Uncertainty in Machine Learning \ Assignment 1

vimmoos

May 24, 2022

Contents

1 Sources of Uncertainty

1.1 Aleatoric

- The first example of Aleatoric uncertainty can be when we are dealing with robots and the input to the neural network is a sensor. If the sensor is not perfect or is not correctly calibrated or even worse has some technical problems, the data that we will gather will be noisy/imperfect. This will be a case of aleatoric uncertainty since the uncertainty is an intrinsic property of the data we get.

- Another example of Aleatoric uncertainty can be when we train a neural network (for classification) with blurred images. This is a clear instance of Aleatoric uncertainty since the uncertainty comes from the data itself and not from the model. Moreover, having more training examples does not alleviate this type of uncertainty.

1.2 Epistemic

- A famous example of epistemic uncertainty, happened when some service for facial recognition failed to recognize afro-american women. This happened because of the lack of data. In particular, the problem was that the data they used to train the network was biased on white men and there were few or no data points for afro-american in general. This is an example of epistemic uncertainty since given more data the neural network would have been able to solve this problem and correctly categorise every face.

- Another example of epistemic uncertainty, can be when we train a network on some data set, let's say MNIST (digits), and then we try to categorise letters. This is a clear and simple example of model misspecification.

2 Are They Probabilities?

2.1 DUQ

In the case of DUQ, the confidence outputs can be considered probabilities but not in the intuitive sense. More specifically, DUQ uses a radial basis function (RBF) for measuring uncertainty. The RBF measures the distance between the model output and the centroids. Generally, RBFs are bounded between 0 and 1. Which is in line with a probabilistic interpretation. Another important point, in interpreting the confidence outputs of the DUQ under a probabilistic framework is that the confidence outputs are not probabilities but likelihoods.

Take a look at the formula of the RBF:

$$K_c(f_\theta(x), e_c) = exp\left(-\frac{\frac{1}{n}\|W_c f_\theta(x) - e_c\|_2^2}{2\sigma^2}\right) \tag{1}$$

we can notice that it is structurally similar to the probability density function of an isotropic (rotationally invariant) D-dimensional gaussian distribution:

$$\mathcal{N}(x|\mu, \sigma^2 I) = (2\pi\sigma^2)^{-\frac{D}{2}} exp\left(-\frac{\|x-\mu\|^2}{2\sigma^2}\right) \tag{2}$$

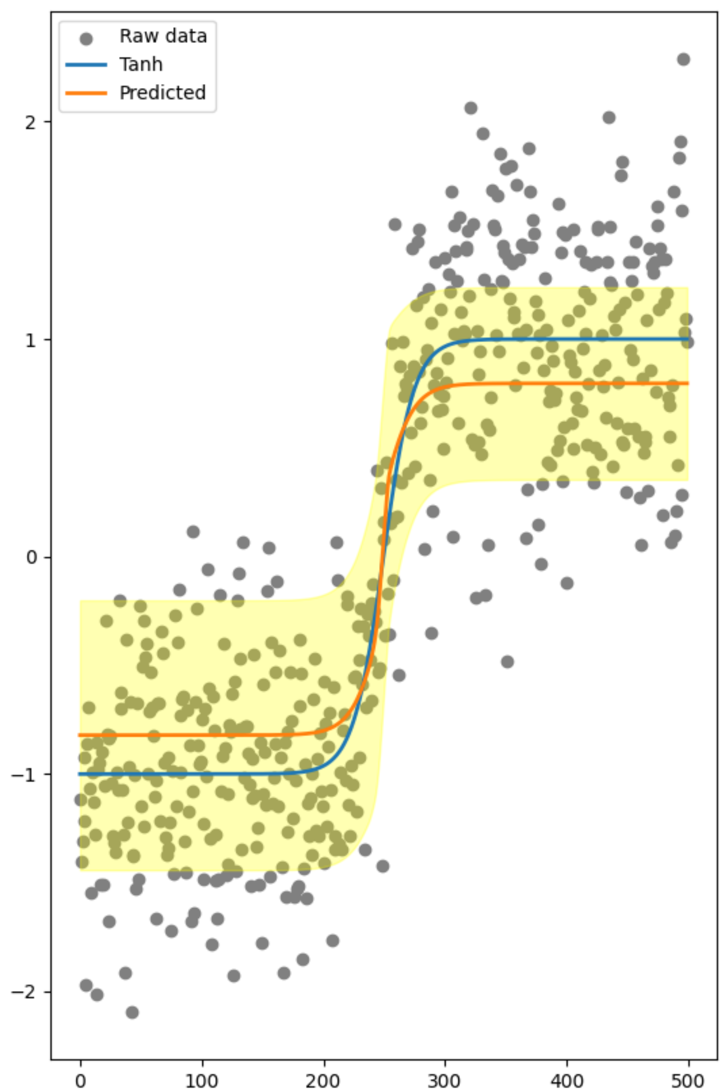
In light of this, we can say that the output of DUQ is proportional to the probability density under an isotropic Gaussian. Therefore, it is clear that the confidence outputs can be considered as probabilities (to be strict we should say likelihoods and not probabilities)

2.2 Gradient Uncertainty

In the case of the Gradient Uncertainty, the confidence outputs cannot be considered as probabilities. In the paper, they stated: "We interpret this 're-learning-stress' as uncertainty". This 're-learning-stress' is based on the gradient and therefore is highly coupled to the model and its parameters. It is therefore impossible to interpret this type of uncertainty as some kind of probability or likelihood.

3 Programming

We have created a dataset based on the tanh function. We have added a Gaussian noise with parameters $\mu = 0$ and $\sigma = 0.5$. The results show that our neural network learned the function quite well as we can see from the predicted mean. On the other hand, for the predicated variance, we can see that the neural network correctly estimates the aleatoric uncertainty. The mean of the predicted σ is 0.55891913 which is a slightly overestimate but it is quite good. Below is the graph of the data points, predictions and actual function.


Raw data
Tanh
Predicted
2
1
0
−1
−2
0
100
200
300
400
500