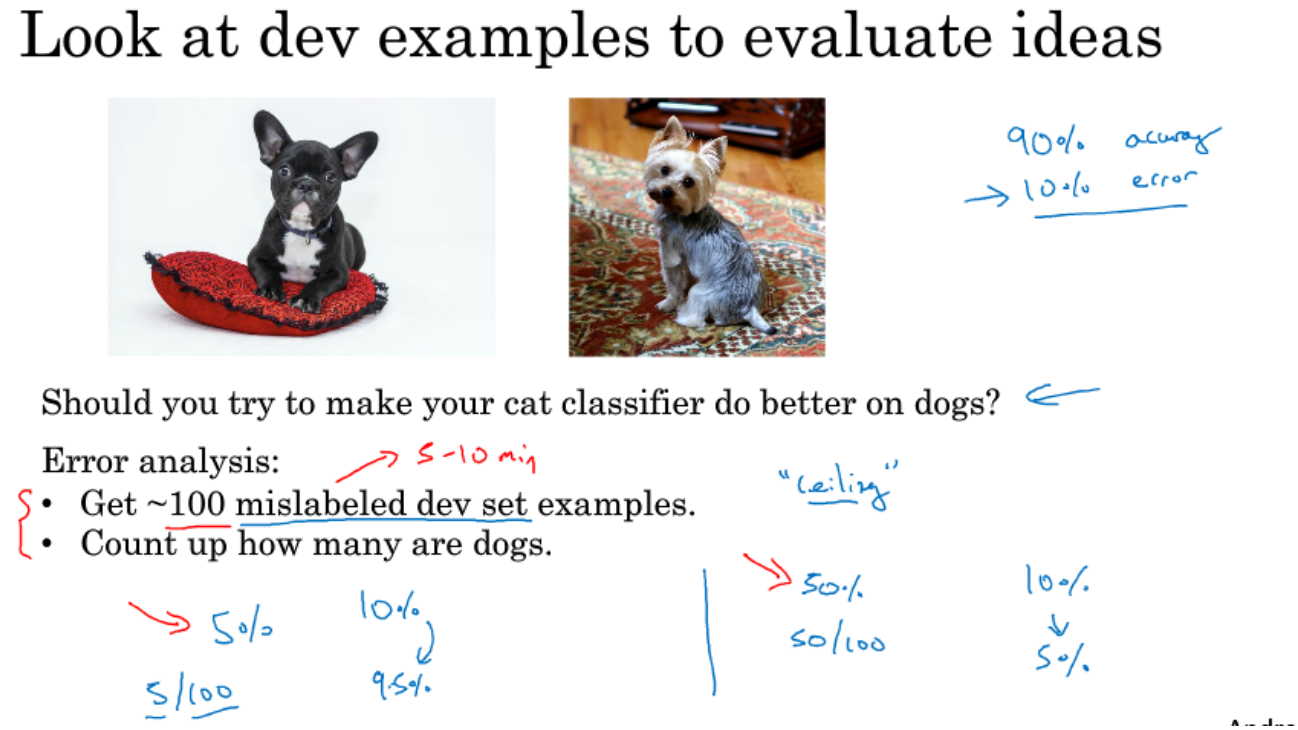
结构化机器学习项目 第二周 机器学习策略

2-1 进行误差分析

深度学习算法对训练集中的随机误差具有相当的鲁棒性。



收集错误样例：

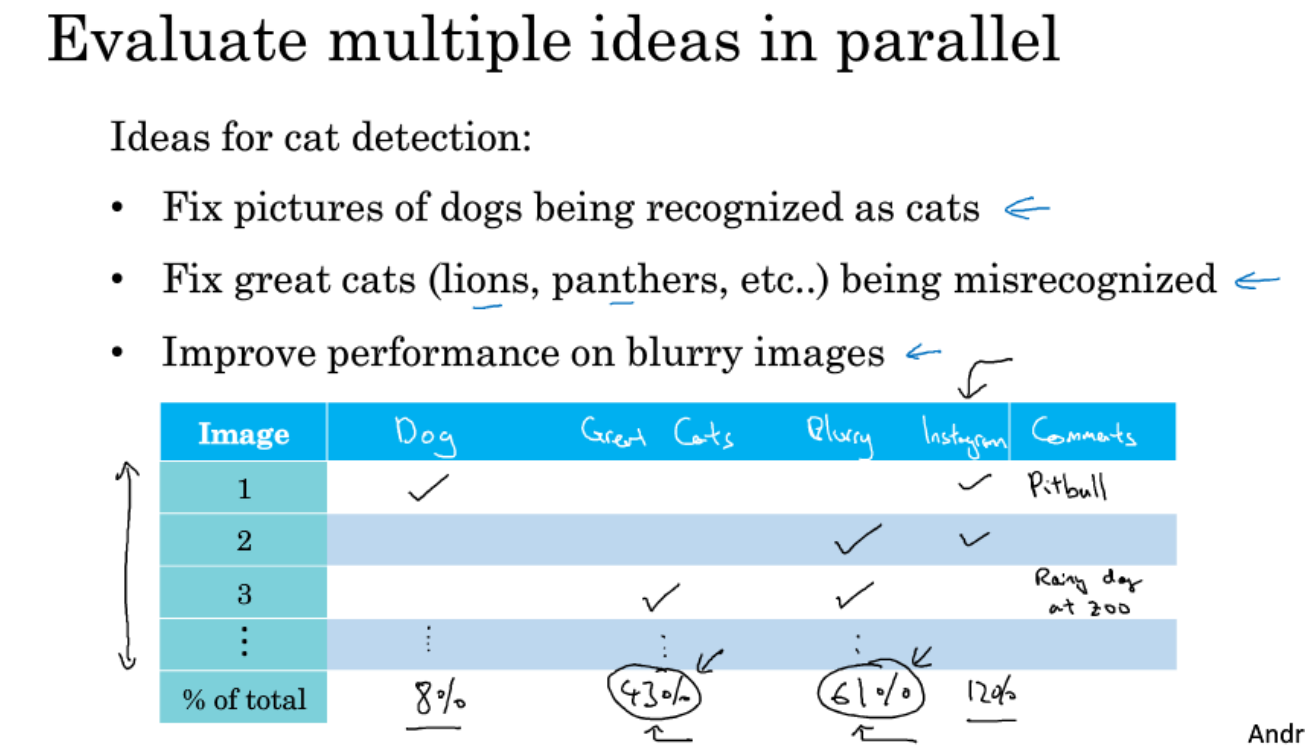
在开发集（测试集）中，获取大约100个错误标记的例子，并统计其中有多少个是狗。

- 假设一种情况是100个数据中，有5个样例是狗，那么如果我们对数据集的错误标记做努力去改进模型的精度，那么可以提升的上限就是5%5%，即仅仅可以达到9.5%9.5%的错误率，这有时称为**性能上限**。
  那么这种情况下，可能这样耗时的努力方向就不是很值得的一件事情。
- 另外一种假设是100个数据中，有50多个样例是狗，那么这种情况下，我们去改进数据集的错误标记，就是一个比较值得的改进方向，可以将模型的精确度提升至95%95%。

