

# 机器学习概论

主讲：高阳，李文斌

<http://cs.nju.edu.cn/rl>, 2021.3.02

# 主讲：高阳



1997-2000，南京大学攻读博士学位

博士论文题目：

多agent强化学习研究

目前任：

- ▣ 南京大学计算机系副主任，南京大学健康医疗大数据国家研究院常务副院长
- ▣ 中国人工智能学会机器学习专委会副主任、粒计算与知识发现专委会副主任，智能服务专委会副主任
- ▣ 中国计算机学会人工智能与模式识别专委会秘书长/常委
- ▣ 江苏省人工智能学会副理事长
- ▣ 2018年度江苏省科学技术二等奖、2017年度吴文俊人工智能自然科学二等奖

# 主讲：李文斌



2015-2019，南京大学攻读博士学位

博士论文题目：

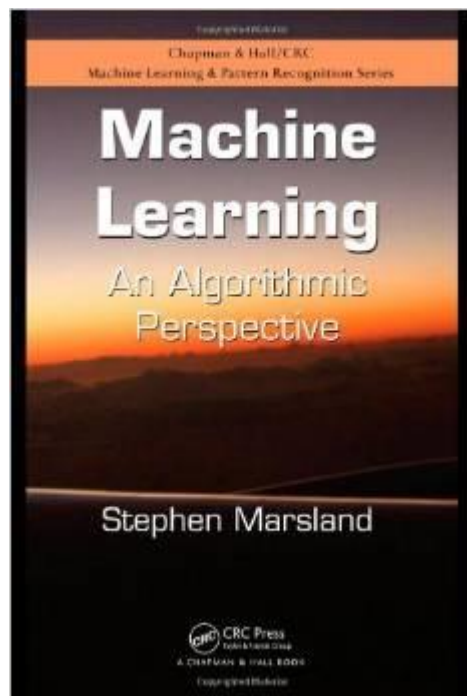
基于度量的小样本图像分类

目前任：

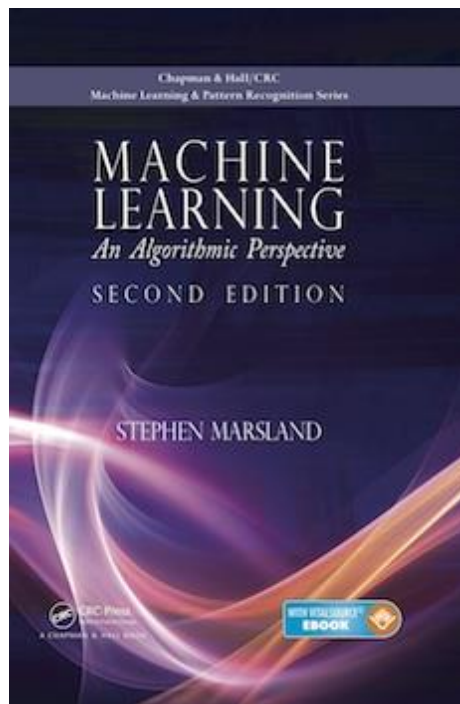
- ▣ 南京大学计算机科学与技术系，助理研究员
- ▣ 2020年度，江苏省计算机学会优秀博士学位论文

# 课程安排

# 教材



第一版



第二版



中文版

英文第二版、中文版的电子稿将分享到课程群。欢迎大家对中文版进行勘误。

# 章节内容

- 第一讲 机器学习概论
- 第二讲 神经元网络
- 第三讲 多层感知机
- 第四讲 维度约简
- 第五讲 概率学习
- 第六讲 支持向量机

考虑到综合实验和任课教师的工作安排，授课次序不严格按此排列。

# 章节内容

- 第七讲 优化和搜索
- 第八讲 演化学习
- 第九讲 强化学习
- 第十讲 决策树学习
- 第十一讲 集成学习
- 第十二讲 无监督学习

考虑到综合实验和任课教师的工作安排，授课次序不严格按此排列。

# 授课方式

## ■ 授课方式

- 第一、二周：腾讯会议直播(主讲教师)
- 第一、二周：课件录屏(主讲教师)
- 如疫情缓和：从第三周起恢复为线下上课
- 实验辅导和检查(助教和支持团队)

■ 助教团队：王健琦、杨雪松、陈嘉言

■ 支持团队：顾峥博士生、董绍康博士生、葛振兴博士生等



# 考核方式

## ■ 考核方式

- 期末闭卷考试 40分
- 综合实验 30分 (4题中选作1题, 每5人组1队)
- 课后必做小实验 20分 (5题, 每题4分)
- 课堂考勤 10分 (每缺课1次, 扣1分, 直至扣完)

# 综合实验一

## ■ 风格迁移

风格迁移是将一张图像的内容和另一张图像的风格进行融合，生成一张艺术画图像的过程。其输入是一张内容图和一张风格图，输出是图像风格迁移之后的结果。神经风格迁移是指一类通过神经网络进行风格迁移的方法。其主要代表方法有Neural Style、WCT、AdaIN等。



# 综合实验一

## 漫画生成

内容：

- （1）前期准备：深度学习基础知识、深度学习框架的搭建和使用。
- （2）算法设计：实现主流的基于深度学习的风格迁移算法（如Neural Style、AdaIN、WCT、Style Swap等）。
- （3）系统研发：基于算法开发相应的漫画生成系统，能够对输入照片进行漫画风格的风格迁移，并支持多种不同的输入风格。

参考：<http://style.airi.kr/demo>

目标：开发一套漫画生成系统，能够将输入照片转换为漫画风格，并完善相关技术文档。

负责人：博士研究生顾峥

# 综合实验二

## ■ RLCard

RLCard是一个用于牌类游戏强化学习研究的开源工具包，其接口简单易用，支持多种牌类环境。RLCard 的目标是在强化学习与非完美信息博弈之间搭建桥梁，推动强化学习研究在多智能体、高维状态和动作空间以及稀疏奖励领域的进步。融合了中西方最流行的几种牌类游戏（包括斗地主、麻将、21 点、德州扑克、UNO 等）。

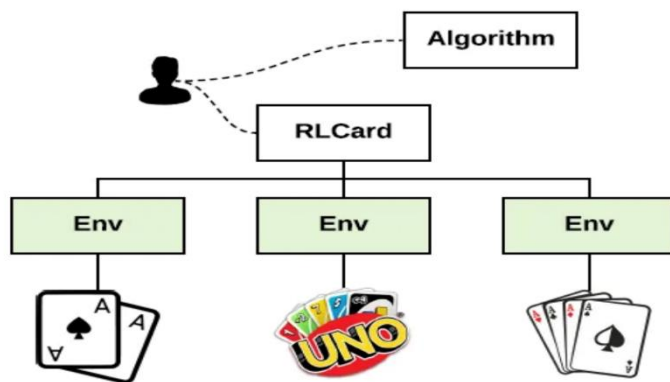


Figure 1: An overview of RLCard. It supports various styles of card games, such as betting games, Chinese Poker, and boarding games, wrapped by easy-to-use interfaces.

# 综合实验二

## 基于机器学习的掼蛋AI

内容：

- （1）巩固经典博弈形式与博弈均衡求解方法等基础知识。
- （2）学习非完全信息下博弈抽象与求解的现有方法。
- （3）研究领域内的最新进展。
- （4）针对掼蛋进行算法针对性设计。

目标：实现一个人类水平的掼蛋AI算法，能够实现人机对弈。

负责人：博士研究生葛振兴、博士研究生孟林建

# 综合实验三

## ■ SMAC

SMAC是Github上的一个用于在暴雪星际争霸2上进行多智能体协同强化学习（MARL）的环境。SMAC用了暴雪星际争霸2的机器学习API和DeepMing的PySC2为智能体与星际争霸2的交互提供了友好的接口，方便开发者观察和执行行动。



# 综合实验三

## 多智能体强化学习博弈系统

内容：

- (1) 学习深度学习、多智能体强化学习基础知识；
- (2) 通过Spinning Up \ Rllab等开源框架学习典型强化学习模型和算法；
- (3) 学习VDN,QMIX,MADDPG等多智能体强化学习典型模型和算法，实现各种AI算法自博弈；
- (4) 学会在MPE(multiagent-particle-envs)等经典环境中验证各种算法的有效性；
- (5) 挑战典型算法中尚未解决的问题，修改并完善算法；

目标：掌握多智能体深度强化学习核心技术,最终能够在经典场景中复现、改善算法框架。

负责人：博士研究生 董绍康

# 综合实验四

## 无人机目标跟踪与定位

内容：

- （1）前期准备：目标检测与跟踪、无人机图像识别、无人机控制
- （2）算法设计：设计一个无人机目标跟踪与定位算法，能够帮助无人机在指定范围内对给定目标进行定位。
- （3）系统研发：根据所设计算法，开发一个无人机目标定位系统，并在无人机上进行实验验证。

支持：DJI无人机\*2

目标：设计一个无人机目标定位系统，能够帮助无人机在指定范围内对给定目标进行定位，并完成相应的设计和技术文档。

负责人：博士研究生顾峥



# 课后必做实验

- 基本机器学习算法设计，提交报告

- 作业安排(5题，每题4分)

- 神经网络 (助教，邮箱:)

- SVM (助教，邮箱:)

- 强化学习 (助教，邮箱:)

- K-Means (助教，邮箱:)

- 决策树 (助教，邮箱:)

# 课外学习

## 国际学术组织

1. IJCAI, International Joint Conference on Artificial Intelligence,  
<http://ijcai.org>.
2. AAI, Association for the Advancement of Artificial Intelligence,  
<http://www.aaai.org>.
3. IMLS, International Machine Learning Society,  
<http://www.machinelearning.org>.
4. IFAAMAS, International Foundation for Autonomous Agents and  
Multiagent Systems, <http://www.aamas-conference.org>.

