Differentially Private Bayesian Optimization

Matt J. Kusner\textsuperscript{1}, Jacob R. Gardner\textsuperscript{1,2}, Roman Garnett\textsuperscript{1}, Kilian Q. Weinberger\textsuperscript{1,2}

\textsuperscript{1}Department of Computer Science & Engineering, Washington University in St. Louis, USA
\textsuperscript{2}Department of Computer Science, Cornell University, USA

Privacy in Learning

learning can reveal information about the training set!

[Chaudhuri & Hsu, 2012; Jain et al., 2012; Kifer et al., 2012; Smith & Thakurta, 2013; Jain & Thakurta, 2014; Bassily et al., 2014]


Bayesian Optimization

- \(f(\lambda)\) is very expensive to compute
- \(f(\lambda)\) is nonconvex

idea: model \(f(\lambda)\) with an easy-to-evaluate surrogate

A formalization of “privacy through randomness”

Differentially Private Bayesian Optimization

Goal: mask change in \(A\) when run on \(V\) vs. \(V'\)

Definition 2. The global sensitivity of an algorithm \(A\) over all neighboring datasets \(V, V'\) (i.e., \(V, V'\) differ by the value of one record) is

\[
\Delta_A = \max_{A(V) \neq A(V')} |A(V) - A(V')|.
\]

Our Results

Assumption 1: \(f(\lambda)\) and \(f'(\lambda)\) are GP distributed

Theorem 1. Given Assumption 1 and the assumptions in Theorem 2 of de Freitas et al. (2012), for neighboring datasets \(V, V'\) we have the following global sensitivity bound,

\[
|f'(\lambda) - f(\lambda)| \leq \frac{Ae}{\gamma} + \epsilon
\]

Assumption 2: \(f(\lambda)\) and is L-Lipschitz (additionally training loss is also L-Lipschitz)

Theorem 3. Given Assumption 2, for neighboring \(V, V'\) and arbitrary \(\lambda < \lambda_{max}\) (and \(\lambda_{max}\) is the smallest hyperparameter) we have that,

\[
|f'(\lambda) - f(\lambda)| \leq \frac{L}{\gamma} + \max_{\lambda' \neq \lambda} |f(\lambda') - f(\lambda)| + \epsilon + q.
\]

References


A Private Mechanism

1. Draw \(\omega \sim \text{Laplace}(0, \Delta_A/\epsilon)\)
2. Release \(A'(V) + \omega\)

Privacy in Hyperparameter Tuning

selecting hyperparameters can reveal information about the validation set!

[Chaudhuri & Vinterbo, 2013]

Choosing Hyperparameters

e.g., validation set 1
2
hyperplane 1
3
hyperplane 2

validation set 2
hyperplane 1
1
hyperplane 2
2
validation set 1
1
hyperplane 1
3
hyperplane 2

Bayesian Optimization

validation set 1
hyperplane 1
1
hyperplane 2
2
validation set 2
hyperplane 1
1
hyperplane 2
2

Differentially Private Bayesian Optimization

A formalization of “privacy through randomness”

BO validation set 1
hyperplane 1
1
hyperplane 2
2
 validation set 2
hyperplane 1
1
hyperplane 2
2

Definition 1. A randomized algorithm \(A\) is \((c, \delta)\) differentially private if for all \(\lambda \in \text{Range}(A)\) and for all neighboring datasets \(V, V'\) (i.e., such that \(V\) and \(V'\) differ in the value of one record) we have that

\[
\Pr[A(V) = f(\lambda)] \leq e^\delta \Pr[A(V') = f(\lambda)] + \delta.
\]

properties

- \(k\) \((c, \delta)\)-differentially private runs is \((k, \delta)\)-diff. private
- post-processing doesn’t decrease privacy
- immune to common attacks (e.g., linkage, differencing attacks)

A Private Mechanism

Differentially Private Bayesian Optimization

Privacy in Learning

learning can reveal information about the training set! [Kasiswathanathan et al., 2008; Dwork & Lei, 2009; Chaudhuri et al., 2011; Chaudhuri & Hsu, 2012; Jain et al., 2012; Kifer et al., 2012; Smith & Thakurta, 2013; Jain & Thakurta, 2014; Bassily et al., 2014]