

# 人工神经网络（深度学习）2

王瑞轩

<http://isee.sysu.edu.cn/~wangruixuan/>

SUN YAT-SEN University



机器智能与先进计算  
教育部重点实验室

声明：该PPT只供非商业使用，也不可视为任何出版物。由于历史原因，许多图片尚没有标注出处，如果你知道图片的出处，欢迎告诉我们 at [wszheng@ieee.org](mailto:wszheng@ieee.org).

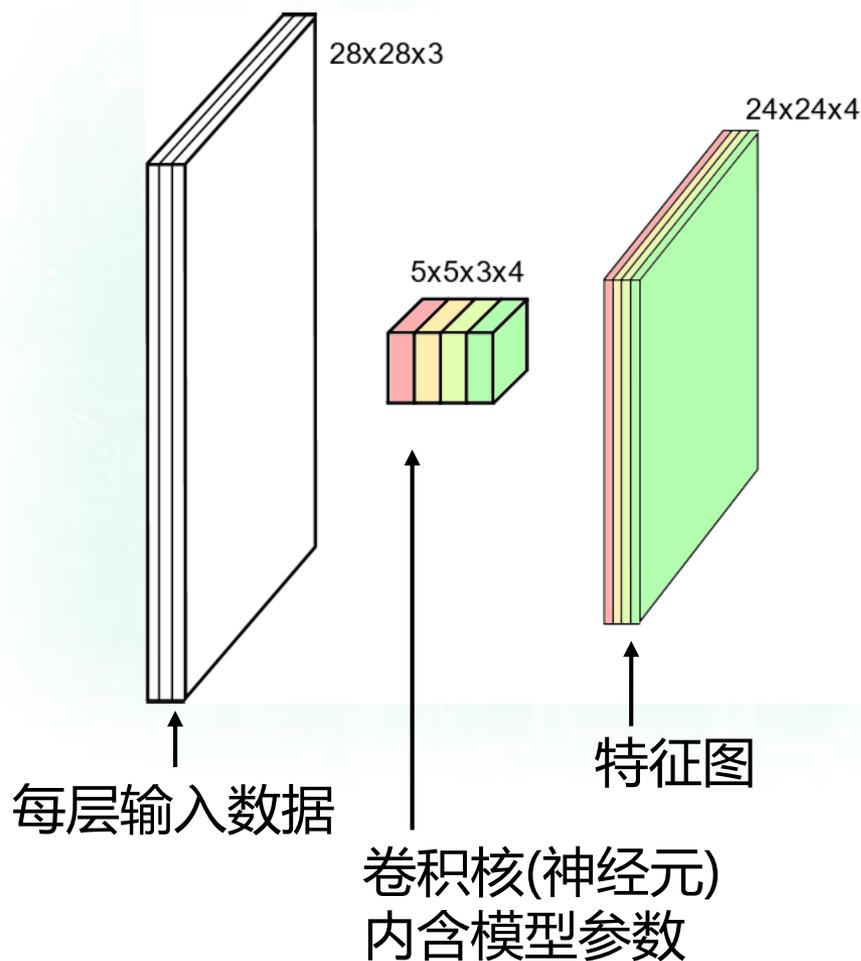


# 深度学习概览

- What: 揭神秘面纱
- Wow: 赏群模乱舞
- Why: 寻万能之源
- Where: 追研究前沿
- Whoops: 探未解之谜
- While: 评大众观点

# Recap: 卷积层

- ❑ 一个卷积层包含多个卷积操作，输出多个特征图
- ❑ 卷积层输出（经过激活函数等）作为下一卷积层的输入



Questions:

每个卷积核的维度?

卷积核通道数与输入通道数 (Channels) 的关系?



# Recap: 学习什么

“多层” 学习什么?

深度

学习

系统输入与输出的关系!  
数据中与任务相关的特征!  
函数 (模型) 的最佳参数!

# Recap: 如何学习

- 比如针对分类任务

$$\begin{aligned} \min_{\boldsymbol{\theta}} L(\boldsymbol{\theta}) &= \frac{1}{N} \sum_{i=1}^N l(\mathbf{y}_i, \mathbf{f}(\mathbf{x}_i; \boldsymbol{\theta})) \\ &= -\frac{1}{N} \sum_{i=1}^N \sum_{k=1}^K y_{ik} \log \hat{y}_{ik} \end{aligned}$$