# 课外学习

## 国际学术期刊 (selected from CCF-A and CCF-B)

(人工智能与模式识别)			
A类			
序号	刊物简称	刊物全称	网址
1	AI	Artificial Intelligence	Elsevier <a href="http://www.journals.elsevier.com/artificial-intelligence/">http://www.journals.elsevier.com/artificial-intelligence/</a>
2	TPAMI	IEEE Trans on Pattern Analysis and Machine Intelligence	IEEE <a href="http://www.computer.org/portal/web/tpami/home">http://www.computer.org/portal/web/tpami/home</a>
3	IJCV	International Journal of Computer Vision	Springer <a href="http://www.springer.com/journal/11223">http://www.springer.com/journal/11223</a>
4	JMLR	Journal of Machine Learning Research	MIT Press <a href="http://www.jmlr.org/">http://www.jmlr.org/</a>
B类			
序号	刊物简称	刊物全称	网址
1	TAP	ACM Transactions on Applied Perception	ACM <a href="http://tap.acm.org/">http://tap.acm.org/</a>
2	TSLP	ACM Transactions on Speech and Language Processing	ACM <a href="http://tslp.acm.org/">http://tslp.acm.org/</a>
3		Computational Linguistics	MIT Press <a href="http://www.mitpressjournals.org/doi/cv">http://www.mitpressjournals.org/doi/cv</a>
4	CVIU	Computer Vision and Image Understanding	Elsevier <a href="http://www.elsevier.com/locate/cviu">http://www.elsevier.com/locate/cviu</a>
5	DKE	Data and Knowledge Engineering	Elsevier <a href="http://www.journals.elsevier.com/data-and-knowledge-engineering/">http://www.journals.elsevier.com/data-and-knowledge-engineering/</a>
6		Evolutionary Computation	MIT Press <a href="http://www.mitpressjournals.org/doi/evco">http://www.mitpressjournals.org/doi/evco</a>
7	TAC	IEEE Transactions on Affective Computing	IEEE <a href="http://www.computer.org/portal/web/tac">http://www.computer.org/portal/web/tac</a>
8	TASLP	IEEE Transactions on Audio, Speech, and Language Processing	IEEE <a href="http://www.speechprocess.org/publications/periodicals/taslp/">http://www.speechprocess.org/publications/periodicals/taslp/</a>
9	TEAC	IEEE Transactions on Evolutionary Computation	IEEE <a href="http://www.computer.org/portal/web/teac">http://www.computer.org/portal/web/teac</a>
10	TFS	IEEE Transactions on Fuzzy Systems	IEEE <a href="http://tsf.elsevier.com/elsevier-transactions-on-fuzzy-systems.html">http://tsf.elsevier.com/elsevier-transactions-on-fuzzy-systems.html</a>
11	TRNLS	IEEE Transactions on Neural Networks and Learning Systems	IEEE <a href="http://tsf.elsevier.com/elsevier-transactions-on-neural-networks-and-learning-systems.html">http://tsf.elsevier.com/elsevier-transactions-on-neural-networks-and-learning-systems.html</a>
12	IJAR	International Journal of Approximate Reasoning	Elsevier <a href="http://www.journals.elsevier.com/international-journal-of-approximate-reasoning/">http://www.journals.elsevier.com/international-journal-of-approximate-reasoning/</a>
13	JAIR	Journal of AI Research	AAAI <a href="http://www.jair.org/">http://www.jair.org/</a>
14	JAR	Journal of Automated Reasoning	Springer <a href="http://www.springer.com/computer/foundations/journal/13217">http://www.springer.com/computer/foundations/journal/13217</a>
15	JSLHR	Journal of Speech, Language, and Hearing Research	American Speech-Language Hearing Association <a href="http://jshr.asha.org/">http://jshr.asha.org/</a>
16		Machine Learning	Springer <a href="http://www.springer.com/computer-ai/journal/15564">http://www.springer.com/computer-ai/journal/15564</a>

Artificial Intelligence, IEEE Trans on Pattern Analysis and Machine Intelligence, International Journal of Computer Vision, Journal of Machine Learning Research, Evolutionary Computation, IEEE Trans on Evolutionary Computation, IEEE Trans on Neural Network and Learning Systems, Journal of AI Research, Machine Learning, Neural Computation, Neural Networks, Pattern Recognition, Autonomous Agents and Multi-Agent Systems .....

<http://www.ccf.org.cn/sites/ccf/biaodan.jsp?contentId=2567814757420>

# 课外学习

## 国际学术会议 (selected from CCF-A and CCF-B)

AAAI Conference on Artificial Intelligence, IEEE Conference on Computer Vision and Pattern Recognition, International Conference on Computer Vision, International Joint Conference on Artificial Intelligence, Annual Conference on Computational Learning Theory, Annual Conference on Neural Information Processing Systems, International Conference on Principles of Knowledge Representation and Reasoning, International Conference on Uncertainty in Artificial Intelligence, International Joint Conference on Autonomous Agents and Multi-agent Systems.....

<http://www.ccf.org.cn/sites/ccf/biaodan.jsp?contentId=2567814757420>

（人工智能与模式识别）				
一、A类				
序号	会议简称	会议全称	出版社	网址
1	AAAI	AAAI Conference on Artificial Intelligence	AAAI	<a href="http://www.aaai.org">http://www.aaai.org</a>
2	CVPR	IEEE Conference on Computer Vision and Pattern Recognition	IEEE	<a href="http://www.pami.org/cvpr13/">http://www.pami.org/cvpr13/</a>
3	ICCV	International Conference on Computer Vision	IEEE	<a href="http://www.iccv2013.org/">http://www.iccv2013.org/</a>
4	ICML	International Conference on Machine Learning	ACM	<a href="http://icml.cc2013/">http://icml.cc2013/</a>
5	IJCAI	International Joint Conference on Artificial Intelligence	Morgan Kaufmann	<a href="http://www.ijcai.org">http://www.ijcai.org</a>
二、B类				
序号	会议简称	会议全称	出版社	网址
1	COLT	Annual Conference on Computational Learning Theory	Springer	<a href="http://orfs.princeton.edu/conferences/colt2013/">http://orfs.princeton.edu/conferences/colt2013/</a>
2	NIPS	Annual Conference on Neural Information Processing Systems	MIT Press	<a href="http://www.nips.cc">http://www.nips.cc</a>
3	ACL	Annual Meeting of the Association for Computational Linguistics	ACL	<a href="http://acl2013.org/program/index.html">http://acl2013.org/program/index.html</a>
4	EMNLP	Conference on Empirical Methods in Natural Language Processing	ACL	<a href="http://www.sigstat.org">http://www.sigstat.org</a>
5	ECAI	European Conference on Artificial Intelligence	IOS Press	<a href="http://www.ecai2013.upit.ro/?i=2542">http://www.ecai2013.upit.ro/?i=2542</a>
6	ECCV	European Conference on Computer Vision	Springer	<a href="http://eccv2012.unibz.it">http://eccv2012.unibz.it</a>
7	ICRA	IEEE International Conference on Robotics and Automation	IEEE	<a href="http://www.icra2013.org/">http://www.icra2013.org/</a>

# 机器学习概论

# 机器学习概论

- 机器学习系统
- 系统建模和模型选择
- 统计学基本概念
- 机器学习技术新进展

# 机器学习系统

# 人工智能的三大基石技术之一

- 推理

- 知识

- 学习

- ✓ 利用**经验****改善**系统的**性能**



# 严格定义

## ■ 机器学习(经典)

- ✓ 学习是一个蕴含特定目的的知识获取过程，其内部表现为新知识的不断建立和修正，而外部则表现为性能改善。
- ✓ 经验(数据和常识)，在此更多指的是数据，即从数据中总结规律用于将来的预测。
- ✓ 具体如何学习--- 视数据包含的信息相应学习。

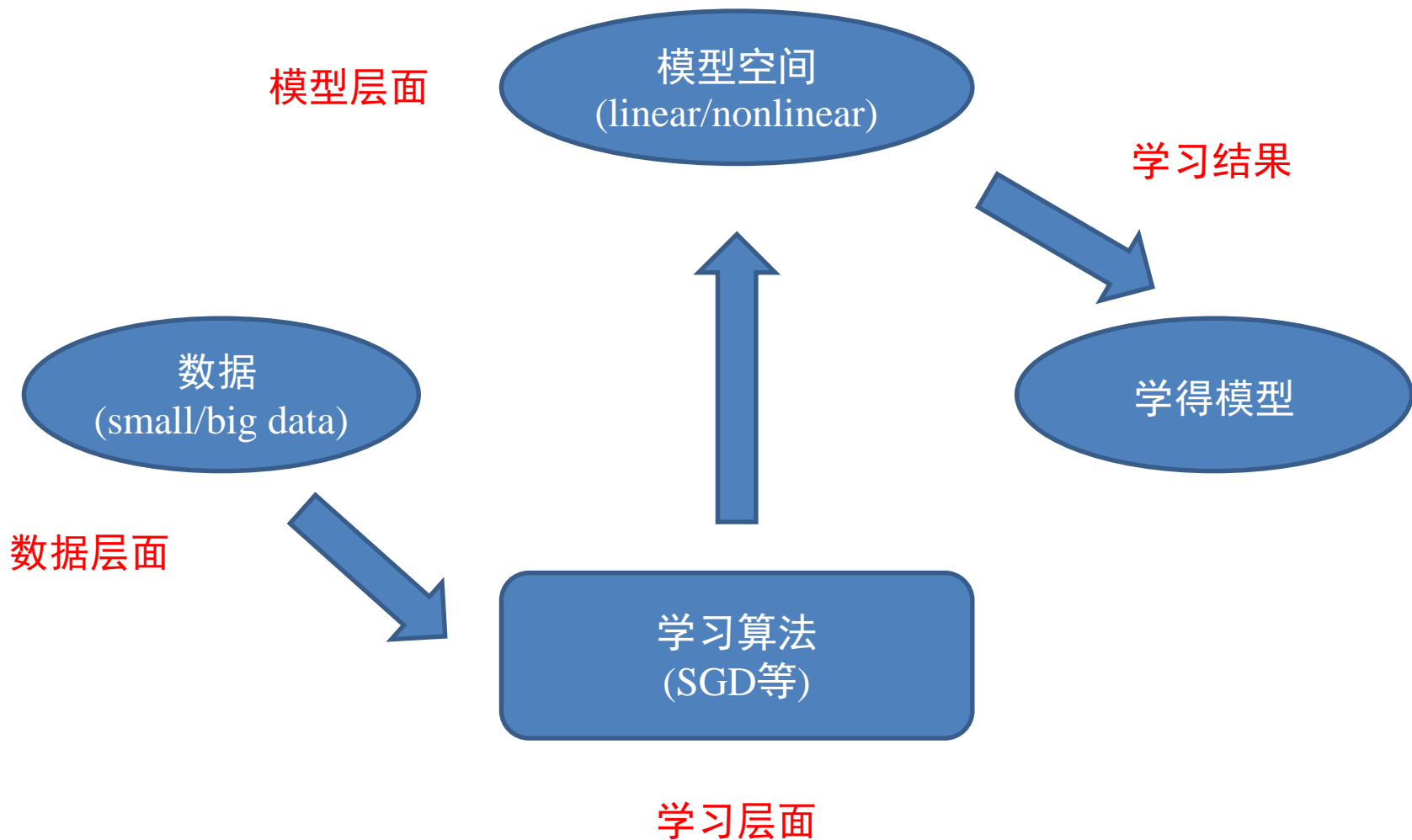
# 通俗定义

## ■ 机器学习(现代, 特别指统计机器学习)

### ✓ 任何通过数据训练的学习算法都属于机器学习

- ✓ 线性回归(Linear Regression)
- ✓ K-均值聚类(K-means)
- ✓ 主成分分析(Principal Component Analysis-PCA)
- ✓ 决策树(Decision Trees)和随机森林(Random Forest)
- ✓ 支持向量机(Support Vector Machines)
- ✓ 人工神经网络(Artificial Neural Networks)

# 学习系统



# 数据层面

## ■ 数据类型或特点

- ✓ 静态与动态 (如照片与视频等)
- ✓ 小数据与大数据 (如异常&正常+类不平衡/代价敏感)
- ✓ 同质与异质 (如实数型与符号&实数的混合等)
- ✓ 单态与多态 (如仅图像与声音&图像等)
- ✓ 小类数与大类数 (如性别与个体识别)
- ✓ 缺失&带噪数据
- ✓ 高维数据&非数值数据 (如串、图等)
- ✓ .....

