Machine Learning **Spring 2021**

Lecture 11: Thompson Sampling, Differential Privacy

Lecturer: Liwei Wang *Scribe: Xiyan Xu, Haoyu Wang, Zhewen Hao, Ningyuan Li, Tianran Zhu*

11.1 Thompson Sampling

Thompson sampling was first proposed by William R. Thompson in 1933. The principle behind Thompson sampling is Beta distribution. Beta distribution forms a family of continuous probability distributions on the interval $(0, 1)$. And for $Beta(\alpha, \beta)(\alpha > 0, \beta > 0)$, the probability density function is given by:

$$f(x, \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

For a Bernoulli bandit problem, we can use Beta distribution to update the Bernoulli loss, because if the prior is a $Beta(\alpha, \beta)$, we can sure that the posterior distribution is $Beta(\alpha + 1, \beta)$ or $Beta(\alpha, \beta + 1)$.
The Thompson Sampling algorithm assumes arm a to have prior $Beta(1, 1)$ on μ_a, and initialize $S_a = 0, F_a = 0$. At time t, the algorithm updates the distribution on $\mu_a$as $Beta(S_a + 1, F_a + 1)$. The algorithm then samples from $\mu_a{}'s$ posterior distributions. According to the probability of its mean being the largest, then plays an arm. And if $r_t(a_t) \notin \{0, 1\}$, the algorithm tosses a $r_t(a_t)$-coin to get a $\{0, 1\}$-result.

Algorithm 1 Thompson Sampling

Initialization $a = 1, 2 \cdots K, S_a = 0, F_a = 0$
for $t = 1, 2, ..., T$ **do**
    For each arm a, select $\Theta_a(t) \sim Beta(S_a + 1, F_a + 1)$
    Play arm $a_t = \arg\max_a \Theta_a(t)$ and get reward $r_t(a_t) \in [0, 1]$
    Toss a $r_t(a_t)$-coin, get $\widetilde{r}_t(a_t) \in \{0, 1\}$
    If $\widetilde{r}_t(a_t) = 1$, $S_a \leftarrow S_a + 1$; Else, $F_a \leftarrow F_a + 1$

Theorem 11.1 *For $\forall \epsilon > 0$, Thompson sampling has regret:*

$$R_T \leq (1 + \epsilon) \sum_{a \neq a^*} \frac{\log T\Delta_a}{d(\mu_a, \mu_{a^*})} + O(\frac{k}{\epsilon^2})$$

where $d(u, v) = u \ln \frac{u}{v} + (1 - u) \ln \frac{1-u}{1-v}$

Proof: We notice that we have the equation

$$R_T = E_{\mathcal{A}} \sum_{t=1}^{T} l_t(a_t) - \sum_{t=1}^{T} \mu_1 = \sum_{a=1}^{k} \Delta_a E_{\mathcal{A}}[n_T(a)]$$

Now we need to bound each arm's $E_{\mathcal{A}}[n_T(a)]$to prove our theorem. It's quite complex so you can refer to [1] to see the detailed calculation:

$$E_{\mathcal{A}}[n_T(a)] \leq (1+\epsilon_0)^2 \frac{\log T}{d(\mu_a, \mu_{a^*})} + O(\frac{1}{\epsilon_0^2})$$

And then we take $\epsilon = 3\epsilon_0$,

$$R_T \leq \sum_{a \neq a^*} (1+\epsilon_0)^2 \frac{\log T\Delta_a}{d(\mu_a, \mu_{a^*})} + O(\frac{1}{\epsilon_0^2}) \leq (1+\epsilon) \sum_{a \neq a^*} \frac{\log T\Delta_a}{d(\mu_a, \mu_{a^*})} + O(\frac{k}{\epsilon^2})$$

■

11.2 Differential Privacy

Data leakage refers to a mistake made by the creator of a machine learning model in which they accidentally share information with the user. For example, in the traditional SVM model, the output classifier $f(x) = \sum_i \alpha_i y_i k(x : x_i)$, gives the information of all of the margin. Before solving this problem, we have to define it first. It's hard to define what's privacy, which is quite abstract and philosophical. Instead, we can define what is a privacy leak.

The primary object of a privacy-preserving algorithm is to release some statistical information about the dataset but do not leak much information about specific data. We now model the privacy leakage in query answering.