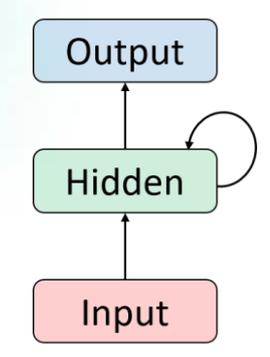
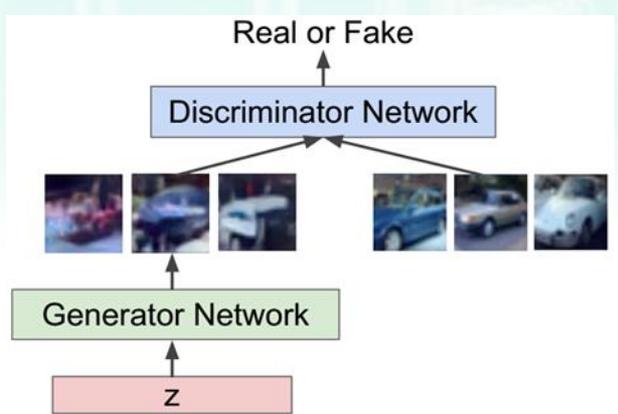
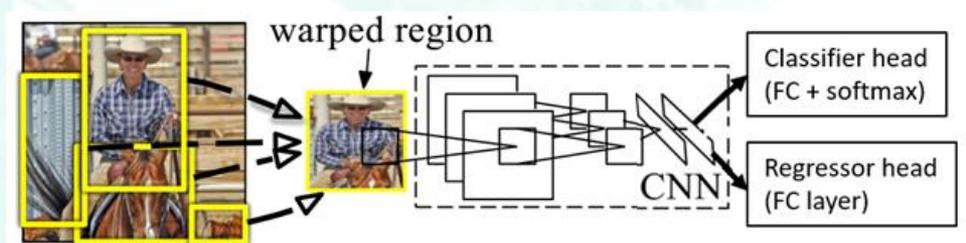
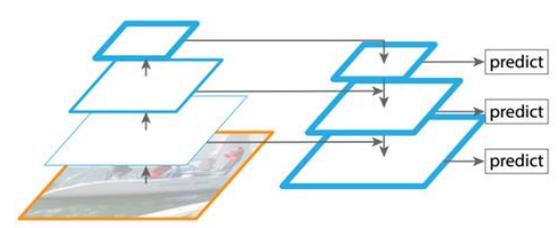
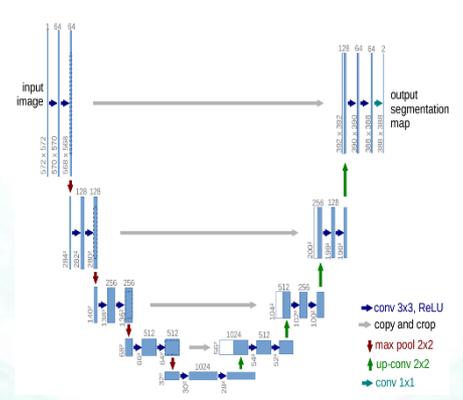
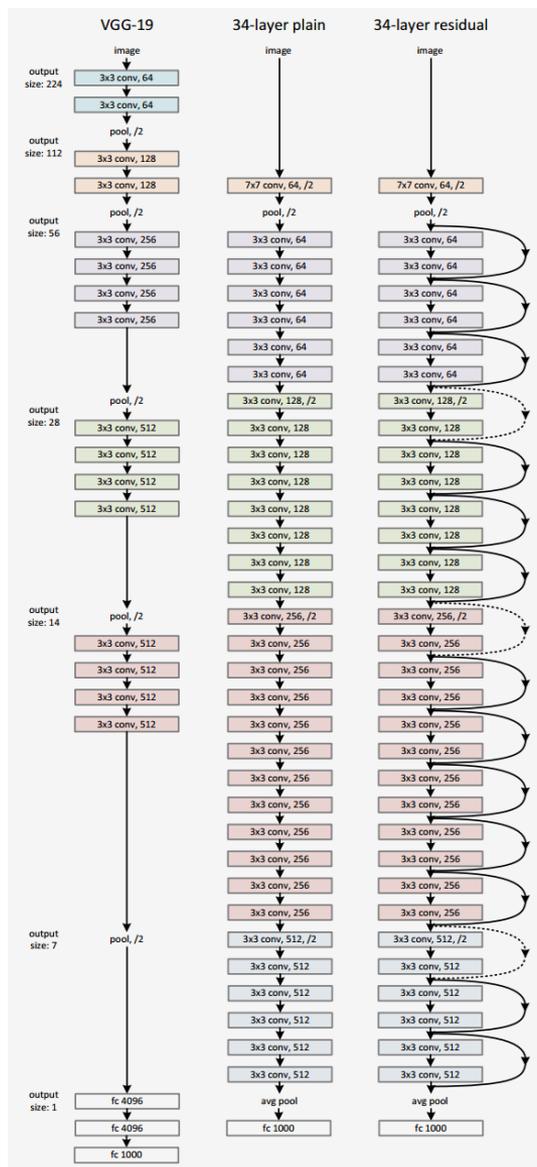
Diagram illustrating the components of the loss function  $L(\boldsymbol{\theta})$ . The terms  $\mathbf{y}_i$ ,  $\mathbf{x}_i$ , and  $\boldsymbol{\theta}$  in the loss function are highlighted with red boxes. Arrows point from these boxes to labels: "训练数据" (Training Data) for  $\mathbf{y}_i$  and  $\mathbf{x}_i$ , and "模型参数" (Model Parameters) for  $\boldsymbol{\theta}$ .

寻找模型（函数）最佳参数 = 最小化损失函数  $L(\boldsymbol{\theta})$

梯度下降法!

基于训练数据，通过梯度下降法最小化损失函数，  
以此找到最佳的模型参数!