# 模型和学习层面

## ■ 模型层面

- ✓ 形式：线性模型/非线性模型
- ✓ 体系：浅层/深度/递归

## ■ 学习层面

- ✓ 经典
- ✓ 现代
- ✓ 混合

# 经典学习方法

## ■ 经典学习方法(-1990')

- ✓ 机械学习
- ✓ 归纳学习
- ✓ 类比学习
- ✓ 解释学习
- ✓ 决策树&森林
- ✓ 贝叶斯分类器
- ✓ 聚类

# 现代学习方法

## NSFC信息学部机器学习(06)代码体系

F060201 机器学习基础理论与方法

F060202 监督学习

F060203 弱监督学习

F060204 无监督学习

F060205 统计学习

F060206 集成学习

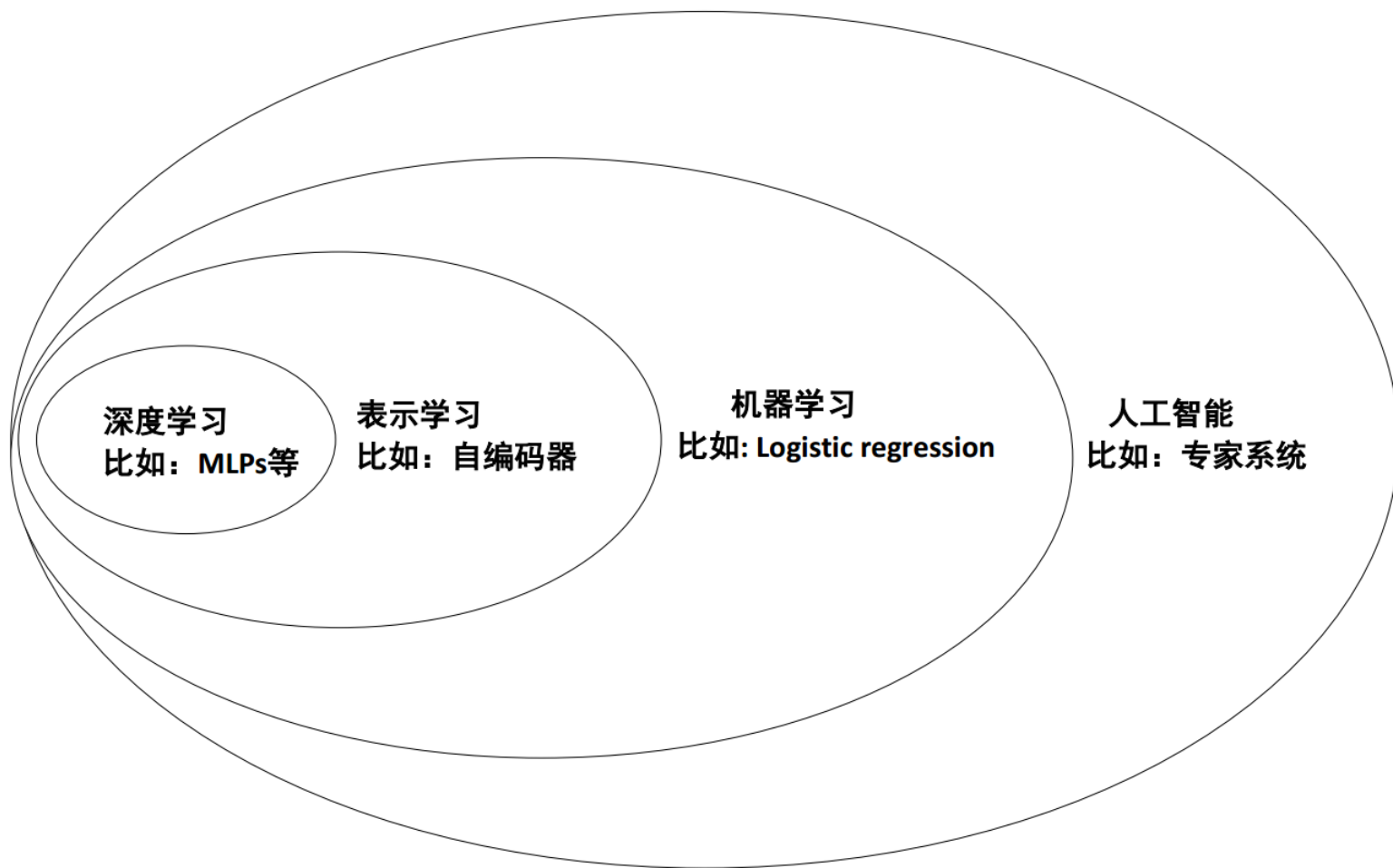
F060207 强化学习

F060208 深度学习理论与方法



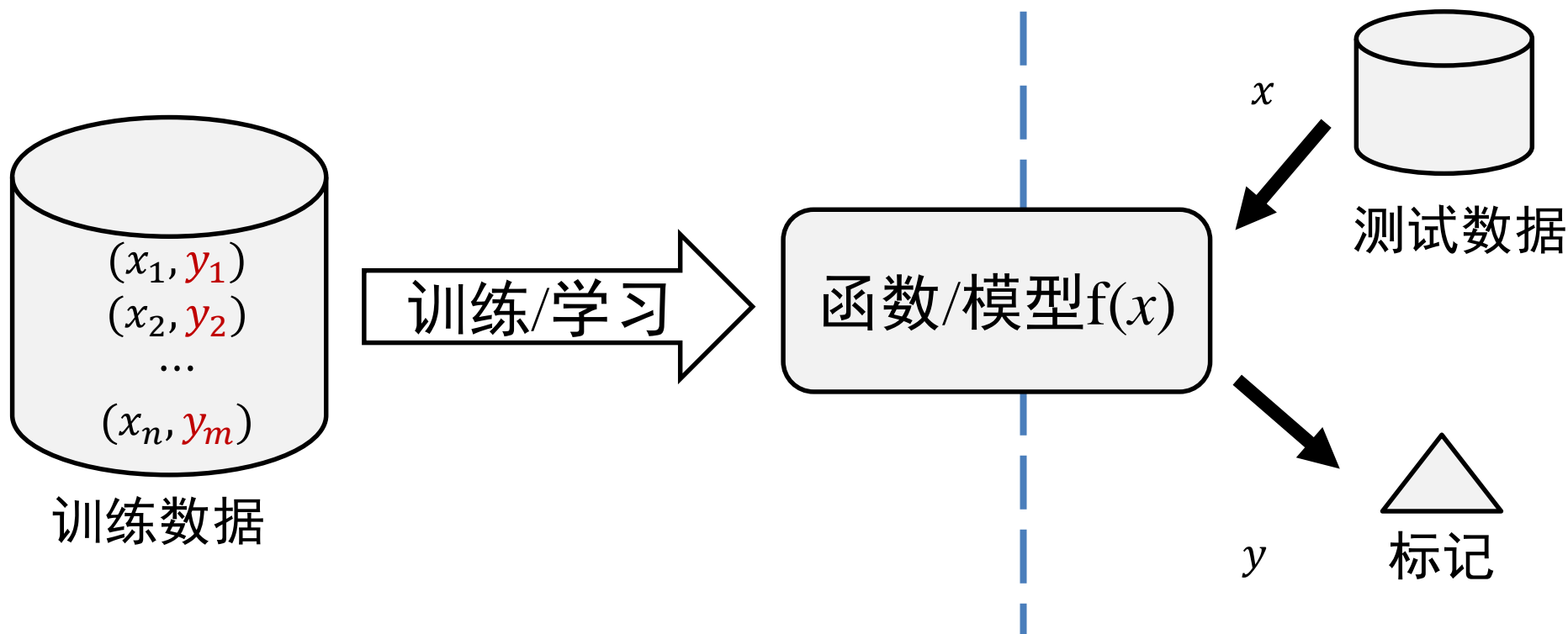
自2021年起,  
该代码体系合并为F0603

# 学习方法关系图





# 学习过程(以监督学习为例)



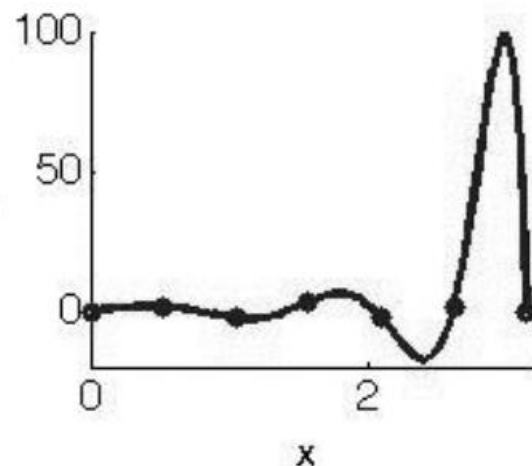
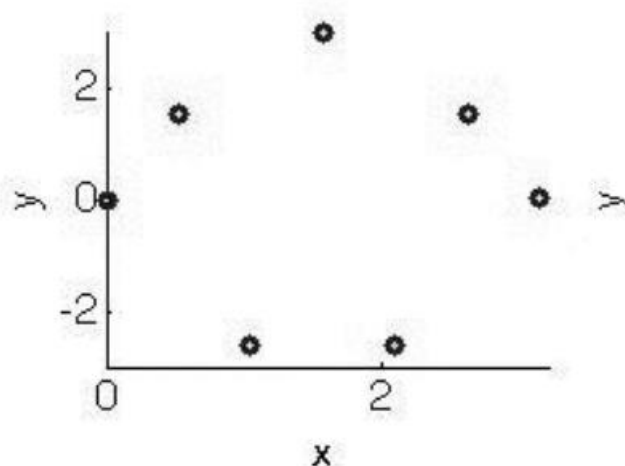
事实上,  $f(x)$ 是一个从 $x$ 到 $y$ 的映射

# 回归

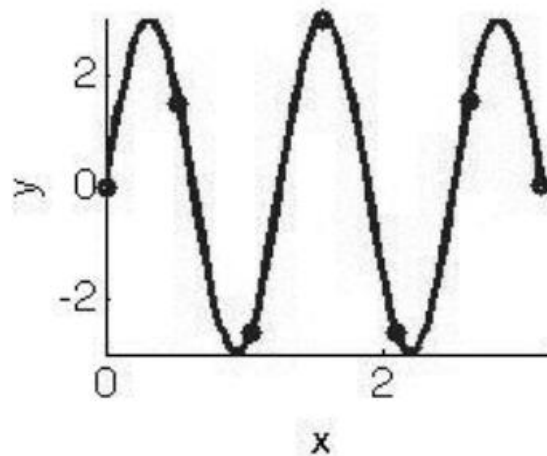
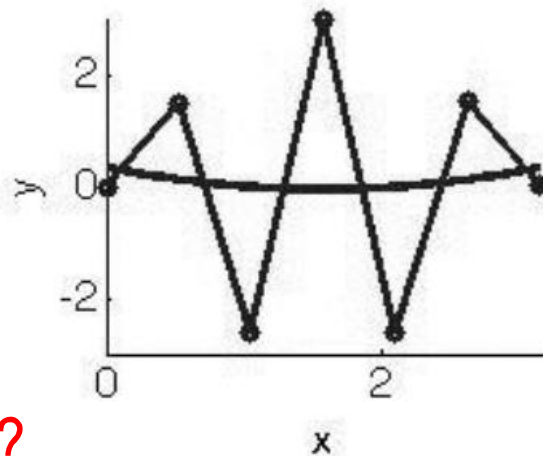
复杂的高次模型

$x$	$t$
0	0
0.5236	1.5
1.0472	-2.5981
1.5708	3.0
2.0944	-2.5981
2.6180	1.5
3.1416	0

