



高级机器学习

第一讲 绪论



主讲教师

- 郭兰哲，助理教授（特聘研究员）
 - 研究方向：稳健机器学习、弱监督机器学习
 - 办公地点：南雍楼523
 - 电子邮箱： guolz@nju.edu.cn
 - 个人主页： www.lamda.nju.edu.cn/guolz
-

参考教材



ISBN: 978-7-302-206853-6

2016年1月第1次印刷

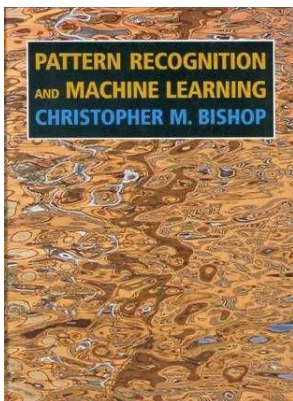
2020年11月第35次印刷

周志华 著. 机器学习,
北京: 清华大学出版社,
2016年1月.

425页, 62.6万字

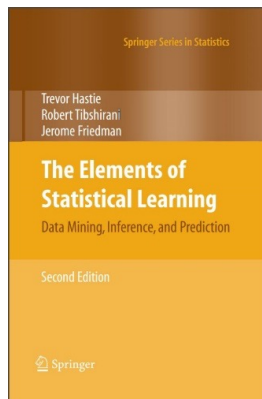
16 章, 3 附录

参考书籍



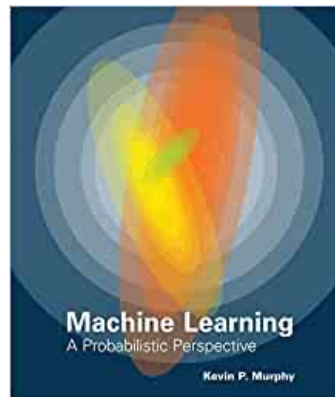
PRML

贝叶斯学派视角



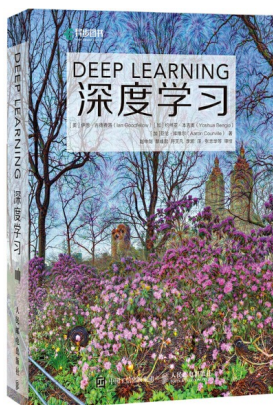
ESL

统计学派(频率主义)视角

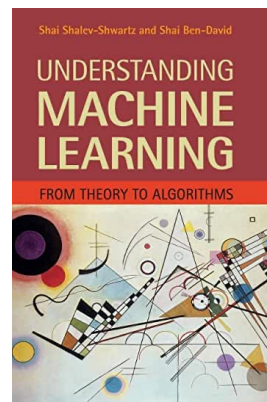


MLAPP

概率学派视角



深度学习



适合具有理论偏好的读者

机器学习框架



考核方式

- Presentation
 - ✓ 选择一个机器学习研究方向进行口头报告
- 期末论文
 - ✓ 选择一个机器学习研究方向进行综述介绍
 - ✓ 论文模版可参考《计算机学报》

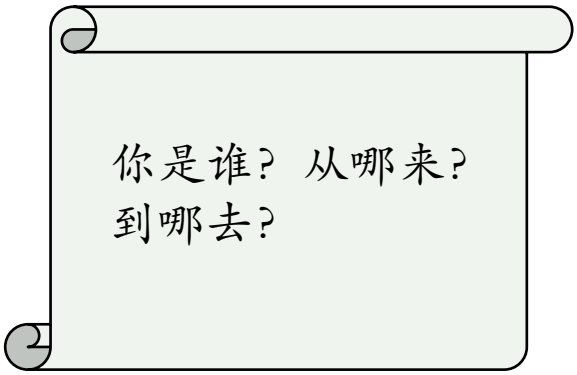
<http://cjc.ict.ac.cn/wltg/new/submit/index.asp>

各占50%

提纲

尝试回答如下问题：

- 机器学习是什么？
- 机器学习能做什么？
- 机器学习从哪儿来？
- 机器学习到哪儿去？
- 机器学习与其它领域的关系？
- 机器学习前沿进展到哪儿找？
- ...



你是谁？从哪来？
到哪去？

机器学习 (Machine Learning)

机器



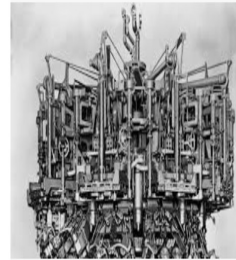
Beaumont Machine offers new va...
aero-mag.com



Auroplus Systems Indi...
amazon.in



FreePoint Technologies - Industry 4.0 | Machine Monitoring | IL...
getfreepoint.com

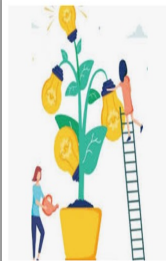


ASME's 20th Century Milestones in Manufacturing | L...
machinedesign.com



The Workplace of the Future Is a Mix of Human an...
adweek.com

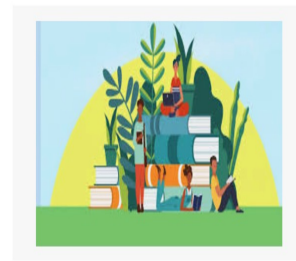
学习



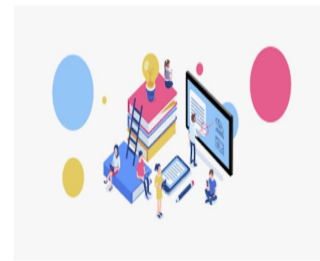
Six characteristics that promote st...
insidehighered.com



Capturing student learning and growth through competen...
reachinghighernh.org



Expanding Access to Summer Learning in Response to COVID-19
tcf.org



How to Implement Active Learning for Classrooms - ViewSonic Educa...
education.viewsonic.com

机器学习 ??

机器学习 (Machine Learning)

- 1) 人类学习利用**经验**不断提高性能
- 2) 机器善于处理**数据**不断提高性能

能否把“经验”变成数据，让机器可以“模仿”人类进行学习

机器学习：机器利用数据学习人类经验，不断提高性能的过程



机器学习 (Machine Learning)

机器学习是人工智能的核心领域之一，是实现智能化的关键

经典定义：利用经验改善系统自身的性能



经验 → 数据



随着该领域的发展，目前主要研究智能数据分析的理论和算法，并已成为智能数据分析技术的源泉之一

图灵奖连续授予在该方面取得突出成就的学者



Leslie Valiant
(1949 -)
(Harvard Univ.)

“计算学习理论” 奠基人

2010
年度



Judea Pearl
(1936 -)
(UCLA)

“图模型学习方法” 先驱

2011
年度

机器学习 (Machine Learning)

机器学习是人工智能的核心领域之一，是实现智能化的关键

经典定义：利用经验改善系统自身的性能



经验 → 数据



随着该领域的发展，目前主要研究智能数据分析的理论和算法，并已成为智能数据分析技术的源泉之一

图灵奖连续授予在该方面取得突出成就的学者



Yoshua Bengio



Geoffrey Hinton



Yann LeCun

“深度学习三驾马车”
获2018年度图灵奖

机器学习

机器学习 (Machine Learning)

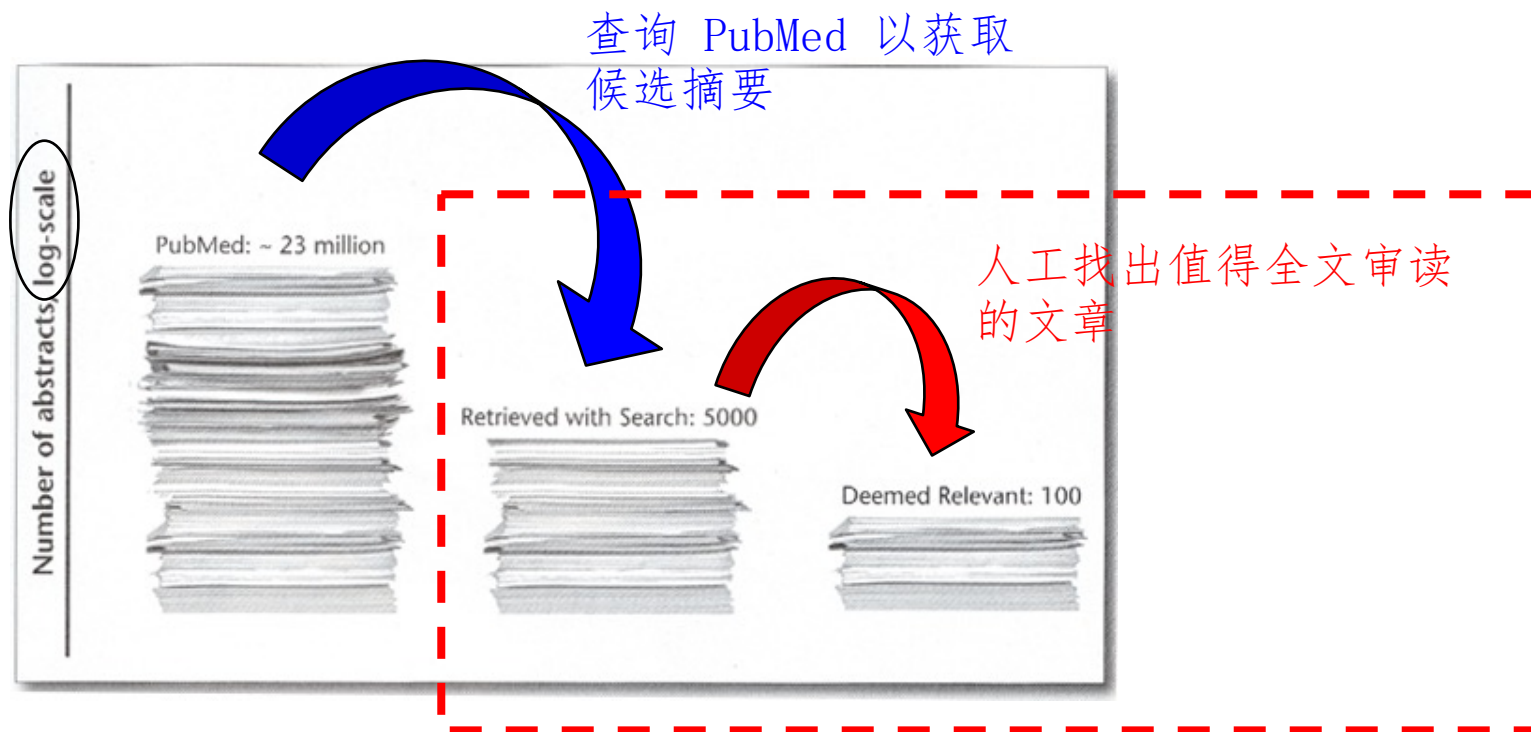
究竟是什么东东？



看两个例子 ⇨

一个例子：“文献筛选”

在“循证医学”（evidence-based medicine）中，针对特定的临床问题，先要对相关研究报告进行详尽评估



“文献筛选”

在一项关于婴儿和儿童残疾的研究中，美国Tufts医学中心筛选了约 33,000 篇摘要

尽管Tufts医学中心的专家效率很高，对每篇摘要只需 30 秒钟，但该工作仍花费了 250 小时



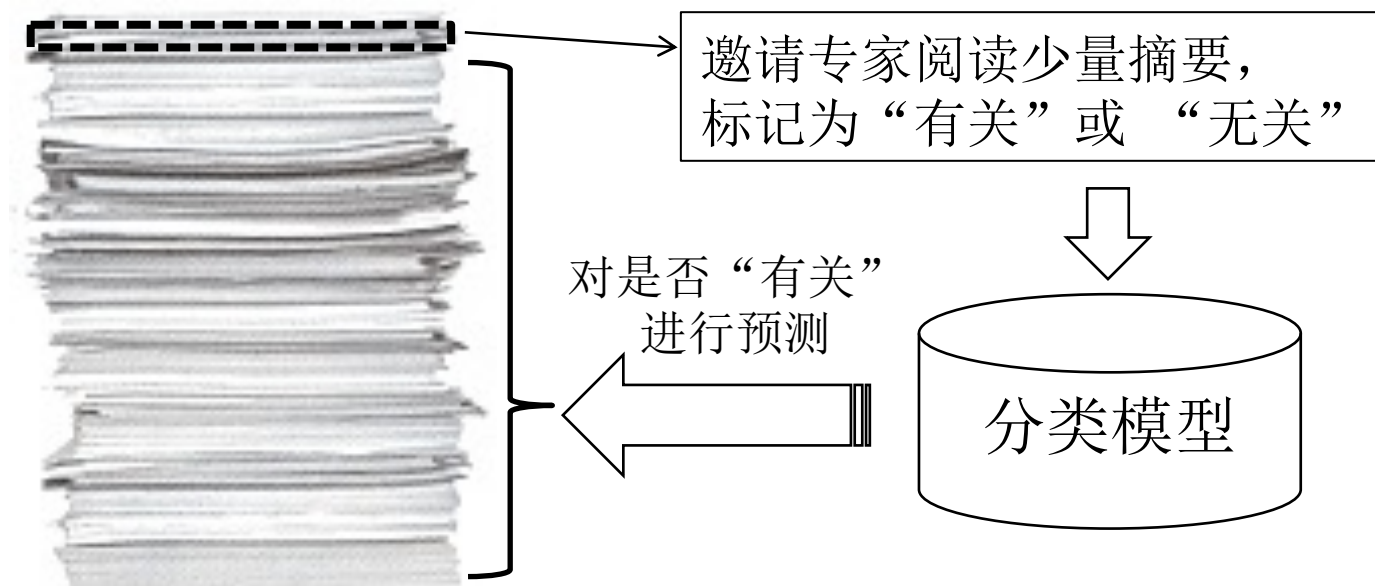
a portion of the 33,000 abstracts

每项新的研究都要重复这个麻烦的过程！

需筛选的文章数在不断显著增长！

“文献筛选”

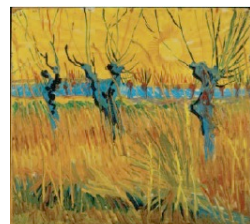
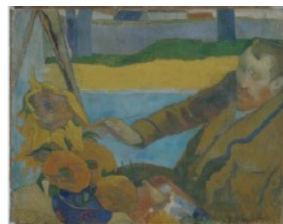
为了降低昂贵的成本, Tufts医学中心引入了机器学习技术



人类专家只需阅读 **50** 篇摘要, 系统的自动筛选精度就达到 **93%**
人类专家阅读 **1,000** 篇摘要, 则系统的自动筛选敏感度达到 **95%**
(人类专家以前需阅读 **33,000** 篇摘要才能获得此效果)