Definition 11.2 (Neighboring Datasets) *Consider dataset $D = \{x_1, x_2, \cdots, x_n\}$, $x_i \in X, D \in X^n$. We say that two datasets $D, D' \in X$ are neighboring if they differ in only a single data element.*

Definition 11.3 (Counting Query) *A counting query Q_h, defined in terms of a predicate $h : X \to \{0, 1\}$ is defined to be*

$$Q_h(D) := \frac{1}{|D|} \sum_i h(x_i), h(x_i) \in \{0, 1\}$$

It evaluates the fraction of elements in the dataset that satisfy the prediction h.

Definition 11.4 (Differential Privacy) *Let A be a randomized algorithm, $A : X^n \to R$, with input D, we say A satisfies ϵ-differential privacy if for all neighboring datasets $D, D^{'} \in X^n$, and all set $S \subseteq Output(A)$, we have*

$$\Pr[A(D) \in S] \leq e^{\varepsilon} \Pr[A(D') \in S]$$

This definition captures the core nature of privacy. It describes the stability of the answer under the data disturbance. If the change of a certain data will cause the result to fluctuate greatly, then this algorithm does not protect the data privacy well. In particular, if ϵ is equal to 0, the answer for adjacent data will be the same.

Definition 11.5 ((α, β)-accuracy) *Say randomized algorithm A has $(\alpha, \beta) -$ accuracy with respect to counting query Q if:*

$$\forall D \in X^n, \quad \mathbb{P}(|A(D) - Q(D)| \geq \alpha) \leq \beta$$

Definition 11.6 (The Laplace Distribution) *The Laplace Distribution(centered at 0) with scale σ is the distribution with probability density function:*

$$f(x|\sigma) = \frac{1}{2\sigma} exp(\frac{-|x|}{\sigma})$$

The Laplace distribution is a symmetric version of the exponential distribution, and we will write $Lap(\sigma)$ to denote the Laplace distribution with scale σ.

Lemma 11.7 *let $f(x|\sigma)$ denote the probability density function of the Laplace Distribution, then*

$$\forall x_1, x_2 \in \mathbb{R}, \frac{f(x_1|\sigma)}{f(x_2|\sigma)} \leq exp(\frac{|x_1 - x_2|}{\sigma})$$

.

Proof:

$$\frac{f(x_1|\sigma)}{f(x_2|\sigma)} = exp(\frac{-|x_1| + |x_2|}{\sigma}) \leq exp(\frac{|x_1 - x_2|}{\sigma})$$

. ■

We will now define the **Laplace Mechanism**. As its name suggests, the Laplace mechanism will simply compute f, and perturb each coordinate with noise drawn from the Laplace distribution.

Definition 11.8 (The Laplace Mechanism) *Given any function $f : X^n \to \mathbb{R}^k$, the Laplace Mechanism responds to f by returning $f(x) + Z$, where $Z = (Y_1, \cdots, Y_k)$ is a k-dimension random variable and $\forall i \in [k], i.i.d. Y_i \sim Lap(\sigma)$.*

In the case where f is just a single query($k = 1$), the Laplace Mechanism return $f(D) + Z, Z \sim Lap(\sigma)$.

Theorem 11.9 *The Laplace Mechanism preserves ϵ-differential privacy and has $(\alpha, \beta) - accuracy$ with respect to the single counting query $Q : X^n \to [0, 1]$, where $\epsilon = \frac{1}{n\sigma}, \alpha = \sigma ln \frac{1}{\beta}, \beta := neg(n)$ i.e.$\forall k \in \mathbb{N}, \beta < n^k$.*

Proof: Let A denotes the Laplace Mechanism(consistent with the notation of the randomized algorithm we defined earlier). According to Lemma 11.7, for every $a \in Output(A)$, the ratio

$$\frac{\mathbb{P}(A(D) = a)}{\mathbb{P}(A(D') = a)} = \frac{f(a - Q(D))}{f(a - Q(D'))} \leq exp(\frac{|Q(D) - Q(D')|}{\sigma}) \leq exp(\frac{1}{n\sigma})$$

As for α, consider the equation

$$\mathbb{P}(|A(D) - Q(D)| \geq \alpha) = 2 \cdot \frac{1}{2\sigma} \int_{\alpha}^{\infty} e^{-\frac{t}{\sigma}} dt = \beta$$

We get $\alpha = \sigma ln \frac{1}{\beta}$. ■

Definition 11.10 (Accuracy(multiple queries)) *Let $Q = (Q_1, \cdots, Q_k) : X^n \to \mathbb{R}^k$ be a counting query sequence. Let A be the algorithm with k output:$A(D) = (A_1(D), \cdots, A_k(D))$.*
We say A has $(\alpha, \beta) - accuracy$ with respect to queries in Q, if for every $D \in X^n$:

$$\mathbb{P}(||A(D) - Q(D)||_\infty \geq \alpha) \leq \beta$$

i.e. with probability at least $1 - \beta$, $\max_{i \in [k]} |Q_i(D) - A_i(D)| \leq \alpha$.