训练数据



线性/三次模型



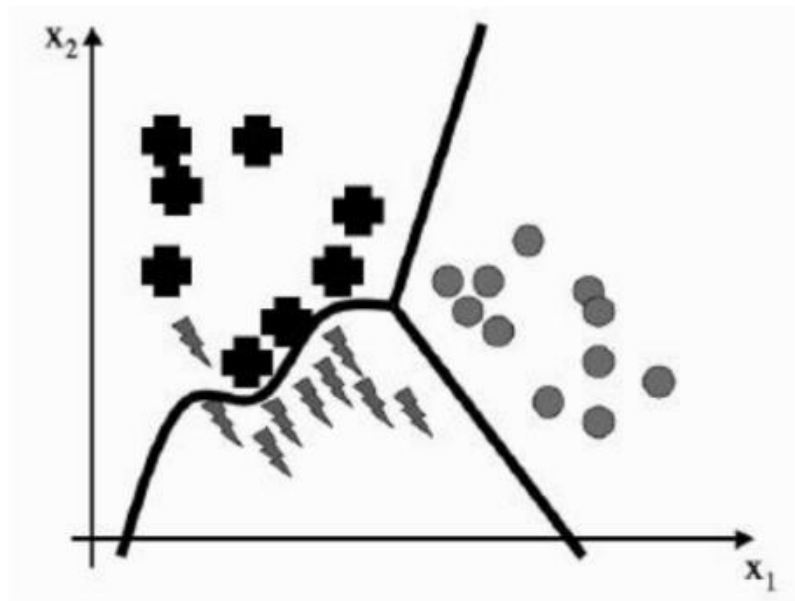
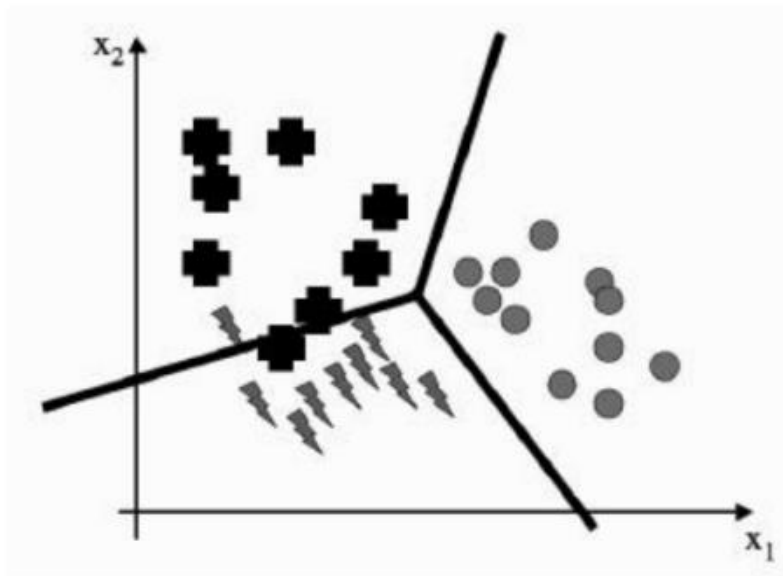
哪一个模型好呢？