并行分析：

- 修改那些被分类成猫的狗狗图片标签；
- 修改那些被错误分类的大型猫科动物，如：狮子，豹子等；
- 提升模糊图片的质量。

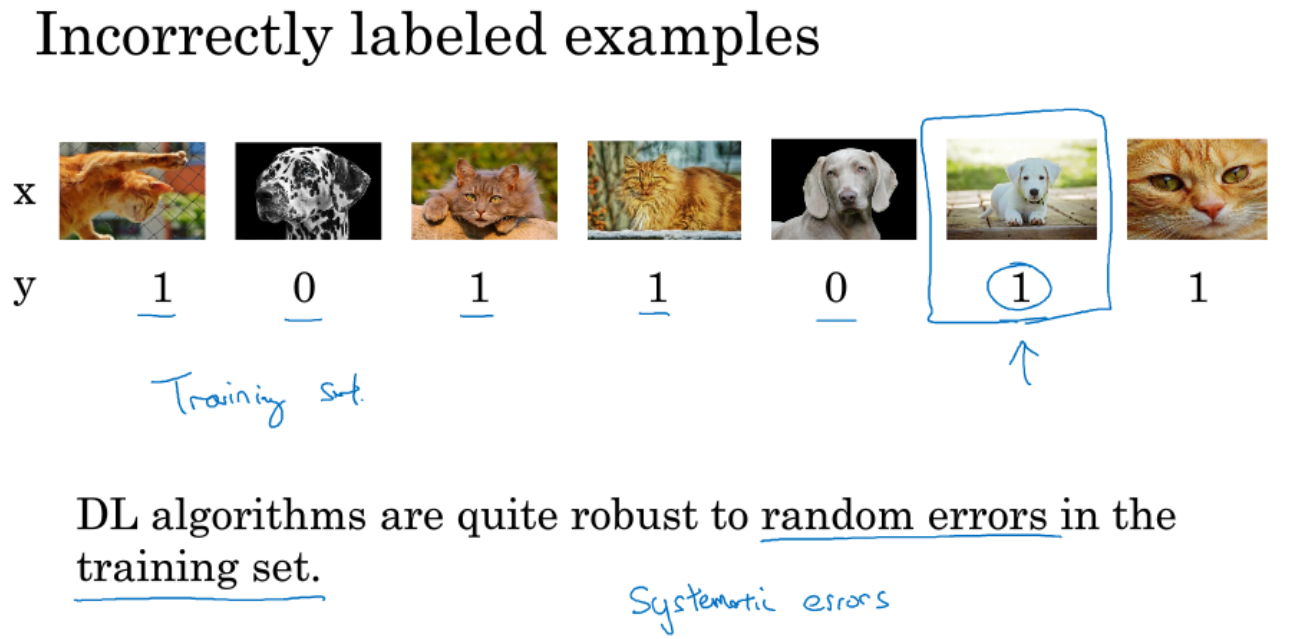
为了并行的分析，建立表格来进行。以单个错误分类样本为对象，分析每个样本错误分类的原因。