画作鉴别

画作鉴别(painting authentication): 确定作品的真伪



勃鲁盖尔 (1525-1569) 的作品？

梵高 (1853-1890) 的作品？

该工作对专业知识要求极高

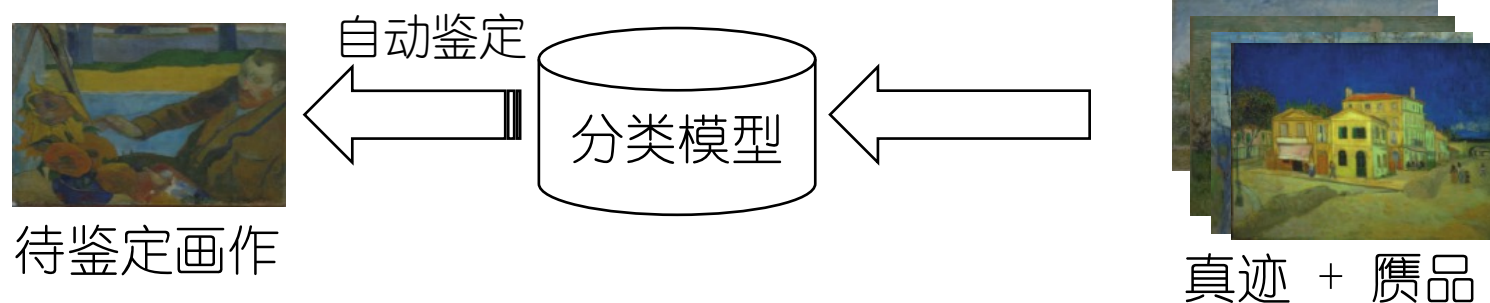
- 具有较高的绘画艺术修养
- 掌握画家的特定绘画习惯

只有少数专家花费很大精力才能完成分析工作！

很难同时掌握不同时期、不同流派多位画家的绘画风格！

画作鉴别

为了降低分析成本，机器学习技术被引入



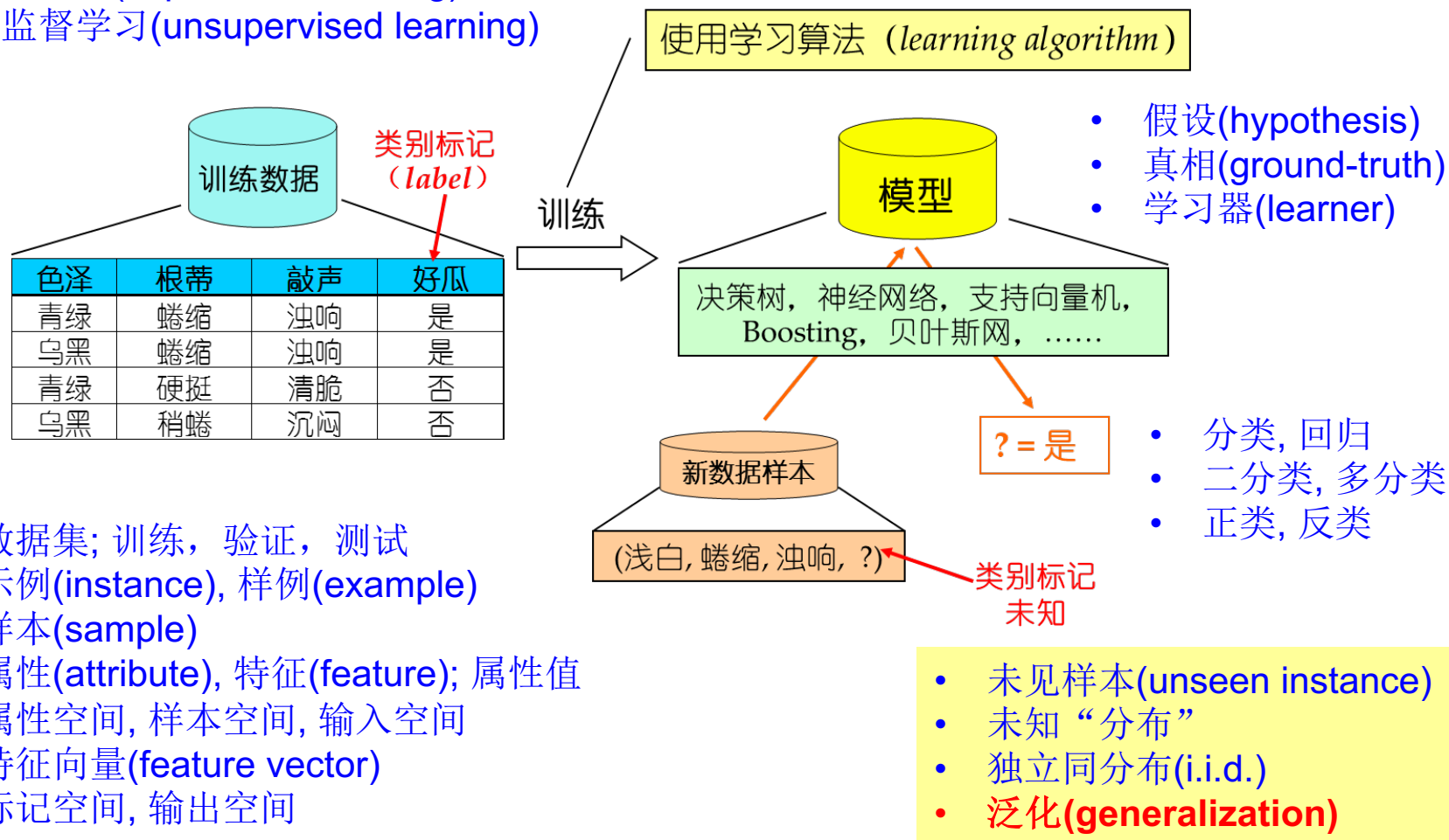
Kröller Müller美术馆与Cornell等大学的学者对82幅梵高真迹和6幅赝品进行分析，自动鉴别精度达 **95%** [C. Johnson et al., 2008]

Dartmouth学院、巴黎高师的学者对8幅勃鲁盖尔真迹和5幅赝品进行分析，自动鉴别精度达 **100%** [J. Hughes et al., 2009][J. Mairal et al., 2012]

(对用户要求低、准确高效、适用范围广)

典型机器学习过程

- 监督学习(supervised learning)
- 无监督学习(unsupervised learning)



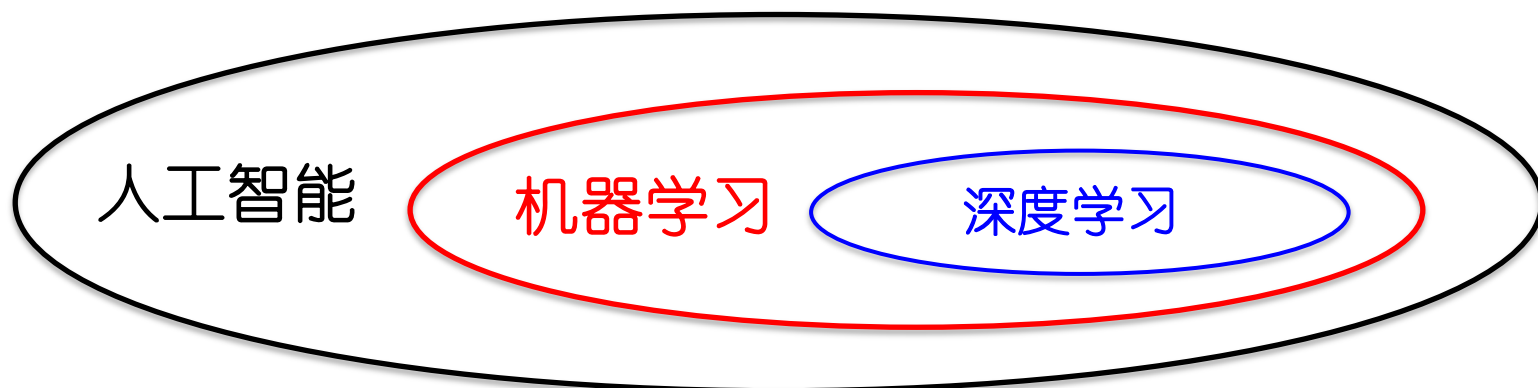
机器学习从何而来？

机器学习与人工智能

机器学习是人工智能的核心研究领域（之一）

今天的“人工智能热潮”

正是由于机器学习、尤其深度学习技术取得了巨大进展
基于大数据、大算力发挥出巨大威力



人工智能的诞生

Computing Machinery and
Intelligence

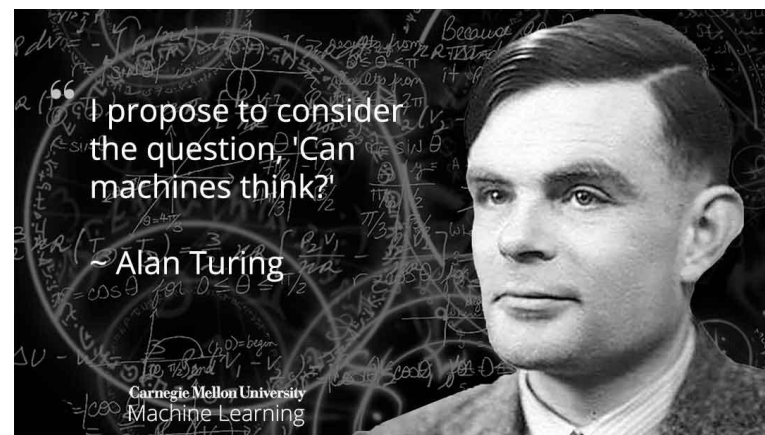
计算机与智能

1950年

艾伦·图灵

“Can machine think?”

机器能思考吗？

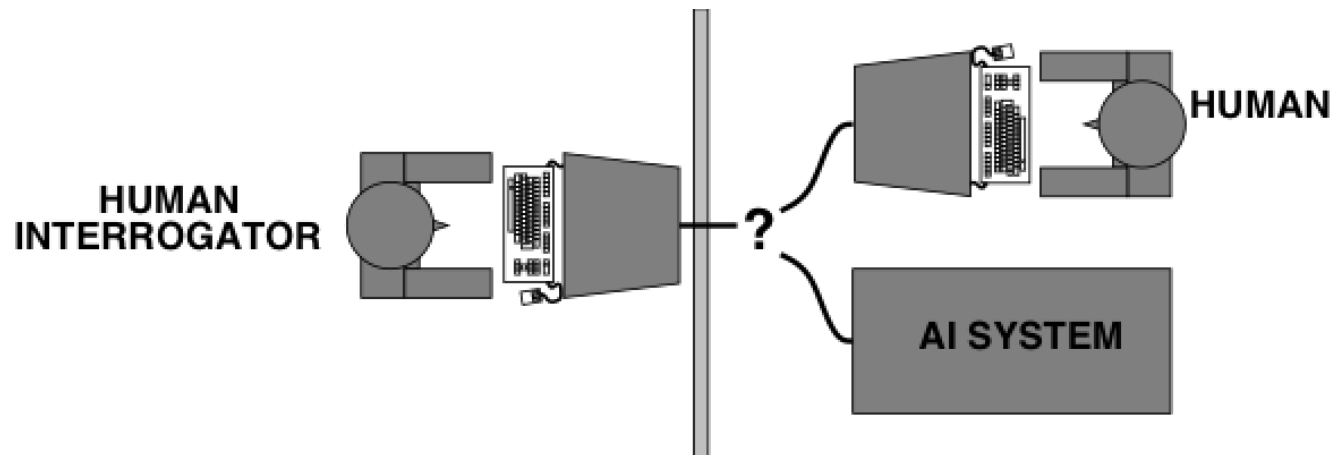


艾伦·图灵

1912-1954

图灵测试

Section 1: Imitation game (模仿游戏)



人工智能的诞生

Artificial Intelligence (AI), 1956 -



1956年夏 美国达特茅斯学院



J. McCarthy
“人工智能之父”
图灵奖(1971)



M. Minsky
图灵奖(1969)



C. Shannon
“信息论之父”



H. A. Simon
图灵奖(1975)
诺贝尔经济学奖(1978)

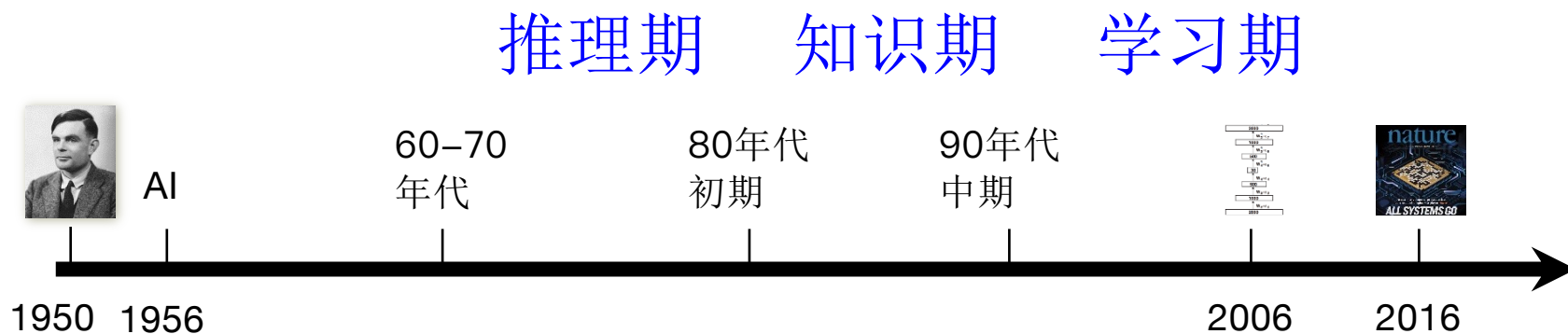


A. Newell
图灵奖(1975)

.....
.....

达特茅斯会议标志着人工智能这一学科的诞生

人工智能的发展阶段



第一阶段：推理期

1956-1960s: Logic Reasoning

- ◆ 出发点：“数学家真聪明！”
- ◆ 把人的**思考逻辑**教给电脑
- ◆ 主要成就：自动定理证明系统（例如，西蒙与纽厄尔的“Logic Theorist”系统）

渐渐地，研究者们意识到，仅有逻辑推理能力是不够的 …



赫伯特·西蒙
(1916–2001)
1975年图灵奖



阿伦·纽厄尔
(1927–1992)
1975年图灵奖

第二阶段：知识期

1970s -1980s: Knowledge Engineering

- ◆ 出发点：“知识就是力量！”
- ◆ 把人的**所有知识**教给电脑
- ◆ 主要成就：专家系统（例如，费根鲍姆等人的“DENDRAL”系统）

渐渐地，研究者们发现，要总结出知识再“教”给系统，实在太难了 …



爱德华·费根鲍姆
(1936-)
1994年图灵奖



瑞吉·芮迪
(1937-)
1994年图灵奖

第三阶段：学习期

1990s -now: Machine Learning

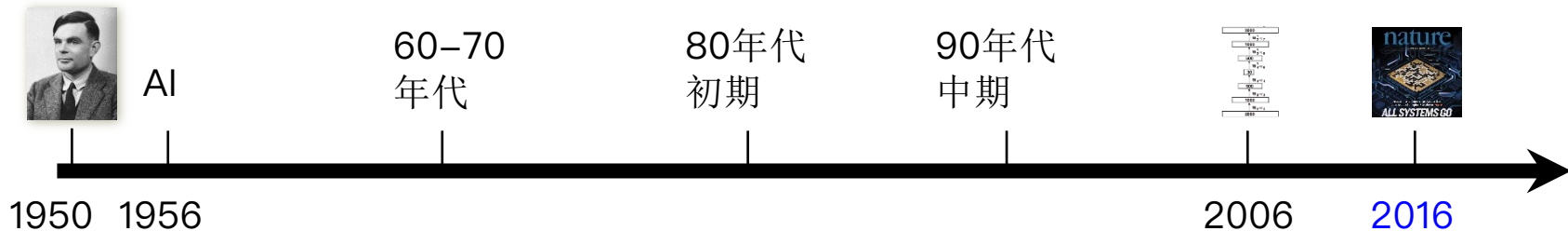
- ◆ 出发点：“让系统自己学！”
- ◆ 把人的所有看见放入电脑
- ◆ 主要成就：

机器学习是作为“突破知识工程瓶颈”之利器而出现的



恰好在20世纪90年代中后期，人类发现自己淹没在数据的汪洋中，对自动数据分析技术——机器学习的需求日益迫切

第三阶段：学习期

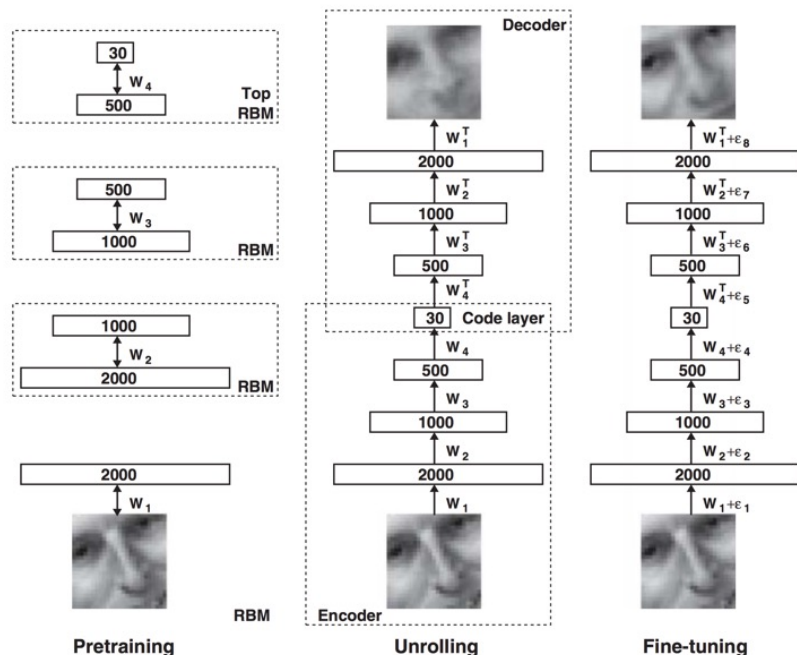


机器学习 → 深度学习



Geoffrey Hinton

深度学习显著降低了机器学习应用者的门槛，
为机器学习技术走向工程实践带来了便利



2015年至今

《[Nature](#)》2015年2月统计学习先驱B. Schölkopf发文评论了基于学习的人工智能

《[Nature](#)》2015年5月发表7篇文章的专栏聚焦机器智能深度学习、强化学习、概率机器学习、小型自主无人机

《[Science](#)》2015年7月发表人工智能专辑机器学习、自然语言处理、计算理性、数据隐私

互联网巨头纷纷开源机器学习 / 深度学习系统

FBCUNN、[TensorFlow](#)、[PaddlePaddle](#)、[Pytorch](#)、SystemML、VELES



专用于机器学习等计算任务的通用GPU



[MyDrivers.com](#)

