), where \( \alpha \) is a scalar hyperparameter.
  - For each word \( n \in \{1, \ldots, N\} \)
    * Draw topic assignments \( z_{dn} \sim \text{Discrete} (\theta_d) \)
    * Draw word \( w_{dn} \sim \text{Discrete} (\beta_{z_{dn}}) \)

where each observed word is represented by an indicator vector \( w_{dn} \) (nth word in the \( d \)th document) of length \( V \), where \( V \) is the number of terms in a fixed vocabulary set. The topic assignment latent variable \( z_{dn} \) is also an indicator vector of length \( K \), where \( K \) is the number of topics.

The LDA falls into the CE family, where we think of \( z_{d1:1:N}, \theta_d \) as two types of latent variables : \( l_d = \{ z_{d1:1:N}, \theta_d \} \), and \( \beta \) as model parameters \( m = \beta \). (1) Complete-data likelihood per document is in exponential family:
\[ p(w_{d1:1:N}, z_{d1:1:N}, \theta_d | \beta) \propto f(D_d, z_{d1:1:N}, \theta_d) \exp(\sum_{n=1}^{N} \sum_{k} [\log \beta_k]^\top [z_{dn} | w_{dn}]) \]
where \( f(D_d, z_{d1:1:N}, \theta_d) \propto \exp(\alpha [1_K]^\top [\log \theta_d] + \sum_{k} \sum_{d} z_{dn}^k \log \beta_k^k) \) (2) Conjugate prior over \( \beta_k : p(\beta_k | \eta 1_V) \propto \exp(\eta 1_V^\top [\log \beta_k]) \) for \( k = \{1, \ldots, K\} \). For simplicity, we assume hyperparameters \( \alpha \) and \( \eta \) are set manually.

In VI, we assume the posteriors are : (1) Discrete for \( q(z_{dn}) \propto \exp(z_{dn}^k \log \phi_{z_{dn}}^k) \), with variational parameters that capture the posterior probability of topic assignment, \( \phi_{z_{dn}}^k \propto \exp(\log \beta_k | q(z_{dn})) w_{dn} + \log \phi_{z_{dn}}^k) \)
(2) Dirichlet for \( q(\theta_d) \propto \)

2
We add Gaussian noise to each coordinate, then map to 0 if the perturbed coordinate becomes $\rho > \rho_d$ for any $s$

(Theorem 1 in [12]) Any Theorem 1.

The privacy gain from subsampling allows us to use a much more relaxed privacy budget

The privacy amplification theorem states the following.

Lemma 2.

Proposition 1. (Proposition 1.3 in [13]) If $\mathcal{M}$ provides $\rho$-zCDP, then $\mathcal{M}$ is $(\rho + 2\sqrt{\rho \log(1/\delta)}, \delta)$-DP for any $\rho > 0$.

So, using Lemma 2 and 3, we obtain $J \Delta^2/(2\tau)$-zCDP after $J$-composition of the Gaussian mechanism. Using Proposition 4, we convert $J \Delta^2/(2\tau)$-zCDP to $(\rho + 2\sqrt{\rho \log(1/\delta)}, \delta)$-DP, where $\rho = J \Delta^2/(2\tau)$.

These seemingly complicated steps can be summarised into two simple steps. First, given a total privacy budget $\epsilon_{tot}$ and total tolerance level $\delta_{tot}$, our algorithm calculates an intermediate privacy
We compare our method to two baseline methods. First, in \( \text{Lin} \) composition (Theorem 3.16 of [11]), privacy degrades linearly with the number of iterations. This result is from the Max Divergence of the privacy loss random variable being bounded by a total budget. Hence, the linear composition yields \((J \epsilon', J \delta')\)-DP. We use eq (6) to map \((\epsilon', \delta')\) to \((\epsilon_{\text{iter}}, \delta_{\text{iter}})\). Second, advanced (Adv) composition (Theorem 3.20 of [11]), resulting from the Max Divergence of the privacy loss random variable being bounded by a total budget including a slack variable \(\delta\), yields \((J \epsilon'(\epsilon' - 1) + \sqrt{2J} \log(1/\delta') \epsilon', \delta'' + J \delta')\)-DP. Similarly, we use eq (6) to map \((\epsilon', \delta')\) to \((\epsilon_{\text{iter}}, \delta_{\text{iter}})\).

As an evaluation metric, we compute the upper bound to the perplexity on held-out documents:

\[
\text{perplexity}(D^{\text{test}}, \lambda) \leq \exp \left[ - \left( \sum_i \log p(n_i^{\text{test}}, \theta_i, z_i|\lambda)q(\theta_i, z_i) - \log q(\theta, z) q(\theta, z) \right) / \sum_{i,n} n_i^{\text{test}} \right],
\]

where \(n_i^{\text{test}}\) is a vector of word counts for the \(i\)th document, \(n_i^{\text{test}} = \{n_i^{\text{test}}\}_i\). In the above, we use the \(\lambda\) that was calculated during training. We compute the posteriors over \(z\) and \(\theta\) by performing the first step in our algorithm using the test data and the perturbed sufficient statistics we obtain during training. The per-word-perplexity is shown in Fig. 1. Due to privacy amplification, it is more beneficial to decrease the amount of noise to add when the mini-batch size is small. The zCDP composition results in a better accuracy than the advanced composition.

\[\text{We used the metric written in the python implementation by authors of [14].}\]
Figure 1: Per-word-perplexity with different mini-batch sizes $S \in \{10, 20, 50, 100, 200, 400\}$. In the private LDA (Top/Right and Bottom), smaller mini-batch size achieves lower perplexity, due to the privacy amplification lemma (See Sec 3). We set the total privacy budget $\epsilon_{tot} = 1$ and the total tolerance $\delta_{tot} = 1e^{-4}$ in all private methods. Regardless of the mini-batch size, the zCDP composition (Top/Right) achieves a lower perplexity than the Advanced (Bottom/Left) and Linear compositions (Bottom/Right).

In Table 1 we show the top 10 words in terms of assigned probabilities under a chosen topic in each method. We show 4 topics as examples. Non-private LDA results in the most coherent words among all the methods. For the private LDA models with a total privacy budget fixed to 0.5, as we move from zCDP, to advanced, and to linear composition, the amount of noise added gets larger, and therefore more topics have less coherent words.
We have developed a practical privacy-preserving topic modeling algorithm which outputs accurate and privatized expected sufficient statistics and expected natural parameters. Our approach uses the zCDP composition analysis combined with the privacy amplification effect due to subsampling of data, which significantly decrease the amount of additive noise for the same expected privacy guarantee compared to the standard analysis.

5 Conclusion

Using the same data, we then tested how perplexity changes as we change the mini-batch sizes. As shown in Fig. 1, due to privacy amplification, it is more beneficial to decrease the amount of noise to add when the mini-batch size is small. The zCDP composition results in a better accuracy than the advanced composition.
References


