南京理工大学
NANJING UNIVERSITY OF SCIENCE & TECHNOLOGY

机器学习-江阴网安1
群号：1003024103

机器学习概述

程煦

xcheng8@njust.edu.cn

计算机科学与工程学院




课程内容

- 以机器学习算法及原理为重点（**考试**）
- 以实现机器学习的应用为目的（课程大作业）

课程目标

- 掌握、理解和推导经典的机器学习算法
- 利用机器学习算法去解决实际问题
- 理解（突破）现有技术的瓶颈
  - 能够区分tricky的技术和扎实的理论技术
  - 能够帮助大家选择硕、博的研究方向

课程目标

- 掌握、理解和推导经典机器学习的机器学习算法
- 利用机器学习算法去解释实际问题
- 理解（突破）现有技术的瓶颈
  - 能够区分tricky的技术和扎实的理论技术
  - 能够帮助大家选择硕、博的研究方向

Besides

- **The most important goal**
  - **What is the future of your career?**
  - **What is the future of AI?**
  - **How to catch up with the fast development of AI?**

课程考核

- 考勤：**10%**
  - 考勤共计三次，请假请提交**请假条**，不接受口头请假。三次考勤不到无考试资格。
- 课程大作业（提交报告的形式）+考试：**90%**
  - 课程大作业会在第5或6周布置，给同学们留充足的完成时间。

联系方式

王慧慧

huihuiwang@njust.edu.cn

计算机学院4073

程煦

xcheng8@njust.edu.cn

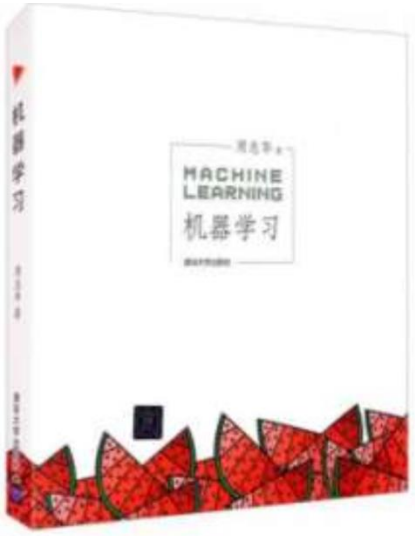
计算机学院2075

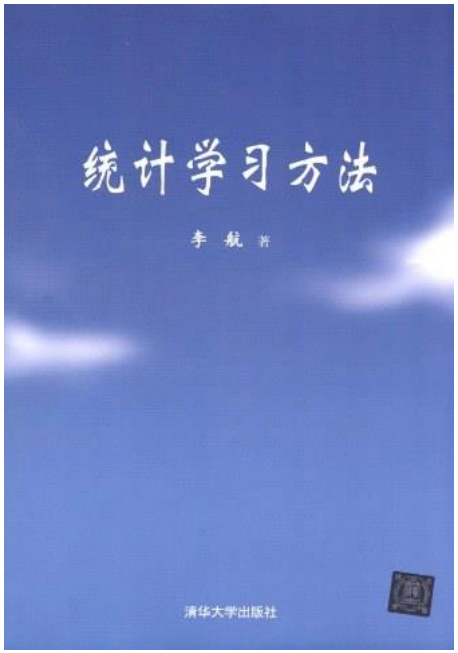
课程考勤：加入QQ群

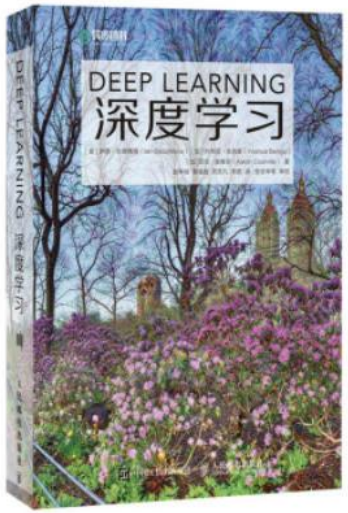
请各位同学在25号之前将群昵称改成**学号+姓名**，记为第一次考勤！

参考书

- 《机器学习》，周志华，清华大学出版社，2016.
- 《统计学习方法》，李航，清华大学出版社，2019.
- 《Deep Learning》， Ian Goodfellow等 , 2017.







- 在线学习资源：

https://www.cs.cmu.edu/~epxing/Class/10715/

http://www.cs.cmu.edu/~epxing/Class/10701

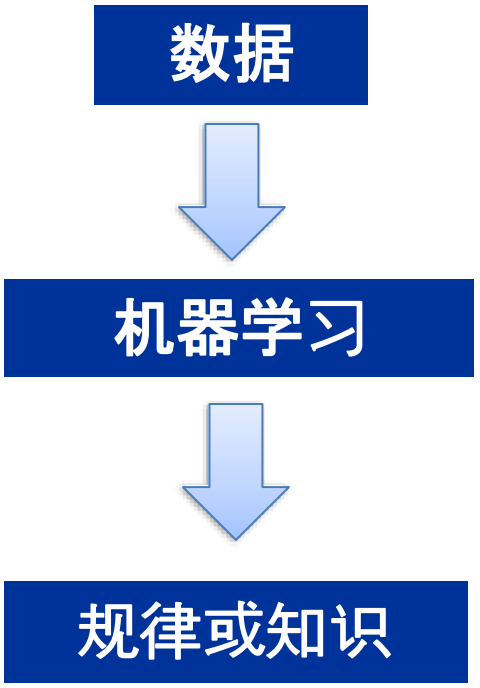
什么是机器学习？

- **机器学习**是近20多年兴起的一门**多领域交叉学科，涉及概率论、 统计学、逼近论、凸分析、算法复杂度理论**等多门学科。机器学习理论主要是设计和分析一些让计算机可以**自动“学习”**的算法。

