HW 6

Ethan Turner

04/08/2024

# 

**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 method of gradient descent locates the direction of steepest descent in some optimization process.

Update rule:

Goal: Minimize

Update rule for regular gradient descent: ) =

Where alpha is the learning rate or step size, though we want to avoid an overly large alpha to accurately give the minimum.

X and Y represent all of the data present in training the algorithm.

Stochastically, gradient descent remains similar with the replacement of a randomly selected tuple from the data concerned, rather than all data at once. For each iteration, then, it is less costly than regular gradient descent.

Its update step:

) =

**Consider the FedAve algorithm.** In its most compact form we said the update step is . However, we also emphasized a more intuitive, yet equivalent, formulation given by .

Prove that these two formulations are equivalent.  
(*Hint: show that if you place 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.*)

*Student Input*

First, as suggested, I substitute the term from the first equation of the second formulation into the second equation from the second formulation.

Next, I will split the sum into two parts.

= \*

\*I am having trouble working the equations, but these sums are all from k=1 to K.

Next, I take out a constant in the first and second sums.

=

Next, we note that the sum of all nk from k=1 to k=K is n. Thus, n/n = 1 and we may simplify.

=

# 

**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.

*Student Input*

The second formulation is more intuitive because it aggregates local estimators in blocks. In federated learning, we might have multiple "blocks" per siloed section, and hence the update of the entire model hinges upon the updating of smaller "blocks" first.

**Explain how the harm principle places a constraint on personal autonomy.** 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.* )

*Student Input*

The harm principle limits personal autonomy by placing restrictions on liberty for the greater good (such as a parent forbidding a child from eating candy), although with caveats. The basic moral conceit that no individual--that one ought not harm another person without good reason--is quite simple. Specifically, "harm" implies the deprivation of rights to which victims are entitled. The harm principle, this noted, does not apply to violation of mere preferences.

Additionally, cases of fully informed, uncoerced consent in which individuals consciously sacrifice their own interests for the interests of others for potential net harm do not violate the harm principle. If I, in my wisdom, forego studying for a STOR 390 quiz in favor of extensively brainstorming topics of conversation to avoid an awkward silence with a seat neighbor in another class, my failure of the quiz clearly dwarfs the mild convenience of my friend experiencing my conversational best. However, clearly I am more at fault for a misalignment of priorities than a violation of the harm principle. Broadly speaking, the harm principle limits personal autonomy insofar as each action must not cause disproportionate harm to an unsuspecting individual or individuals.

Machine learning models display numerous moral conundrums relating directly to the harm principle. However, when examining agency as dichotomous with obligation, it is those who apply and facilitate the models rather than the models themselves who violate the harm principle. As argued by Andy in STOR 390 lecture, human obligations are grounded in sentience. Machine learning models themselves have not yet developed sentience, but the humans who develop them do. Thus, the application of an algorithm or a machine learning model must coexist with a human exercising their unique agency in dealing with a model's real-world ramifications.