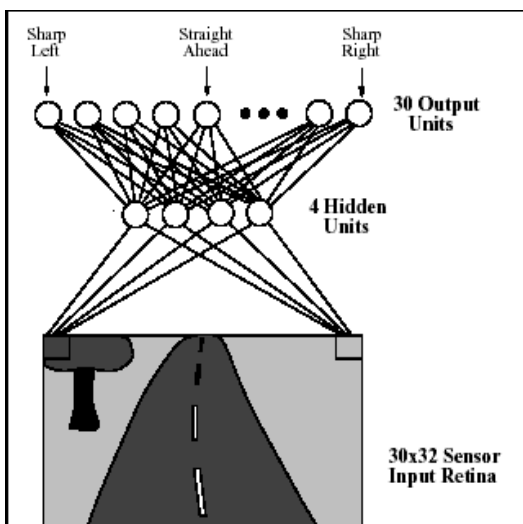
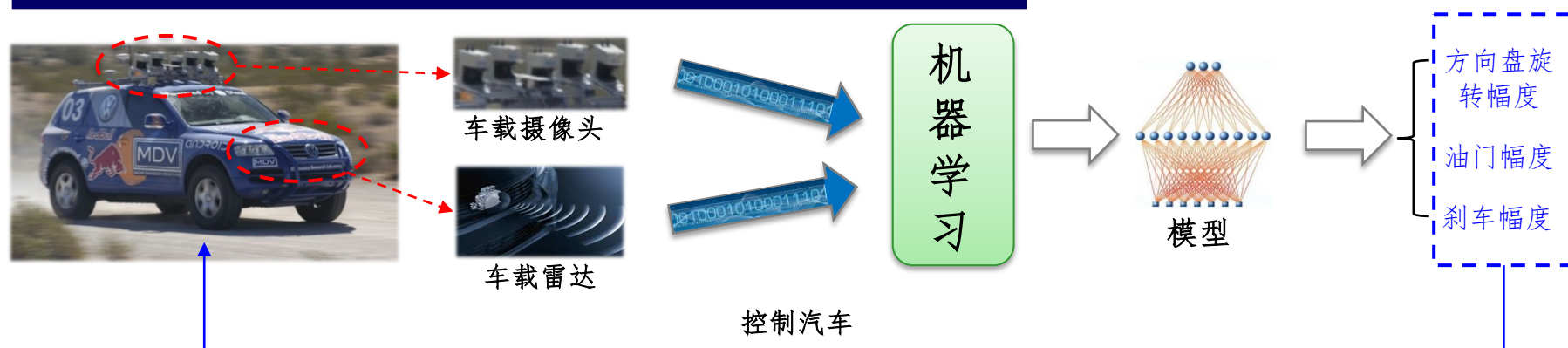
机器学习有哪些应用？

例如：搜索引擎



机器学习技术正在支撑着各种搜索引擎

例如：自动汽车驾驶



美国在20世纪80年代就开始研究基于机器学习的汽车自动驾驶技术

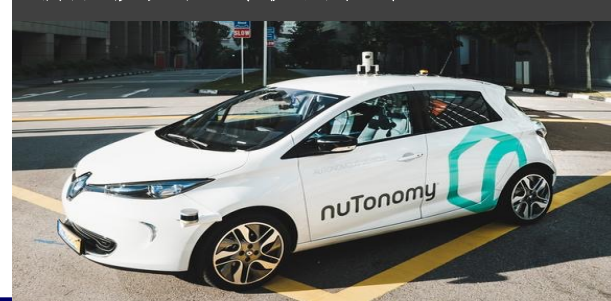


DARPA Grand Challenge - 2004
荒野中的无人车竞赛

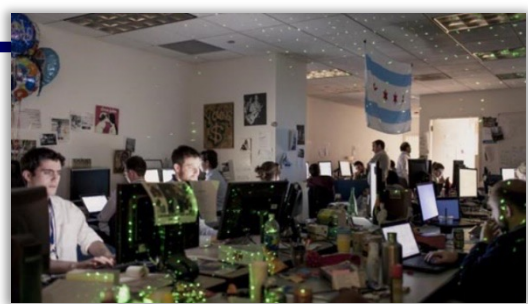
Google 无人驾驶汽车 - 2016



新加坡无人驾驶出租车 - 2016



例如：帮助奥巴马胜选



这个团队行动保密，定期向奥巴马报送结果；被奥巴马公开称为总统竞选的“核武器按钮”（“They are our nuclear codes”）

通过机器学习模型

◆ 个性化宣传

喜欢宠物？
奥巴马也有宠物！



喜欢篮球？
奥巴马也是篮球迷！



◆ 广告购买

精准定位不同选民群体，建议购买冷门广告时段，广告资金效率比2008年提高14%

◆ 筹款



和乔治克鲁尼/奥巴马共进晚餐对于年龄在40-49岁的美西地区女性颇具吸引力…… 乔治克鲁尼为奥巴马举办的竞选筹资晚宴成功募集到1500万美元



例如：AlphaGO



计算/预测出较高胜率的走法？

大量棋谱如何生成/利用









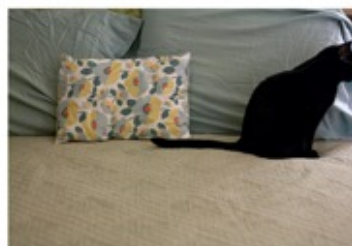


公开的计算难题，意义重大熟知的

日常游戏，影响深远



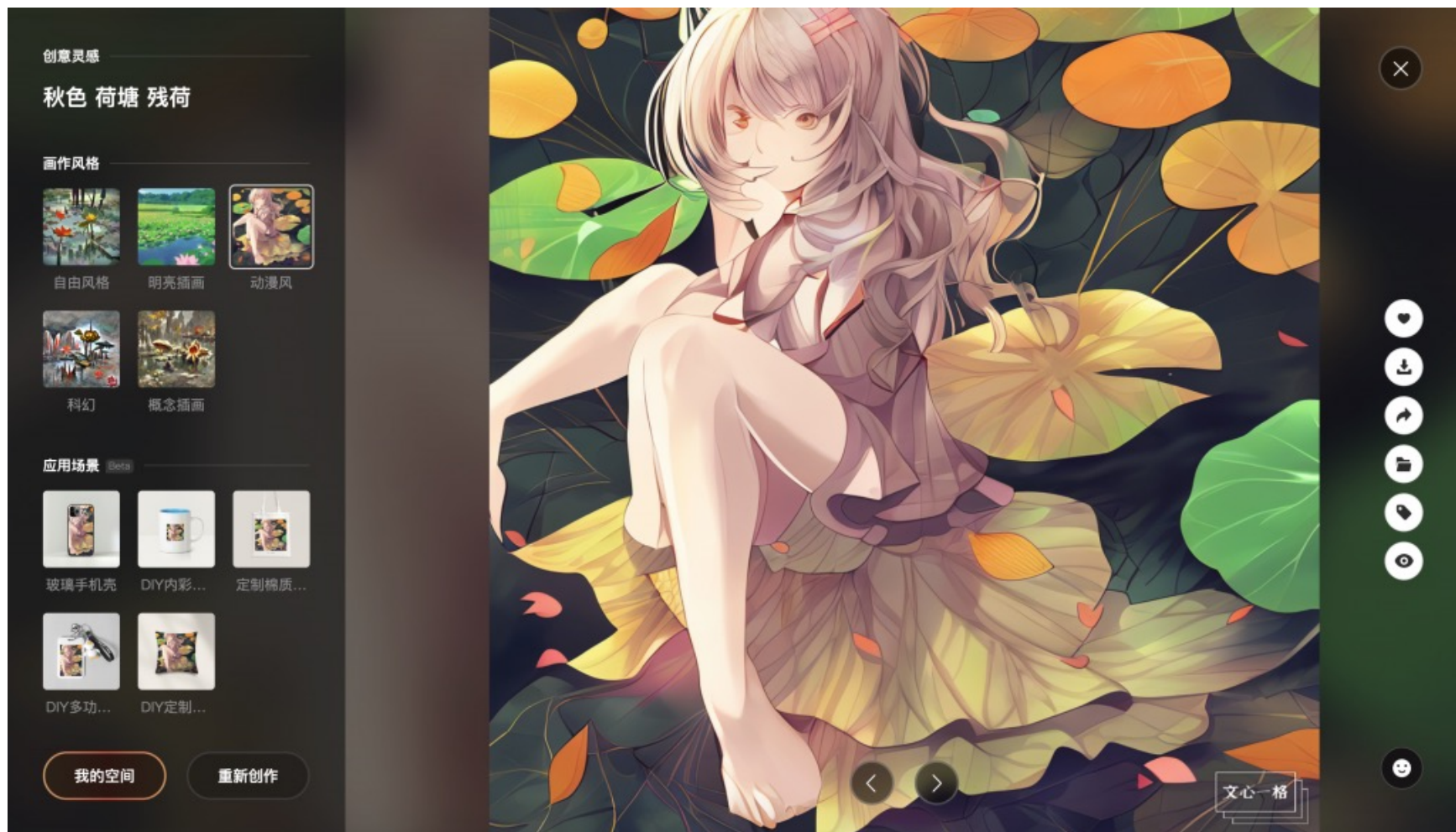
例如：视频理解

计算机已可初步理解视频

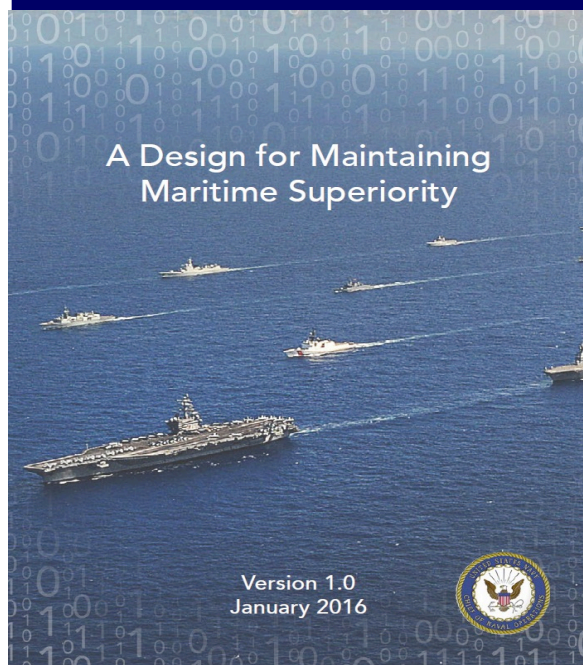
Describes without errors	Describes with minor errors	Somewhat related to the image	Unrelated to the image
 <p>A person riding a motorcycle on a dirt road.</p>	 <p>Two dogs play in the grass.</p>	 <p>A skateboarder does a trick on a ramp.</p>	 <p>A dog is jumping to catch a frisbee.</p>
 <p>A group of young people playing a game of frisbee.</p>	 <p>Two hockey players are fighting over the puck.</p>	 <p>A little girl in a pink hat is blowing bubbles.</p>	 <p>A refrigerator filled with lots of food and drinks.</p>
 <p>A herd of elephants walking across a dry grass field.</p>	 <p>A close up of a cat laying on a couch.</p>	 <p>A red motorcycle parked on the side of the road.</p>	 <p>A yellow school bus parked in a parking lot.</p>

例如：图像生成

根据文字描述生成相应图像




例如：美军海权纲领性文件



Conclusion

We will remain the world's finest Navy **only** if we all fight each other better. Our competitors are focused on taking the lead – we must deny them. The margins of victory are razor thin – but decisive integrity, accountability, initiative, and toughness to execute the plan in this Design, execute our mission, and achieve our end state. I will lead you.


JOHN M. RICHARDSON

8

美海军作战部长John Richardson 2016年初签署的《保障制海权规划》中明确指出人工智能的重要

The third interrelated force is the increasing rate of technological creation and adoption. This is not just in information technologies, where Gordon Moore's projections of exponential advances in processing, storage, and switches continue to be realized. Scientists are also unlocking new properties of commonplace materials and creating new materials altogether at astonishing speeds. Novel uses for increasingly sophisticated robotics, energy storage, 3-D printing, and networks of low-cost sensors, to name just a few examples, are changing almost every facet of how we work and live. Genetic science is just beginning to demonstrate its power. Artificial intelligence is just getting started and could fundamentally reshape the environment. And as technology is introduced at an accelerating rate, it is being adopted by society just as fast – people are using these new tools as quickly as they are introduced, and in new and novel ways.

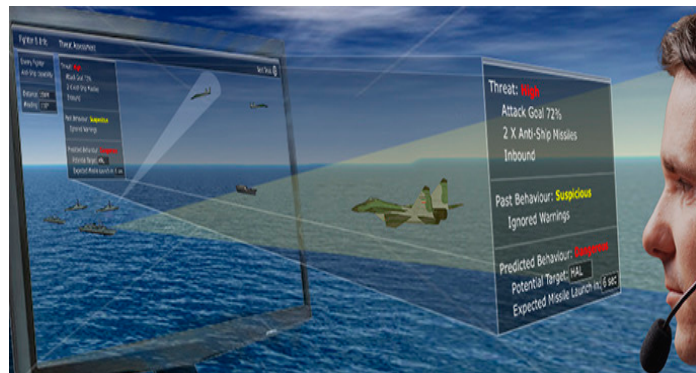
These three forces of information, technology, and competition must do their work together.

And the United States must advance by a growth in capabilities specifically on our vulnerabilities and are increasingly designed from the ground up to leverage the maritime, technological and information systems. They continue to develop and field information-enabled weapons, both kinetic and non-kinetic, with increasing range, precision and destructive capacity. Both China and Russia are also engaging in coercion and competition below the traditional thresholds of high-end conflict, but nonetheless exploit the weakness of accepted norms in space, cyber and the electromagnetic spectrum. The Russian Navy is operating with a frequency and in areas not seen for almost two decades, and the Chinese PLA(N) is extending its reach around the world.

“人工智能开始并可以从根本上重塑（战场）环境...”

Russia and China are not the only actors seeking to gain advantages in the emerging security environment in ways that threaten U.S. and global interests. Others are now pursuing advanced technology, including military technologies that were once the exclusive province of great powers – this trend will only continue. Coupled with a continued dedication to furthering its nuclear weapons and missile programs, North Korea's provocative actions continue to threaten security in North Asia and beyond. And while the recent international agreement with Iran is intended to curb its nuclear ambitions, Tehran's advanced missiles, proxy forces and other conventional capabilities continue to pose threats to which the Navy must remain prepared to respond. Finally, international terrorist groups have proven their resilience and adaptability and now pose a long-term threat to stability and security around the world. All of these actors seek to exploit all three forces described above – the speed, precision and reach that

例如：战场战术层面（美）



眼镜蛇系统：

Coastal Battlefield Reconnaissance and Analysis (COBRA)

用于濒海战斗舰，执行无人空中战术侦察。在两栖攻击之前，于海浪区和海滩区探测和定位雷区和障碍物

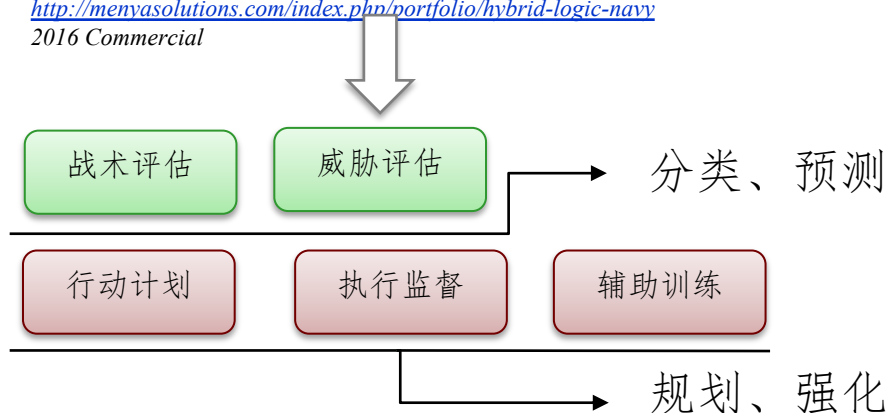
http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=1237&ct=2

http://www.navysbir.com/n15_1/N151-049.htm
2015 US Navy Official

HybridLogic Navy:

一套自动的基于机器学习的代理，帮助人类和无人机理解战术状况，及时做出最佳决策，以对付海军作战中的威胁

<http://menvasolutions.com/index.php/portfolio/hybrid-logic-navy>
2016 Commercial



AN/DVS-1 COASTAL BATTLEFIELD RECONNAISSANCE AND ANALYSIS - (COBRA)

The mission of the AN/DVS-1 Coastal Battlefield Reconnaissance and Analysis (COBRA) system is to conduct unmanned aerial tactical reconnaissance in the littoral battlespace for detection and localization of minefields and obstacles in the surf zone and beach zone prior to an amphibious assault. The COBRA airborne payload will be carried on the MQ-8 Fire Scout unmanned air system. This allows operators and other personnel to remain at a safe distance from the mine and obstacle belts and enemy direct and indirect fire. COBRA will be embarked in the Littoral Combat Ship (LCS) as part of the Mine Countermeasures (MCM) Mission Package (MP).