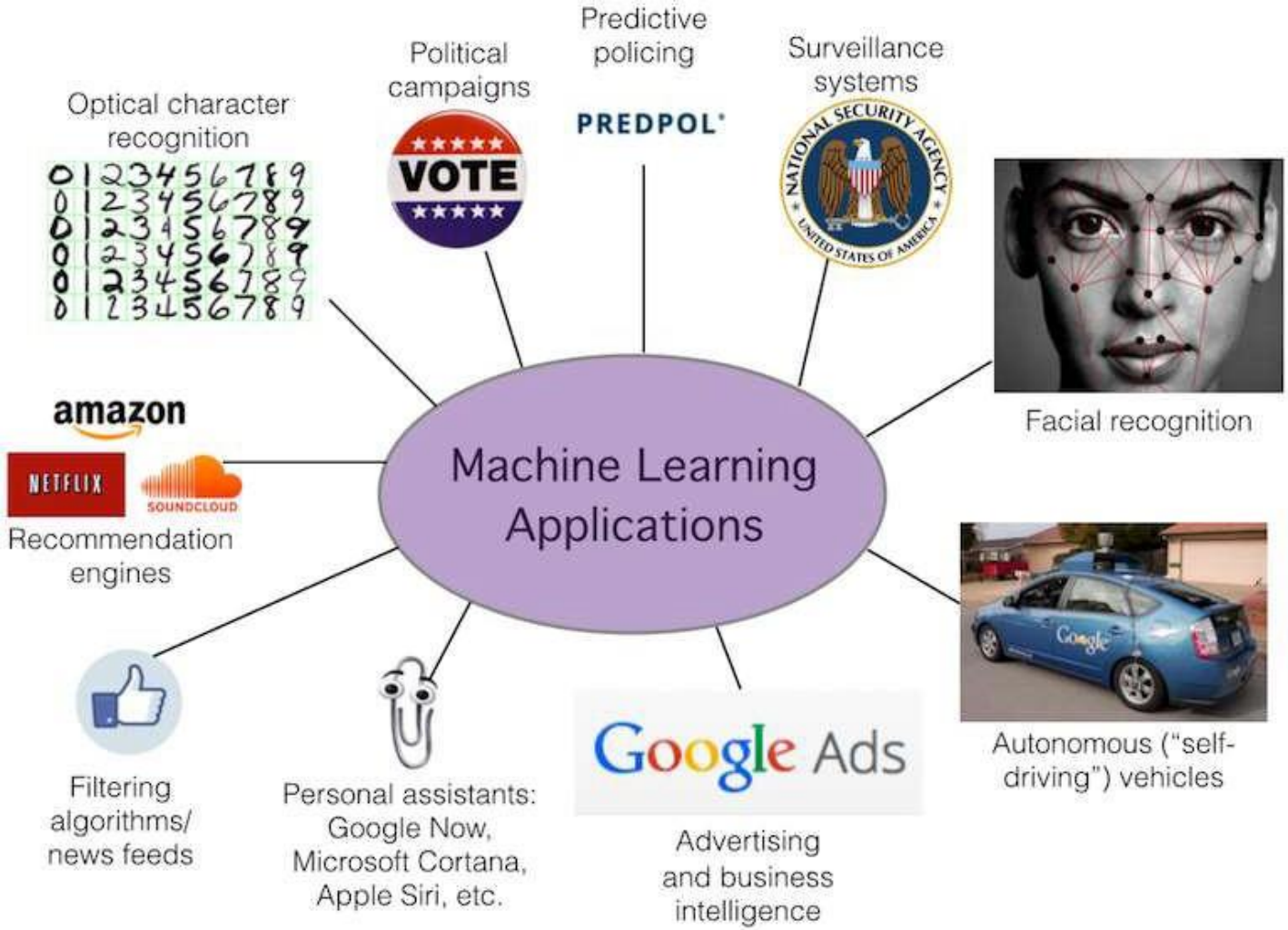
机器（计算机）是否能够跟我们（人类）一样可以从历史数据中学习规律或知识？

什么是机器学习？

- **机器学习**是基于数据或以往的经验，学习并优化具体算法的性能。



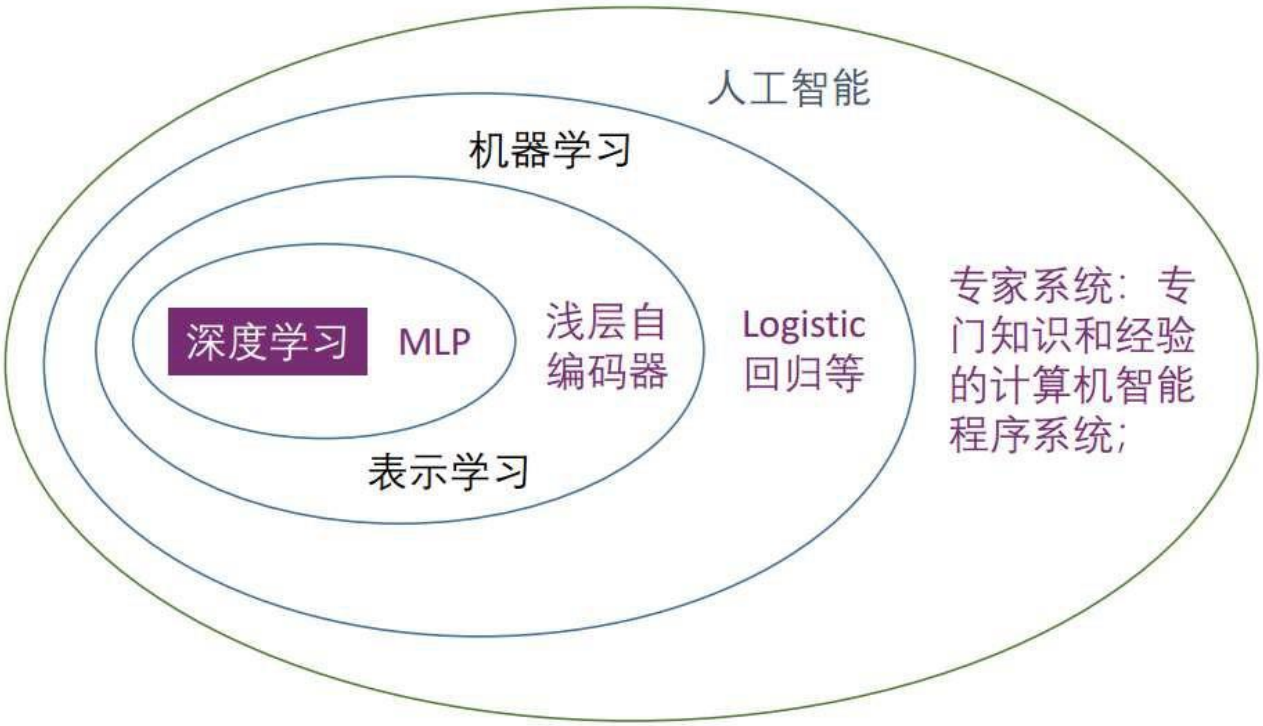
机器学习为什么重要？



广泛应用于我们的生活中！

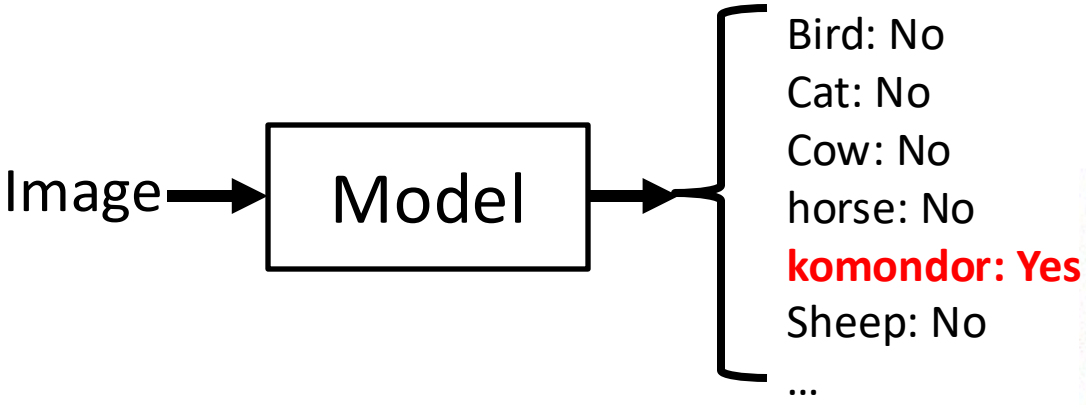
机器学习为什么重要？

- 机器学习是实现人工智能的关键方法，是人工智能的一个子领域。



- **人工智能**：计算机模拟或实现人类智能的技术，为机器赋予视觉/听觉/触觉/推理等智能。
- **机器学习**：专注于让机器从数据中学习并进行预测或决策。

机器学习应用—图像分类（image classification）



GT: horse cart
1: horse cart
2: minibus
3: oxcart
4: stretcher
5: half track

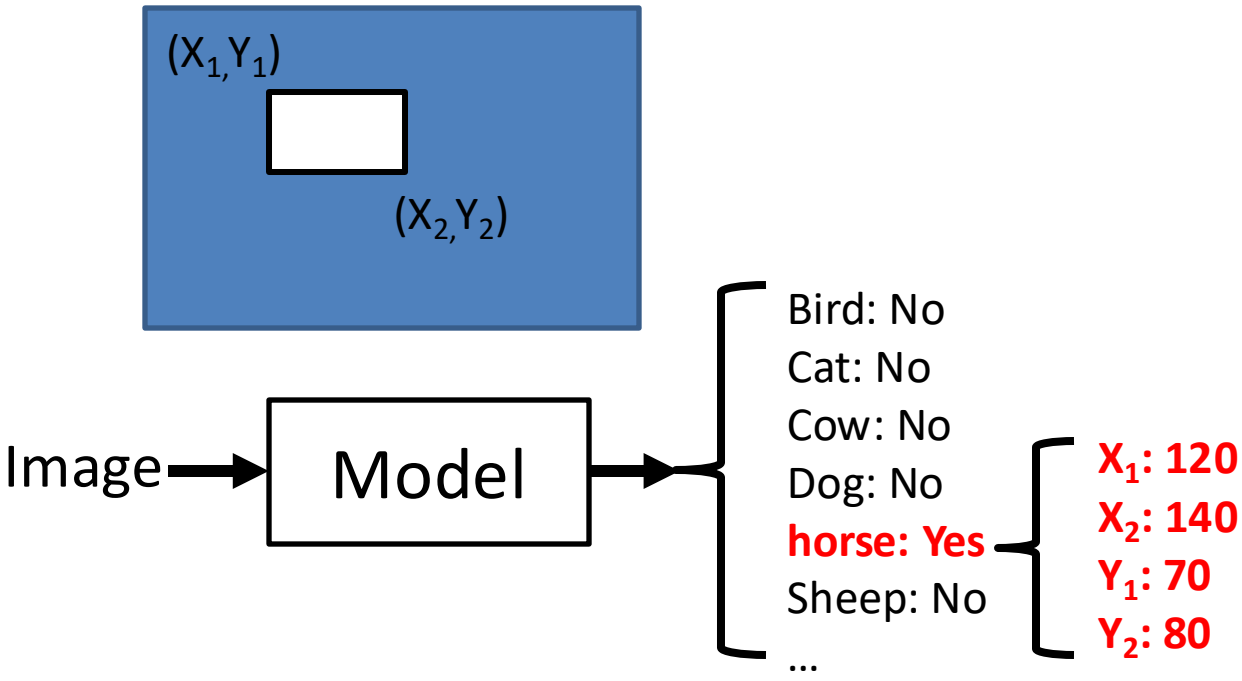
GT: birdhouse
1: birdhouse
2: sliding door
3: window screen
4: mailbox
5: pot