最后，统计错误类型的百分比，这个分析步骤可以给我们一个粗略的估计，让我们大致确定是否值得去处理每个不同的错误类型。

2.2 清楚标记错误的数据

以猫和狗分类问题为例子。

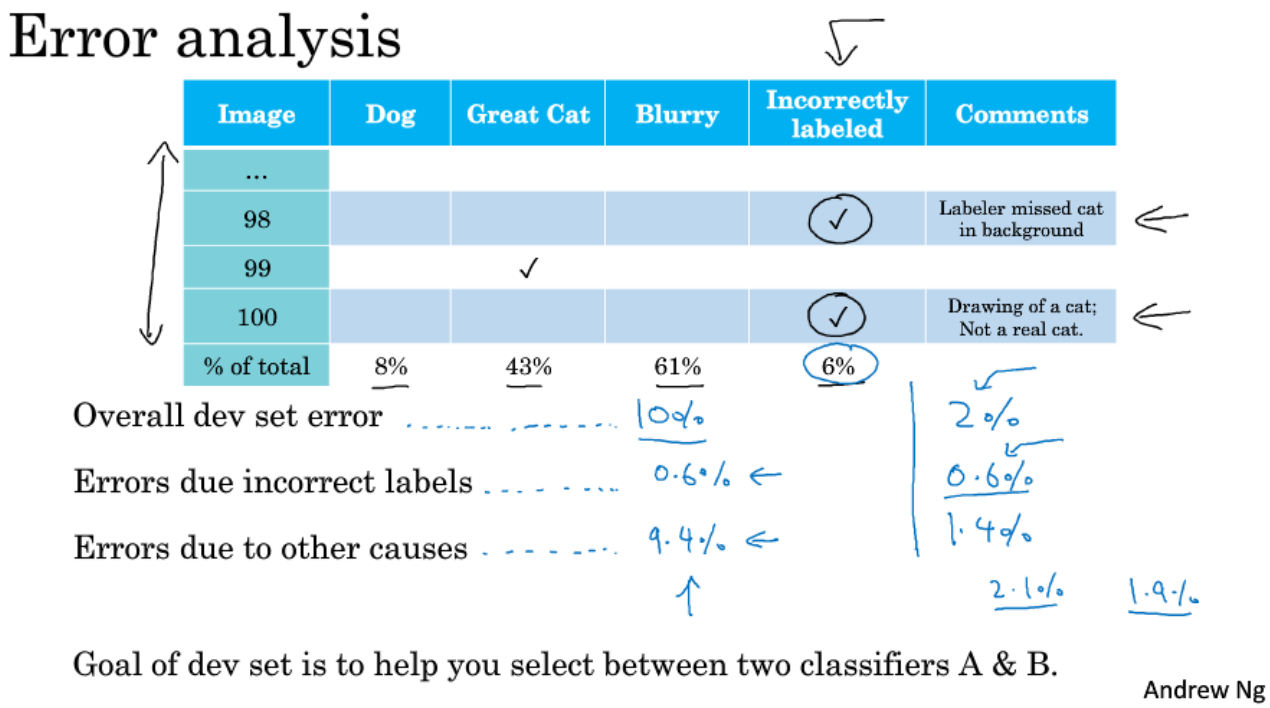


情况一：

深度学习算法对训练集中的随机误差具有相当的鲁棒性。

只要我们标记出错的例子符合随机误差，如：做标记的人不小心错误，或按错分类键。那么像这种随机误差导致的标记错误，一般来说不管这些误差可能也没有问题。

所以对于这类误差，我们可以不去用大量的时间和精力去做修正，只要数据集足够大，实际误差不会因为这些随机误差有很大的变化。

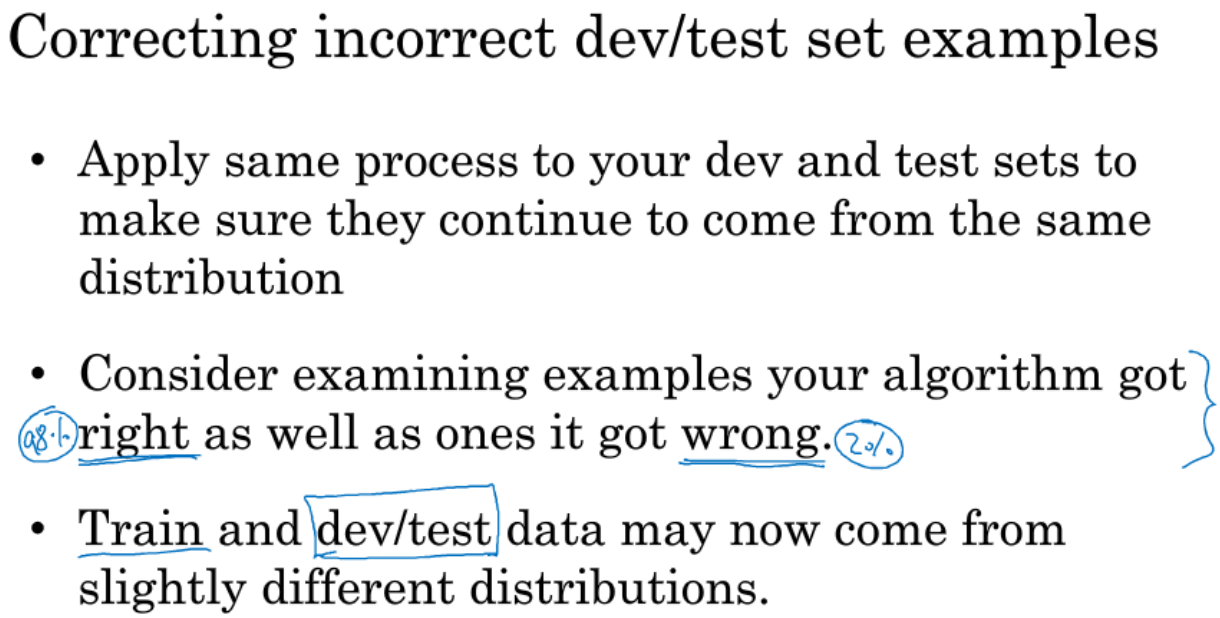


方法二：

训练集均是来自网上下载的20万张高清图片，当然也可以加上5000张手机非高清图片；对于开发和测试集都是手机非高清图片。

- 好处：开发集全部来自手机图片，瞄准目标；
- 坏处：训练集和开发、测试集来自不同的分布。

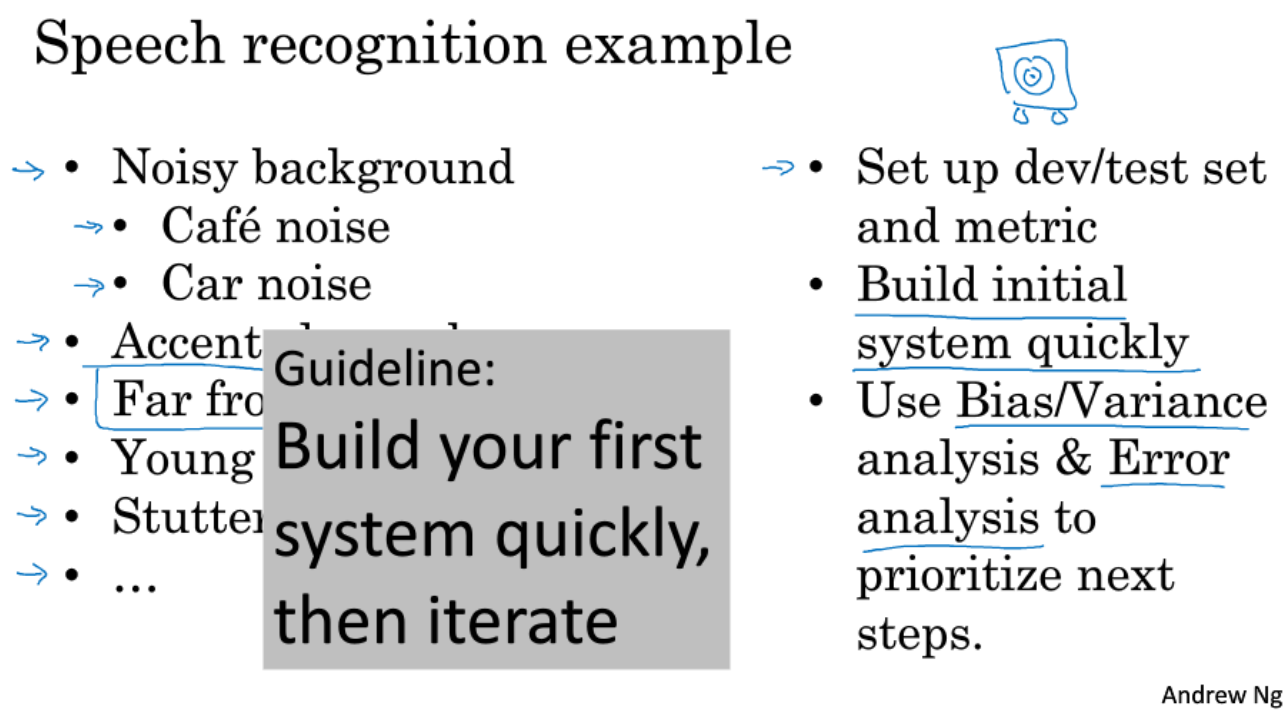
从长期来看，这样的分布能够给我们带来更好的系统性能。



收集正确的开发/测试集样本

- 确保使用来自同一分布的数据处理你的开发集和测试集。
- 考虑检查你的算法是否正确

2.3 快速搭建你的第一个系统并进行迭代

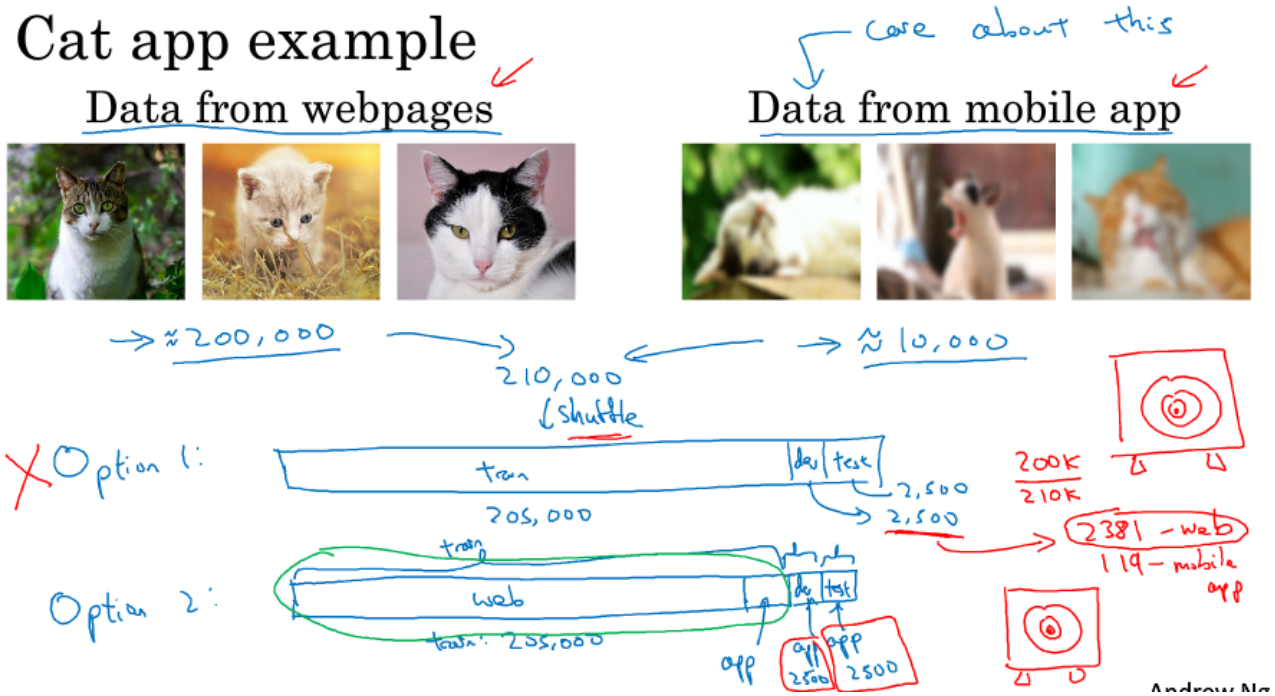


- 设置开发、测试集和优化指标（确定方向）；
- 快速地建立基本的系统；
- 使用偏差方差分析、误差分析去确定后面步骤的优先步骤。

总的来说，如果我们想建立自己的深度学习系统，我们就需要做到：快速的建立自己的基本系统，并进行迭代。而不是想的太多，在一开始就建立一个非常复杂，难以入手的系统。

2.4 在不同划分上的训练和测试

例子1：猫的分类问题



我们可以从网上获取大量的高清晰的猫的图片去做分类，如200000张，但是只能获取少量利用手机拍摄的不清晰的图片，如10000张。但是我们系统的目的是应用到手机上做分类。

也就是说，我们的训练集和开发集、测试集来自于不同的分布。

方法一：

将两组数据合并到一起，总共得到21万张图片样本。将这些样本随机分配到训练、开发、测试集中。

- 好处：三个集合中的数据均来自于同一分布；
- 坏处：我们设立开发集的目的是瞄准目标，而现在我们的目标绝大部分是为了去优化网上获取的高清晰度的照片，而不是我们真正的目标。