DESCRIPTION: The Coastal Battlefield and Reconnaissance (COBRA) program (Ref 1) is interested in technologies that facilitate **automated target recognition (ATR)** capabilities in aerial multi-spectral images for previously unseen environments and target types. Targets of interest include minefields and obstacles in various land and marine environments. **ATR algorithms** are developed offline (post-mission) using previously acquired test data sets. These algorithms on supervised learning methods (Ref 2) that incorporate data from a limited set of test fields. When data is from new environments, the algorithms often must be re-optimized to have good performance in that environment, as well as maintain performance in previously seen environments. The process for performing this offline re-optimization is often costly since it requires the efforts of expert analysts to assimilate data sets, determine target truth, analyze target features, train the **ATR classifiers** and evaluate performance.

There is a need for innovative methods that can 1) incorporate information from new data sets into the ATR system as they are acquired, and 2) **re-optimize ATR algorithms** quickly across all known environments, including those of newly acquired data. **Online Machine Learning (OML)** algorithms (Ref 3-5) can potentially be used to "learn" in the field based on operator-provided results without affecting prior performance. The information collected online can be used to refine the prediction hypothesis (classifier) used in the **ATR algorithms**. In addition, the information may provide input for automated methods of optimizing **ATR performance** across all known data sets.

The proposed effort will develop **innovative OML algorithms** for ATR that can incorporate human operator decisions to optimize probability of detection and probability of false alarm performance in new environments and for new target types. These algorithms will be integrated into mission and post-mission analysis systems in which operators review acquired images. The algorithms will be implemented as object-oriented C++ code for insertion into the operator systems. Development of the online learning algorithms must be combined with identification of how the operator will interact with them to provide updated decision information. Robust optimization of the **ATR algorithms** may be performed post-mission, which will require the development of separate software tools for processing historical data sets. **The OML algorithms** and optimization tools developed in this effort will reduce program costs by minimizing the time required for optimizing ATR algorithms to perform well in unseen operational environments.

自动目标识别、
监督学习以及
在线学习技术
被作为核心技术
并多次提及

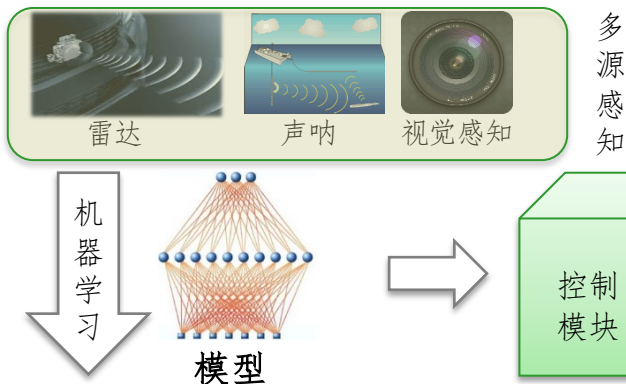
例如：战场战术层面（英）



无人侦察快艇：

无人控制的情况下以50公里时速追踪快速目标并自动避障，进行跟踪、监视和间谍活动，或者用于海岸巡逻

<http://www.telegraph.co.uk/news/2016/09/05/navy-unveils-robot-spy-speedboat/> 2016 Royal Navy Official / Commercial



无人自动驾驶

船舶能源评估-条件优化和路由增强系统

Software to transform ship maintenance

September 21, 2016

SEA-CORES. Credit: University of Southampton

Researchers from the University of Southampton are to develop software that can monitor the equipment, fuel and energy performance of a ship at sea.

The University is part of the Ship Energy Assessment – Condition Optimisation & Routing Enhancement System (SEA-CORES) consortium, which provides a live model of ship performance on global operations. The development of the software is led by BAE Systems and is sponsored by Innovate UK.

SEA-CORES is able to correlate variables that could affect a ship's performance, such as energy consumption and different weather conditions. Using genetic algorithms to track and capture the live data, SEA-CORES provides those on board with a greater understanding of the vessel's capabilities across a wide range of operations.

Researchers from Electronics and Computer Science at the University of Southampton will work on monitoring loads on the ship and applying novel machine learning techniques to a domain that has largely been data poor.

Dr Sarvapali Ramchurn, who is leading the Southampton research group, said: "Unleashing such technologies on the marine sector is likely to have a huge impact. The work we are doing at Southampton in terms of autonomous systems and machine learning will help improve the efficiency of ships and detect potential issues before they cause major damage."

BAE Systems is developing and testing SEA-CORES on a commercial tanker provided by James Fisher Marine Services. The trial will analyse the vibration and trim performance of the vessel, its hull state and monitor the integrity of the ship's superstructure.

Chris Courtaux, Head of Engineering and Energy Services at BAE Systems, said: "SEA-CORES is able to consider all of the important components which affect the performance of a vessel during deployment.

"For instance, reducing speed may save fuel but increase the wear to the engine if below its optimum performance. This could in turn increase the maintenance requirements for these vessels and reduce their availability. It is crucial that we continue to analyse what more can be done to maintain these vessels in an efficient manner and increase the number of ships available for the Royal Navy fleet."

The software connects technologies in delivering fuel and engine optimisation through the use of the BAE Systems' Ship Energy Assessment System (SEAS), together with big data analysis by using System Information Exploitation (SIE) technology.

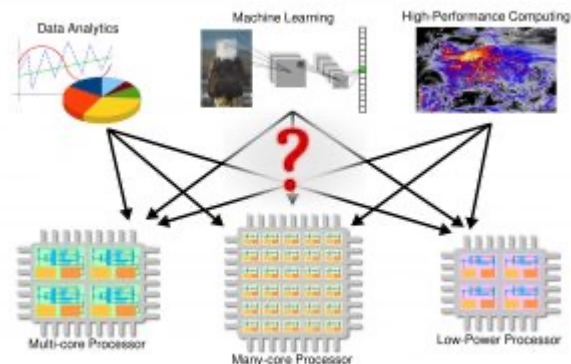
SEA-CORES has been developed in response to the increasing complexities of modern warships and the amount of data their systems produce. The technology could transform how the Royal Navy and BAE Systems maintain and support warships in the future by using the genetic algorithms to identify the relationships between a ship's systems, calculate their different permutations and ultimately recommend a strategy to optimise the vessel's performance.

应对现代军舰日益复杂系统结构、针对其系统产生的海量数据而开发，能够有机组织军舰各个子系统，最终优化全舰效能

<https://phys.org/news/2016-09-software-ship-maintenance.html>
2016 Royal Navy Official / Commercial

遗传算法以及其他一些机器学习方法用于获取追踪数据和确定舰船子系统关联的任务中

例如：中长期战略层面——基础/技术研发



军用下一代机器学习处理器：

依托学习技术消除了海军开发人员选择架构的问题，由程序直接分析出最适合的处理器平台，最大化指令执行效率

<http://futureforce.navylive.dodlive.mil/2017/07/popcorn-linux-software-for-a-diverse-world/>

2017 US DOD Official

The screenshot shows the ONR website with a navigation bar at the top. The main content area is titled 'Machine Learning, Reasoning and Intelligence Program'. It includes a sidebar with a dropdown menu for 'Code 31' and a main text area describing the program's goals and thrusts. The text describes the program's focus on building intelligent agents and lists three thrusts: Intelligence for Autonomous Agents, Image Understanding, and Human-Agent Collaboration. A note at the bottom encourages proposers to contact the program officer.

Office of Naval Research
Science & Technology

Technology Locator | Glossary | Careers | Events

ONR Global | Marine Corps Warfighting Lab | Naval Research Laboratory

About ONR | Science & Technology Organization | Contracts & Grants | Education & Outreach

Home » Organization » Departments » Code 31 » All Programs » Division 311 » Machine Learning and Intelligence

Code 31

All Programs

Division 311

Machine Learning and Intelligence

Division 312

Division 313

Contacts

Machine Learning, Reasoning and Intelligence Program

The Office of Naval Research (ONR) Machine Learning, Reasoning and Intelligence program is concerned with building intelligent agents that can function in the environments in which warfighters operate, that is, environments that are unstructured, open, complex and dynamically changing. Agents (cyber or physical) do not yet have the level of intelligence needed to operate in such open, uncertain and unpredictable environments either independently or alongside warfighters. The program's main objectives are to develop principles of machine intelligence, efficient computational methods, algorithms and tools for building versatile smart agents that can perform missions autonomously with minimal human supervision and collaborate seamlessly with teams of warfighters and other agents. Program focus areas include the following thrusts:

- Intelligence for Autonomous Agents:** This thrust focuses on developing the intelligence needed for agents to function autonomously in a variety of situations. The following are of particular interest. (1) Building Blocks of Machine Intelligence. Some suggested topics of interest are: (a) Methods for building knowledge bases from diverse sources; (b) Learning complex concepts and tasks from examples, instructions, and demonstrations; (c) Reasoning with uncertain and qualitative information, as well as methods for meta-reasoning for self-assessment; (d) Planning in large domains in partially known environments and incompletely modeled goals and domains; (e) Intelligent architectures that seamlessly integrate knowledge-bases, learning, reasoning, and planning, for decision-making. (2) Teams of Unmanned Vehicles. Some suggested topics of interest are: (a) Computational methods for building decentralized collaborating teams of autonomous agents, in particular agents that are fairly capable in terms of sensing, communication and computational resources; (b) Mathematical theories of swarm control, particularly engineered swarms with desired behaviors. (3) Human-Agent Collaboration. Some suggested topics of interest are: (a) Multi-modal, multi-participant, human-agent dialogue systems for seamless interactions that are natural to humans; (b) Computational models of human behavior and decision-making for use by autonomous agents.
- Image Understanding:** The goal of this thrust is to develop theory and algorithms for understanding surveillance imagery, for semantic search of visual datasets, and for autonomous agent perception. The main focus is on reconstructing 3D scenes, recognizing object classes and specific objects, recognizing activities and events, inferring intentions, as well as succinct natural language descriptions of images and video. Of particular interest is developing visual representations, methods for building visual knowledge bases optimized for inference, and methods for integrating reasoning with high-level knowledge and image data

Note: Proposers are encouraged to contact the program officer to discuss their research interest prior to the submission of formal proposals.

美海军研究院：

针对机器学习，特别对自主代理、图像理解展开全面研究

<https://www.onr.navy.mil/en/Science-Technology/Departments/Code-31/All-Programs/311-Mathematics-Computers-Research/Machine-Learning-Reasoning-Intelligence>

2017 US Navy Official / US Naval Research Division 311.

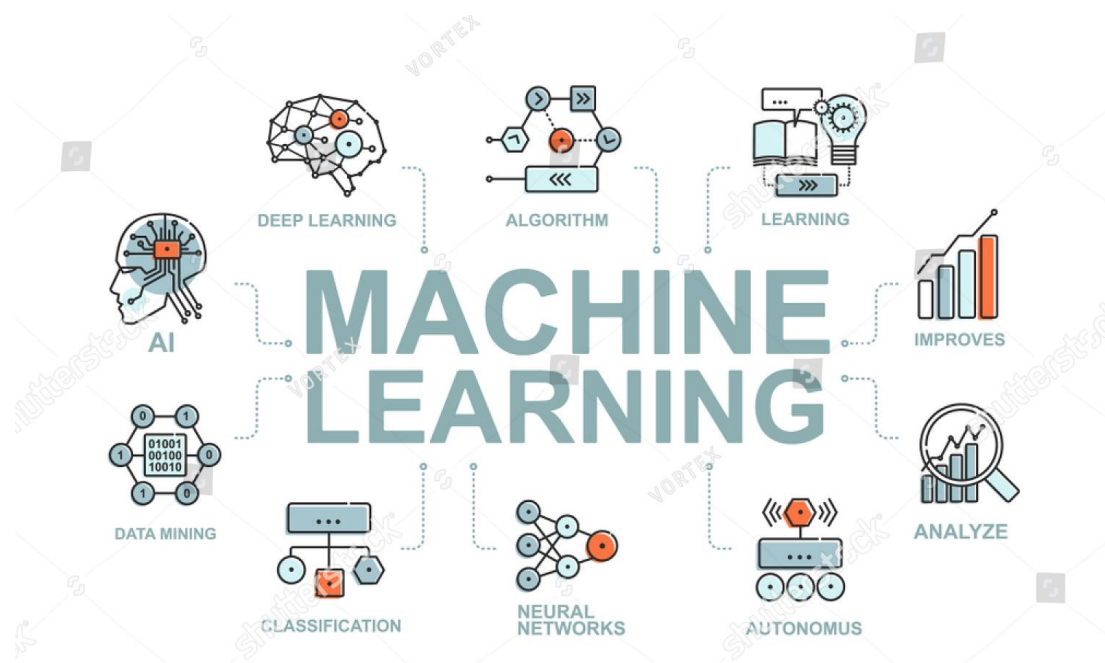
机器学习跟其它领域的关系

机器学习

机器学习：以数据为经验的载体，利用经验数据不断提高性能的计算机系统/程序/算法

广袤的交叉学科

内容非常丰富



机器学习与其它领域的关系

- 机器学习与数据挖掘

- 机器学习和数据挖掘都涉及数据分析
- 机器学习、数据库、统计学是数据挖掘的关键支撑技术
- 机器学习更偏技术方法，数据挖掘更偏应用些

- 机器学习与数据科学

- 机器学习是数据科学实现智能化的关键步骤——数据智能分析
 - 数据科学还包括很多内容，例如收集、存储、传输、管理大数据
 - 大数据研究目的是为了利用大数据，没有机器学习提供数据分析技术，大数据利用无从谈起
-

机器学习与其它领域的关系

- 机器学习和计算机视觉
 - 机器学习是计算机视觉的核心技术
 - 计算机视觉是机器学习的重要应用
 - 机器学习和自然语言处理、模式识别
 - 参考计算机视觉
 - 机器学习和统计学
 - 统计学是机器学习的重要理论基础
 - 机器学习和神经科学
 - 机器学习发展过程中，经常受到神经科学思想的启发
 - 神经科学发展比较缓慢，不够成熟，机器学习通常借鉴其思想，不会借鉴它的技术基础（例如，借鉴鸟儿造飞机，但是飞机的原理技术跟鸟没关系，主要靠物理、机械、材料等科学）
-

机器学习主要学术进展从哪得到

学术会议

- ICML (International Conference on Machine Learning)
 - NeurIPS (Neural Information Processing Systems)
 - ICLR (International Conference on Learning Representation)
 - KDD (ACM SIGKDD Conf. on Knowledge Discovery and Data Mining)
 - AAI (AAAI conference on Artificial Intelligence)
 - IJCAI (International Joint Conference on Artificial Intelligence)
 - COLT (Conference on Learning Theory)
 - 国内：MLA、Valse、CCML、CCDM....
-

中国机器学习及其应用研讨会

为了促进智能信息处理领域同行间的交流，陆汝钤院士发起组织了“智能信息处理系列研讨会”。“机器学习及其应用”研讨会自2002年开始，先后在上海、南京、北京、西安等地举行。该研讨会每年邀请海内外从事机器学习及相关领域研究的专家与会进行学术交流。研讨会不征文，不收取注册费，欢迎机器学习及相关领域的学者、研究生前来旁听特邀报告并参加讨论。为了促进机器学习及相关领域的研究生之间以及研究生与资深学者之间的交流，2006-2010年在机器学习及其应用研讨会（MLA）期间，同时举行了机器学习及其应用学生研讨会（SSMLA），此后该研讨会融入MLA的Poster session.