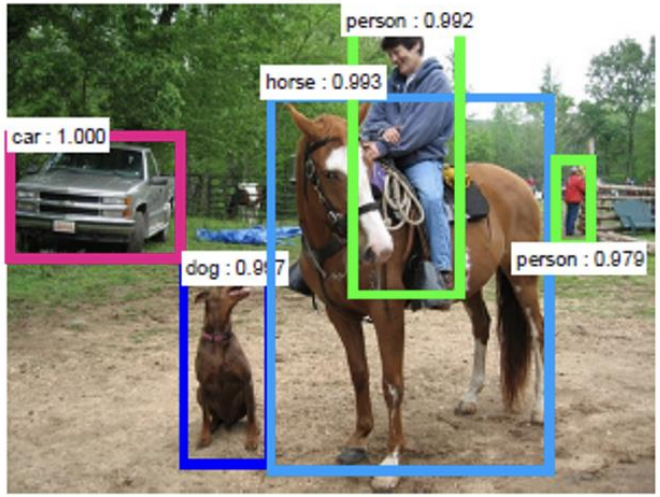
GT: coucal
1: coucal
2: indigo bunting
3: lorikeet
4: walking stick
5: custard apple

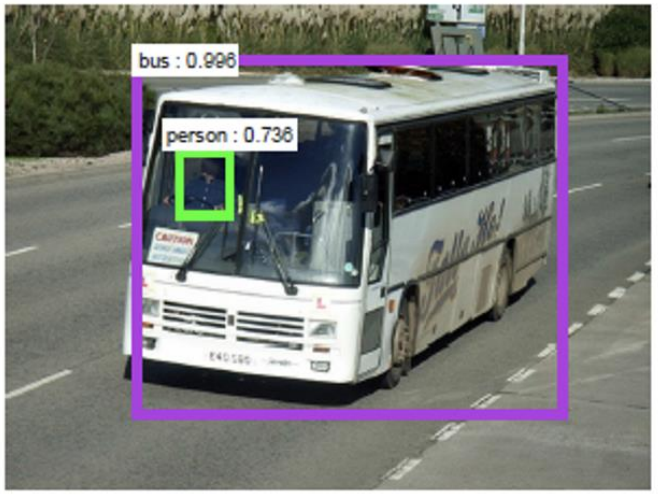
GT: komondor
1: komondor
2: patio
3: llama
4: mobile home
5: Old English sheepdog

He et al. Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification, in ICCV 2015