# Recap: 各种模型结构





# 追研究前沿

- ❑ 深度学习方法用于解决越来越多的挑战性问题！
- ❑ 什么问题可以（潜在）用深度学习来解决？

输入与输出有（复杂非线性）相关性！

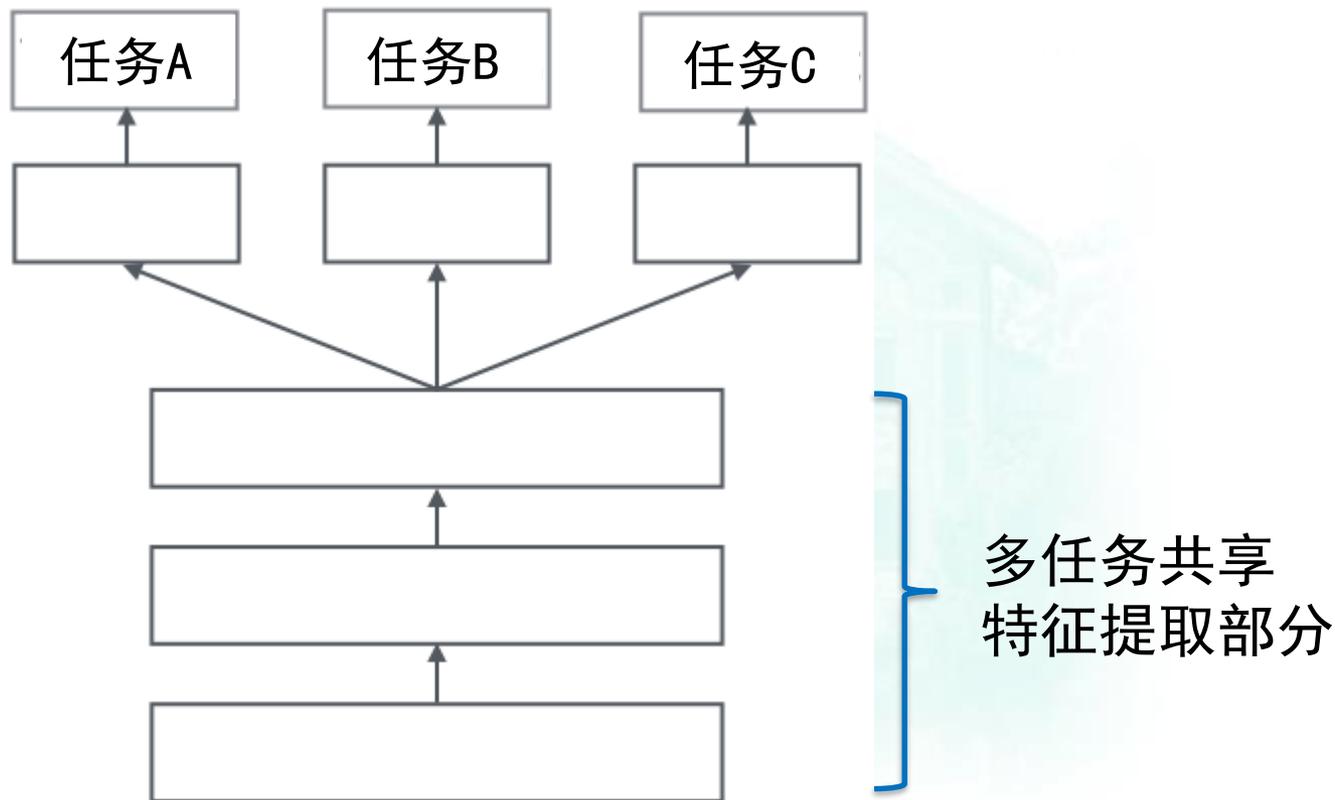


# 追研究前沿：小样本下深度学习

- ❑ 迁移学习（一般步骤）
  - 在其它大数据集上预训练一个模型（如分类器）
  - 保留中低层（特征提取）部分，输出端换为与当前任务相关
  - 在当前小样本数据集上对模型进行训练微调
- ❑ 迁移学习简单有效，在大量应用中得到证实
- ❑ 为什么迁移学习有效？
  - 模型低层部分提取的（纹理、形状）特征具有跨任务特性
  - 需要更新的模型参数较少，减少过拟合