真实模型/数据发生器

# 分类



5分类问题：新西兰硬币，  
<尺寸\重量, 币值>

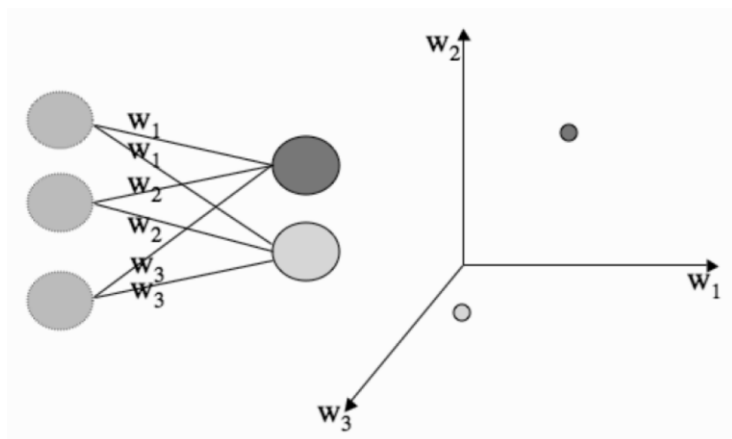


# 系统建模和模型选择

# 常规术语及其标记

常用向量或矩阵表示法：

表达机器学习技术中的向量、元素、矩阵



以神经网络为例

□ 输入：  $\mathbf{x}, x_i$

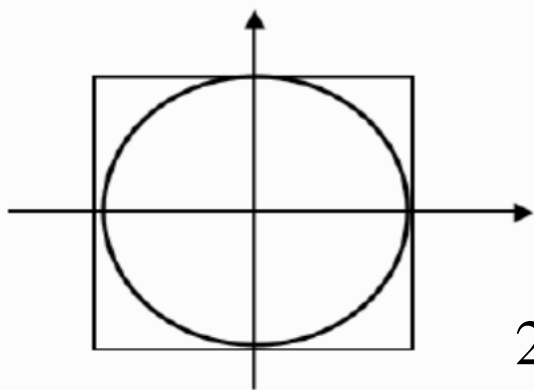
□ 权重：  $\mathbf{w}, w_{ij}$

□ 输出：  $\mathbf{y}, y(\mathbf{x}, \mathbf{w})$

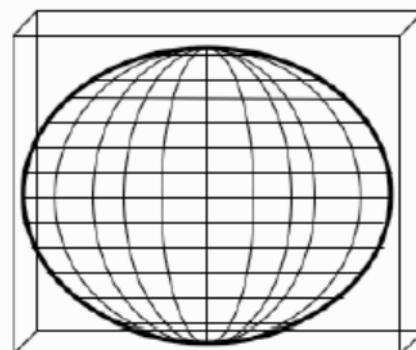
□ 目标：  $\mathbf{t}, t_j$

□ 误差：  $\mathbf{E}$

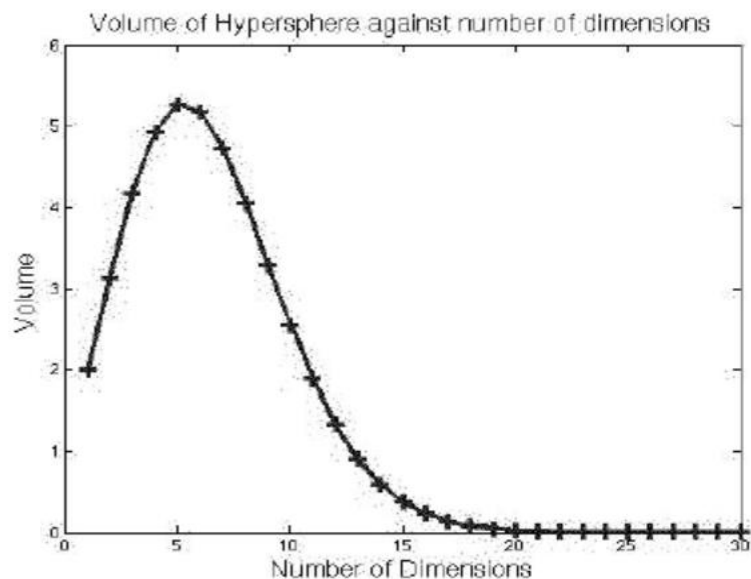
# 维数灾难



2D单位圆



3D单位球

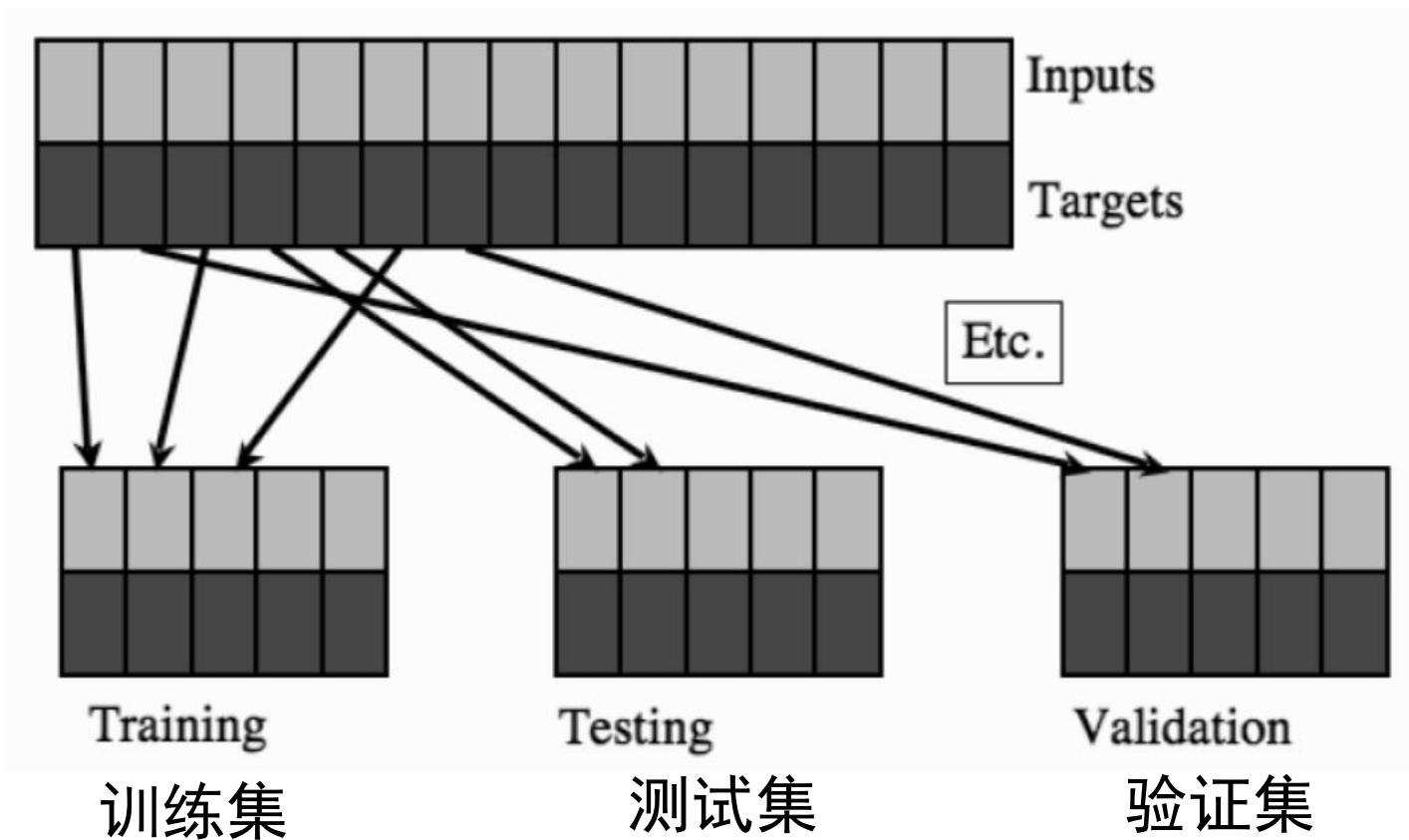


高维空间单位球体积

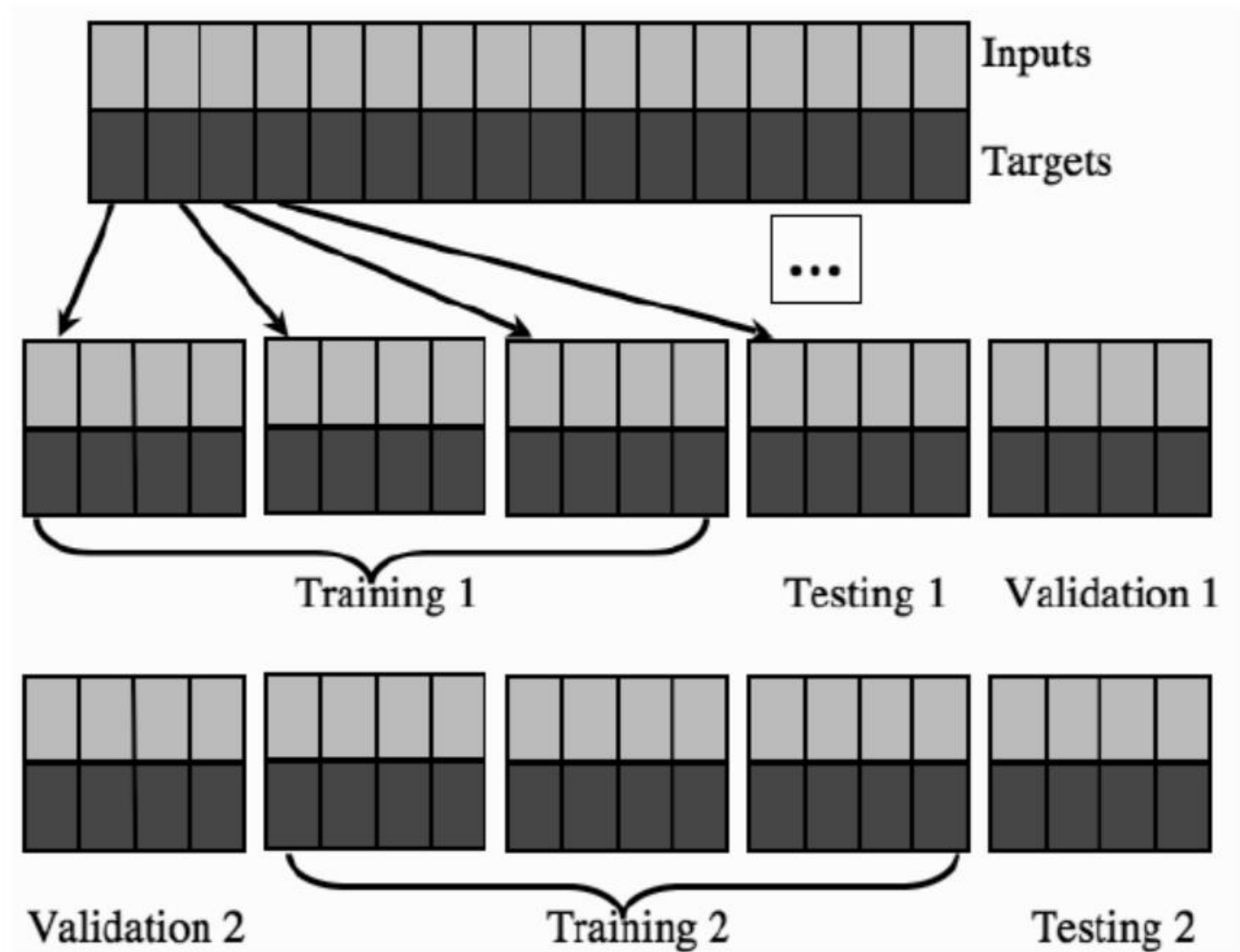
$$v_n = (2\pi/n)v_{n-2}$$

随着输入维数的增加，算法将需要更多的数据

# 数据集



# 数据集的划分



多模型数据集划分方法：

□ 留出法

□ 交叉验证



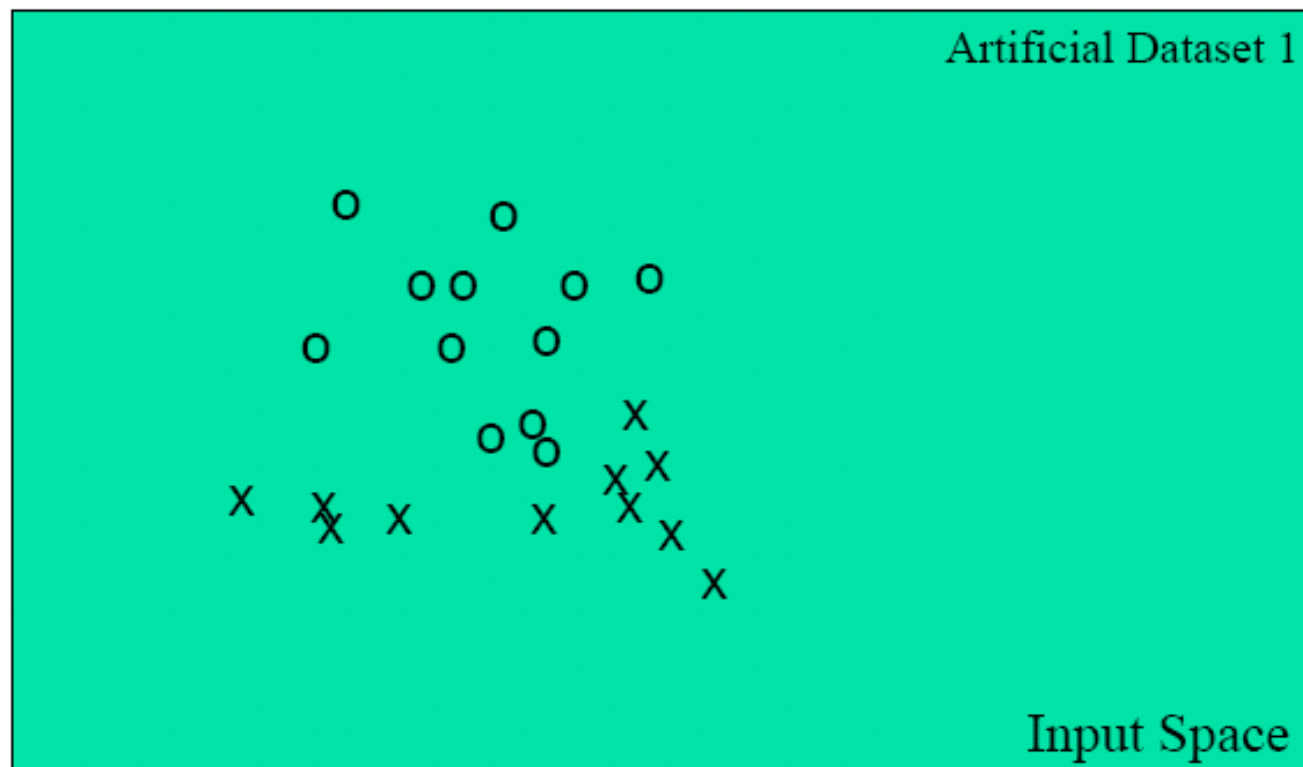
# 建模有关要素

函数或模型 $f$ 哪来？就需按先验作假设！如神经网络，依据？

## 相关要素

- ✓ **模型/映射函数** $f(\cdot)$ 刻画（如线性机, SVM, 神经网络等）
- ✓ 确定 **目标/损失函数** (如平方损失, 互熵等, 更一般的是 **凸与非凸**) 并 **优化** 获得模型
- ✓ 评测: **泛化性能** (可解释为举一反三的能力, 在未知样本上的预测能力)

# 示例

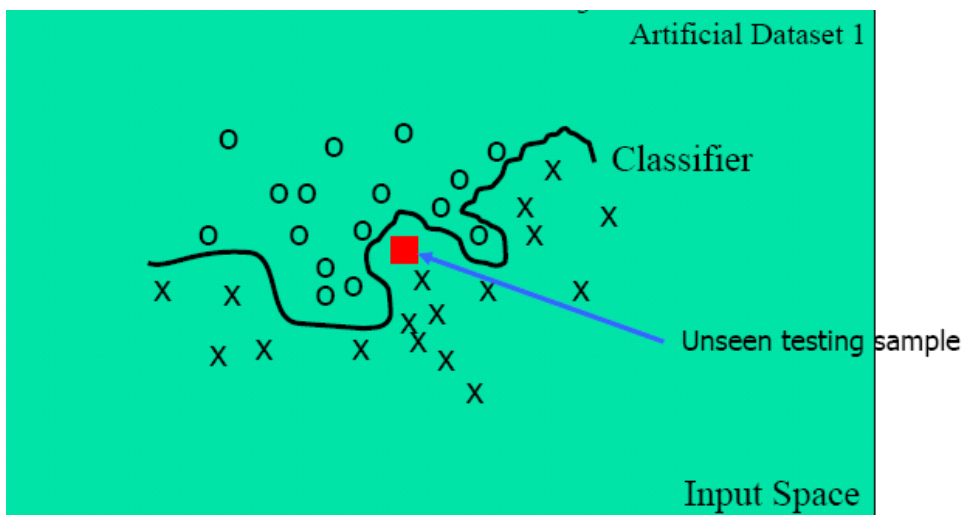


o: Training Sample in Class 1    x: Training Sample in Class 2

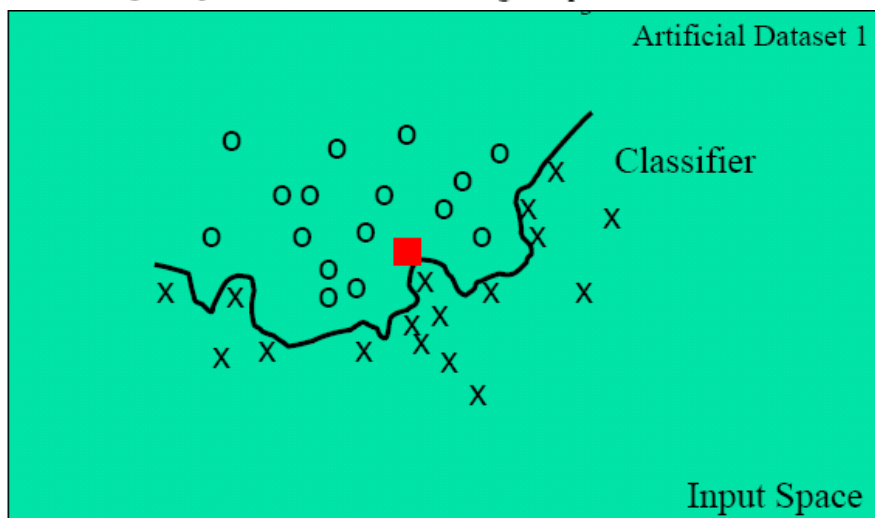
目标:

分离 2 个 类  
的 给定 样本,  
让 学得 模型  
具有 好的 预  
测 性能/行为

# 过拟合(Over-fitting)

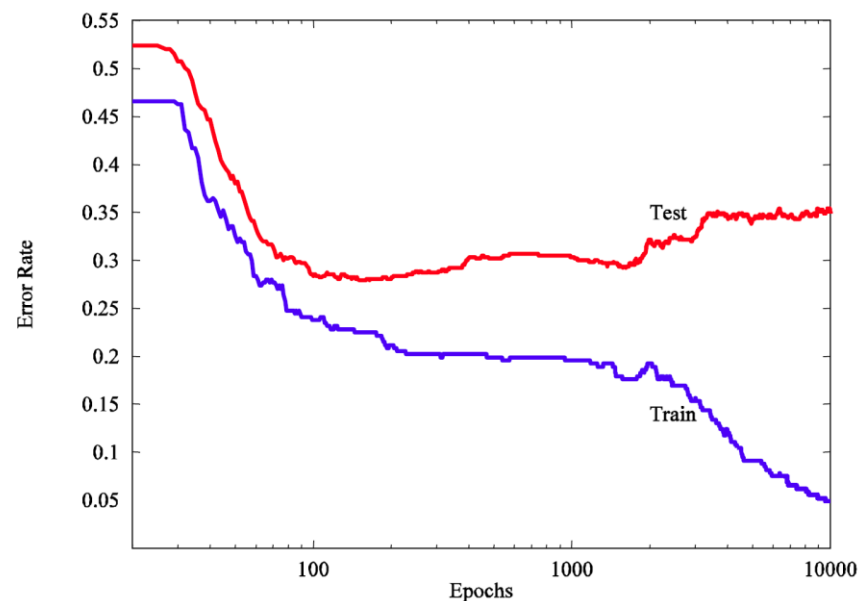


○: Training Sample in Class 1 X: Training Sample in Class 2

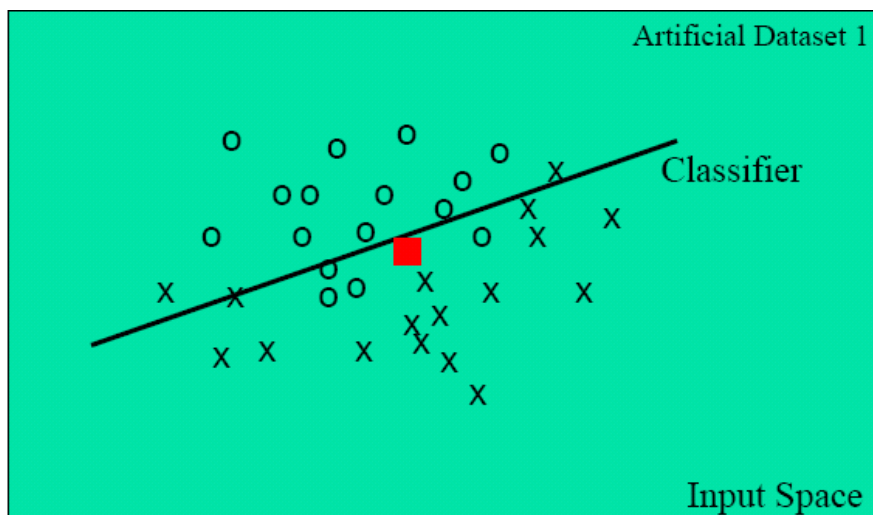


○: Training Sample in Class 1 X: Training Sample in Class 2

## 过拟合性能

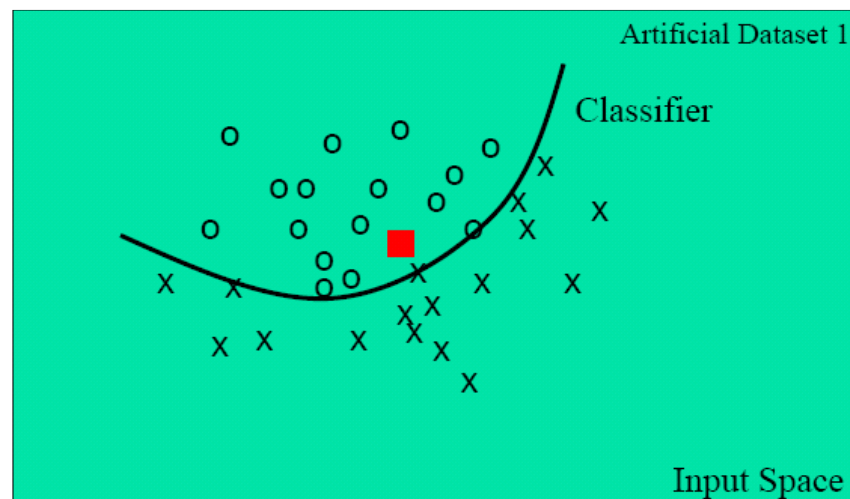


# 欠拟合和好的拟合



o: Training Sample in Class 1    x: Training Sample in Class 2

欠拟合(under-fitting)



o: Training Sample in Class 1    x: Training Sample in Class 2

好的拟合(good-fitting)

# 机器学习的共性问题

□ 有限的样本数或规模

□ 大量甚至无穷个拟合函数/模型能够满足这些给定的有限观察

==》 **病态问题!!!**

**例子：** 给定部分序列：1 3 5 ? ?

- ✓ 如何确定或选择一个拟合函数实现对先前未见过数据的良好预测，所谓的好的泛化性能；
- ✓ 困难所在：**病态问题！**
- ✓ 即小(甚至零)的训练误差但实际仅有少量模型能有好的泛化性能！

# 评价指标

## 混淆矩阵(Confusion Matrix)

		预测类			多分类
		Outputs			
		$C_1$	$C_2$	$C_3$	
真实类	$C_1$	5	1	0	
	$C_2$	1	4	1	
	$C_3$	2	0	4	

## 精度矩阵(Accuaracy Matrix)

		真实类(P/N)	
预测类 (P/N)	True Positives	False Positives	
	False Negatives	True Negatives	

## 二分类 $F_1$ 度量

精度

$$\text{Accuracy} = \frac{\#TP + \#TN}{\#TP + \#FP + \#TN + \#FN}$$

敏感率

$$\text{Sensitivity} = \frac{\#TP}{\#TP + \#FN}$$

特异率

$$\text{Specificity} = \frac{\#TN}{\#TN + \#FP}$$

查准率

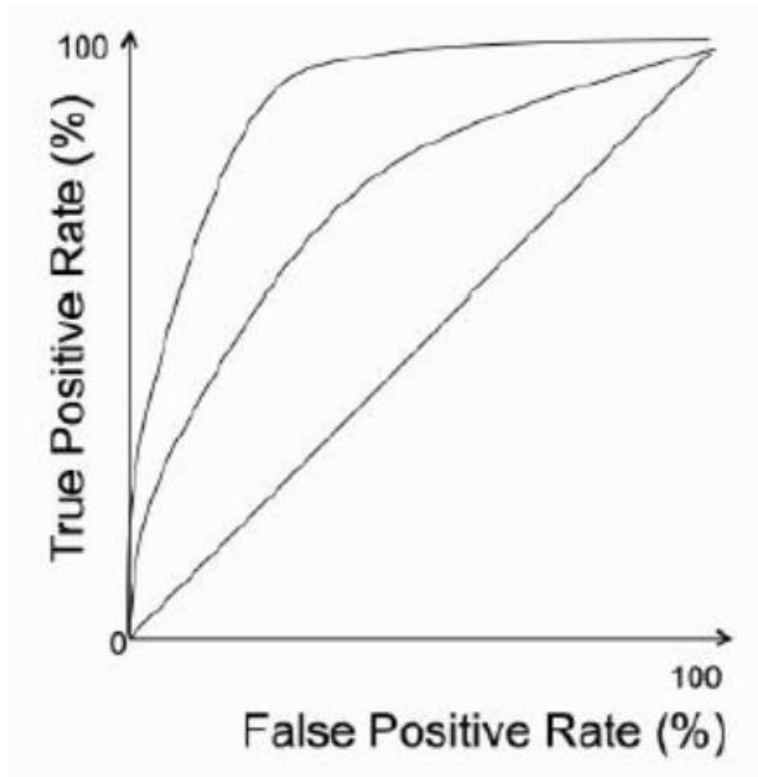
$$\text{Precision} = \frac{\#TP}{\#TP + \#FP}$$

查全率

$$\text{Recall} = \frac{\#TP}{\#TP + \#FN}$$

$$F_1 = 2 \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}} = \frac{\#TP}{\#TP + (\#FN + \#FP)/2}$$

# ROC曲线



□ 受试者工作特征(Receiver Operator Characteristic)曲线

- ✓ 用于比较不同参数分类器或者不同分类器的性能
- ✓  $(0,1)$  – 完美分类器
- ✓  $(1,0)$  – 反分类器
- ✓ 通过交叉验证将产生多个测试点
- ✓ 比较AUC，面积越大，分类器性能越好

# 不平衡数据集

## □不平衡数据集

- ✓ 正例数量与反例数量 相差巨大
- ✓ (敏感率+特异率)/2，并不能正确反应分类器处理不平衡数据时的性能
- ✓ Matthew相关系数(Matthew's Correlation Coefficient)

$$MCC = \frac{\#TP \times \#TN - \#FP \times \#FN}{\sqrt{(\#TP + \#FP)(\#TP + \#FN)(\#TN + \#FP)(\#TN + \#FN)}}$$

注: 分母如果有为0,则置为1;

Q1: 如果是多分类问题, 如何处理?



# 测量精度

## □ Measurement Precision

- ✓ 系统的可重复性：类似输入，产生相近的输出
- ✓ 物理意义 类似于 概率分布中的方差



高测量精度  
高准确度



低测量精度  
高准确度



高测量精度  
低准确度



可接受的测量精度  
低准确度

# 初探模型选择

□ No Free Lunch Theorem (没有免费午餐定理)