机器学习应用—目标检测（object detection）

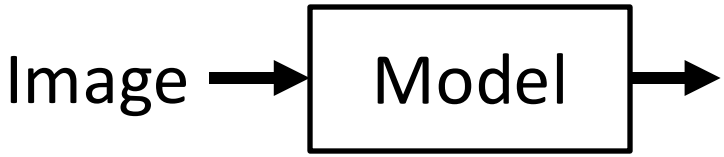




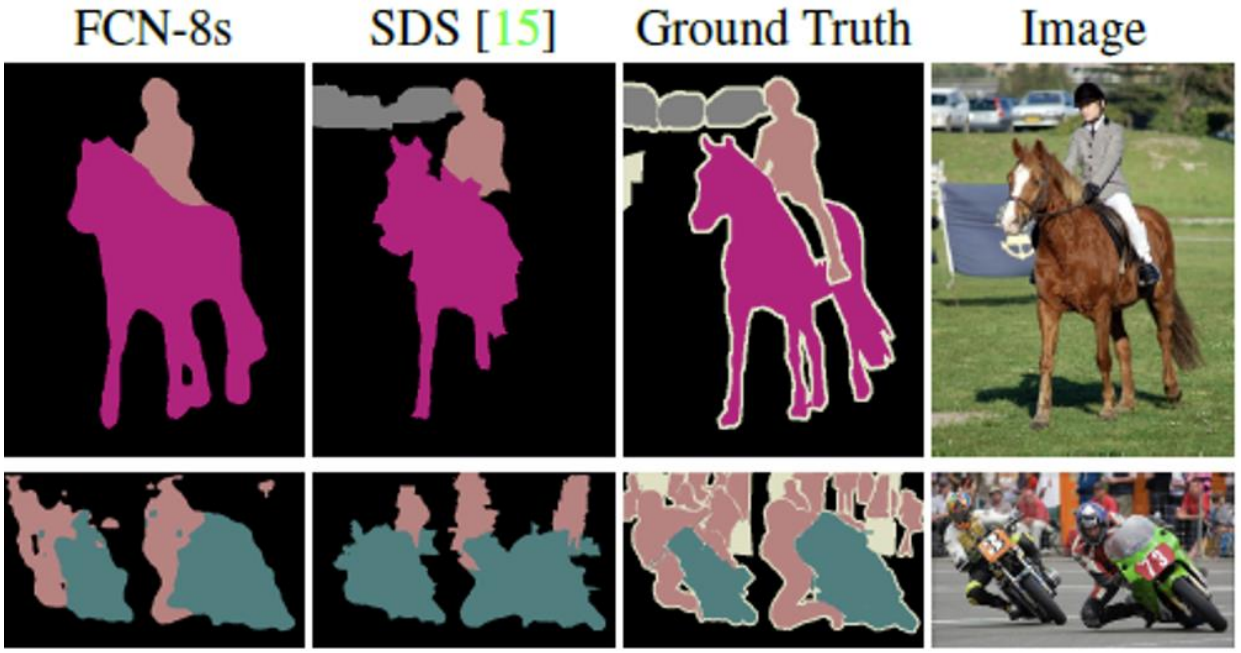


Ren et al., Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks, in NIPS 2015

机器学习应用—图像分割（image segementation）



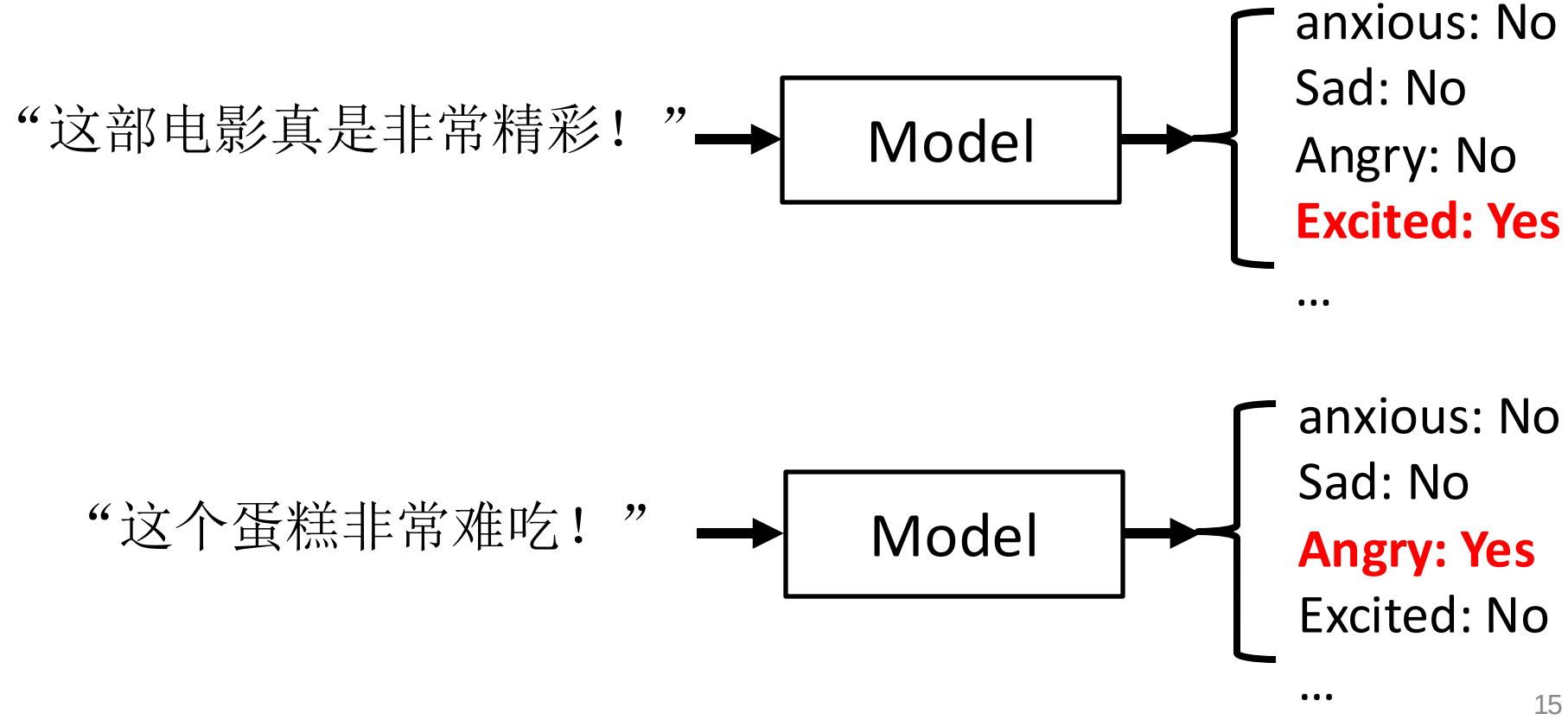
A	A	A	A	A	A	A	B	D	D
A	A	A	A	A	A	A	B	B	D
A	A	A	A	A	A	B	B	B	D
A	A	A	A	B	B	B	B	B	D
B	B	A	B	B	B	B	B	D	D
C	C	B	B	B	B	B	D	D	D
C	C	C	C	B	B	D	D	D	D
C	C	C	C	C	B	D	D	D	D



Long et al., Fully Convolutional Models for Semantic Segmentation, in CVPR, 2015

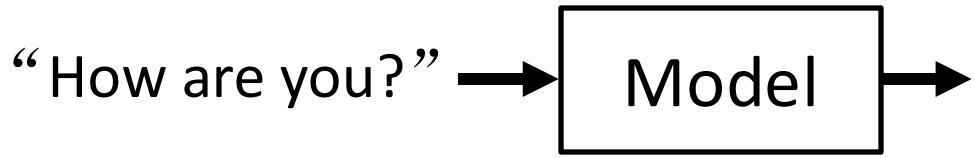
机器学习应用—自然语言处理（natural language processing）

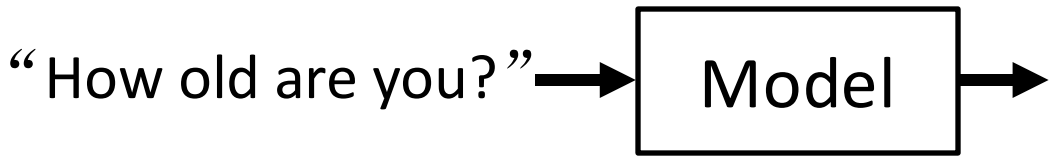
- 情感语义分类（Sentiment classification）



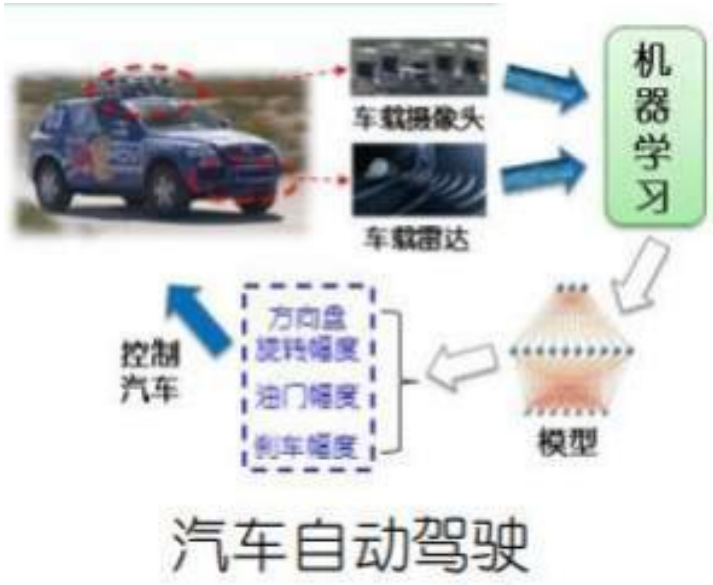
机器学习应用—自然语言处理（natural language processing）

- 翻译（translation）



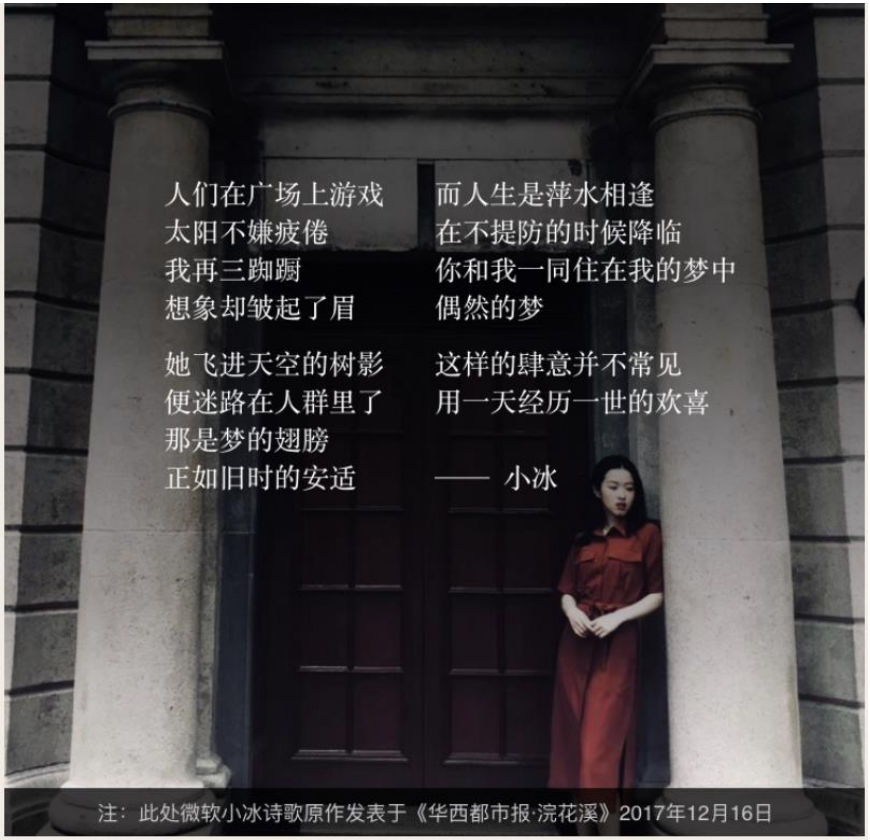


机器学习应用—自动驾驶（Autonomous driving）



汽车自动驾驶

机器学习应用—人工智能生成（AIGC）



人工智能作诗

首页 › 智能体验 › 全球首张人工智能编曲"AI专辑"首发单曲《Break Free》MV（附相关研究论文）

全球首张人工智能编曲"AI专辑"首发单曲《Break Free》MV（附相关研究论文）

发布 大白 - 2017年8月30日

如果你在电台上听到了塔伦·萨瑟恩（Taryn Southern）的新曲《Break Free》，十有八九不会停下手头的工作。但实际上，这首歌曲的幕后故事非常惊奇，因为它是通过人工智能创作出来的。此外，这支 LP 并不是一次浅尝则止的尝试，因为塔伦借助 AI 创作平台 Ampere Music 打造了一整张专辑 ——《我是人工智能》（I AM AI）。