以下是各年会议的信息：

MLA'20		2020年11月，南京大学
MLA'19		2019年11月，天津大学
MLA'18		2018年11月，南京大学
MLA'17		2017年11月，北京交通大学
MLA'16		2016年11月，南京大学
MLA'15		2015年11月，南京大学
MLA'14		2014年11月，西安电子科技大学
MLA'13		2013年11月，复旦大学
MLA'12		2012年11月，清华大学
MLA'11		2011年11月，清华大学
MLA'10	SSMLA'10	2010年11月，南京大学
MLA'09	SSMLA'09	2009年11月，南京大学
MLA'08	SSMLA'08	2008年11月，南京大学
MLA'07	SSMLA'07	2007年11月，南京大学、南京师范大
MLA'06	SSMLA'06	2006年11月，南京大学、南京航空航



MLA'18 - The 16th China Symposium on Machine Learning and Applications
第十六届中国机器学习及其应用研讨会
2018年11月2-4日，南京大学，南京

会议首页

组织机构

特邀专家

会议日程

顶会论文交流

食宿安排

赞助支持

会议地点

会议文集

以往会议

会议照片

会议照片

所有照片均已缩小，若要查看原图，请点击图片

开幕式：



Michael K. Ng教授做大会报告：



学术期刊

- AIJ 《Artificial Intelligence》
 - JMLR 《Journal of Machine Learning Research》
 - TPAMI 《IEEE Trans. on Pattern Analysis and Machine Intelligence》
 - TKDE 《IEEE Trans. on Knowledge and Data Engineering》
 - MLJ 《Machine Learning》
 - TNNLS 《IEEE Trans. on Neural Network and Learning Systems》
 - 国内：《中国科学 信息科学》
 - ...
-

<https://arxiv.org/>

Physics

- Astrophysics (**astro-ph** new, recent, search)
includes: Astrophysics of Galaxies; Cosmology and Nongalactic Astrophysics; Earth and Planetary Astrophysics; High Energy Astrophysical Phenomena; Instrumentation and Methods for Astrophysics; Solar and Stellar Astrophysics
- Condensed Matter (**cond-mat** new, recent, search)
includes: Disordered Systems and Neural Networks; Materials Science; Mesoscale and Nanoscale Physics; Other Condensed Matter; Quantum Gases; Soft Condensed Matter; Statistical Mechanics; Strongly Correlated Electrons; Superconductivity
- General Relativity and Quantum Cosmology (**gr-qc** new, recent, search)
- High Energy Physics – Experiment (**hep-ex** new, recent, search)
- High Energy Physics – Lattice (**hep-lat** new, recent, search)
- High Energy Physics – Phenomenology (**hep-ph** new, recent, search)
- High Energy Physics – Theory (**hep-th** new, recent, search)
- Mathematical Physics (**math-ph** new, recent, search)
- Nonlinear Sciences (**nlin** new, recent, search)
includes: Adaptation and Self-Organizing Systems; Cellular Automata and Lattice Gases; Chaotic Dynamics; Exactly Solvable and Integrable Systems; Pattern Formation and Solitons
- Nuclear Experiment (**nucl-ex** new, recent, search)
- Nuclear Theory (**nucl-th** new, recent, search)
- Physics (**physics** new, recent, search)
includes: Accelerator Physics; Applied Physics; Atmospheric and Oceanic Physics; Atomic and Molecular Clusters; Atomic Physics; Biological Physics; Chemical Physics; Classical Physics; Computational Physics; Data Analysis, Statistics and Probability; Fluid Dynamics; General Physics; Geophysics; History and Philosophy of Physics; Instrumentation and Detectors; Medical Physics; Optics; Physics and Society; Physics Education; Plasma Physics; Popular Physics; Space Physics
- Quantum Physics (**quant-ph** new, recent, search)

Mathematics

- Mathematics (**math** new, recent, search)
includes: (see detailed description): Algebraic Geometry; Algebraic Topology; Analysis of PDEs; Category Theory; Classical Analysis and ODEs; Combinatorics; Commutative Algebra; Complex Variables; Differential Geometry; Dynamical Systems; Functional Analysis; General Mathematics; General Topology; Geometric Topology; Group Theory; History and Overview; Information Theory; K-Theory and Homology; Logic; Mathematical Physics; Metric Geometry; Number Theory; Numerical Analysis; Operator Algebras; Optimization and Control; Probability; Quantum Algebra; Representation Theory; Rings and Algebras; Spectral Theory; Statistics Theory; Symplectic Geometry

Computer Science

- Computing Research Repository (**CoRR** new, recent, search)
includes: (see detailed description): Artificial Intelligence; Computation and Language; Computational Complexity; Computational Engineering, Finance, and Science; Computational Geometry; Computer Science and Game Theory; Computer Vision and Pattern Recognition; Computers and Society; Cryptography and Security; Data Structures and Algorithms; Databases; Digital Libraries; Discrete Mathematics; Distributed, Parallel, and Cluster Computing; Emerging Technologies; Formal Languages and Automata Theory; General Literature; Graphics; Hardware Architecture; Human-Computer Interaction; Information Retrieval; Information Theory; Logic in Computer Science; Machine Learning; Mathematical Software; Multiagent Systems; Multimedia; [Networking and Internet Architecture](#); Neural and Evolutionary Computing; Numerical Analysis; Operating Systems; Other Computer Science; Performance; Programming Languages; Robotics; Social and Information Networks; Software Engineering; Sound; Symbolic Computation; Systems and Control

Quantitative Biology

- Quantitative Biology (**q-bio** new, recent, search)
includes: (see detailed description): Biomolecules; Cell Behavior; Genomics; Molecular Networks; Neurons and Cognition; Other Quantitative Biology; Populations and Evolution; Quantitative Methods; Subcellular Processes; Tissues and Organs

Quantitative Finance

- Quantitative Finance (**q-fin** new, recent, search)
includes: (see detailed description): Computational Finance; Economics; General Finance; Mathematical Finance; Portfolio Management; Pricing of Securities; Risk Management; Statistical Finance; Trading and Market Microstructure

Statistics

- Statistics (**stat** new, recent, search)
includes: (see detailed description): Applications; Computation; Machine Learning; Methodology; Other Statistics; Statistics Theory

公众号



AI科技评论

雷峰网旗下AI新媒体。聚焦AI前沿研究，关注AI工程落地。

深圳英鹏图灵科技有限公司 [已关注](#)

AI+X

大模型



机器之心

专业的人工智能媒体和产业服务平台

机器之心(北京)科技有限公司 [已关注](#)

课程资源

2024秋招



量子位

追踪人工智能新趋势，关注科技行业新突破

北京极客伙伴科技有限公司 [已关注](#)

智库

文章搜索

AI年度评选

投稿爆料

新智元 - 公众号

[更多 >](#)



新智元

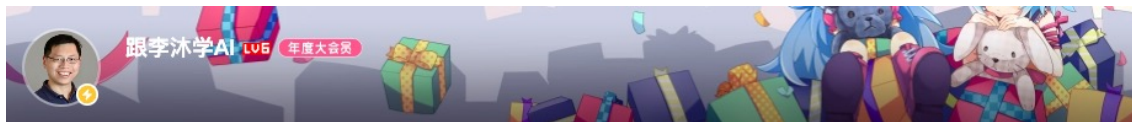
智能+中国主平台，致力于推动中国从互联网+迈向智能+新纪元。重点...

北京中经智元科技发展有限公司 [已关注](#)

搜索

投稿

视频



🏠 主页

📌 动态

📁 投稿 240

📁 合集和列表 7

🔍 搜索视频、动态

合集·【更新中】AI 论文精读 53

▶ 播放全部 更多 >

如何读论文

如何读论文【论文精读·1】

▶ 34.8万 2021-10-6

AlexNet的报告也曾被大佬们喷过?

9年后重读深度学习奠基作之一: AlexNet【论文精读·2】

▶ 23.3万 2021-10-14

AlexNet论文中有多少观点现在看都不对?

AlexNet论文逐段精读【论文精读】

▶ 22.3万 2021-10-15

网络越深效果越差?

撑起计算机视觉半边天的ResNet【论文精读】

▶ 17.2万 2021-10-21

残差连接在做什么?

ResNet论文逐段精读【论文精读】

▶ 23.1万 2021-10-22

合集·【更新中】动手用AI 11

▶ 播放全部 更多 >



Windows 上安装和使用 AutoGluon v0.4

▶ 8万 2022-3-29



AutoGluon背后的技术

▶ 6.8万 2021-5-17



10行代码战胜90%数据科学家?

▶ 21万 2021-5-9



使用 AWS 最便宜的 GPU 实例 - 动手学深度学习v2

▶ 8.1万 2021-4-9



Windows 下安装 CUDA 和 Pytorch 跑深度学习 - 动手学

▶ 23.9万 2021-4-6

合集·斯坦福2021秋季·实用机器学习【中文】【合集】 29

▶ 播放全部 更多 >



1.1 课程介绍【斯坦福21秋季: 实用机器学习中文版】

▶ 33.1万 2021-9-17



1.2 数据获取【斯坦福21秋季: 实用机器学习中文版】

▶ 10.3万 2021-9-20



1.3 网页数据抓取【斯坦福21秋季: 实用机器学习中文版】

▶ 8万 2021-9-22



1.4 数据标注【斯坦福21秋季: 实用机器学习中文版】

▶ 7万 2021-9-24



2.1 探索性数据分析【斯坦福21秋季: 实用机器学习中文

▶ 6.1万 2021-9-27

机器学习预往何处？

只是畅想一种可能的未来

人工智能寒冬

- 1) 低估智能的复杂性
- 2) 脱离现实问题

90年代初，第二次人工智能寒冬

- AI硬件市场需求下跌
 - 专家系统维护成本高昂
 - 日本五代机失败
 - DARPA大幅缩减AI项目资助
-

稳健性是硬伤

Machine Learning (

AlphaGo 并非“解决之道”

AlphaGo is not the solution to AI

Tags: AI, Machine Learning, Reinforcement - jli@ 4:46 pm

Congratulations are in order for the folks at Google Deepmind who ha

However, some of the discussion
Machines have conquered the la
need any big new breakthroughs



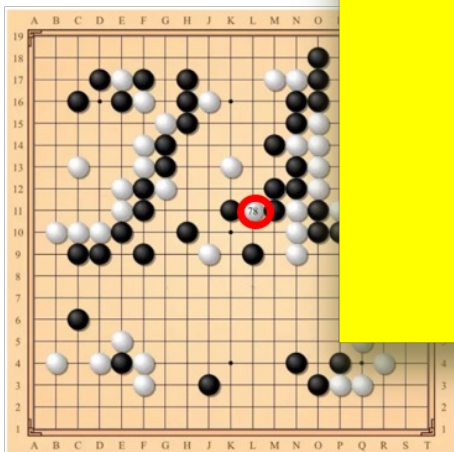
John Langford

国际机器学习大会
ICML'12的程序主席

人类犯错：水平从九段降到八段
机器犯错：水平从九段降到业余

离“超越人类棋手”还远

“鲁棒性”是关键！



3月13日李世石九段的
“神之一手”



是的

刘菁八段

后面的招法一看机器离认输不远了

刘菁八段

就和您说的一样 后面的下法就跟不会下棋一样了

会了，以后还



AlphaGo以为自
做得很好，但
第87手迷惑了。
我们有麻烦了

错误出现在第79
手犯了错误，但
AlphaGo在第87
手才发现



Mistake was on move 79, but #AlphaGo
only came to that realisation on around
move 87



350

163

国际上对AI发展的探讨

AAAI “主席报告” (“Presidential Address”)



STEPS TOWARD ROBUST ARTIFICIAL INTELLIGENCE

走向鲁棒的人工智能

Tom Dietterich
President, Association for the Advancement of Artificial
Intelligence

Tom Dietterich

AAAI/AAAS/ACM Fellow

AAAI 现任主席

国际机器学习学会创始主席 (2001-2008)

国际上对AI发展的探讨

T. Dietterich强调：随着人工智能技术的发展，越来越多地面临“高风险应用”

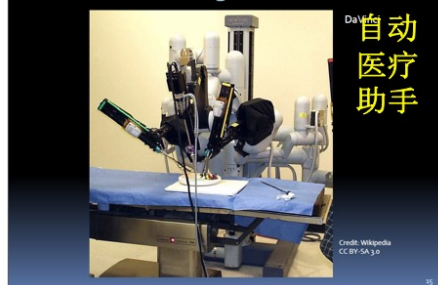
因此，必须要有“鲁棒的AI”

