

# 为什么需要不确定度 (uncertainty) ?

深度学习模型已经在各类视觉任务上取得了非常好的效果。但是有一个普遍的问题是：不管遇到什么情况，模型总能给出一个结果。即使你让一个猫狗分类模型对一张“只包含一个人的图片”进行预测，模型也(不得不)输出结果(猫或狗)，有的时候甚至给出非常高的score。

简单来说，模型会预测结果，但是不会告诉我们它对结果到底有多确定。（一般来说，score作为不确定度是不合适的，因为经常对错误预测，模型也经常输出比较高的score）。

相反，如果模型不仅能给出预测结果，还能告诉我们它对该结果有多确定，那我们就可以决定是否相信模型预测的结果，从而避免一些不合常理的错误。

## 如何让网络输出不确定度？

那么如何能够让模型输出不确定度呢？贝叶斯网络(BNN)是常用的方法。下面以regression任务为例解释。

如果是纯regression问题，loss可以定义为：

$$\mathcal{L}_{NN}(\theta) = \frac{1}{N} \sum_i \|y_i - f(x_i)\|^2 \quad (4)$$

实际使用时，loss会加weight decay项，比如L2 regularization。这里为了简化没有写weight decay项，下面也一样

在BNN中，我们假设模型参数不是确定的，而是服从Gaussian的分布，那么输出也服从Gaussian，我们有：

$$\mathcal{L}_{BNN}(\theta) = \frac{1}{N} \sum_i \frac{1}{2\sigma(x_i)^2} \|y_i - f(x_i)\|^2 + \frac{1}{2} \log \sigma(x_i)^2 \quad (2)$$

其中， $y_i$ 为真值，与传统NN不同，我们让网络同时预测 $\sigma(x_i)$ 、 $f(x_i)$ ， $\sigma^2$ 为variance, 可用于表示uncertainty。

直观上看，相比于传统的MSE loss，这个loss：

- 首先，对所有的input， $\sigma^2$ 不会很大。原理和L2 regularization会抑制模型参数变大一样，这个loss会抑制variance变得很大。即，模型输出的variance都会比较小。这保证了用网络 estimate variance是可能的，且相对容易。
- 但是，这个loss会惩罚高MSE，但是variance  $\sigma^2$ 小（低uncertainty）的情况。因为此时loss会很大，网络通过学习会抑制这种情况的发生。什么情况下MSE会比较高呢？
  - 想象一下这种情况：如果我先用比较好的数据训练，得到了一个不错的模型，随着训练

集增大，训练集中的noise data增多（除非数据太脏了，否则这应该是普遍情况）。

- 什么是noise? 对当前模型，noise样本的MSE会比较高，但是真值却是positive的，或者反过来。
- 如果用传统的MSE loss，模型只能通过学习拟合noise data以降低loss，这是我们不希望看到的。而用BNN loss，网络可以通过对noise data预测一个比较大的uncertainty来降低loss，而保持预测结果的正确性，这是我们愿意看到的。

在训练模型的时候，我们让模型直接estimate  $s_i = \log \sigma(x_i)^2$ ，则上式等价于：

$$\mathcal{L}_{BNN}(\theta) = \frac{1}{N} \sum_i \frac{\|y_i - f(x_i)\|^2}{\exp(-s_i)} + \frac{1}{2} s_i \quad (3)$$

这么做可以避免除以0的情况，因为exp是positive的，可以避免除以0的情况。而且，log可以降低回归变量variance的scale，比较利于学习。

另外，有比较解释一下，为什么学习 $\sigma^2$ 是可能的。是因为有的时候，模型不确定度和input data的确是相关的。举例来说，在depth regression任务中，模型预测特征明显的物体边缘的depth，就会比预测一面白墙的depth更加容易、更加确定。在检测任务中，物体边缘清晰时，回归bbox也会比物体边缘不清晰（e.g.逆光、下雨等造成物体边缘成像模糊）容易、且确定度更高。

以上的例子假设数据是足够的。那么如果数据不是足够的，也会产生不确定度。这种由于数据不够产生（即意味着可以通过增加标注数据解决）的不确定度被称为模型不确定度(也成epistemic uncertainty)。关于它如何建模计算，可以查阅参考文献。

## 参考文献

[What Uncertainties Do We Need in Bayesian Deep Learning for Computer Vision?](#)

[Uncertainty in Deep Learning. How To Measure?](#)

[Uncertainty Estimation in CV](#)