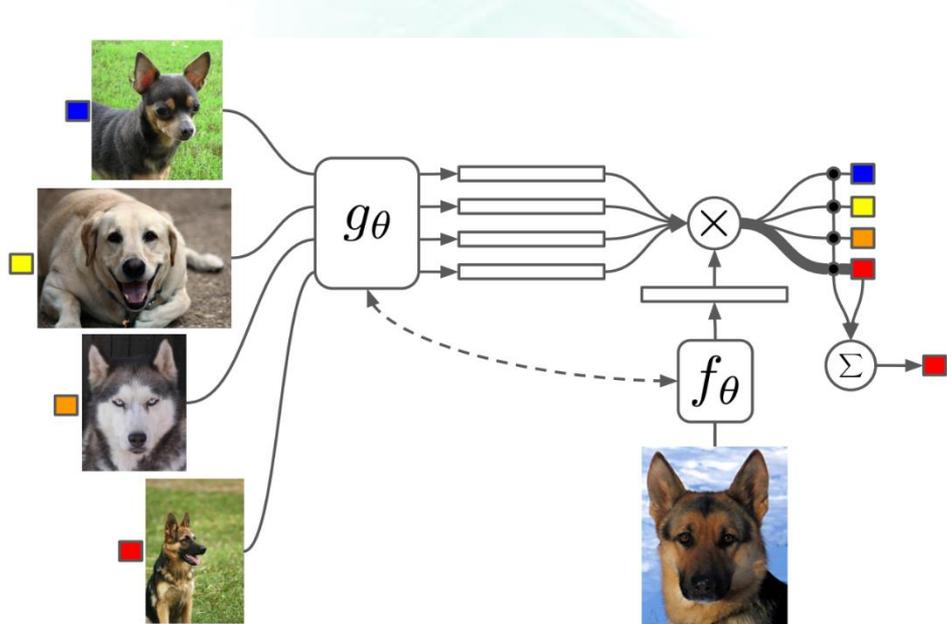
# 追研究前沿：小样本下深度学习

- 多任务学习，使得特征提取部分更具有普适性（对照迁移学习）



# 追研究前沿：小样本下深度学习

- 元学习 (Meta-learning): 训练能生成模型的模型
- 传统分类器：输入一个数据，输出数据的类别
- 元分类器：输入一组数据，输出一个分类器

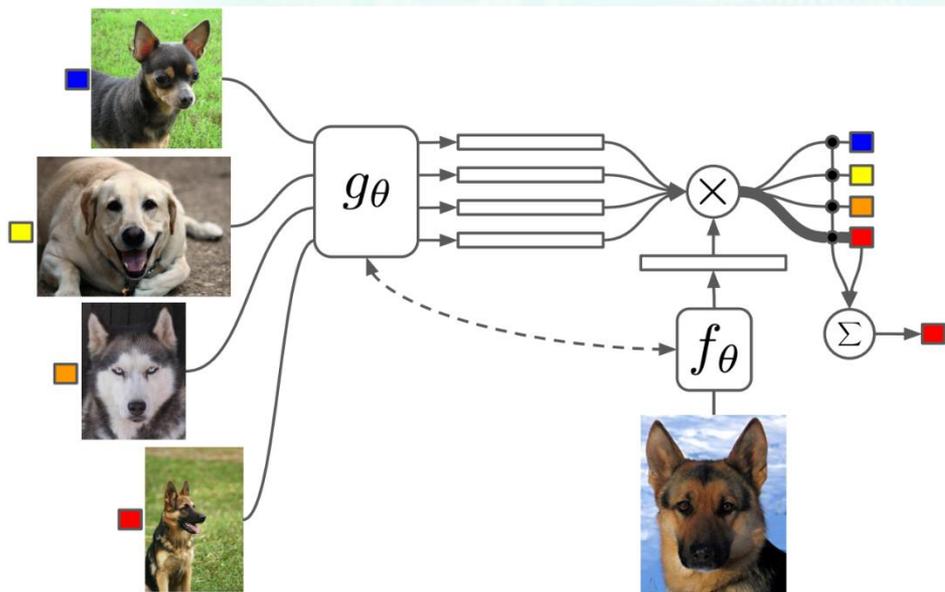


$$\hat{y} = \sum_{i=1}^k a(\hat{x}, x_i) y_i$$

$$a(\hat{x}, x_i) = e^{c(f(\hat{x}), g(x_i))} / \sum_{j=1}^k e^{c(f(\hat{x}), g(x_j))}$$

# 追研究前沿：小样本下深度学习

- ❑ 元分类器的训练：训练特征提取器  $f(\cdot)$  和  $g(\cdot)$ ，使得对任意一组训练数据，元分类器能够输出一个“好分类器”
- ❑ 如何评价原分类器输出（即一个分类器）的好坏？
  - 用另一组有标签的数据衡量分类器的好坏
- ❑ 每次更新元分类器，训练数据对应的类别与上次的可以不一样
- ❑ 训练完成后，给任意一组新类的少量数据，输出新类的分类器



$$\hat{y} = \sum_{i=1}^k a(\hat{x}, x_i) y_i$$



# 追研究前沿：小样本下深度学习

- 目前元学习解决小样本问题在实际场景下有时不适用
- 探索方向：将人类知识有效融入到模型学习中！

示例：将图象超分辨重构的优化过程转化为深度模型的模块

## Iterative optimization algorithm

For  $k = 1:K$  do:

$$\mathbf{X}^{(k)} = \mathbf{Y}\mathbf{A} + \hat{\mathbf{Y}}^{(k)}\mathbf{B}$$

$$\mathbf{E}^{(k)} = \mathbf{C}\mathbf{X}^{(k)} - \mathbf{Z}$$

$$\mathbf{G}^{(k)} = \eta \mathbf{C}^T \mathbf{E}^{(k)} \mathbf{B}^T$$

$$\mathbf{Y}^{(k+1)} = \text{prox}_{\lambda\eta}(\hat{\mathbf{Y}}^{(k)} - \mathbf{G}^{(k)})$$

## Network design

In stage  $k = 1:K$  of the network do:

$$\mathcal{X}^{(k)} = \mathcal{Y} \times_3 \mathbf{A}^T + \hat{\mathcal{Y}}^{(k)} \times_3 \mathbf{B}^T$$

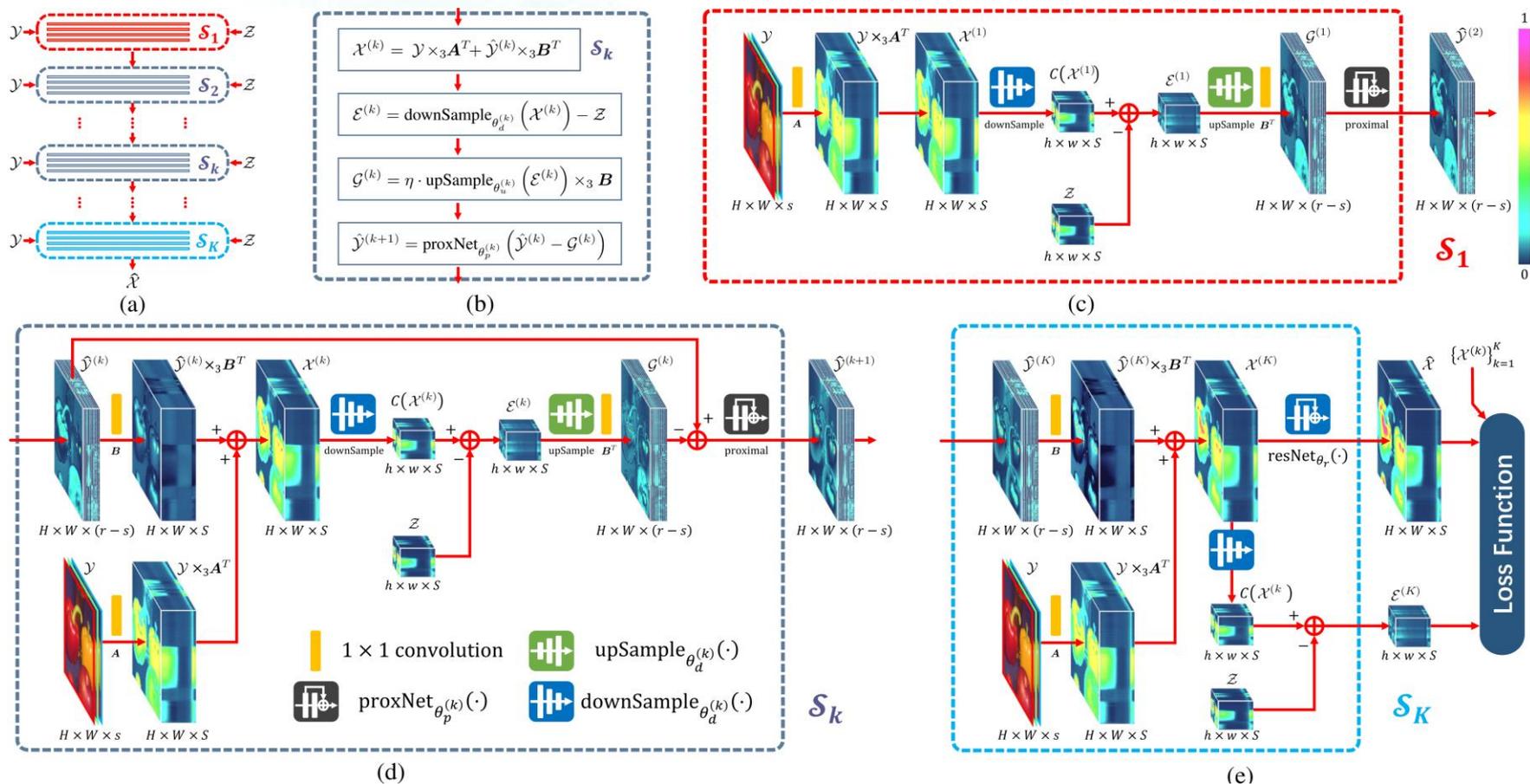
$$\mathcal{E}^{(k)} = \text{downSample}_{\theta_d^{(k)}}(\mathcal{X}^{(k)}) - \mathcal{Z}$$