- 对人类用户错误鲁棒
- 对网络攻击鲁棒
- 对错误目标鲁棒
- 对不正确模型鲁棒
- 对未建模现象鲁棒

Self-Driving Cars 自动驾驶汽车



Automated Surgical Assistants



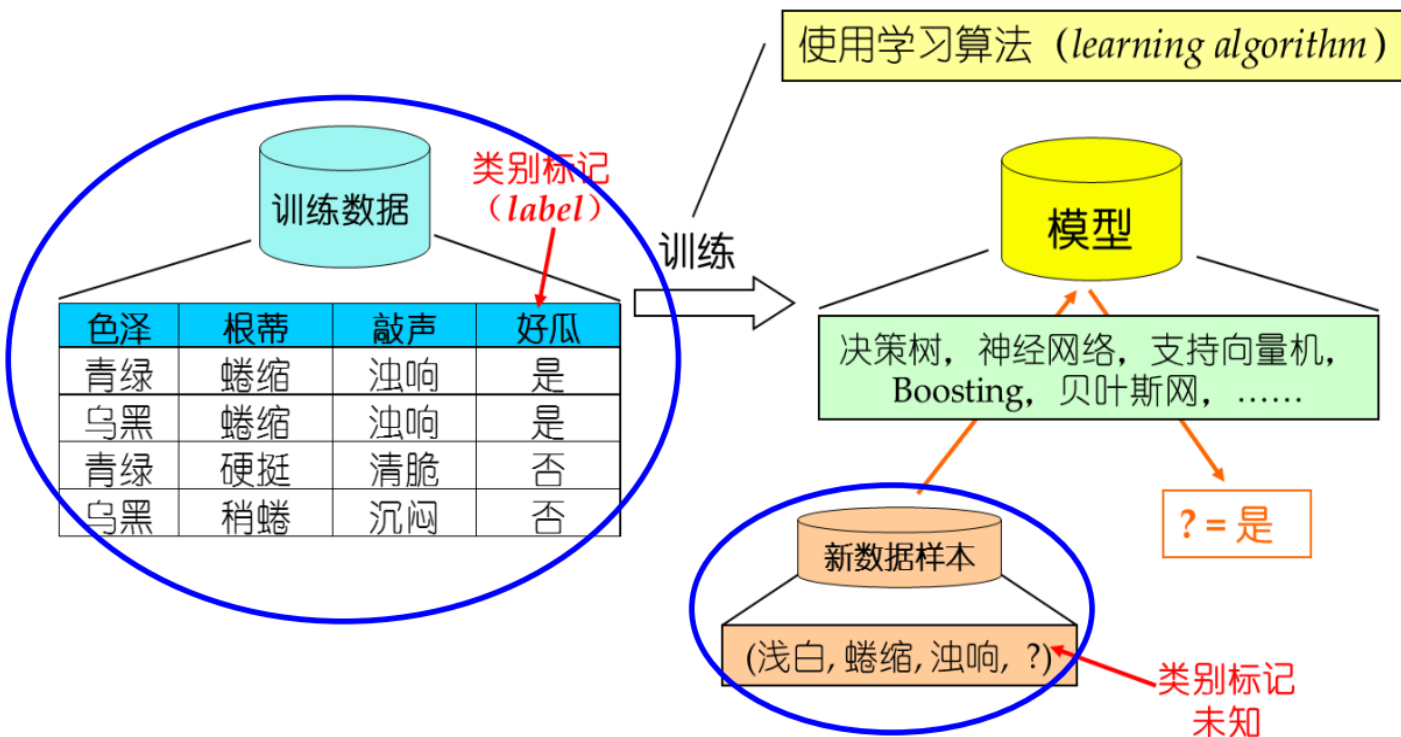
Autonomous Weapons 自主武器



传统机器学习任务

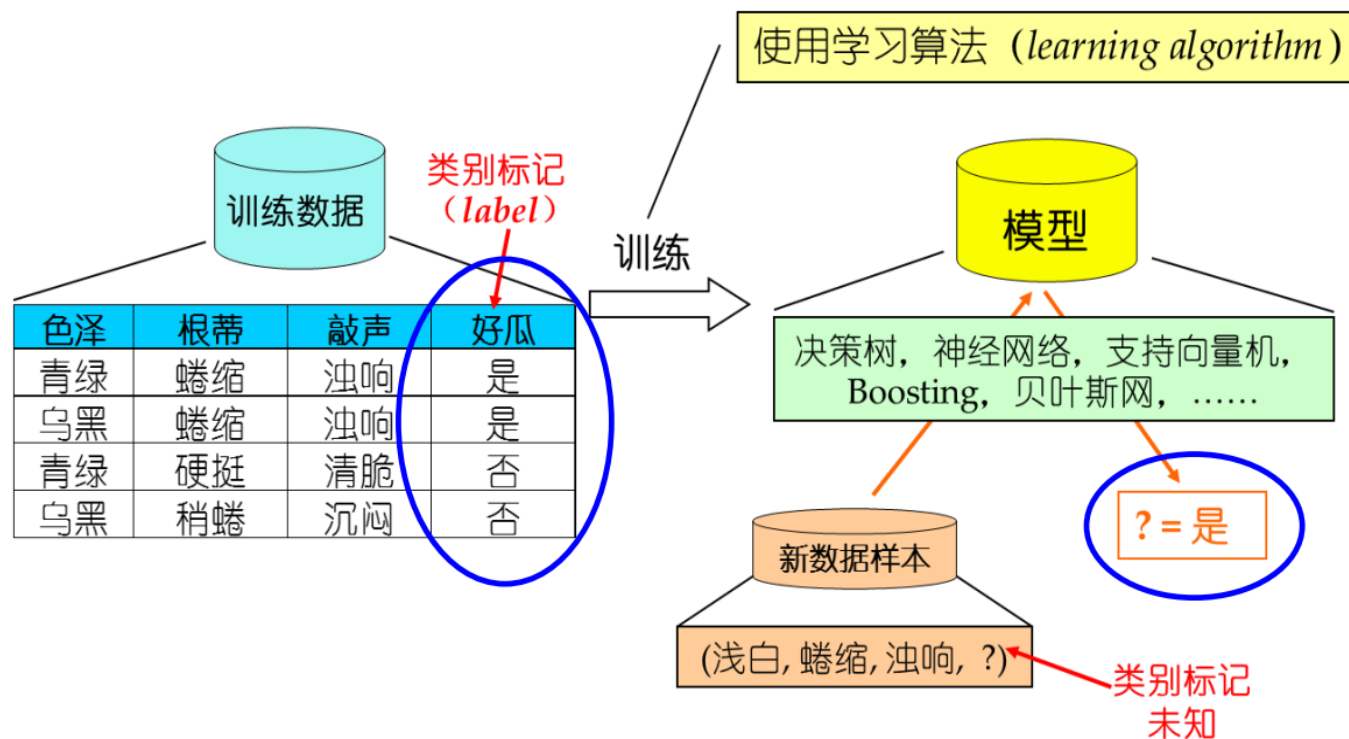
主要针对封闭静态环境（重要因素大多是“定”的）

数据分布恒定



传统机器学习任务

主要针对封闭静态环境（重要因素大多是“定”的）

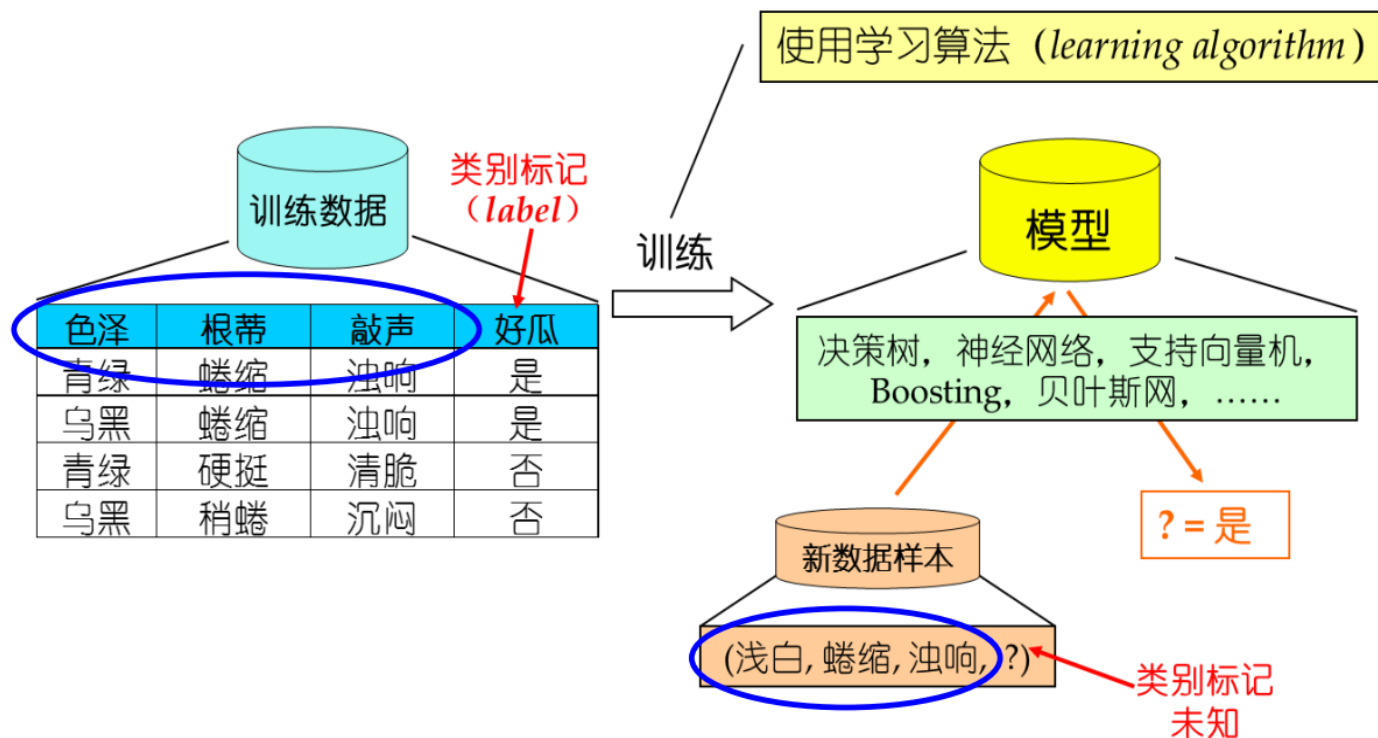


数据分布恒定

样本类别恒定

传统机器学习任务

主要针对封闭静态环境（重要因素大多是“定”的）



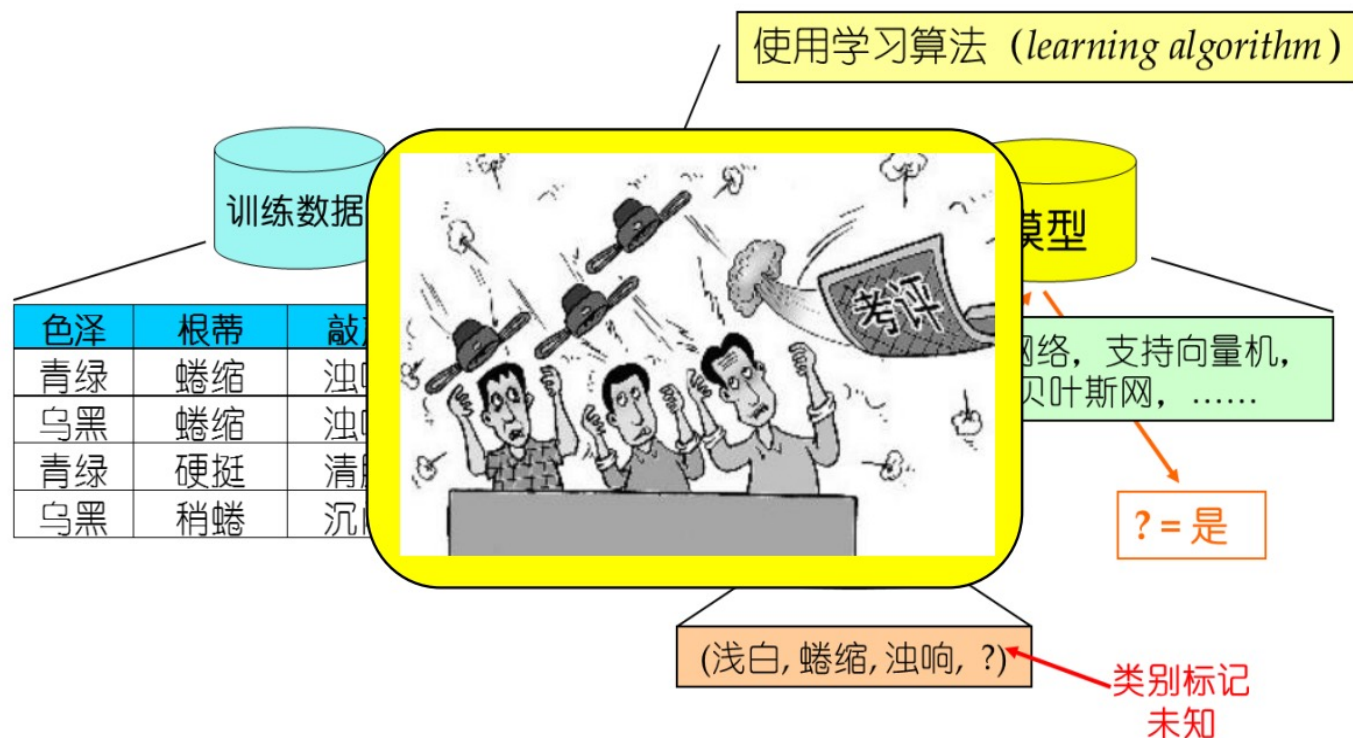
数据分布恒定

样本类别恒定

样本属性恒定

传统机器学习任务

主要针对封闭静态环境（重要因素大多是“定”的）



数据分布恒定

样本类别恒定

样本属性恒定

评价目标恒定

传统机器学习任务

主要针对封闭静态环境（重要因素大多是“定”的）

使用学习算法 (*learning algorithm*)

数据分布恒定

类别恒定

属性恒定

目标恒定

色泽	根蒂
青绿	蜷缩
乌黑	蜷缩
青绿	硬挺
乌黑	稍蜷

封闭静态环境 → 开放动态环境

一切都可能“变”！

雪龙号面临的难题



极地海冰数据分析与航行指导



海洋变化

海冰分布
持续变化

分布
偏移



极地风暴

冰川断裂

未知险情
时有发生

类别
增长



电磁暴

信息获取
干扰严重

属性
退化



航线安全

破冰效率

海冰收集

航路优化
任务兼顾

目标
多样

知识数据双驱动的机器学习

人工智能领域的“圣杯问题”:

A unified framework which accommodates and enables **machine learning** and **logical reasoning** to **work together**

Why ?

- ✓ “逻辑推理” 易于利用 知识
- ✓ “机器学习” 易于利用 数据
 - 大多数“人类决策” 是基于 知识+数据

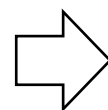
然而，在人工智能学科历史上，逻辑推理与机器学习几乎是完全独立发展

- 1956~1990s: 逻辑推理 + 知识工程
 - 1990s~: 机器学习
-

主要障碍

- 逻辑推理一般基于一阶逻辑表示，例如，

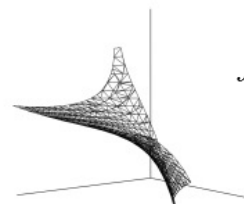
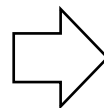
$\forall x \forall y. \text{Parent}(x, y) \Rightarrow \text{Older}(x, y)$
 $\forall x \forall y. \text{Mother}(x, y) \Rightarrow \text{Parent}(x, y)$
 $\text{Mother}(\text{Lulu}, \text{Fifi})$



Who is older?
- Lulu

- 机器学习往往建立在特征表示的基础上，

Name	Rank	Years	Tenured
Mike	Assistant Prof	3	no
Mary	Associate Prof	7	yes
Bill	Professor	2	yes
Jim	Associate Prof	7	yes
Dave	Assistant Prof	6	no
Anne	Associate Prof	3	no



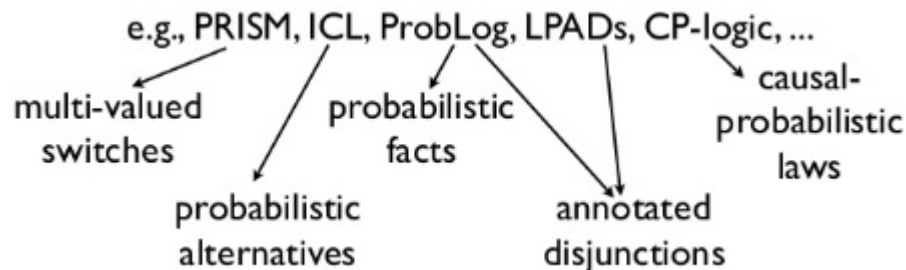
$$f(\mathbf{x}) = \sum_{i=1}^N \alpha_i K(\mathbf{x}_i, \mathbf{x})$$

$$K(\mathbf{x}_i, \mathbf{x}) = \langle \phi(\mathbf{x}_i), \phi(\mathbf{x}) \rangle$$

以往的努力

➤ 概率逻辑程序设计 (Probabilistic Logic Programming, PLP)

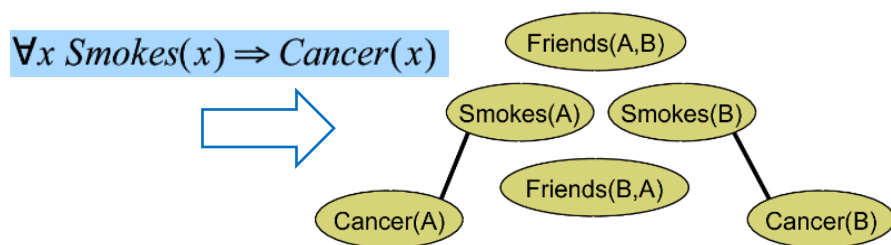
试图通过扩展一阶逻辑来获得概率内涵，从而使得概率推理得以引入



推理 “重”、学习 “轻”

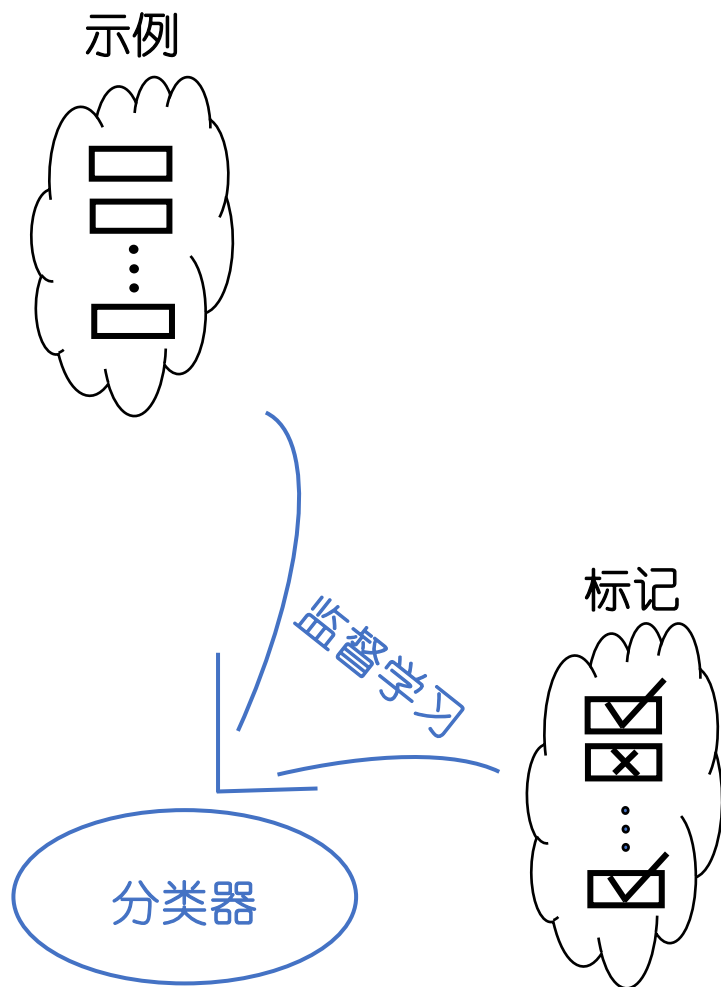
➤ 统计关系学习 (Statistical Relational Learning, SRL)

试图基于一阶逻辑子句表达的领域知识来构造/初始化一个概率模型

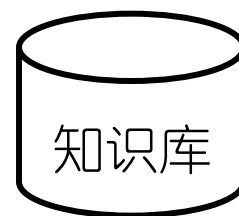
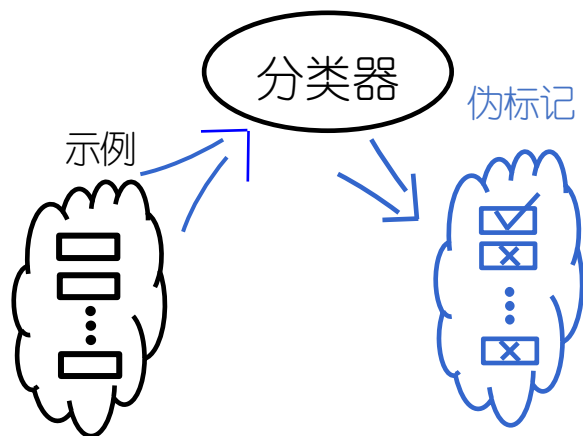


学习 “重”、推理 “轻”

