李宏毅深度学习 p6

Why we need machine learning

老师认为之后应该会出现一种新的职业叫做AI训练师。

主要工作为1、选择合适的loss function 和 model
2、某些模型的最优化较为困难，需要有经验的人员

李宏毅深度学习 p7

The next step for machine learning

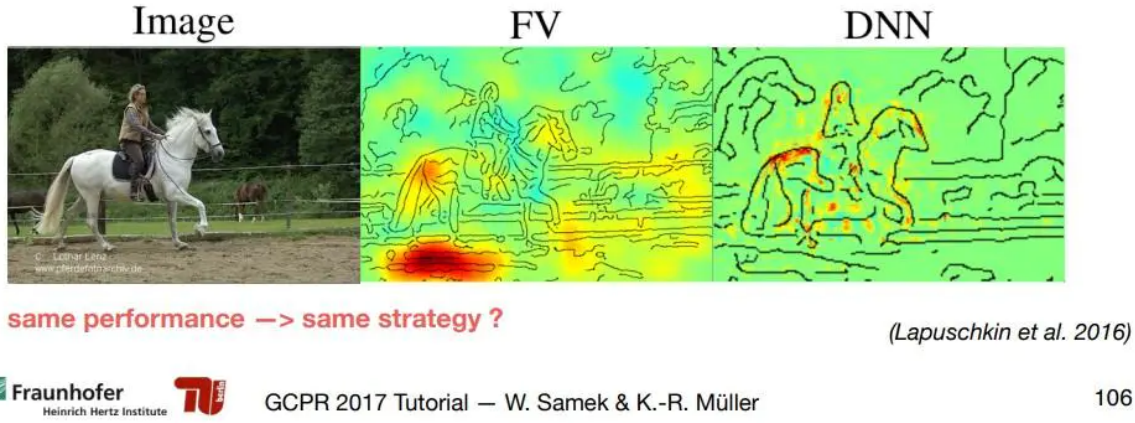
1. Anomaly Detection机器能不能知道“我不知道”

例如当你做了一个猫狗识别的AI上线后，用户不一定会真的给一张猫狗图片，如果用户给了一张人物照片之类的非猫狗照片，它能知道自己不知道还是会将照片硬是归为一种猫狗

2. Explainable AI 说出为什么“我知道”

神马汉斯的故事：18世纪的德国，一匹叫汉斯的马火了，因为它能算出简单的算术题，并用蹄子敲出正确答案，但后来发现它实际上是通过观察周围人的反应来给出答案。

机器学习的成果，是否同汉斯一样，通过一些意想不到的渠道，获得的答案。在 GCPR 2017 Tutorial 的研究中，研究者通过注意力机制，研究机器判断的依据。



实验者测试了两个模型，两个模型均为马匹识别。DNN 模型的焦点集中在马匹身上，是一个正常的模型。但 FV 的交点却集中在图片左下角。原来，图片的左下角有图片的出处，所有的包含马匹的图都有这个标记。所以，FV 模型学到的重点在于这些标记。同样的表现，却是不一样的判断依据。显然，FV 模型的判断依据是滑稽和不可靠的。

我们需要一些技术，让 AI 不仅给出结果，同时要给出判断的依据。即：模型的可解释性。

3. 抵御Adversarial Attack

对于机器，有研究表明通过改变个别像素点就可以达到迷惑机械的作用，这种技术叫做Adversarial Attack。这是非常危险的。

4. Life-long learning终身学习

现在我们通常来讲一个模型学习一个任务。，但这样就会有很多问题。首先，随着建模的增多，我们的模型数量会不断增长。其次，模型之前学到的技能对他之后的学习是没有帮助的。还有一种现象叫catastrophic forgetting,同一个网络，学习完一个任务之后的权重在学习新的任务的时候可能完全改变，由于不同任务最优化的目标往往不同，即使目标函数相同数据集也不同，旧的权重被损坏是完全有可能的，但理论上这也是可以解决的。

5. Meta-learning / Learn to learn 学习如何学习

6. Reinforcement learning 增强学习

增强学习现在非常流行，但它真的有那么强吗?就以Alphastar为例它确实很强，但它的训练花了大量的时间。

增强学习为什么这么慢？它能不能再快一点。

7. Network Compression 神经网络压缩

机器学习目前多运行在大型服务器上，配备极强的 GPU、相当大的内存和数目众多的 CPU。但若想要把机器学习广泛应用于生活中，IoT 物联网这类设备的计算和存储都是十分有限的。我们能不能把模型缩小，同时保留其能力呢。我们能不能把大型神经网络进行剪枝，或者是参数二元化，以此来减轻内存和计算压力呢。我们现在有 tensorflow lite，有 coreML，但这些还不够。

8. Few-shot/Zero-shot learning 一定需要很多训练数据吗

现实场景中样本之少，一直是一个很严重的问题。现在我们希望通过少量的样本，扩展到大量的未标记数据，这样的研究我们称为Few-shot learning。甚至，模型能不能通过我对川菜的描述：麻辣、重油，就识别出桌面上的是否是川菜呢？这样的模型我们称之为 Zero-shot learning,不需要样本进行学习。

9. 机器学习的谎言 训练数据和测试数据很不一样

当我们在学习机器学习各类算法时，教科书都会有这样一个假设：训练数据和测试数据拥有相同的分布。但在真实世界中，这就是个谎言。这会对我们的正确率有影响。