该专辑的作词作曲是Taryn Southern，编曲则交给人工智能程序，在旋律中加入配乐……人工智能程序交出来的作品非常完整，包括和声、和弦，应用了多种乐器……详见《美流行歌手首张AI专辑发布 人工智能编曲不输音乐人》

人工智能编曲

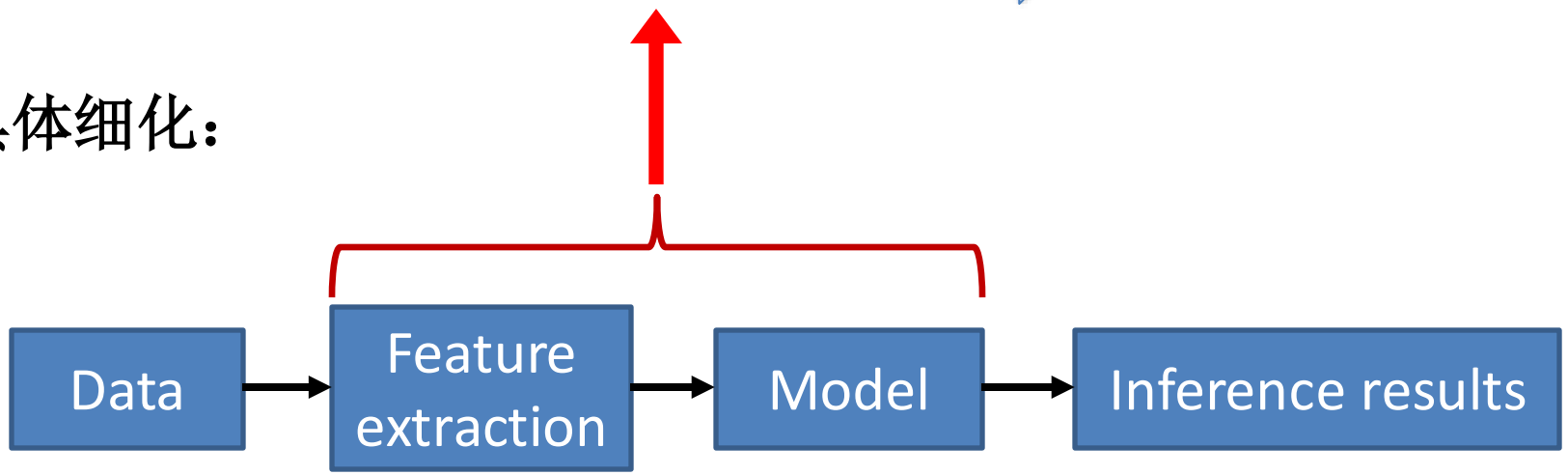
机器学习应用—人工智能生成（AIGC）

人工智能作画

机器学习基本概念与术语

- **机器学习**是基于数据或以往的经验，学习并优化具体算法的性能。

- 具体细化：



机器学习基本概念与术语

- 数据集（dataset）： $D = \{(x_i, y_i) | i \in \{1,2, \dots, n\}\}$

  - For image classification, x_i represents an input image, y_i represents the ground-truth label of the image

x_i:

$y_i = 3$

1: cat
2: bird
3: dog

  - For language translation, x_i represents an input sentence, y_i represents the target output sentence.

x_i: “How are you?” **y_i: “你好吗？”**

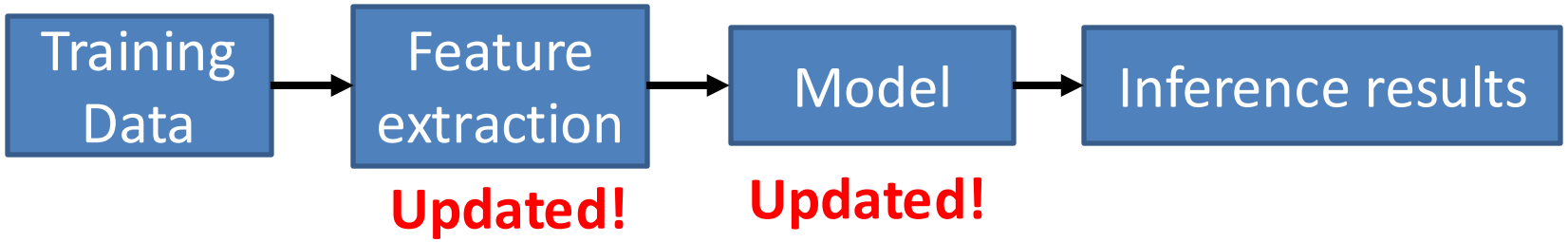
机器学习基本概念与术语

训练数据∩测试数据=∅

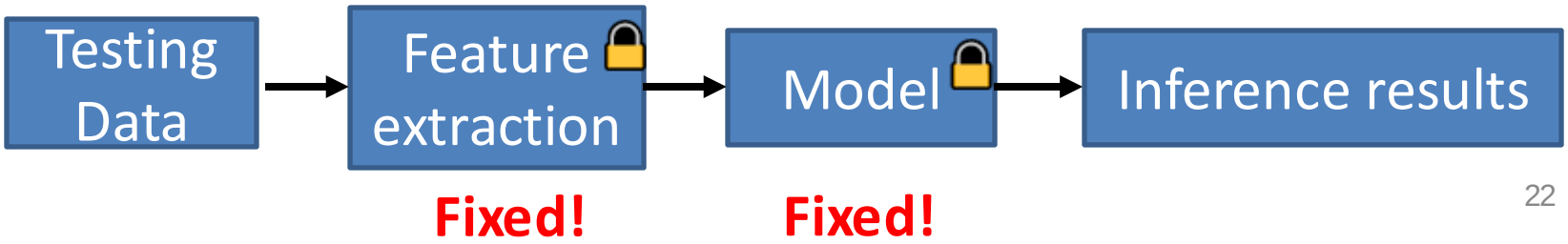
- 数据集（dataset）： $D = \{(x_i, y_i)\}_{i=1,2,\ldots,n}$

① 训练数据（**Training data**）：用来训练模型

- Learn a model $\hat{y}_i = g_\theta(x_i)$, where θ denotes parameters of the model
- Update model parameters to make the prediction $\hat{y}_i$ approximate the ground-truth y_i



②测试数据（**Testing data**）：用来测试模型的性能

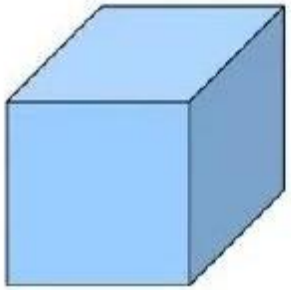


机器学习基本概念与术语

- 特征（feature）
  - f=h(x)
  - Represent discriminative information
  - Discard irrelevant information
  - Robust to noise