这个方法不是一个好的方法。

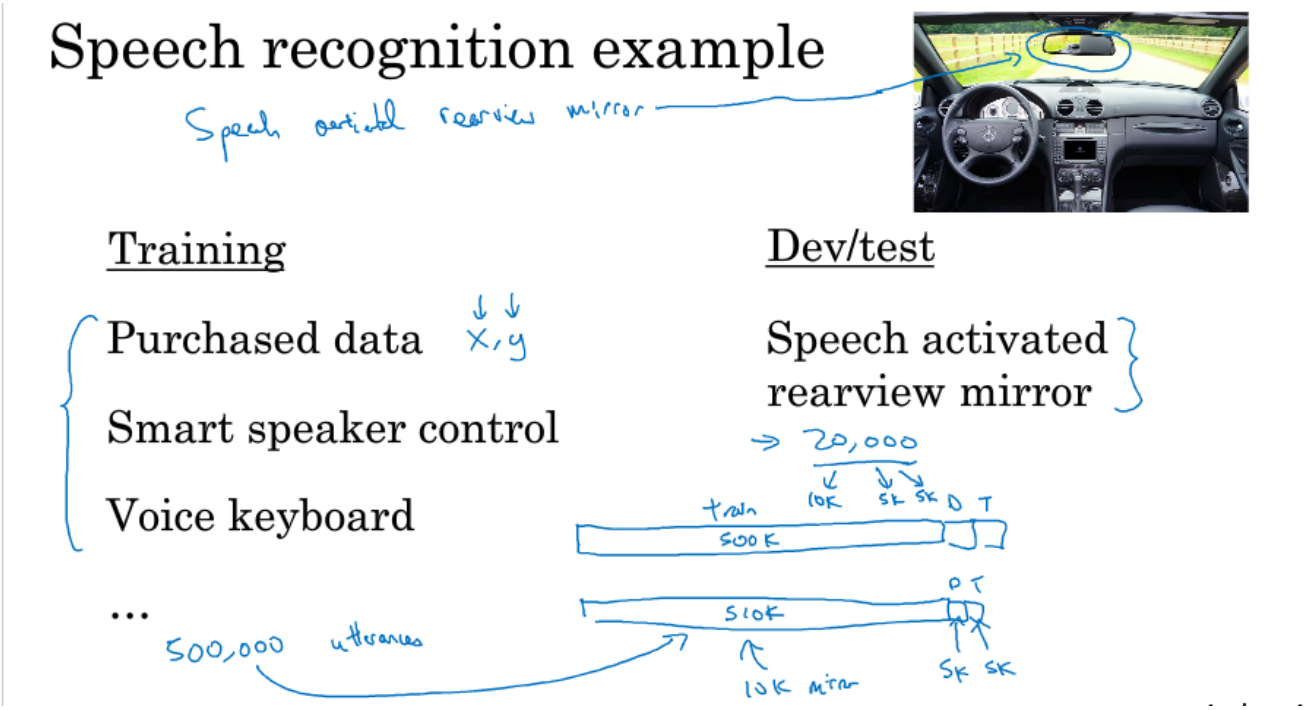
方法二：

训练集均是来自网上下载的20万张高清图片，当然也可以加上5000张手机非高清图片；对于开发和测试集都是手机非高清图片。

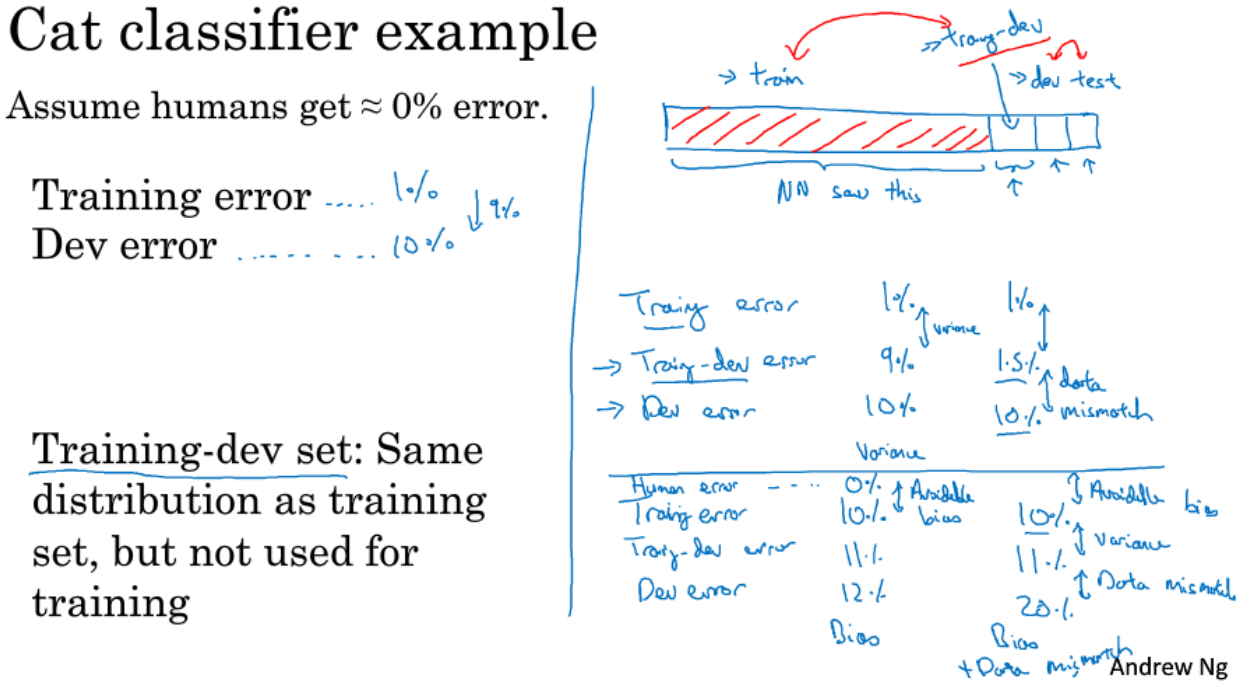
- 好处：开发集全部来自手机图片，瞄准目标；
- 坏处：训练集和开发、测试集来自不同的分布。

从长期来看，这样的分布能够给我们带来更好的系统性能。

例子2：



2.5 不匹配数据划分的偏差和方差



以猫分类为例，假设以人的分类误差0%0%作为贝叶斯误差。若我们模型的误差为：

- Training error：1%1%
- Dev error：10%

如果我们的训练集和开发、测试集来自相同的分布，那么我们可以说模型存在很大的方差问题。但如果数据来自不同的分布，那么我们就不能下这样的定论了。

那么我们如何去确定是由于分布不匹配的问题导致开发集的误差，还是由于算法中存在的方差问题所致？

设立"训练开发集"