$$\mathcal{G}^{(k)} = \eta \cdot \text{upSample}_{\theta_d^{(k)}}(\mathcal{E}^{(k)}) \times_3 \mathbf{B}$$

$$\hat{\mathcal{Y}}^{(k+1)} = \text{proxNet}_{\theta_p^{(k)}}(\hat{\mathcal{Y}}^{(k)} - \mathcal{G}^{(k)})$$

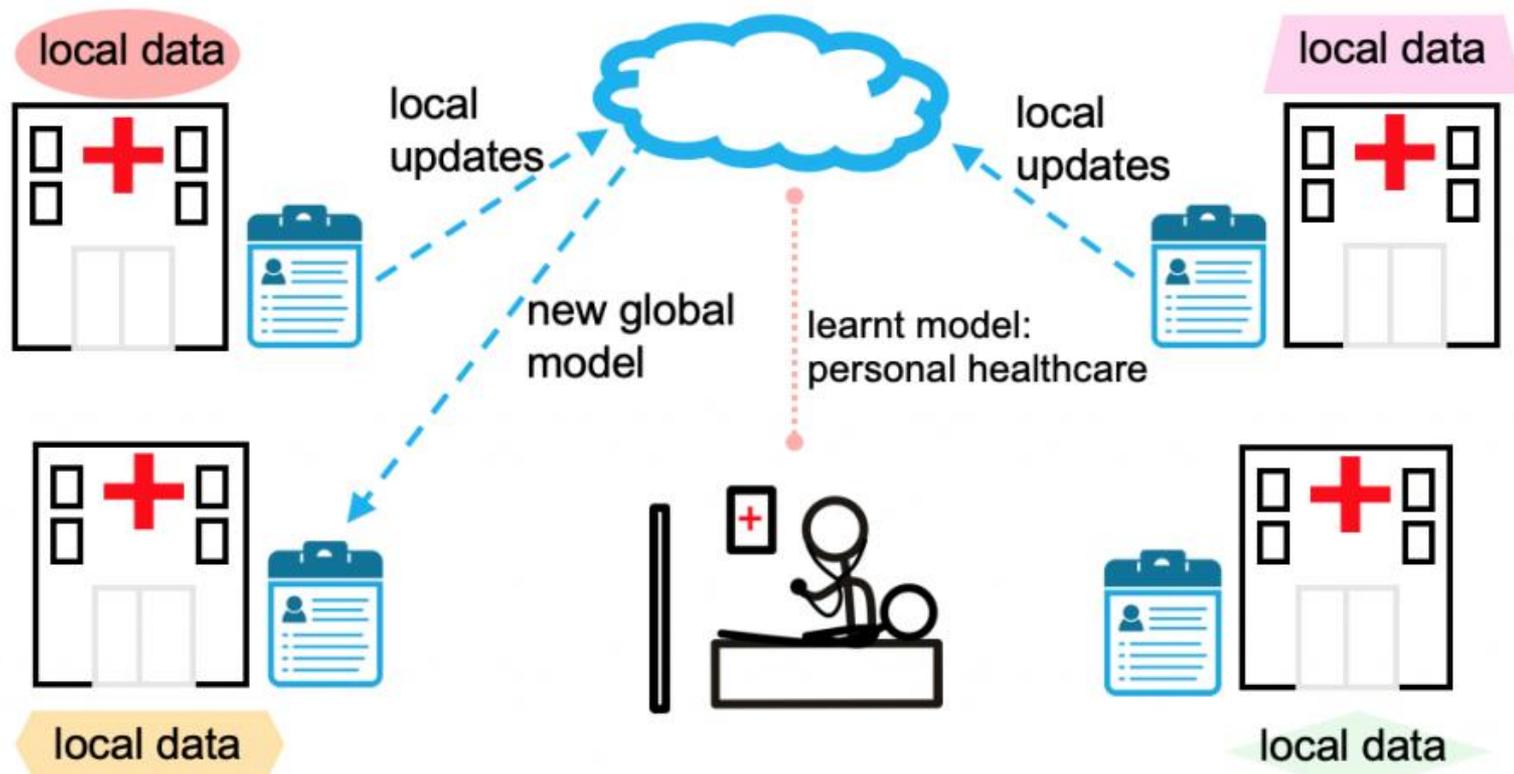
# 追研究前沿：小样本下深度学习

- 目前元学习解决小样本问题在实际场景下有时不适用；
- 探索方向：将人类知识有效融入到模型学习中！



# 追研究前沿：隐私保护下的大数据学习

- 出于隐私保护、合法性、管理因素，多家医院的数据难于共享



联邦学习提供了一种解决方案：各个医院分别更新模型，传递给中心服务器，服务器融合更新总的模型，分发给各地医院，...