1-order tensor:
Vector

2-order tensor:
Matrix

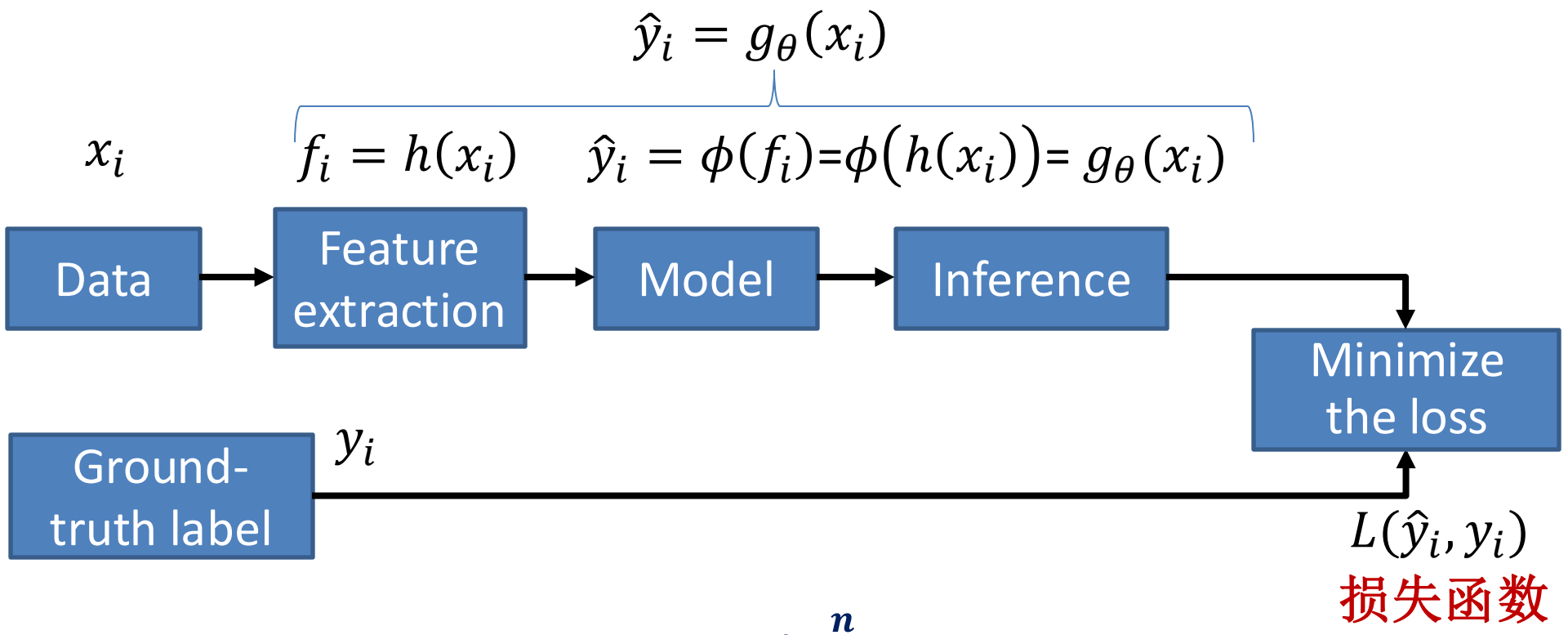


3-order Tensor

A 3-order tensor: 200 x 140 x 3

机器学习基本概念与术语

- 模型$\hat{y}_i = g_\theta(x_i)$：encode the relationship between the input and output, such as deep neural network, SVM…



模型训练目标：$\min_\theta \frac{1}{n}\sum_{i=1}^{n} L(\hat{y}_i, y_i)$

机器学习基本概念与术语

- 模型$\hat{y}_i = g_\theta(x_i)$：encode the relationship between the input and output

$$\min_{\theta} \frac{1}{n}\sum_{i=1}^{n} L(\hat{y}_i, y_i)$$

➢ 均方误差损失（Mean Squared Error loss，MSE Loss）

$$L(\hat{y}_i, y_i) = \|\hat{y}_i - y_i\|^2 \qquad \|\mathbf{x}\|_2 = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$$

➢ 交叉熵损失（Cross entropy loss）

$$L(\hat{y}_i, y_i) = \text{crossEntropy}(\hat{y}_i, y_i) = -\sum_j y_{ij} \log \hat{y}_{ij}$$

if y_i represents a distribution of probabilities, $y_i = [y_{i1}, y_{i2}, \ldots, y_{in}]$, $y_{ij} \geq 0$, $\sum_j y_{ij} = 1$

机器学习基本概念与术语

- 模型$\hat{y}_i = g_\theta(x_i)$：encode the relationship between the input and output

$$\boldsymbol{\min_{\theta}} \ \frac{1}{n}\sum_{i=1}^{n} \boldsymbol{L(\hat{y}_i, y_i)}$$

如何优化？

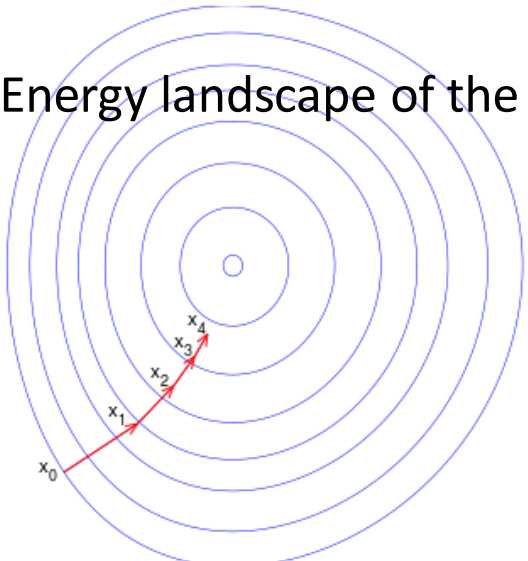
- **优化方法**：解析解、梯度下降、随机梯度下降、牛顿法、 拟牛顿法(BFGS)、有限内存BFGS (L-BFGS)、共轭梯度法

Gradient descent method

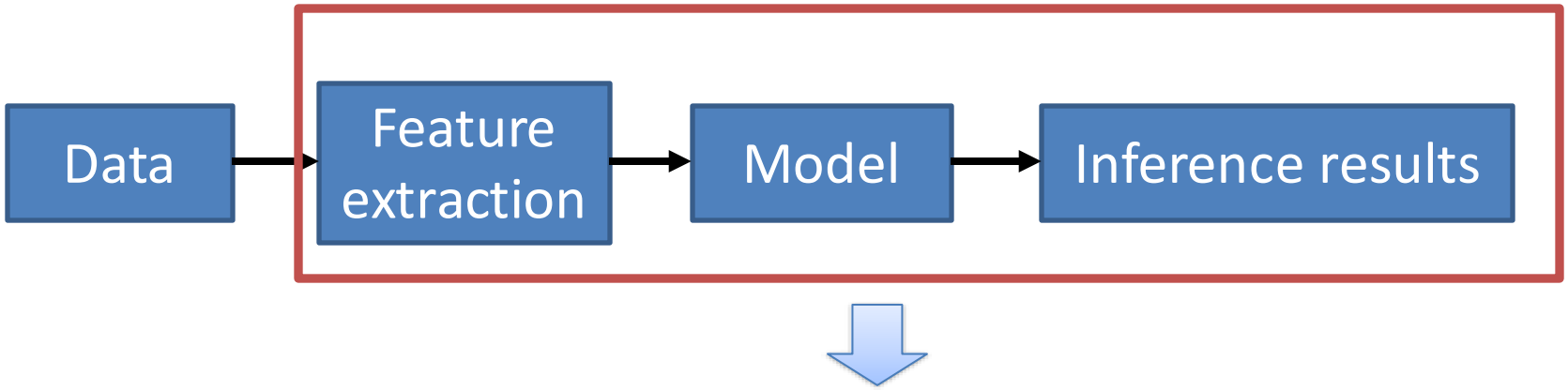
$$\min_{\theta} \frac{1}{n}\sum_{i=1}^{n} L(\hat{y}_i, y_i)$$

$$\theta^{t+1} = \theta^{t} - \eta \frac{\partial \sum_{i=1}^{n} L(\hat{y}_i, y_i)}{\partial \theta}$$