训练开发集，其中的数据和训练数据来自同一分布，但是却不用于训练过程。

如果最终，我们的模型得到的误差分别为：

- Training error：1%1%
- Training-dev error：9%9%
- Dev error：10%

那么，由于**训练开发集**尽管和训练集来自同一分布，但是却有很大的误差， 模型无法泛化到同分布的数据，那么说明我们的模型存在**方差问题**。

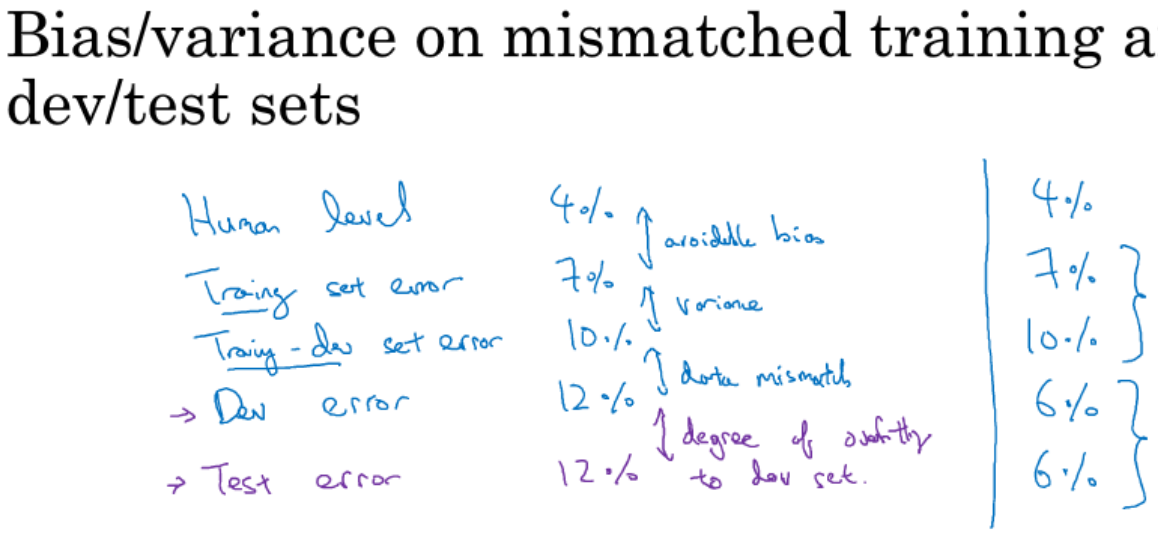
但如果我们的模型得到的误差分别为：

- Training error：1%1%
- Training-dev error：1.5%1.5%
- Dev error：10%10%

那么在这样的情况下，我们可以看到，来自同分布的数据，模型的泛化能力强，而开发集的误差主要是来自于**分布不匹配**导致的。

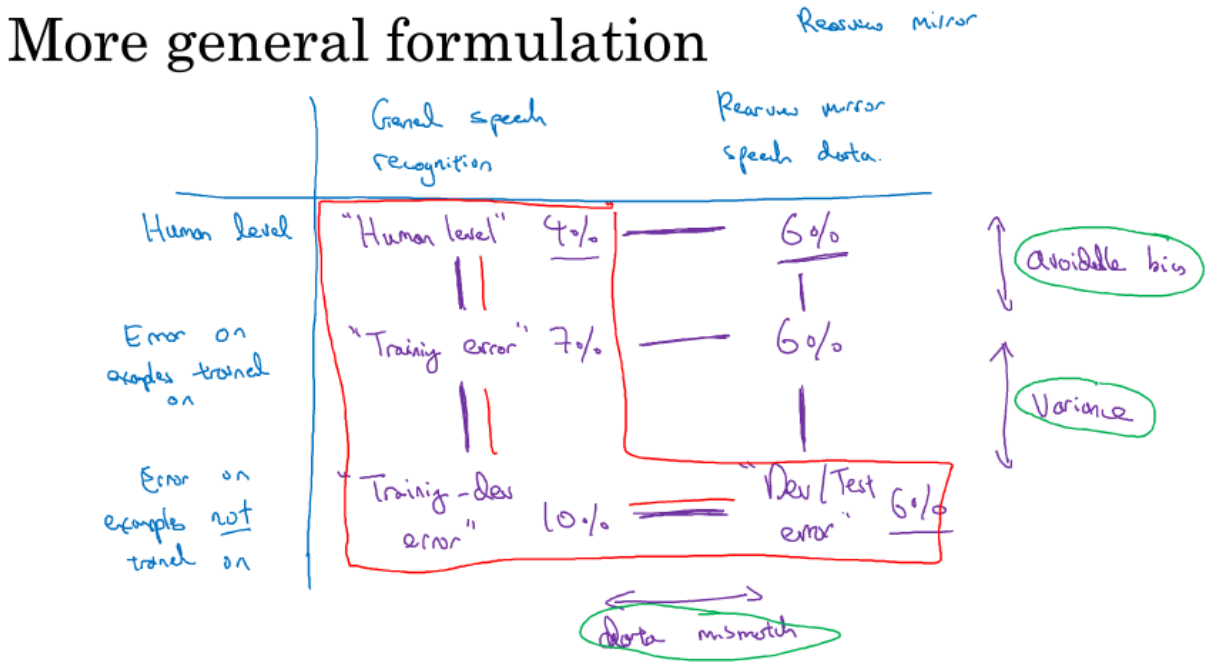
分布不同的偏差方差分析

通过：Human level、Training set error、Training-dev set error、Dev error、Test error 之间误差的大小，可以分别得知我们的模型，需要依次在：可避免的偏差、方差、数据分布不匹配、开发集的或拟合程度，这些方面做改进。



通常情况下来说，通过不同的集合上的误差分析，我们得出的结果会是中间一列误差由小变大，即误差上升的情况。但是也有一定的可能会出现右边一列误差在开发测试集上又表现的好的情况。

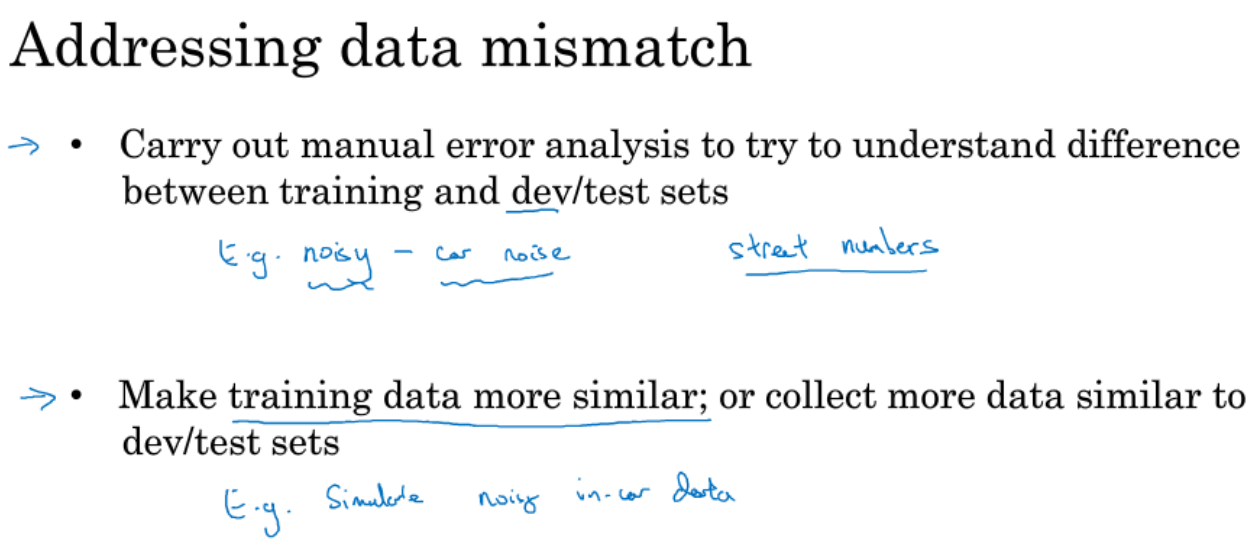
下面通过一个后视镜语音检测的例子来说明。我们以该例子建立更加一般的表格。



其中，横向分别是：普通语音识别数据、后视镜语音识别数据；纵向分别是：Human level、训练数据误差、未训练数据误差。表格中不同的位置分别代表不同的数据集。

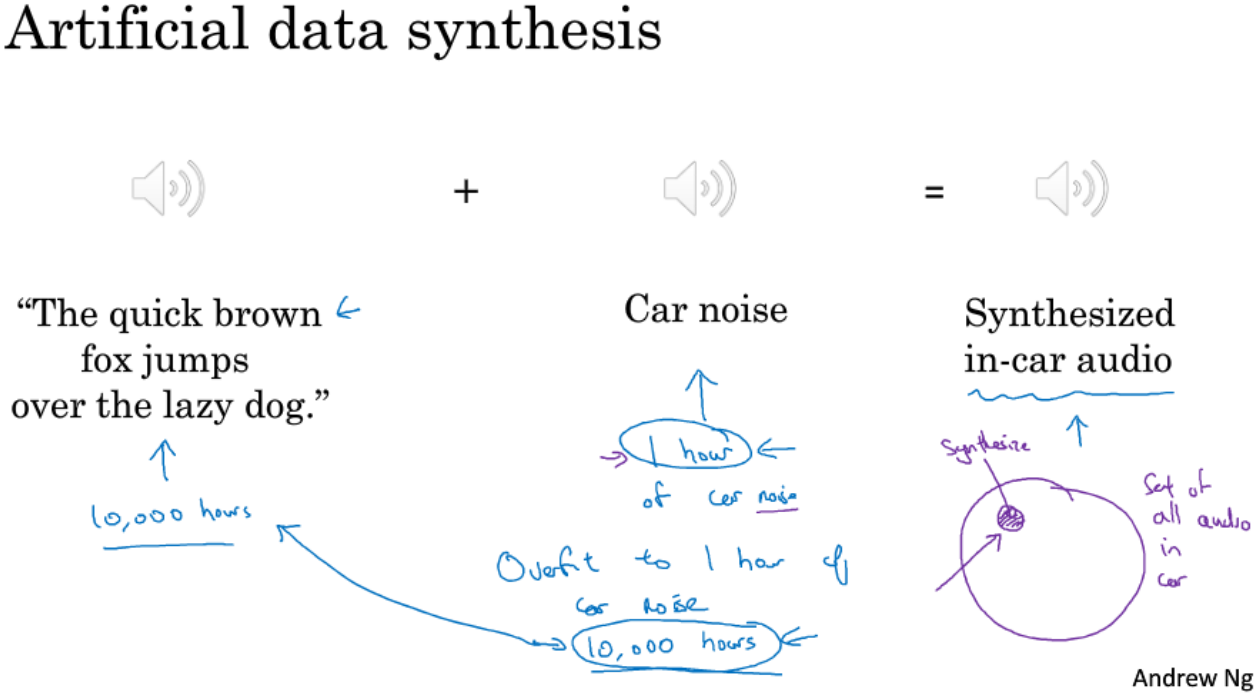
通常情况下，我们分析误差会是一个递增的情况，但是可能对于我们的模型，在后视镜语音识别的数据数据上，已经可以达到人类水平误差的6%6%了，所以最终的开发测试集也会是6%6%的误差，要比训练误差和训练开发误差都要小。所以如果遇到这种情况，就要利用上表进行分析。