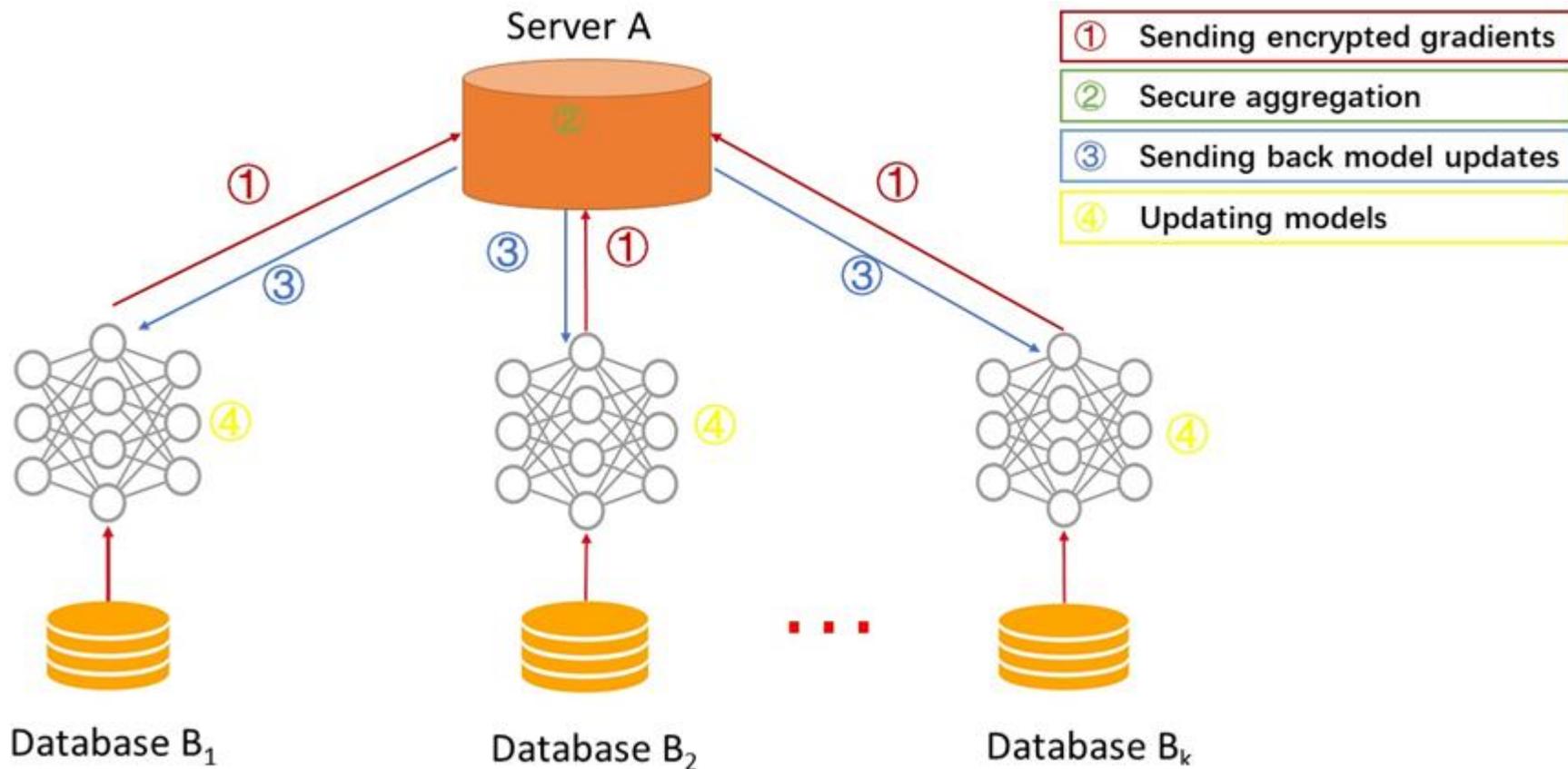
# 追研究前沿：隐私保护下的大数据学习

- 出于隐私保护、流量限制、能耗等考虑，个人不愿意共享数据



# 追研究前沿：隐私保护下的大数据学习

## 联邦学习基本架构



# 追研究前沿：隐私保护下的大数据学习

## 与传统分布式学习不同之处



Expensive Communication

信息传递较慢

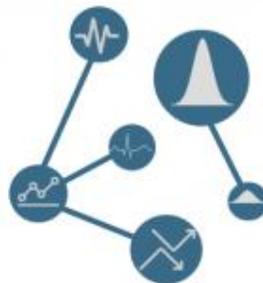
如何传递少量  
信息更新模型



Systems Heterogeneity

系统设备差异

部分设备工作  
运算传递速度



Statistical Heterogeneity

统计特性差异

非独立同分布  
各自数量差异



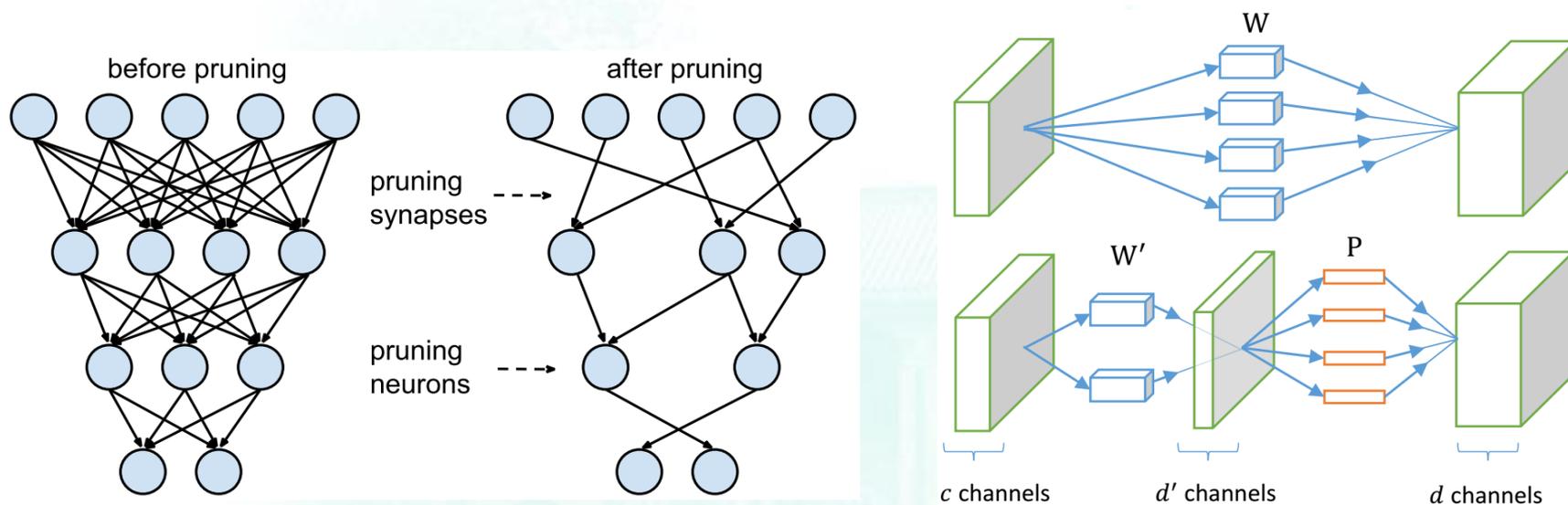
Privacy Concerns