Energy landscape of the loss



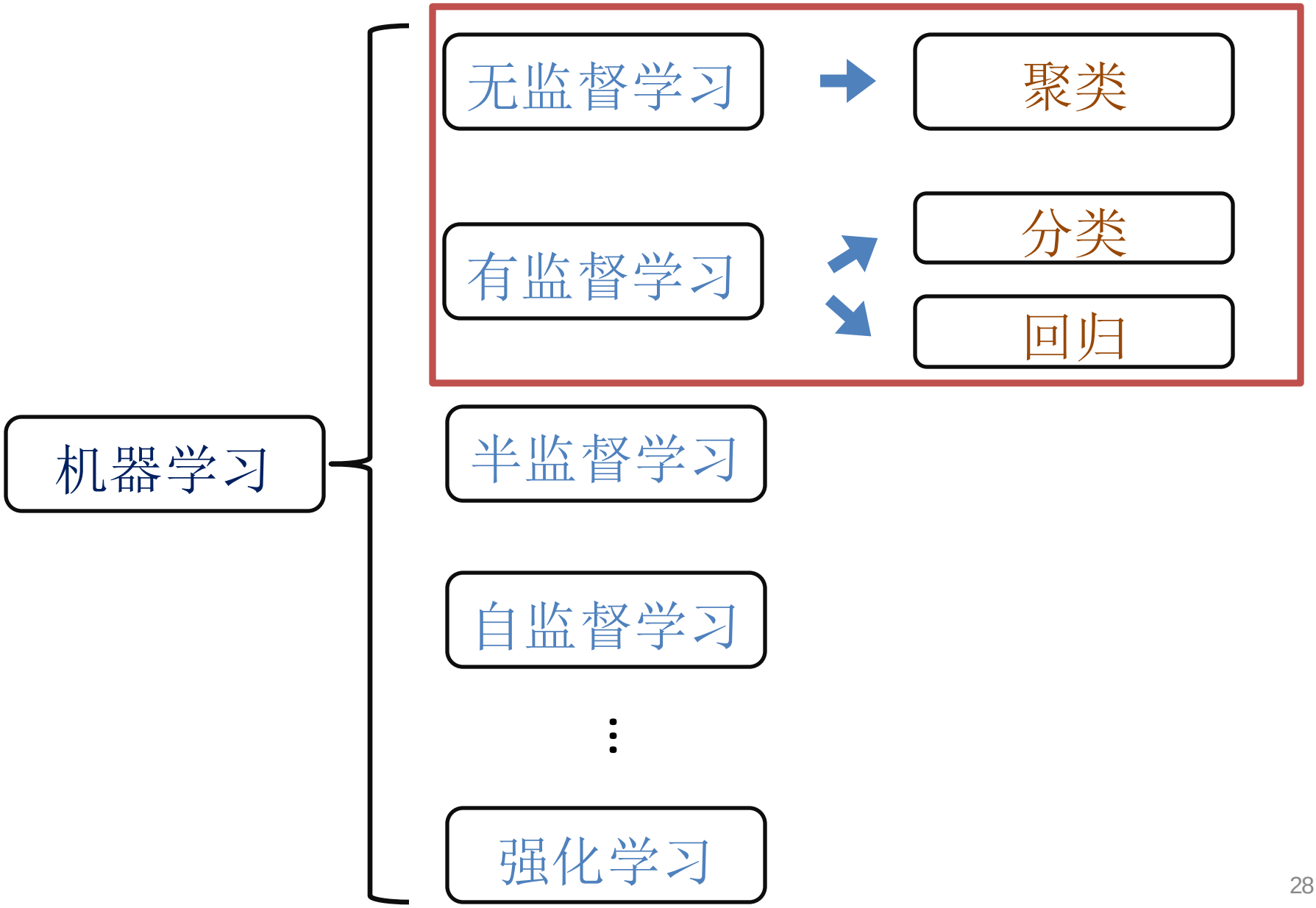
机器学习基本概念与术语



可以总结为：**假设—学习—决策**

- **假设**：具有（未知）参数（或结构）的数学模型，用于建模输入与输出的关系→ $\hat{y}_i = g_\theta(x_i)$
- **学习**：**通过训练数据找到最佳假设**，使得模型能够准确预测新数据→求解$\min_\theta \frac{1}{n}\sum_{i=1}^{n} L(\hat{y}_i, y_i)$
- **决策**：训练完成后，模型需要基于新输入数据x_j**做出决策**，输出预测结果$\hat{y}_j$

机器学习分类

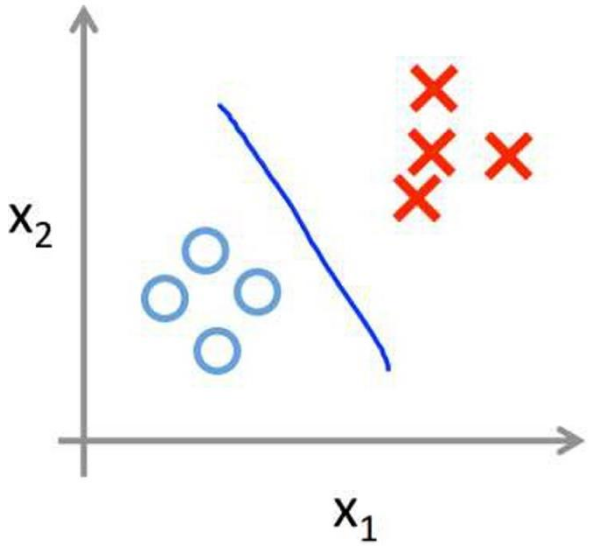


有监督学习（supervised learning）

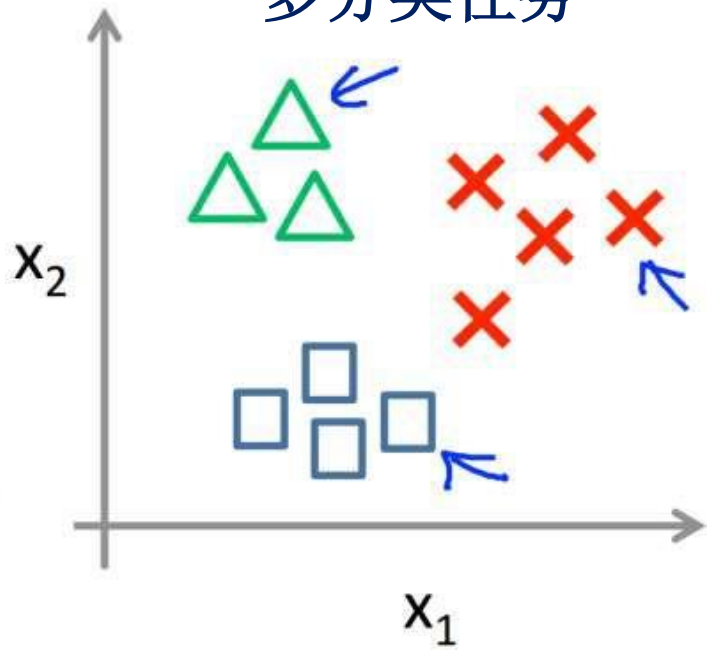
- 定义：从给定的有标注的训练数据集（已知y_i）中学习出一个假设(模型)，当新的数据到来时可以根据该假设预测结果。