## 模型选择

□ 没有天生优越的学习器，只有充分利用了与问题相关先验知识的模型才是优的！

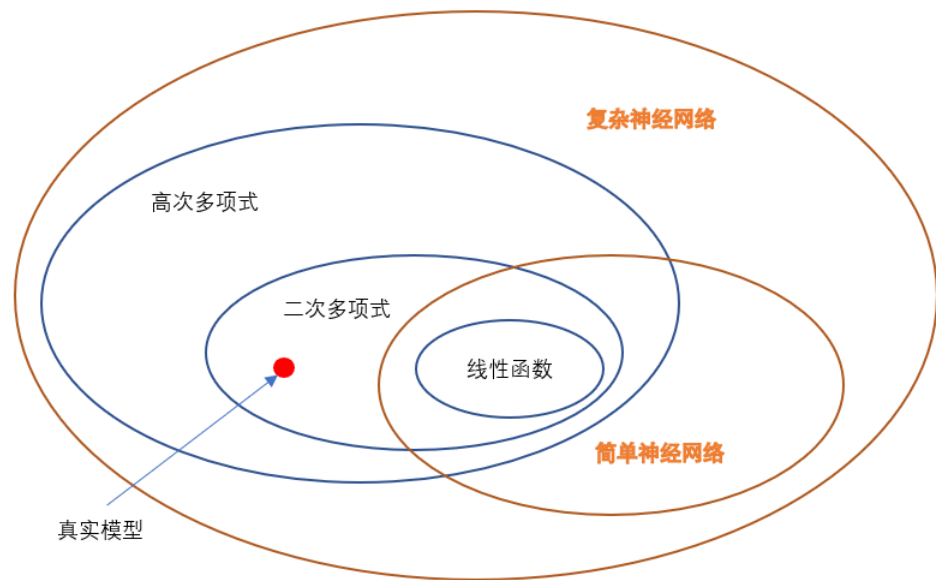
事实是：

□ 样本(经验)有限，先验甚少，因此从中所建的模型几乎没有一个是对的，只有相对好的！

# 典型方法

## 四类方法

1. 模型选择
2. 正则化/或规整化
3. 模型组合或集成
4. 多视图方法



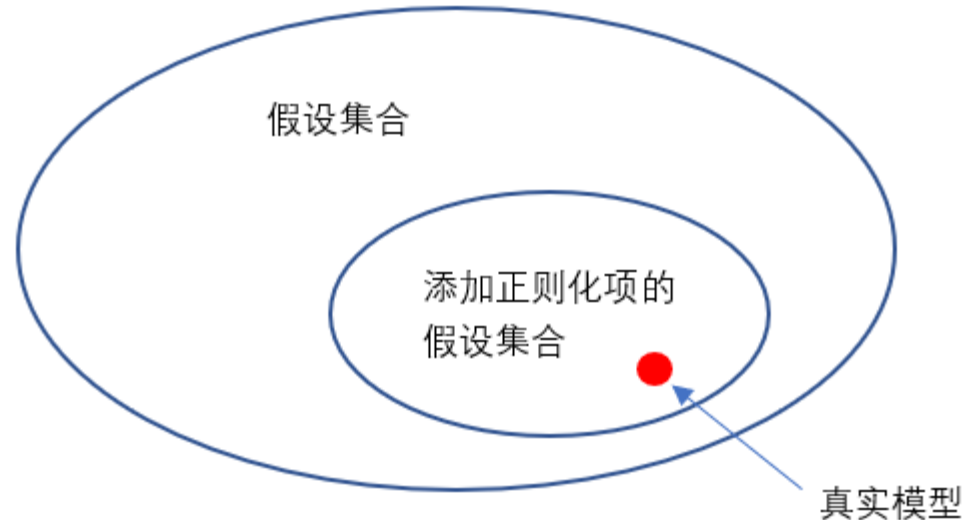
模型选择

# 为何正则化可用？

意图：病态 $\rightarrow$ 良态

所谓良态问题，满足

- ✓ 存在性
- ✓ 唯一性
- ✓ 连续性/稳定性



关键是如何转变？

# Tikhonov(吉洪诺夫)正则化

1963, Tikhonov 提出了正则化或规整化去解病态问题.

## 动机

- 借助某个辅助非负泛函/模型实现解的稳定化!
- 其中在泛函中嵌入了解或问题的先验信息
  - ✓ 如神经网络中权衰减!
  - ✓ 在深度网络中用退出(Dropout)! 早期终止,.....

# 先验的重要性

结合问题的先验去建模

Generalization(泛化)=Data(数据)+Knowledge(知识)

常用先验知识

输入与输出间的映射应当光滑(Smooth)

意即：相似输入对应相似输出！

# 丑小鸭定理

特征层面的原则

Ugly Duckling Theorem (丑小鸭定理) → 特征表示

没有天生好的特征，只有结合了与问题相关知识的才是好的。

Why?

# 统计学基本概念



# 数据集的统计量

□ 均值、中位数、众数

$$E = -1 \times \frac{199,999}{200,000} + 99,999 \times \frac{1}{200,000} = -0.5$$

□ 期望：概率加权和

□ 方差、均方根

$$\text{var}(\{\mathbf{x}_i\}) = \sigma^2(\{\mathbf{x}_i\}) = E\left((\{\mathbf{x}_i\} - \boldsymbol{\mu})^2\right) = \sum_{i=1}^N (\mathbf{x}_i - \boldsymbol{\mu})^2.$$

□ 协方差(covariance)

$$\text{cov}(\{\mathbf{x}_i\}, \{\mathbf{y}_i\}) = E(\{\mathbf{x}_i\} - \boldsymbol{\mu})E(\{\mathbf{y}_i\} - \boldsymbol{\nu})$$

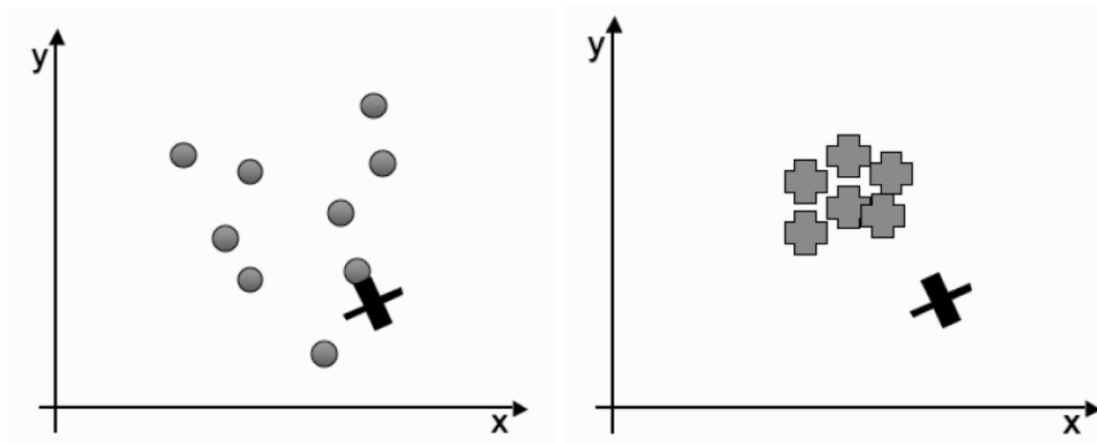
□ 协方差矩阵(covariance matrix)

$$\Sigma = \begin{pmatrix} E[(\mathbf{x}_1 - \boldsymbol{\mu}_1)(\mathbf{x}_1 - \boldsymbol{\mu}_1)] & E[(\mathbf{x}_1 - \boldsymbol{\mu}_1)(\mathbf{x}_2 - \boldsymbol{\mu}_2)] & \cdots & E[(\mathbf{x}_1 - \boldsymbol{\mu}_1)(\mathbf{x}_n - \boldsymbol{\mu}_n)] \\ E[(\mathbf{x}_2 - \boldsymbol{\mu}_2)(\mathbf{x}_1 - \boldsymbol{\mu}_1)] & E[(\mathbf{x}_2 - \boldsymbol{\mu}_2)(\mathbf{x}_2 - \boldsymbol{\mu}_2)] & \cdots & E[(\mathbf{x}_2 - \boldsymbol{\mu}_2)(\mathbf{x}_n - \boldsymbol{\mu}_n)] \\ \cdots & \cdots & \cdots & \cdots \\ E[(\mathbf{x}_n - \boldsymbol{\mu}_n)(\mathbf{x}_1 - \boldsymbol{\mu}_1)] & E[(\mathbf{x}_n - \boldsymbol{\mu}_n)(\mathbf{x}_2 - \boldsymbol{\mu}_2)] & \cdots & E[(\mathbf{x}_n - \boldsymbol{\mu}_n)(\mathbf{x}_n - \boldsymbol{\mu}_n)] \end{pmatrix}$$

理解协方差矩阵中对角线和非对角线上值的物理意义，=0、>0、<0的含义

# 马氏距离

## □ 协方差矩阵的用途



✓ ‘十’点离数据集的距离(上图哪一个最近呢)?

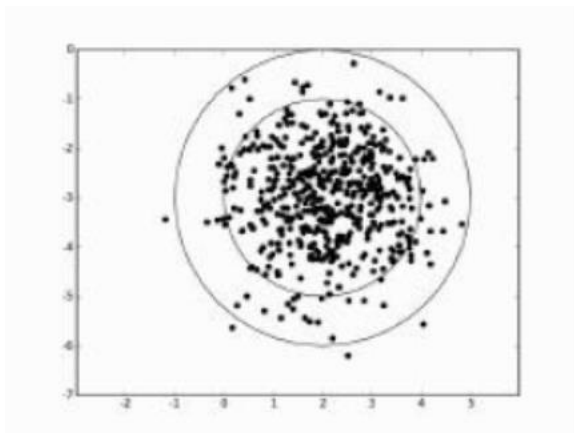
✓ 马氏距离(Mahalanobis distance)

$$D_M(\mathbf{x}) = \sqrt{(\mathbf{x} - \mathbf{u})^T \Sigma^{-1} (\mathbf{x} - \mathbf{u})}$$

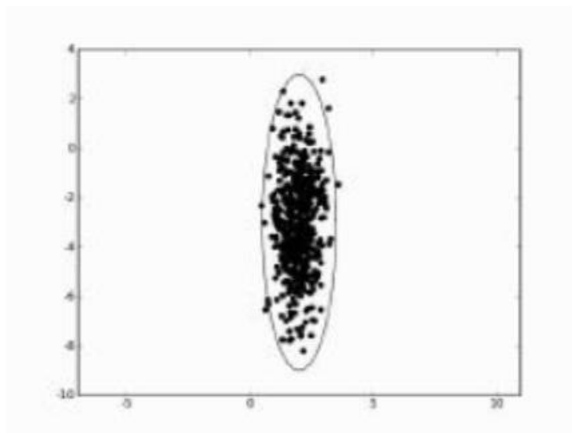
# 高斯分布

□ 高斯分布(Gaussian)或正态分布(Normal distribution)

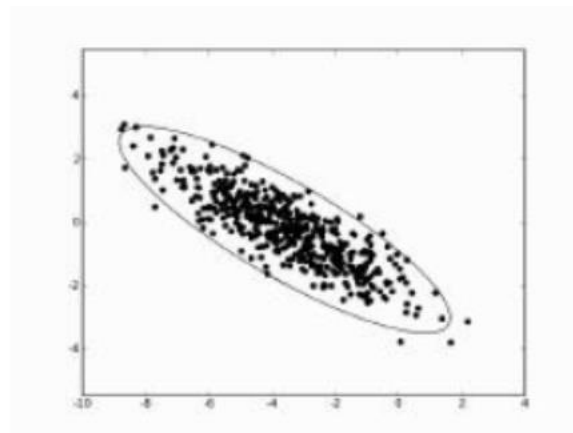
$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x-u)^2}{2\sigma^2}\right) \quad p(\mathbf{x}) = \frac{1}{(2\pi)^{\frac{d}{2}} |\Sigma|^{\frac{1}{2}}} \exp\left(-\frac{1}{2} (\mathbf{x} - \boldsymbol{\mu})^T \Sigma^{-1} (\mathbf{x} - \boldsymbol{\mu})\right)$$



