HW 6

Marin Mato

1/21/2024

What is the difference between gradient descent and *stochastic* gradient descent as discussed in class? (*You need not give full details of each algorithm. Instead you can describe what each does and provide the update step for each. Make sure that in providing the update step for each algorithm you emphasize what is different and why.*)

The difference between gradient descent and stochastic gradient descent relates to the amount of data used in the process of computing the gradient. GD or gradient descent uses the entire data set when computing the gradient. However, SDG or stochastic descent gradient uses a random subset of the data. That way, SDG ends up being more efficient at finding a global optimal solution.

Consider the `FedAve` algorithm. In its most compact form we said the update step is $\omega_{t+1} = \omega_t - \eta \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(\omega_t)$. However, we also emphasized a more intuitive, yet equivalent, formulation given by $\omega_{t+1}^k = \omega_t - \eta \nabla F_k(\omega_t); w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$.

Prove that these two formulations are equivalent.
(*Hint: show that if you place ω_{t+1}^k from the first equation (of the second formulation) into the second equation (of the second formulation), this second formulation will reduce to exactly the first formulation.*)

$\omega_{t+1} = \omega_t - \eta \sum_{k=1}^{K}$

$\omega_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_{t+1}^k$
$\sum_{k=1}^{K} \frac{n_k}{n} (\omega_t - \eta \nabla F_k(\omega_t))$
$\omega_t \sum_{k=1}^{K} \frac{n_k}{n} - \eta \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(\omega_t)$
$\omega_t - \eta \sum_{k=1}^{K} \frac{n_k}{n} \nabla F_k(\omega_t)$

Now give a brief explanation as to why the second formulation is more intuitive. That is, you should be able to explain broadly what this update is doing.

This update depicts how federated learning enables collaborative model training while preserving data privacy.(trained local models on siloed data then aggregated them to improve the global model)

Prove that randomized-response differential privacy is ϵ-differentially private.

Student Input

Define the harm principle. Then, discuss whether the harm principle is *currently* applicable to machine learning models. (*Hint: recall our discussions in the moral philosophy primer as to what grounds agency. You should in effect be arguing whether ML models have achieved agency enough to limit the autonomy of the users of said algorithms.*)

The harm principle revolves around the idea that individuals are free to act until they are causing harm to others. Therefore, it cannot be applied to ML directly as models do not posses the consciousness of a human. However, the harm principle can be applied indirectly as developers of these models should know whether the outcome harms a certain group of people. In other words, the harm principle is not directly applicable to ML models currently, but as researchers explore the concept of models possessing consciousness, this might be subject to change.