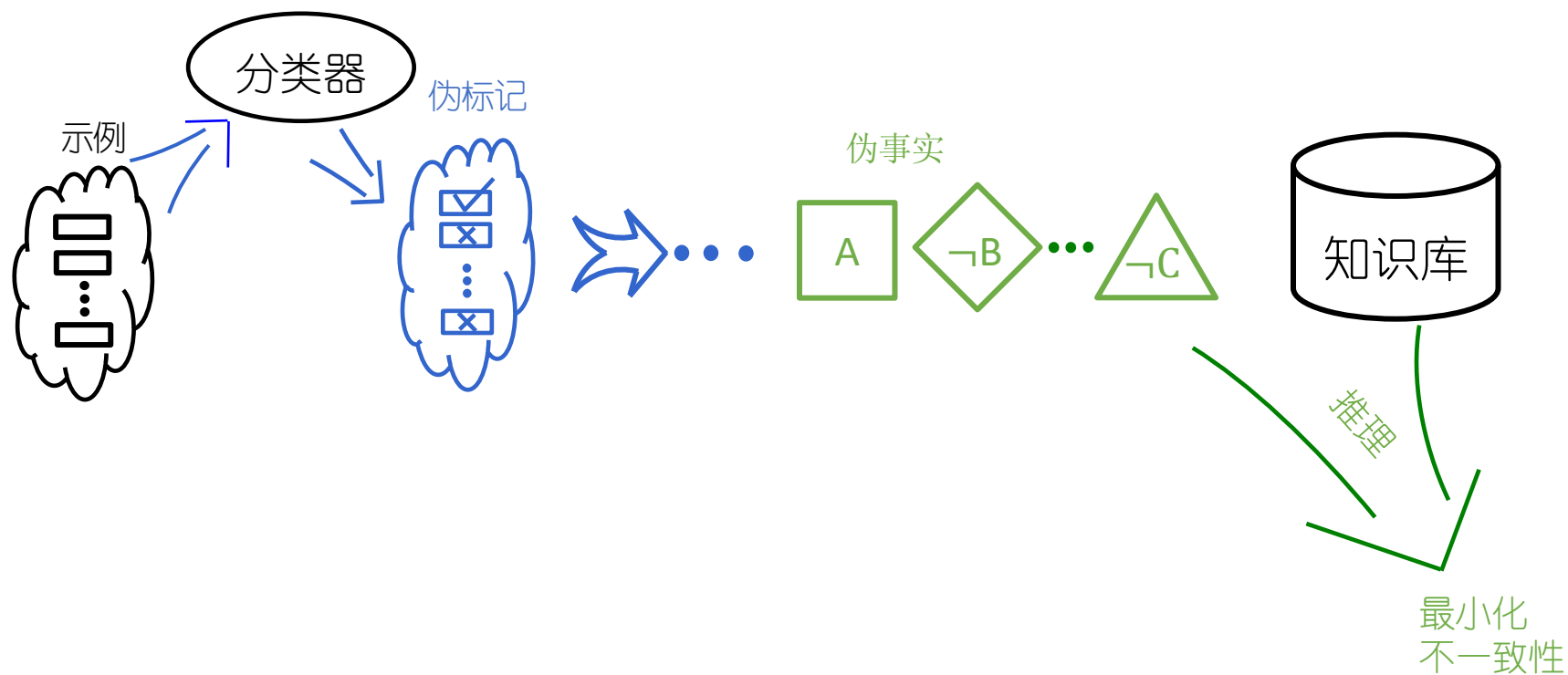
目前的机器学习：数据驱动



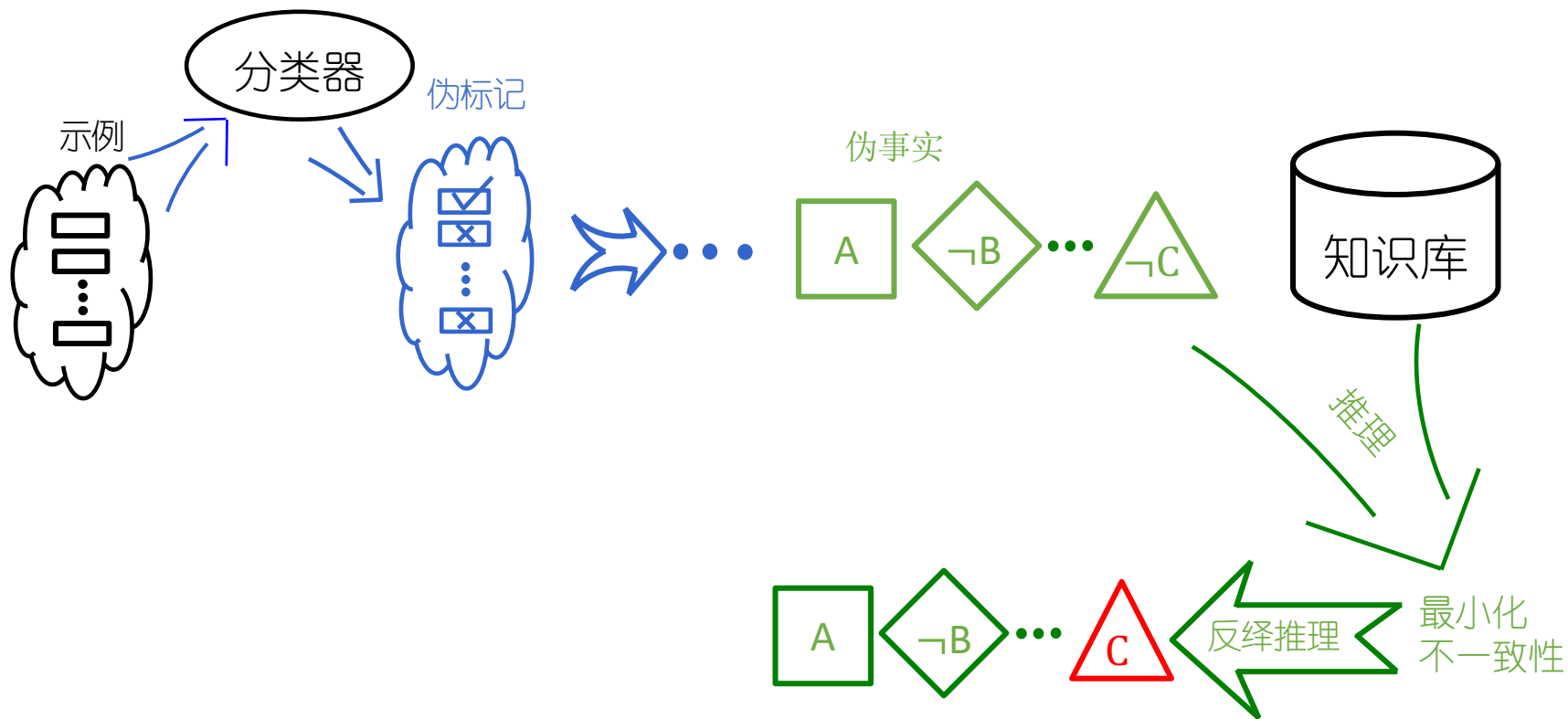
反绎学习：知识数据双驱动



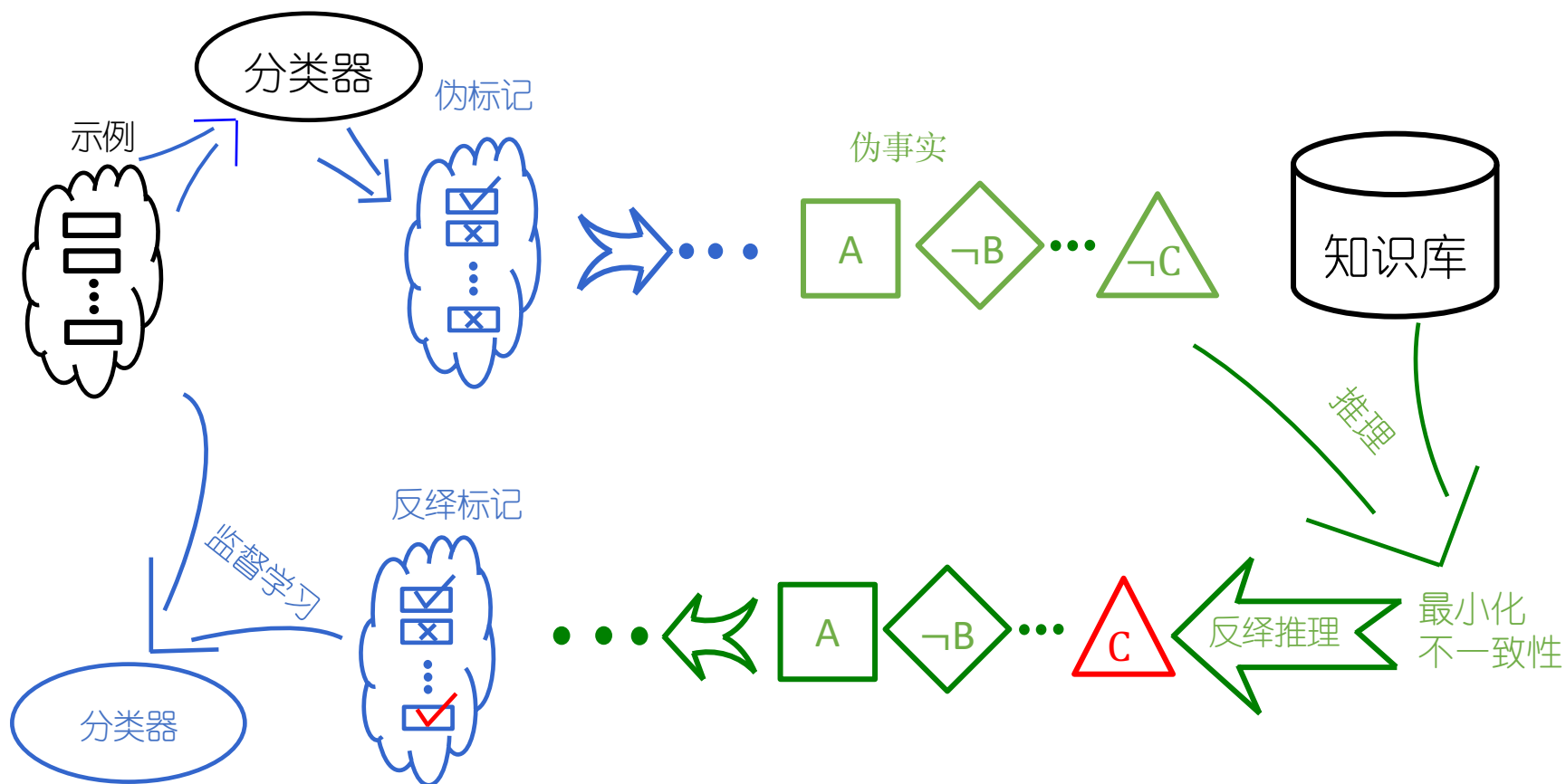
反绎学习：知识数据双驱动



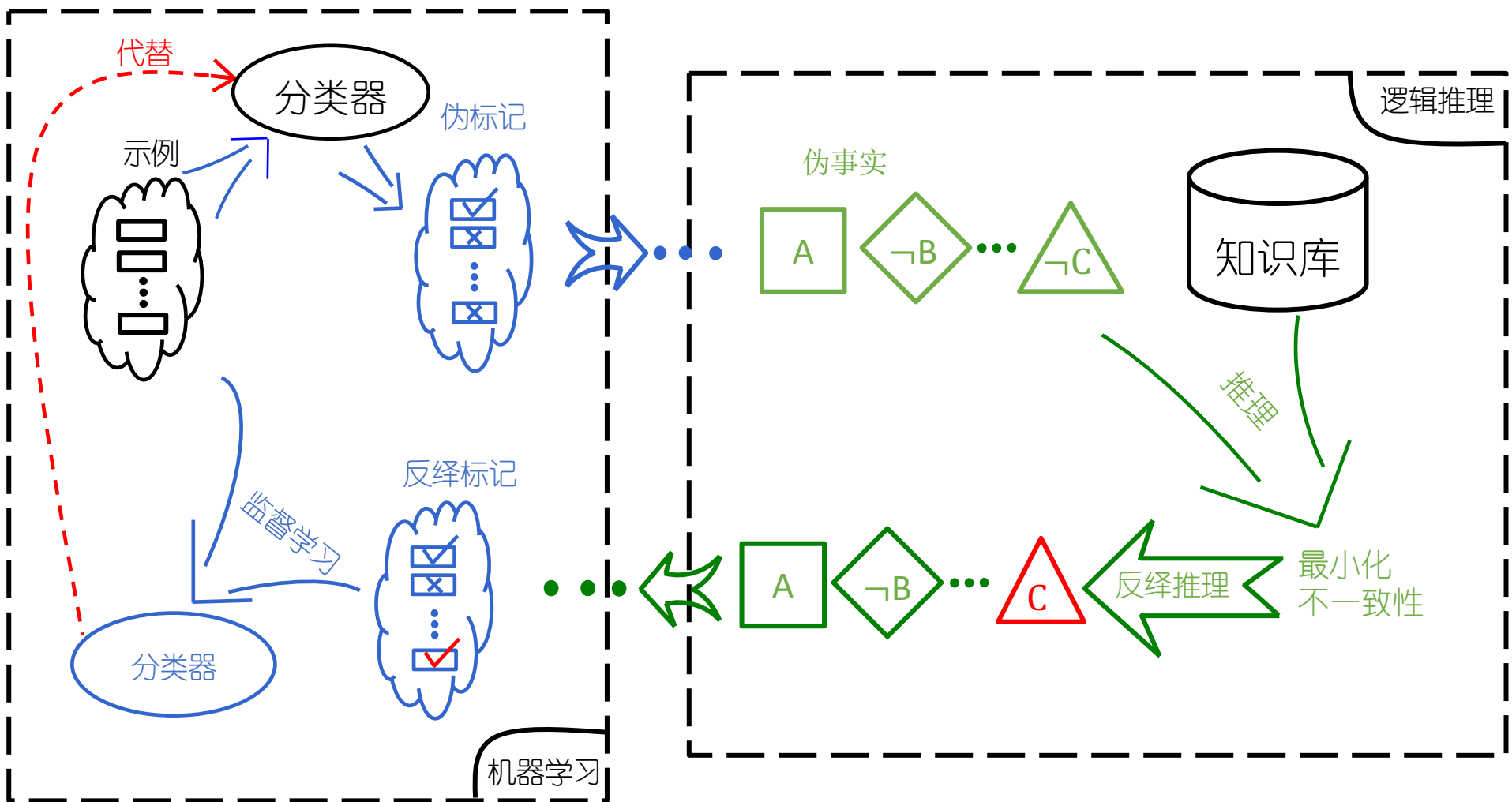
反绎学习：知识数据双驱动



反绎学习：知识数据双驱动



反绎学习：知识数据双驱动



形态

“机器学习” 的形态是什么？

算 法 + 数 据

有哪些技术局限/瓶颈？

技术局限 (1): 需要大量训练样本

大数据时代, 训练样本数量不再是问题? **NO!**

样本总量少



油田定位: 数据必须通过昂贵的人工诱发深海地震获取, 数量很少

.....

特定类样本少



信用卡欺诈检测: 相对于正常交易数量, 信用卡欺诈数量很少

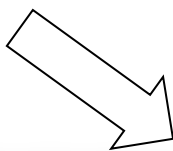
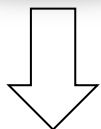
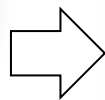
有标记样本少



软件缺陷检测: 被程序员标注的缺陷数量少

技术局限 (2): 难以适应环境变化

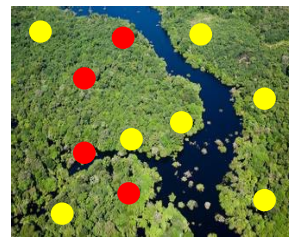
环境变化



环境监控



一周后:



60% 传感器失效, 新增 60% 传感器

难点: 属性变动

物种监测



夏天



冬天



背景随季节改变

难点: 分布变化

自动驾驶



汽车厂商设想的场景

上路后遇到的场景



.....