单位阵

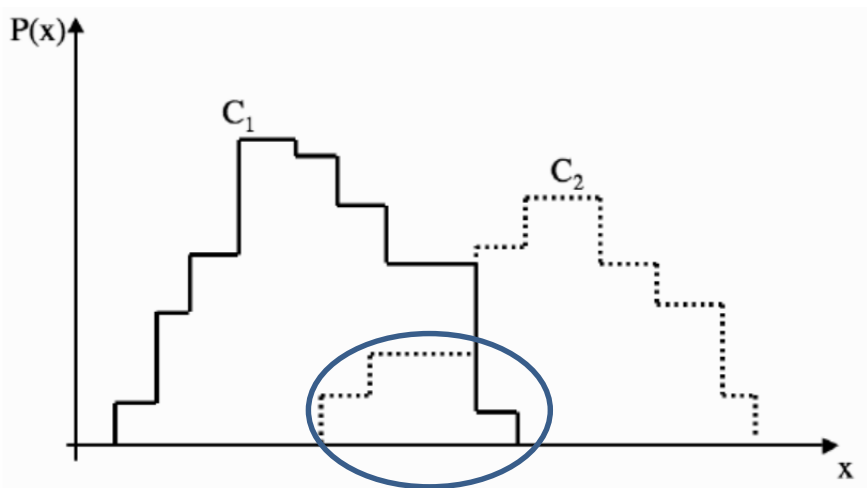


对角阵

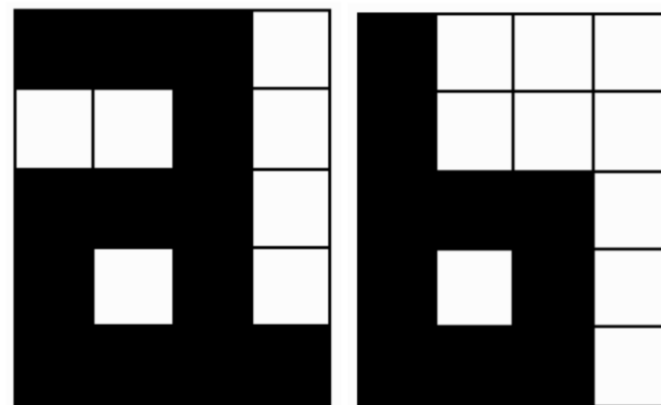


一般阵

# 先验概率



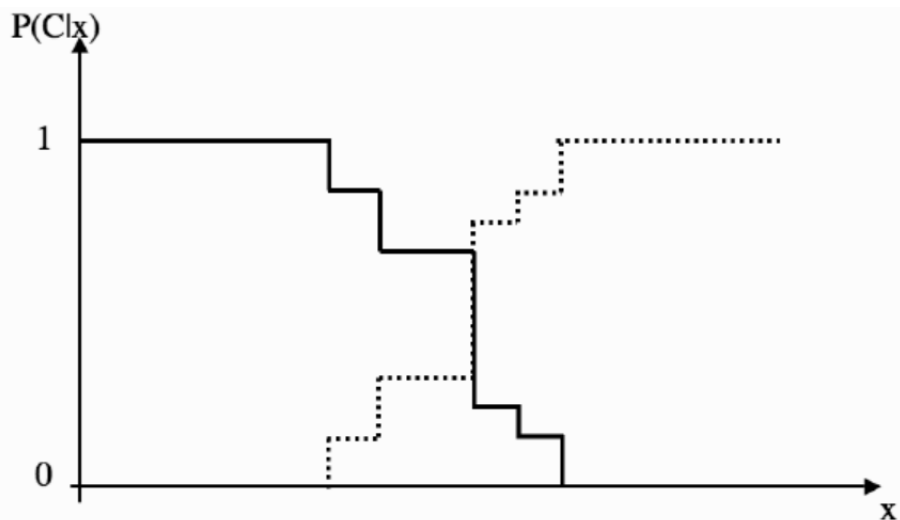
$C_2$ 类在 $x$ 属性上有较大的值  
交叉区域的样本如何区分呢？



统计英文字母：a出现的机率是b的  
三倍。

$$P(C_1 = 'a') = 0.75, P(C_2 = 'b') = 0.25$$

# 后验概率和贝叶斯法则



类C关于特征x的后验概率

最大后验 (maximum a posteriori) 或MAP假设

$$P(C_i|\mathbf{x}) > P(C_j|\mathbf{x}) \quad \forall i \neq j$$

$$P(C_i, X_j) = P(X_j|C_i)P(C_i)$$

$$P(C_i, X_j) = P(C_i|X_j)P(X_j)$$



贝叶斯法则

$$P(C_i|X_j) = \frac{P(X_j|C_i)P(C_i)}{P(X_j)}$$

$$P(X_k) = \sum_i P(X_k|C_i)P(C_i)$$

# 朴素贝叶斯分类

高维时面临的维数灾难：假设所有特征相互独立

$$P(X_j^1 = a_1, X_j^2 = a_2, \dots, X_j^n = a_n | C_i)$$

$$P(X_j^1 = a_1 | C_i) \times P(X_j^2 = a_2 | C_i) \times \dots \times P(X_j^n = a_n | C_i) = \prod_k P(X_j^k = a_k | C_i)$$

朴素贝叶斯分类法则

$$P(C_i) \prod_k P(X_j^k = a_k | C_i).$$

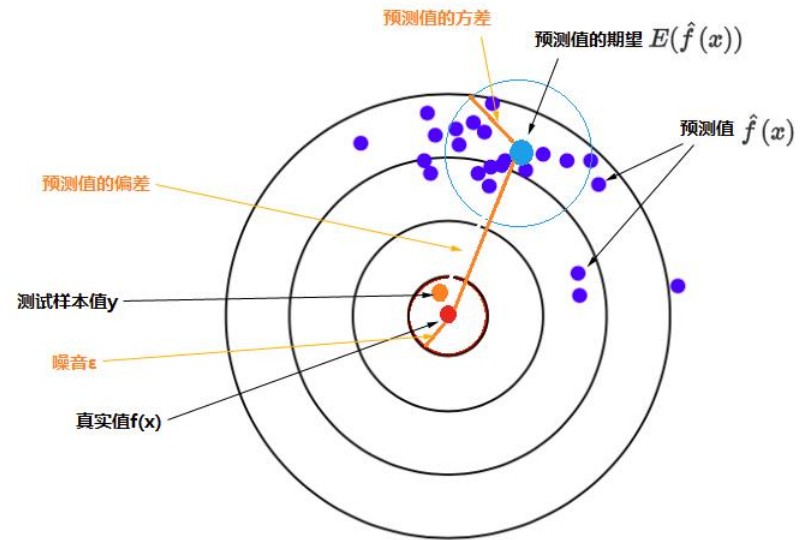
# 再探模型选择

$$(x_1, y_1), (x_2, y_2), (x_3, y_3) \dots \dots$$

$$y = f(x) + \varepsilon$$

$$Bias = E[\hat{f}(x)] - f(x)$$

$$Variance = E[(\hat{f}(x) - E[\hat{f}(x)])^2]$$



Bias-Variance两难

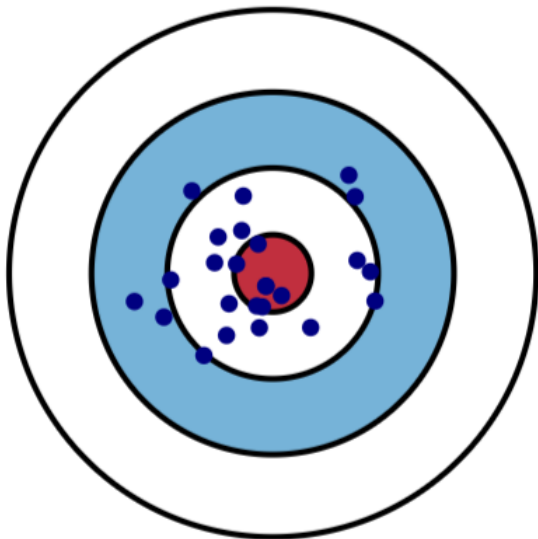
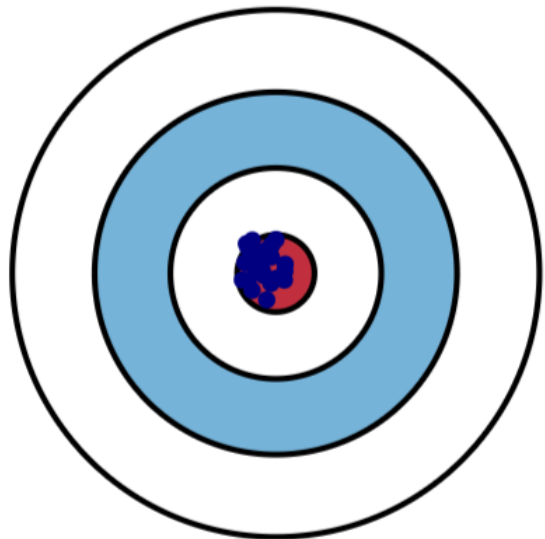
$$E[(y - \hat{f})^2] = E[y^2 - 2y\hat{f} + \hat{f}^2]$$

$$E = Bias^2 + Variance + Irreducible Error$$

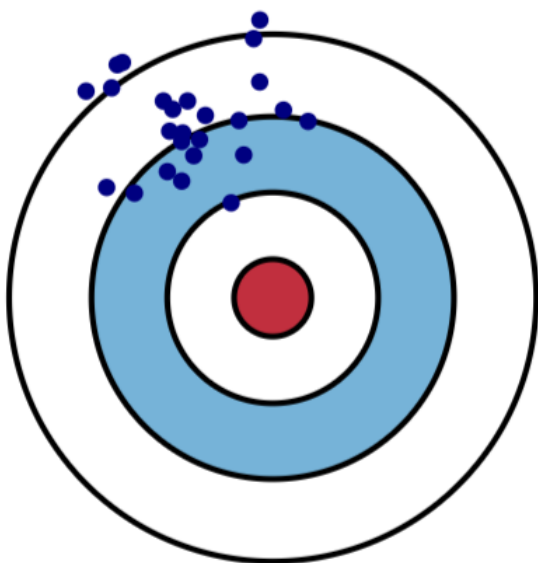
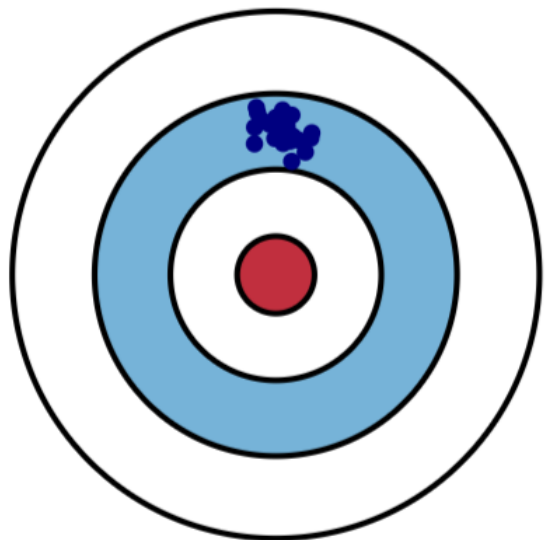
Low Variance

High Variance

Low Bias



High Bias



## 模型选择的次序

〈方差小, 偏差小〉

优于 〈方差小, 偏差大〉

优于 〈方差大, 偏差小〉

优于 〈方差大, 偏差大〉



# 机器学习技术新发展

# 机器学习技术本质

在有限样本/经验下为预测未来建模，涉及

- 特征层面
- 模型层面
- 优化层面
- .....

# 新型机器学习技术

- ❑ Lifelong/Continual Learning (终身/连续学习)
- ❑ Transfer Learning & Domain Adaption (迁移学习和域适应)
- ❑ Reinforcement Learning (强化学习)
- ❑ Adversarial Learning (对抗学习)
- ❑ Meta-Learning (元学习)
- ❑ Few-shot Learning (小样本学习) .....

# 机器学习核心技术要点

越来越小？越来越大？越来越深？越来越快？

## □ 1. 模型层面

- ✓ 大模型，大模型+领域知识→结合时空+特征类型+描述性知识+结构+.....

## □ 2. 优化层面(依赖目标函数性状，如凸性等)

- ✓ Online/Incremental Learning(联机/增量学习)
- ✓ Distributed(分布)/parallel(并行)学习+异步优化
- ✓ Speedup existing algorithms(加速现有算法)

## □ 3. 数据层面

- ✓ 总结(Summarizing)或提炼(Distilling)数据, 如用coreset/sketching技术→结合上面的1或2

# 谢 谢

更多信息: <http://cs.nju.edu.cn/rl>

联系方式: [gaoy@nju.edu.cn](mailto:gaoy@nju.edu.cn)

18951991288