2.6 定位数据不匹配问题



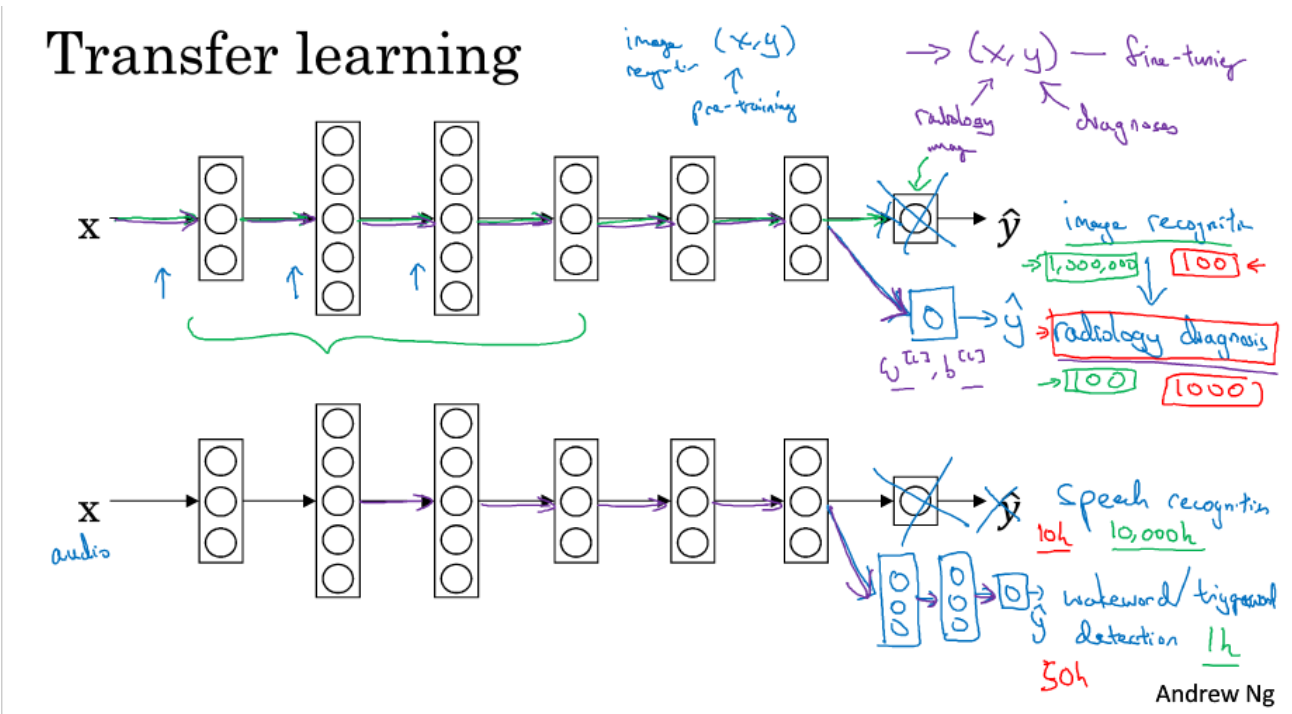
如果通过上一节的误差分析，我们可以得知，模型最终在开发和测试集上的误差最终是由于数据分布不匹配而导致。那么这样的情况下如何解决？

- 进行人工误差分析，尝试去了解训练集和开发测试集的具体差异在哪里。如：噪音等；
- 尝试把训练数据变得更像开发集，或者收集更多的类似开发集和测试集的数据，如增加噪音；



2.7 迁移学习

将从一个任务中学到的知识，应用到另一个独立的任务中。

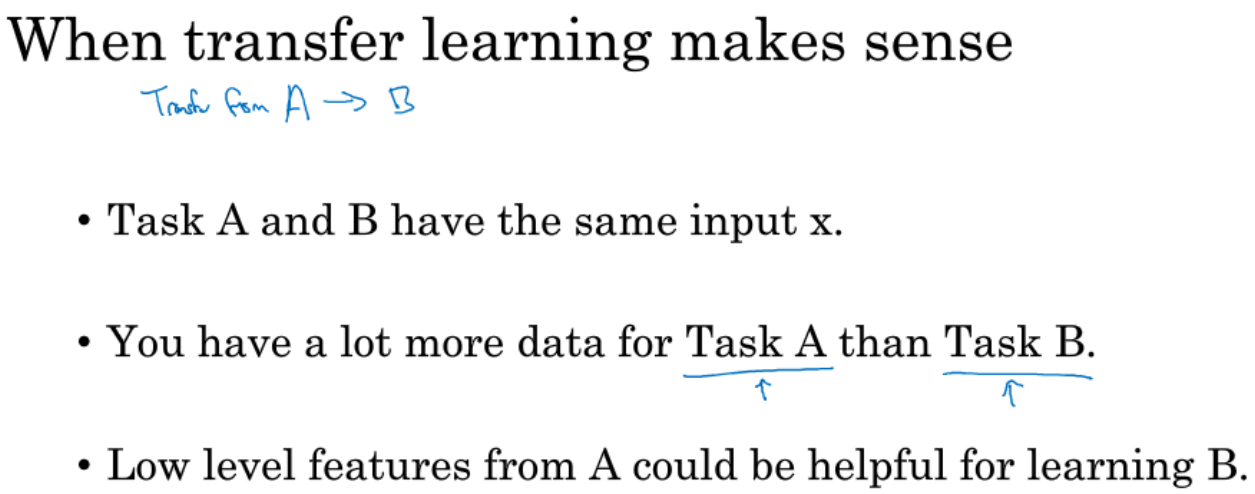


迁移学习的意义：

迁移学习适合以下场合：迁移来源问题有很多数据，但是迁移目标问题却没有那么多的数据。

假设图像识别任务中有1百万个样本，里面的数据相当多；但对与一些特定的图像识别问题，如放射科图像，也许只有一百个样本，所以对于放射学诊断问题的数据很少。所以从图像识别训练中学到的很多知识可以迁移，来帮助我们提升放射科识别任务的性能。

同样一个例子是语音识别，可能在普通的语音识别中，我们有庞大的数据量来训练模型，所以模型从中学到了很多人类声音的特征。但是对于触发字检测任务，可能我们拥有的数据量很少，所以对于这种情况下，学习人类声音特征等知识就显得相当重要。所以迁移学习可以帮助我们建立一个很好的唤醒字检测系统。