隐私安全保护

真正去掉隐私  
有效模型更新

# 追研究前沿: 轻量化神经网络模型

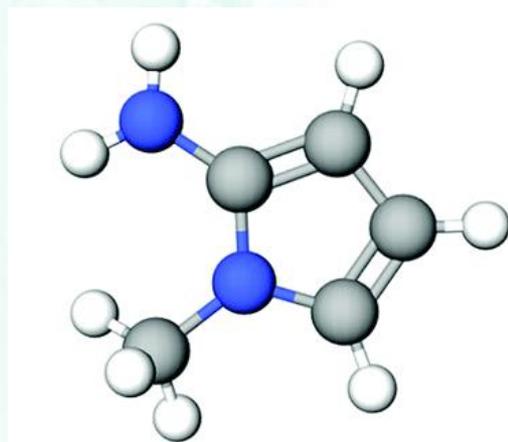
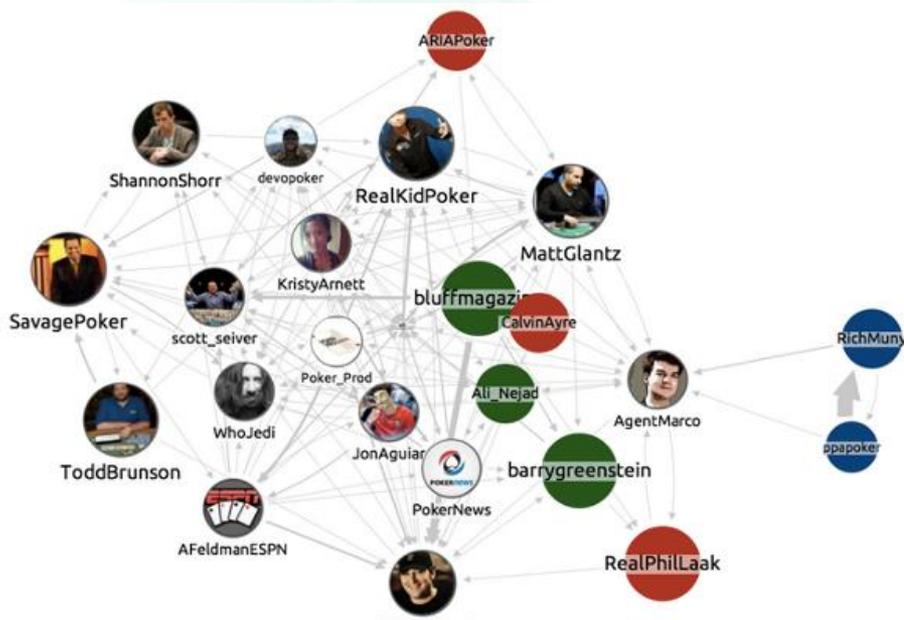
- ❑ 模型小和/或运算速度快
- ❑ 参数少, 耗电少, 易于部署在移动/嵌入式终端设备



将在模型压缩课程部分作详细介绍!

# 追研究前沿：图神经网络GNN

- ❑ 数据为图 (Graph)；应用于社交网络、推荐系统、分子结构等
- ❑ 图可以表示为  $G = (V, E, W, X)$ 
  - $V$ : 节点集,  $n = |V|$ 。  $E$ : 边的集合。  $W \in R^{n \times n}$ : 邻接矩阵
  - 每个节点  $v \in V$  由一个  $d$  维向量表示, 对应  $X \in R^{n \times d}$  中一行