难点: 类别增加

技术局限 (3): 黑箱模型

黑箱模型难以用于高风险应用



智能医疗：个性化治疗方案

若学习器不能给出治疗理由，则难以说服患者接受昂贵的治疗方案



智能电网：大型变电站停机检测

若学习器不能给出停机检测的理由，则难以判断停机检测的风险和代价

技术局限 (3): 黑箱模型

黑箱模型难以用于高风险应用



智能医疗：个性化治疗方案

若学习器不能给出治疗理由，则难以说服患者接受昂贵的治疗方案



智能电网：大型变电站停机检测

若学习器不能给出停机检测的理由，则难以判断停机检测的风险和代价



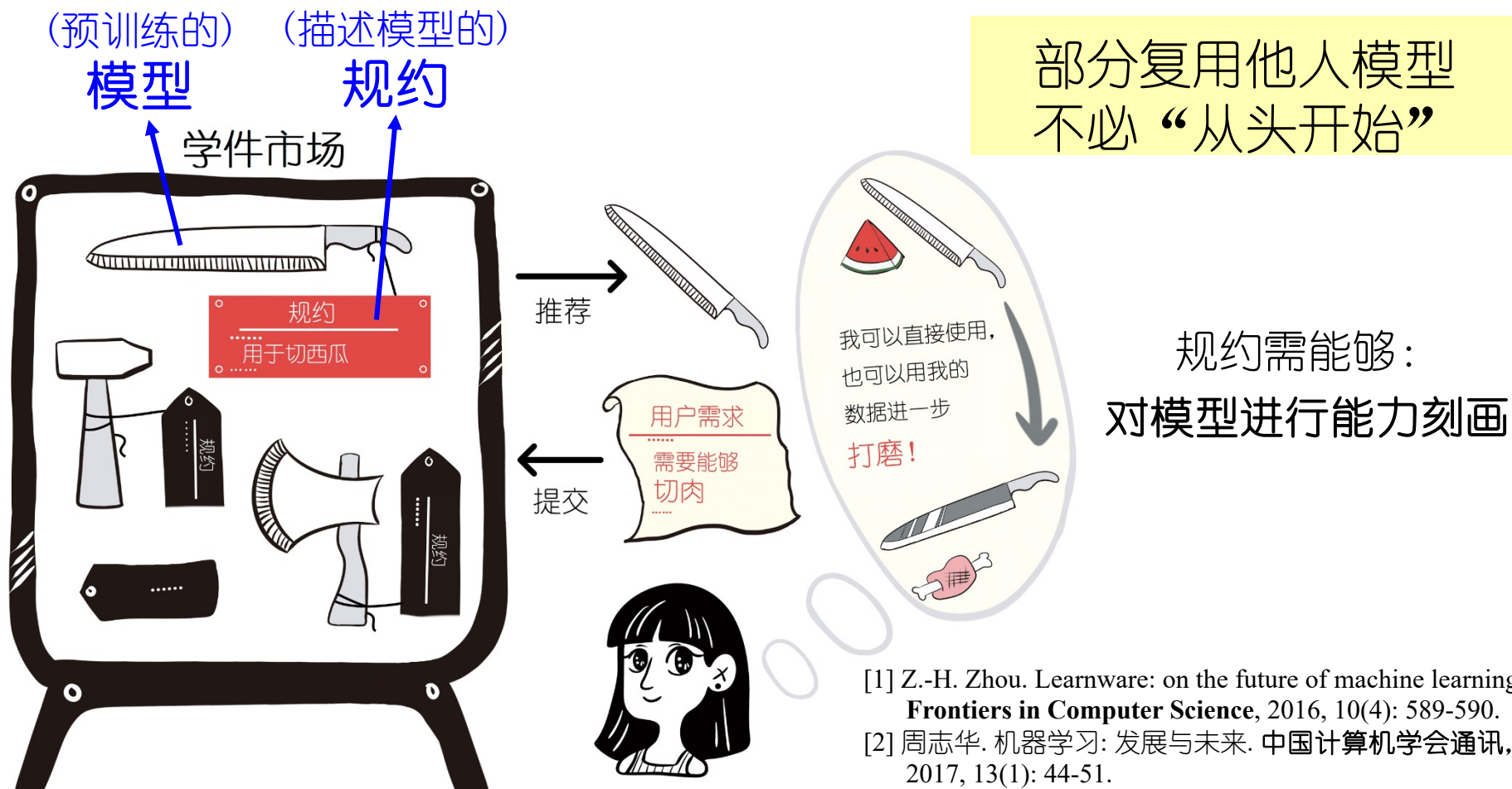
即便相同数据，普通用户很难获得机器学习专家级性能

数据隐私和安全



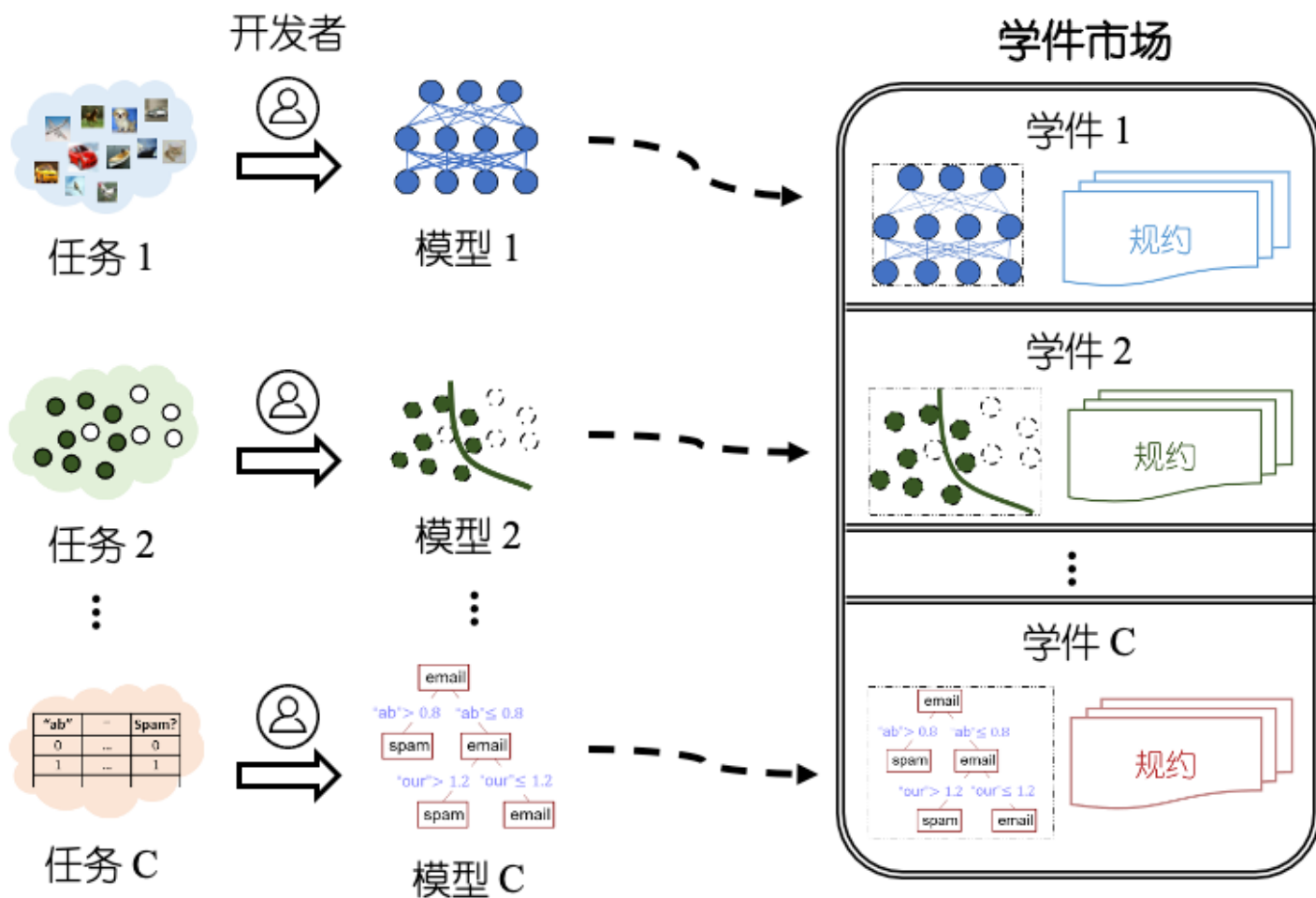
学件 (Learnware)

学件 (Learnware) = 模型 (model) + 规约 (specification)

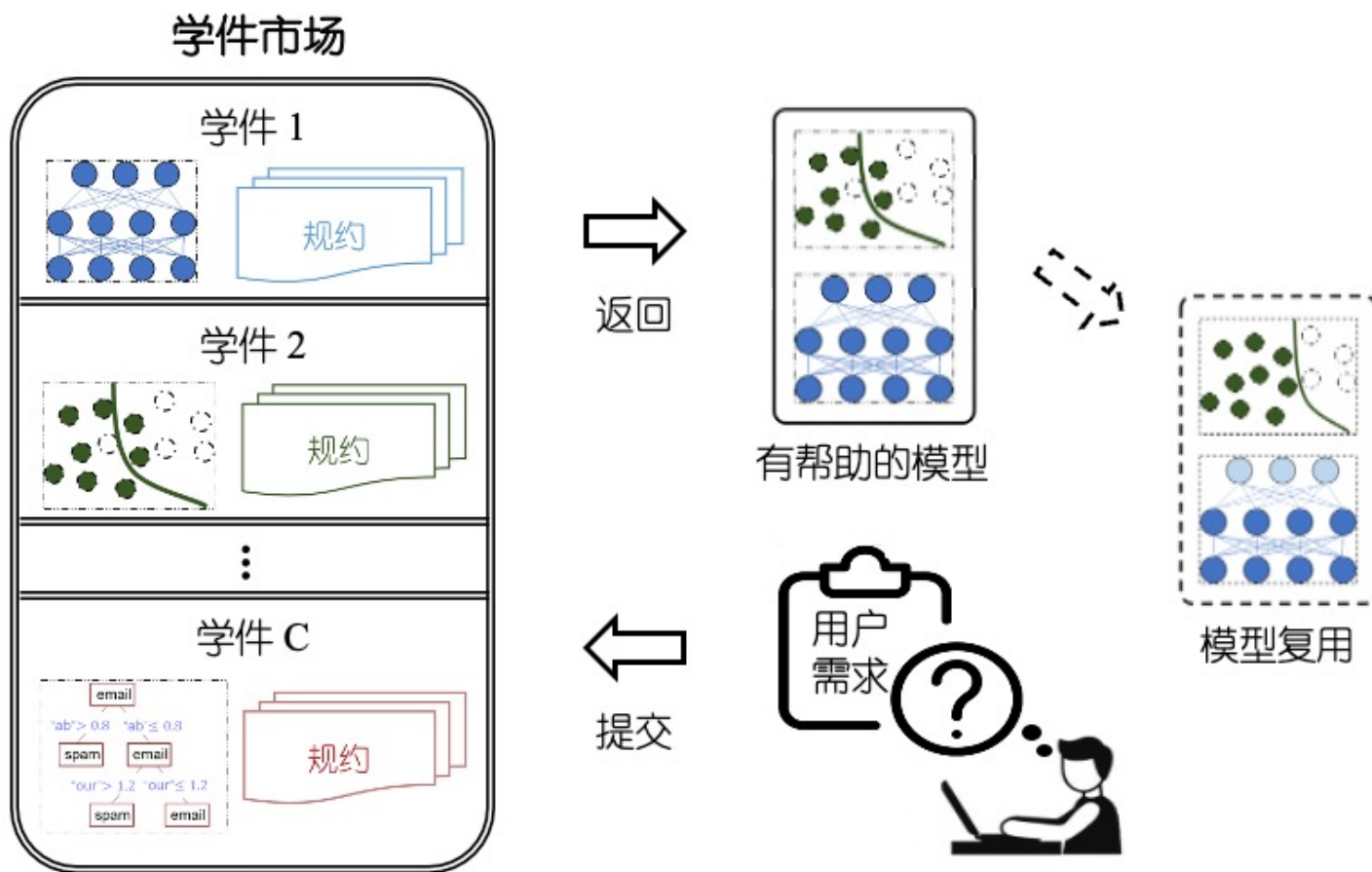


- [1] Z.-H. Zhou. Learnware: on the future of machine learning. *Frontiers in Computer Science*, 2016, 10(4): 589-590.
- [2] 周志华. 机器学习: 发展与未来. 中国计算机学会通讯, 2017, 13(1): 44-51.

学件工作流程：提交阶段



学件工作流程：部署阶段



机器学习是无所不能的吗？ No!

并非“一切皆可学”，例如：

- ◆ 特征信息不充分

- 例如，重要特征信息没有获得

- ◆ 样本信息不充分

- 例如，仅有很少的数据样本
-

机器学习具有坚实的理论基础

计算学习理论

Computational learning theory

最重要的理论模型：

PAC (Probably Approximately Correct,
概率近似正确) learning model [Valiant, 1984]

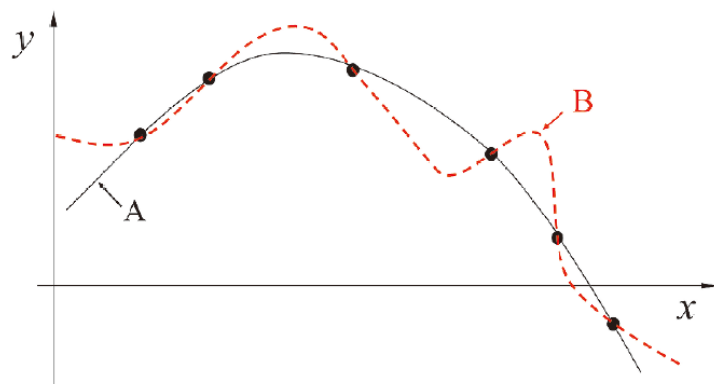
$$P(|f(\mathbf{x}) - y| \leq \epsilon) \geq 1 - \delta$$



Leslie Valiant
(莱斯利·维利昂特)
(1949-)
2010年图灵奖

归纳偏好 (inductive bias)

机器学习算法在学习过程中对某种类型假设的偏好



A更好?
B更好?

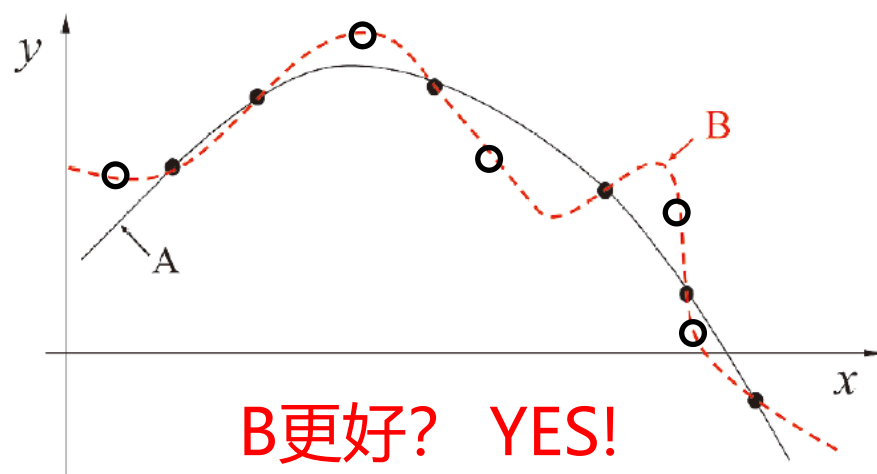
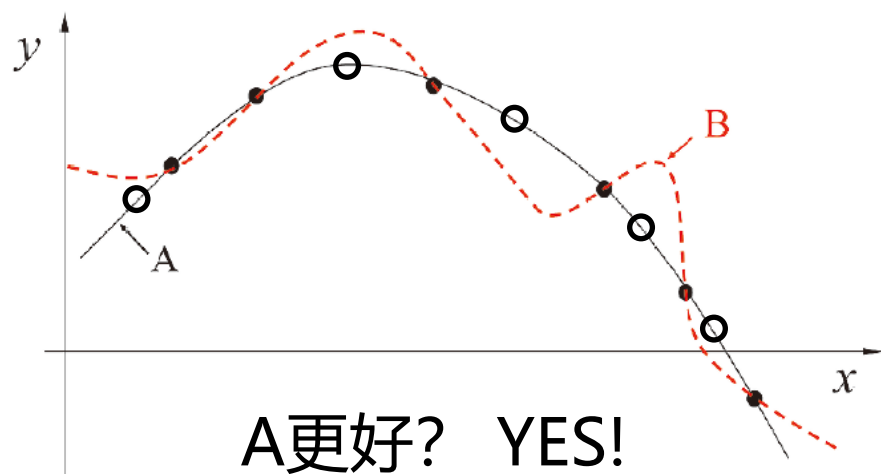
一般原则:
奥卡姆剃刀
(Occam's razor)

任何一个有效的机器学习算法必有其偏好

**学习算法的归纳偏好是否与问题本身匹配，
大多数时候直接决定了算法能否取得好的性能！**

哪个算法更好？

黑点：训练样本；白点：测试样本



没有免费的午餐！

NFL定理：一个算法 \mathcal{L}_a 若在某些问题上比另一个算法 \mathcal{L}_b 好，必存在另一些问题， \mathcal{L}_b 比 \mathcal{L}_a 好

哪个算法更好?

简单起见, 假设样本空间 \mathcal{X} 和假设空间 \mathcal{H} 离散, 令 $P(h|X, \mathfrak{L}_a)$ 代表算法 \mathfrak{L}_a 基于训练数据 X 产生假设 h 的概率, f 代表要学的目标函数, \mathfrak{L}_a 在训练集之外所有样本上的总误差为

$$E_{ote}(\mathfrak{L}_a|X, f) = \sum_h \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) P(h | X, \mathfrak{L}_a)$$

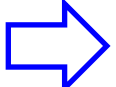
考虑二分类问题, 目标函数可以为任何函数 $\mathcal{X} \mapsto \{0, 1\}$ 函数空间为 $\{0, 1\}^{|\mathcal{X}|}$ 对所有可能的 f 按均匀分布对误差求和, 有

$$\sum_f E_{ote}(\mathfrak{L}_a|X, f) = \sum_f \sum_h \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) P(h | X, \mathfrak{L}_a)$$

哪个算法更好?

考虑二分类问题, 目标函数可以为任何函数 $\mathcal{X} \mapsto \{0, 1\}$ 函数空间为 $\{0, 1\}^{|\mathcal{X}|}$ 对所有可能的 f 按均匀分布对误差求和, 有

$$\begin{aligned}\sum_f E_{ote}(\mathcal{L}_a | X, f) &= \sum_f \sum_h \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) P(h | X, \mathcal{L}_a) \\&= \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \sum_f \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) \\&= \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \frac{1}{2} 2^{|\mathcal{X}|} \\&= \frac{1}{2} 2^{|\mathcal{X}|} \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \\&= 2^{|\mathcal{X}|-1} \sum_{\mathbf{x} \in \mathcal{X} - X} P(\mathbf{x}) \cdot 1\end{aligned}$$

总误差与学习算法无关!  所有算法同样好!

NFL定理的寓意

NFL定理的重要前提：

所有“问题”出现的机会相同、或所有问题同等重要

实际情形并非如此；我们通常只关注自己正在试图解决的问题

脱离具体问题，空泛地谈论“什么学习算法更好”
毫无意义！

具体问题，具体分析！

现实机器学习应用

把机器学习的“十大算法”“二十大算法”都弄熟，
逐个试一遍，是否就“止于至善”了？

NO !

机器学习并非“十大套路”“二十大招数”的简单堆积

现实任务千变万化，

以有限的“套路”应对无限的“问题”，焉有不败？

最优方案往往来自：**按需设计、度身定制**

前往第二站.....