Lemma 11.11 *The Laplace Mechanism satisfies $k\epsilon$-differential privacy and $(\alpha, k\beta)$-accuracy with respect to a sequence of k queries $Q = (Q_1, \cdots, Q_k)$, if for every Q_i $(i = 1, \ldots, k)$, the Laplace Mechanism satisfies ϵ-differential privacy and (α, β)-accuracy respectively.*

Proof: Let $A_i(D)$ denote the i-th output of the Laplace Mechanism. By definition, $[A_i(D) - Q_i(D)] \sim Lap(\sigma)$ independently, and the joint probability density function of $A(D) = (A_1(D), \cdots, A_k(D))$ is

$$f_{A(D)}(\vec{x} = (x_1, \ldots, x_k)) = \prod_{i=1}^{k} f_{A_i(D)}(x_i) = \prod_{i=1}^{k} f_\sigma(x_i - Q_i(D)) \ .$$

From ϵ-differential privacy of A_i, we have $f_{A_i(D)}(x_i) \leq e^\epsilon f_{A_i(D')}(x_i)$, and thus

$$f_{A(D)}(\vec{x}) \leq e^{k\epsilon} f_{A(D')}(\vec{x}) \ .$$

Therefore $\forall S \subseteq R^k$, we have

$$\frac{\mathbb{P}(A(D) \in S)}{\mathbb{P}(A(D') \in S)} = \frac{\int_{\vec{x} \in S} f_{A(D)}(\vec{x})\, d\vec{x}}{\int_{\vec{x} \in S} f_{A(D')}(\vec{x})\, d\vec{x}} \leq e^{k\epsilon} \ ,$$

so the Laplace Mechanism satisfies $k\epsilon$-differential privacy for $Q = (Q_1, \cdots, Q_k)$.
By union bound,

$$\mathbb{P}(||A(D) - Q(D)||_\infty \geq \alpha) \leq \sum_{i=1}^{k} \mathbb{P}(|A_i(D) - Q_i(D)| \geq \alpha) \leq k\beta,$$

the $(\alpha, k\beta)$-accuracy is satisfied. ■

As a corollary, we have

Theorem 11.12 *The Laplace Mechanism satisfies $\frac{k}{n\sigma}$-differential privacy and (α, β)-accuracy with respect to a sequence of k counting queries $Q = (Q_1, \cdots, Q_k)$, where $\alpha = \sigma \ln \frac{k}{\beta}$.*

Given a fixed β, when n is sufficiently large, we expect that $\alpha = O(\frac{1}{\sqrt{n}})$, which is close to the sampling error, or that $\alpha = o(1)$, so that the output gets better accuracy as n grows. To preserve privacy, people usually demand that $\epsilon = O(1)$. These requirements put a limit on k, the available number of queries.

Theorem 11.13 *If a Laplace Mechanism satisfies ϵ-differential privacy and (α, β)-accuracy with respect to a sequence of k counting queries $Q = (Q_1, \cdots, Q_k)$, where $\epsilon = O(1)$, $\alpha = o(1)$, and given $\beta \in (0, 1)$, then it's required that $k = o(\frac{n}{\ln n})$.*

Proof: From $\epsilon = \frac{k}{n\sigma} = O(1)$ we have $k = O(n\sigma)$. From $\alpha = \sigma \ln \frac{k}{\beta} = o(1)$ we have $\sigma = o(\frac{1}{\ln \frac{k}{\beta}}) = o(\frac{1}{\ln k})$. Thus we have $k \ln k = o(n)$, therefore $k = o(\frac{n}{\ln n})$. ■

References

[1] Shipra Agrawal and Navin Goyal(2017). Near-Optimal Regret Bounds for Thompson Sampling.

[2] Cynthia Dwork and Aaron Roth. The Algorithmic Foundations of Differential Privacy.