- 常见任务包括分类与回归。

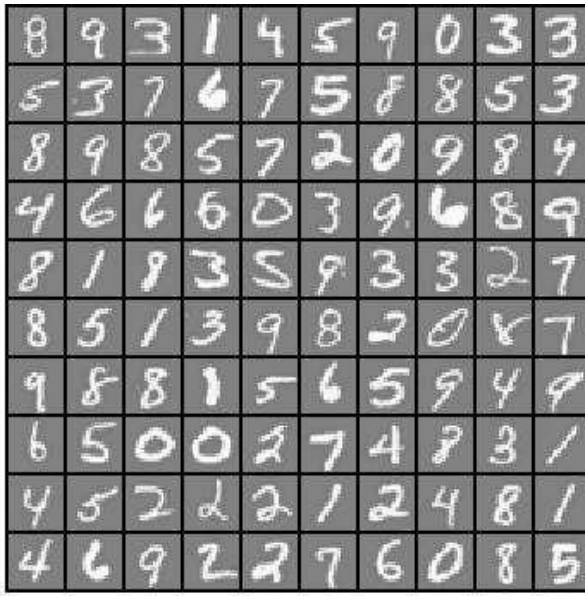
二分类任务



多分类任务



多分类任务

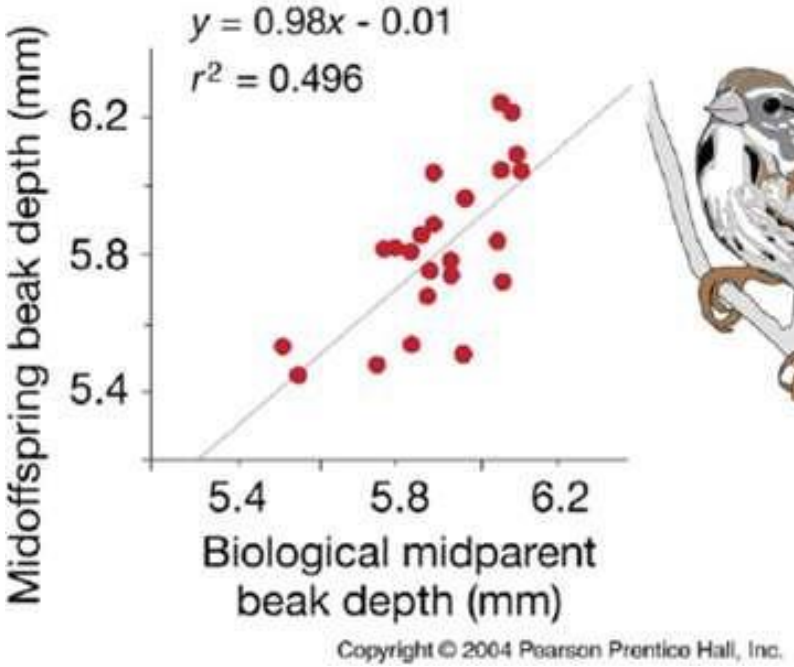


分类任务的输出是离散类别

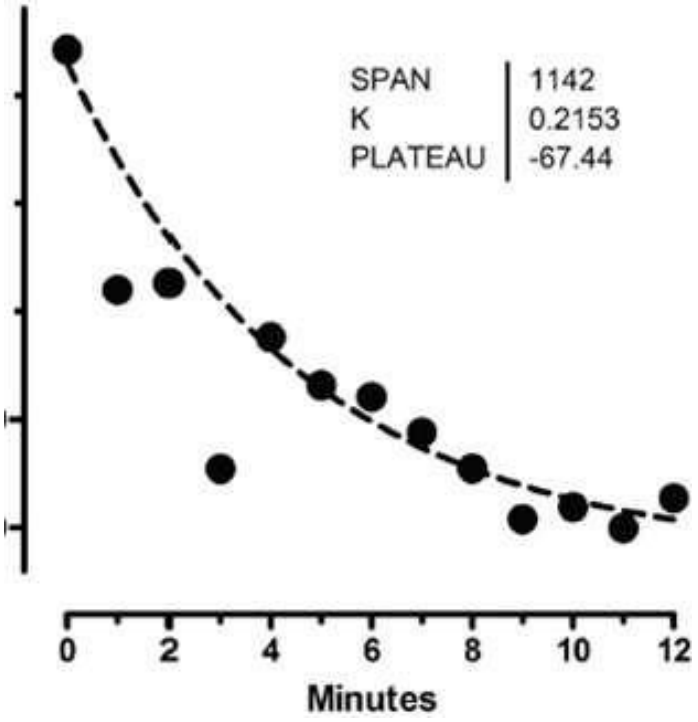
有监督学习（supervised learning）

- **回归**：目标是预测**连续值**，即找到输入特征x与目标变量y之间的映射关系$y = f(x;\theta)$

线性回归



非线性回归



有监督学习（supervised learning）

- 分类 **vs.** 回归

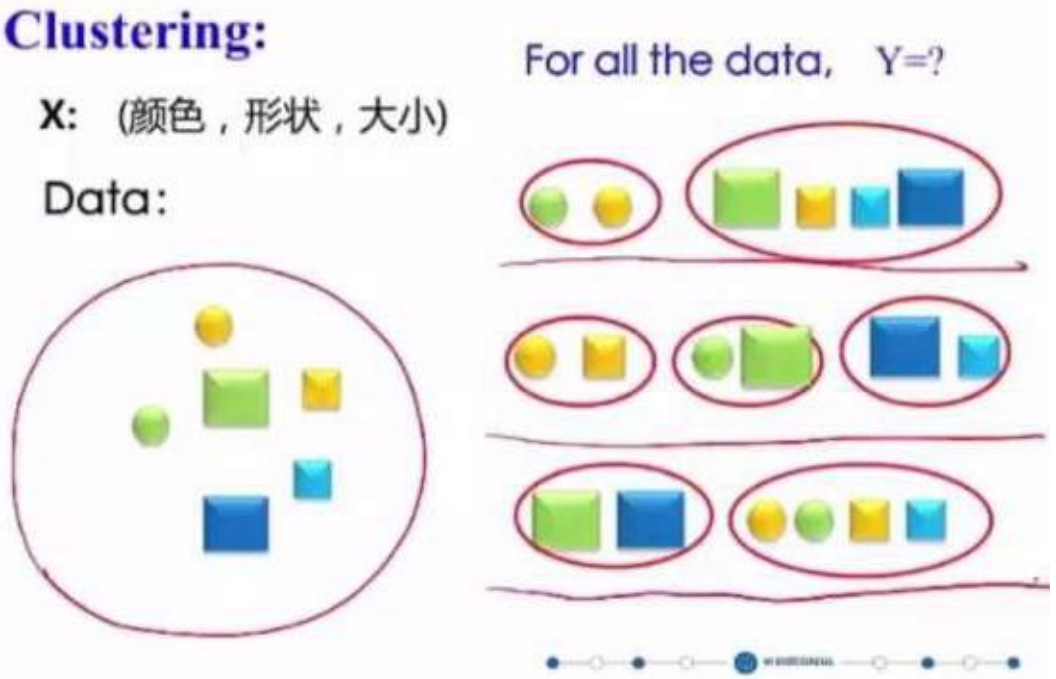
	分类	回归
目标	预测**离散类别** （如0/1，多类别）	预测**连续数值** （如房价、气温）
输出类型	类别标签 （如“猫/狗”）	实数值 （如15.7°C,¥250w）
决策边界	划分不同类别区域	近似数值关系的曲线或函数
应用场景	图像分类、文本情感语义分类	房价预测、销量预测、气温预测

如果输出是类别（离散值）→ 分类任务
如果输出是数值（连续值）→ 回归任务

无监督学习（unsupervised learning）

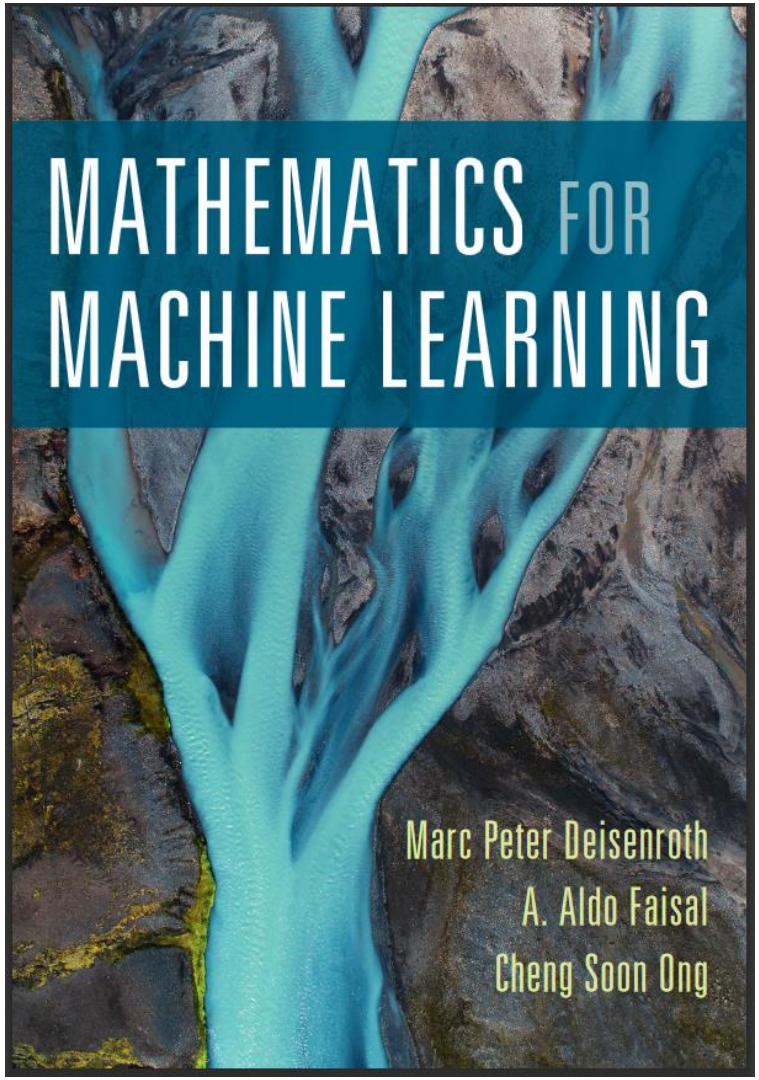
- **定 义 ：** 基 于 **没有标注的训练数据集（仅包含x_i, 不包含y_i ）**，需要根据数据间的统计规律对数据集进行分析，从数据中发现隐藏的模式或结构，而不是进行明确的分类或预测。
- **常见方法**：聚类、降维。

聚类：将数据按相似性分成不同组



必备的数学知识

- 微积分
- 线性代数、矩阵理论
- 概率论与数理统计
- 最优化方法



https://mml-book.github.io/book/mml-book.pdf


Thank You!