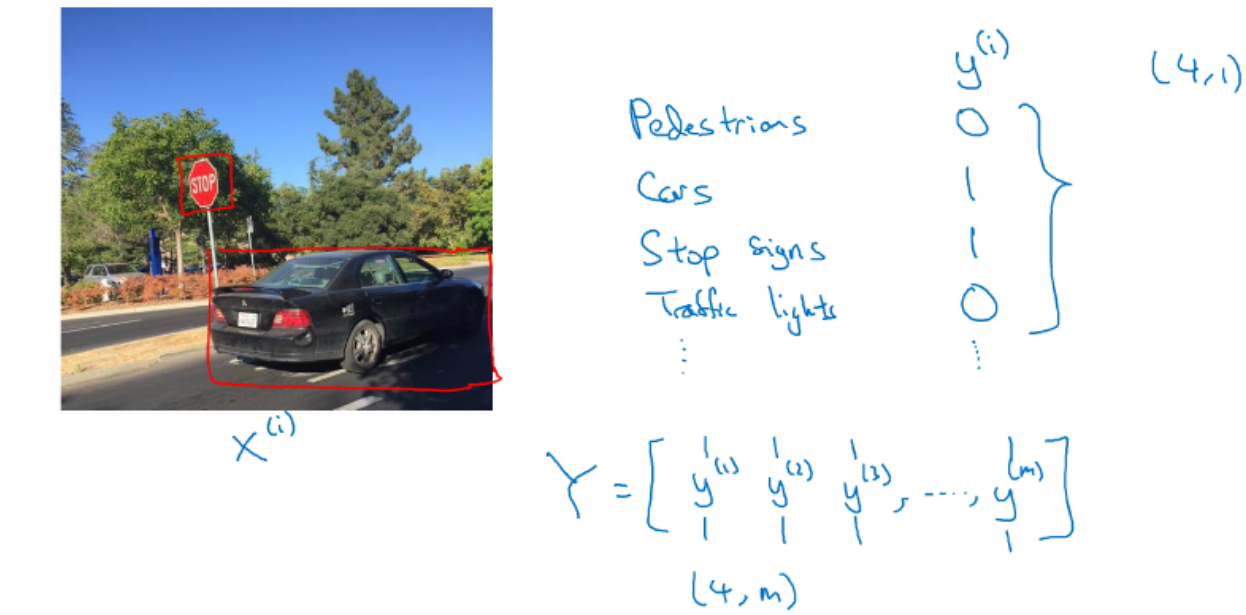


迁移学习有意义的情况：

- 任务A和任务B有着相同的输入；
- 任务A所拥有的数据要远远大于任务B（对于更有价值的任务B，任务A所拥有的数据要比B大很多）；
- 任务A的低层特征学习对任务B有一定的帮助；

2.8 多任务学习

与迁移学习的串行学习方式不同，在多任务学习中，多个任务是并行进行学习的，同时希望各个任务对其他的任务均有一定的帮助。



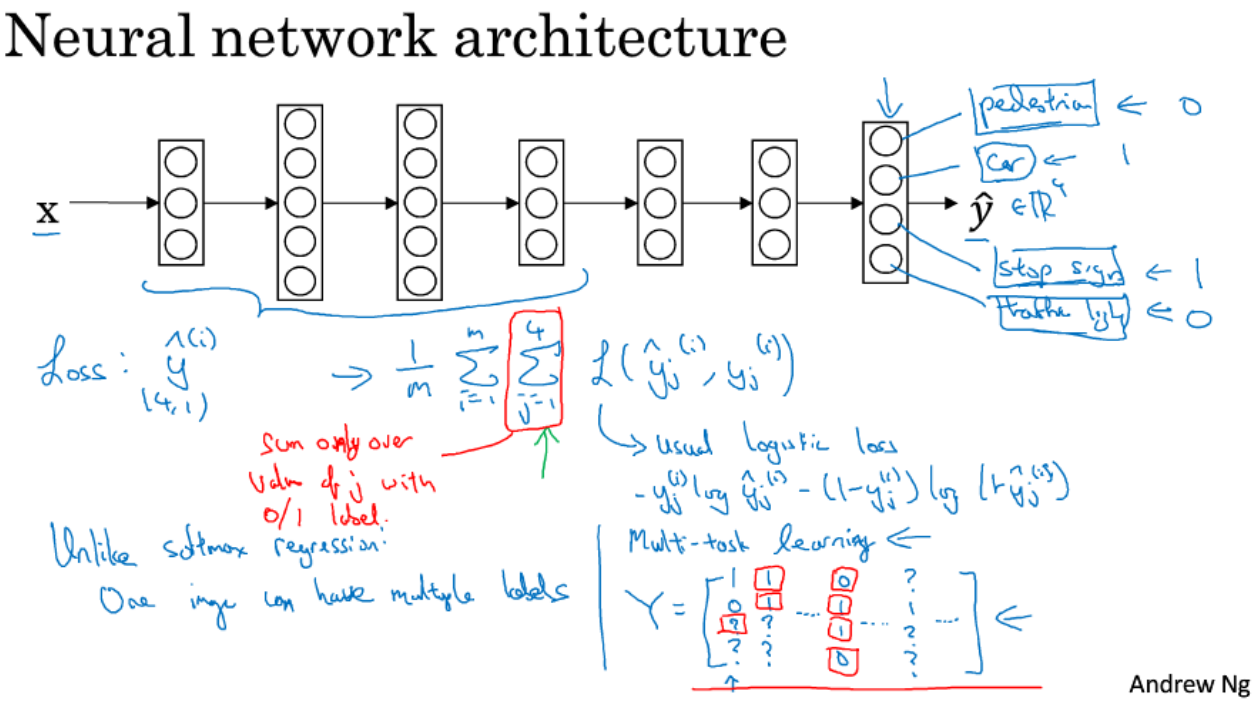
自动驾驶的例子

假设在自动驾驶的例子中，我们需要检测的物体很多，如行人、汽车、交通灯等等。

对于现在的任务，我们的目标值变成了一个向量的形式向量中的每一个值代表检测到是否有如行人、汽车、交通灯等，一张图片有多个标签。

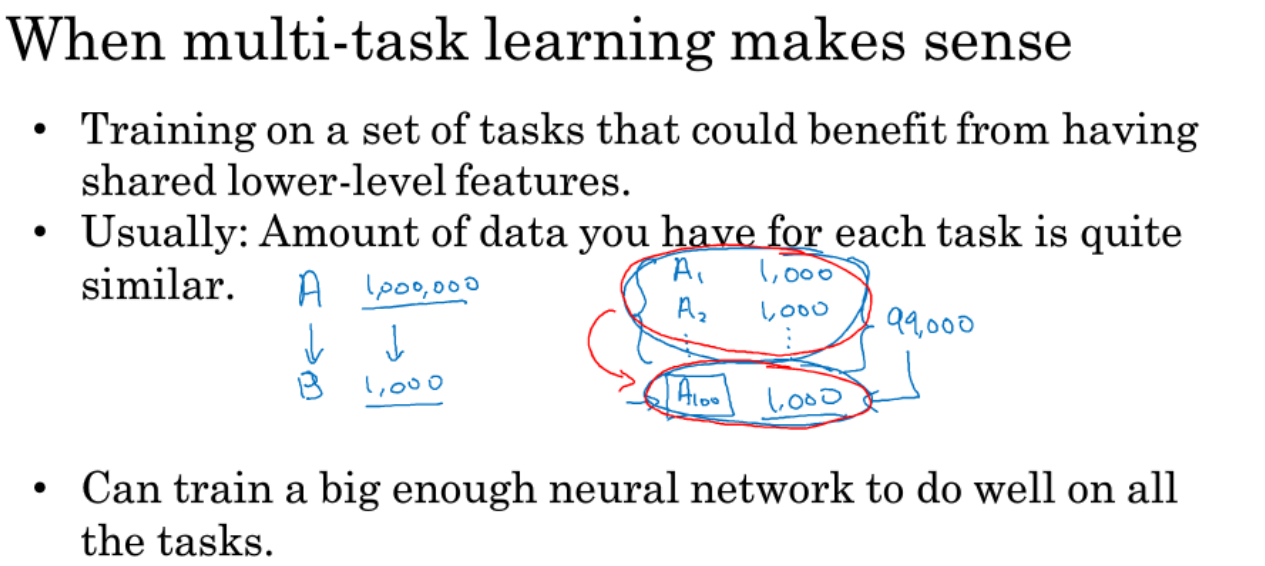
$$y^(i) = [|||| 1010]|||| \ |||||| \ Pedestrians Cars Roadsigns - Stop Traffic lights$$

模型的神经网络结构如下图所示：



什么时候使用多任务学习有效？

- 如果训练的一组任务可以共用低层特征；
- 通常，对于每个任务大量的数据具有很大的相似性；（如，在迁移学习中由任务A“100万数据”迁移到任务B“1000数据”；多任务学习中，任务A1，...，AnA1，...，An，每个任务均有1000个数据，合起来就有1000n个数据，共同帮助任务的训练）
- 可以训练一个足够大的神经网络并同时做好所有的任务。



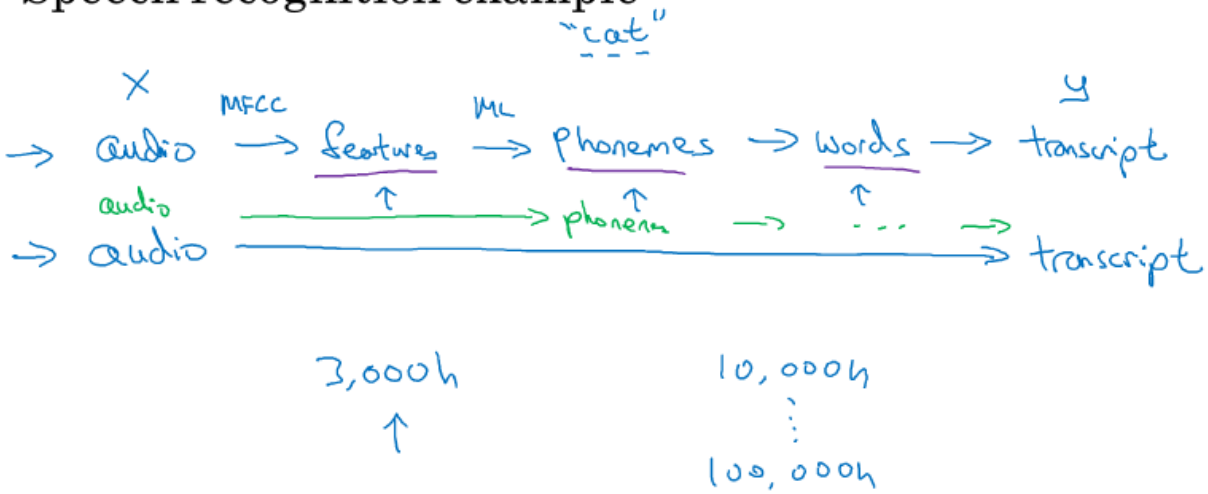
2.9 什么是端到端的深度学习？

定义：

相对于传统的一些数据处理系统或者学习系统，它们包含了多个阶段的处理过程，而端到端的深度学习则忽略了这些阶段，用单个神经网络来替代。

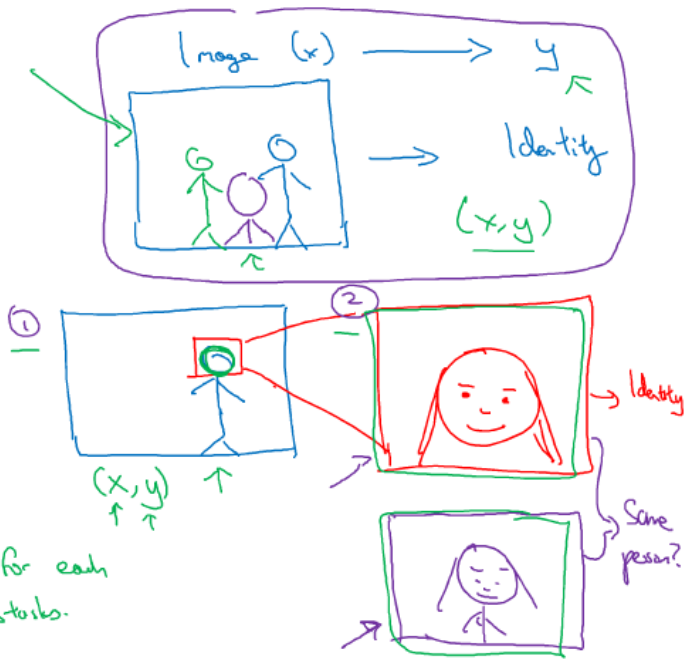
What is end-to-end learning?

Speech recognition example



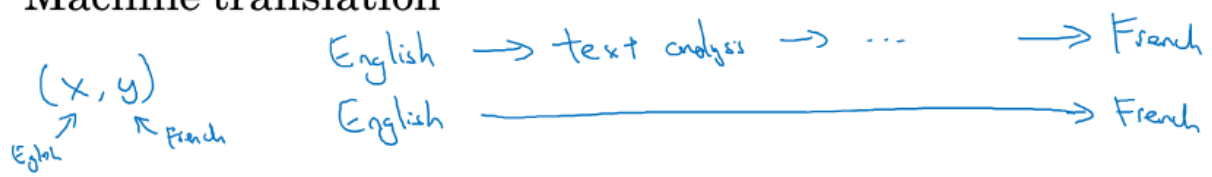
Face recognition

[Image courtesy of Baidu]



More examples

Machine translation



Estimating child's age:

Andrew Ng

优缺点：

- 优点：

端到端学习可以直接让数据"说话"； 所需手工设计的组件更少。

- 缺点：

需要大量的数据； 排除了可能有用的手工设计组件。

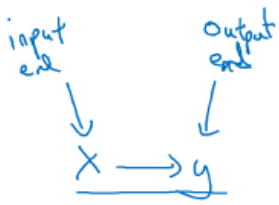
Pros and cons of end-to-end deep learning

Pros:

- Let the data speak

- Less hand-designing of components needed

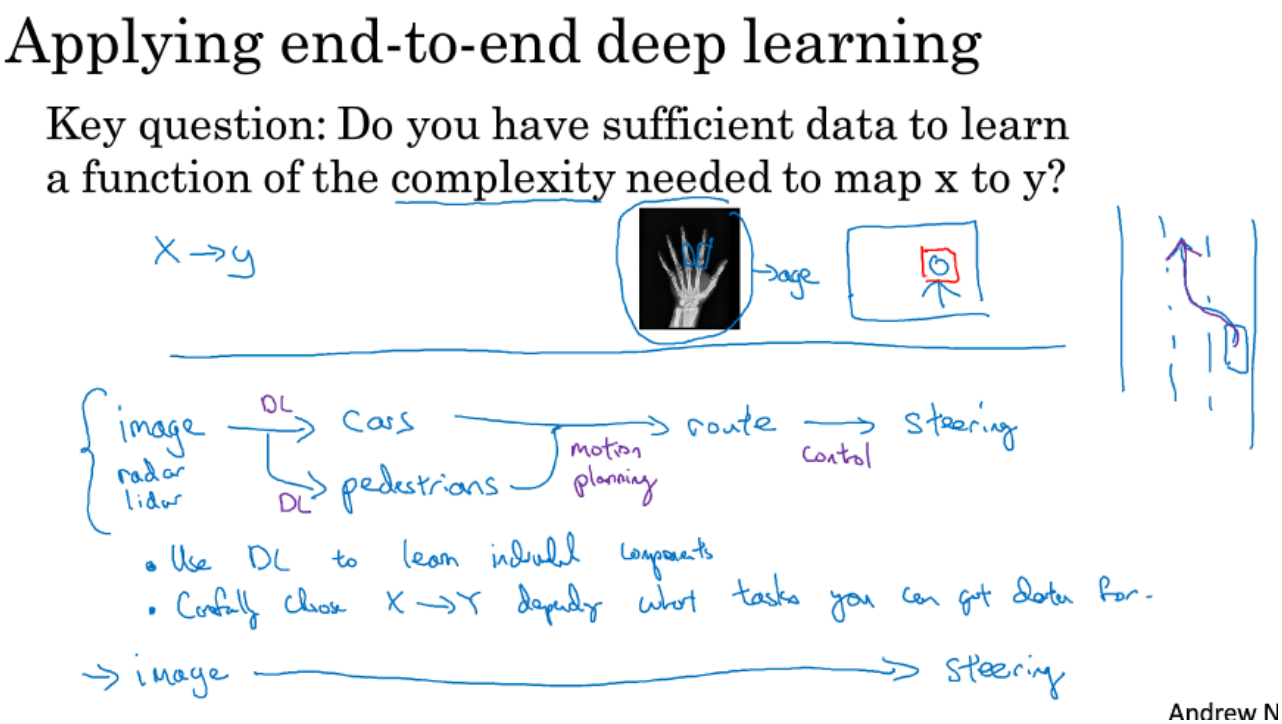
Cons:



- May need large amount of data
- Excludes potentially useful hand-designed components

Andrew

关键问题



例如在无人驾驶中。