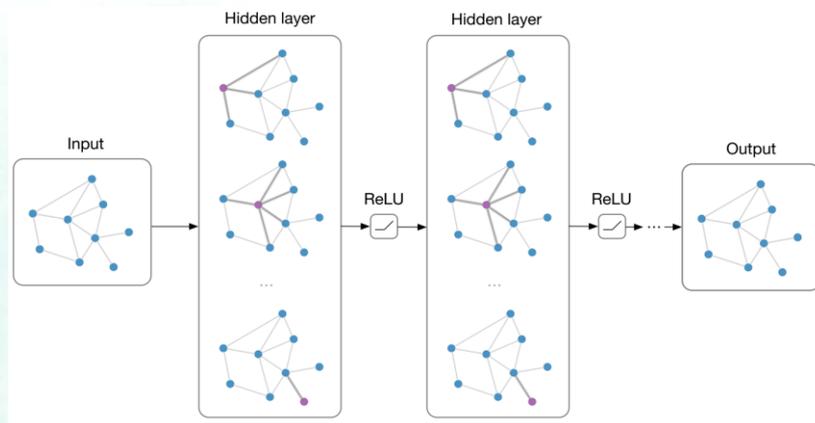
Molecular or crystal structure

- ❑ 挑战：如何处理非结构化/不规则下的局部运算/卷积

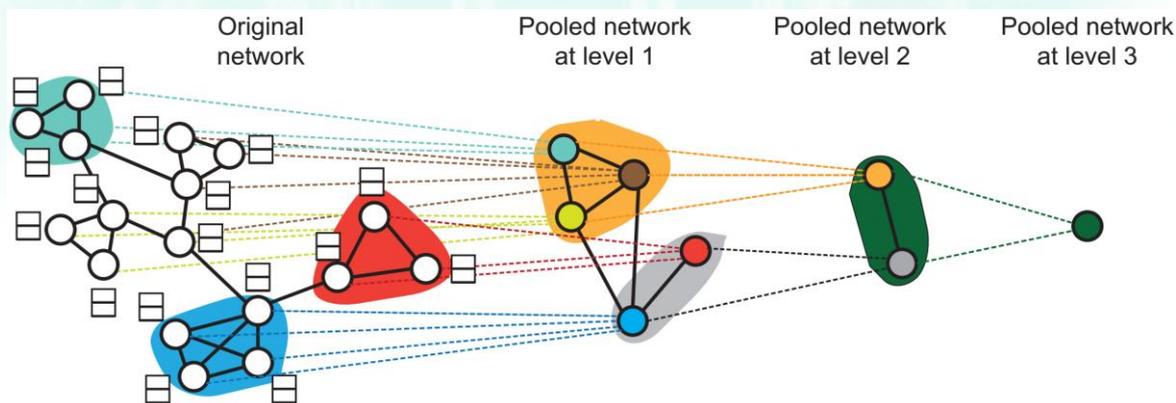
# 追研究前沿：图神经网络GNN

## 基于图神经网络的分类任务

- 节点分类：学习每个节点的特征表示，进而对其分类



- 图分类：学习整个图的特征表示，进而对其分类



Ying et al., Hierarchical graph representation learning with differentiable pooling, NeurIPS, 2018.

Kipf & Welling, Semi-supervised classification with graph convolutional networks, ICML, 2017



# 追研究前沿：图神经网络GNN

- GNNs为节点分类和图分类提供了有效的解决方案
  - 能够利用**节点初始特征**和**图结构**对每个节点或整图进行有效的特征学习和表示
  - 每层核心操作：围绕每一个节点进行Aggregate+Combine

$$\mathbf{a}_v^k = \text{AGGREGATE}^k(\{\mathbf{h}_u^{k-1} : u \in N(v)\})$$

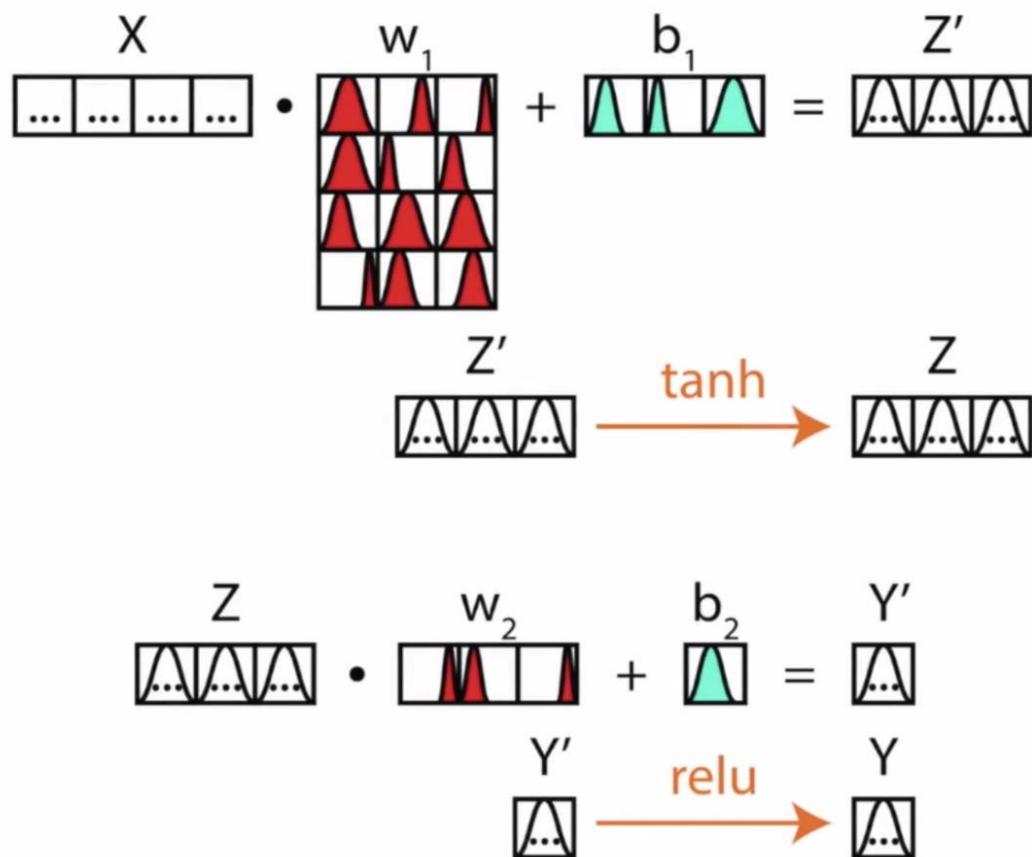
↑  
节点 $v$ 的邻居节点集合

$$\mathbf{h}_v^k = \text{COMBINE}^k(\mathbf{h}_v^{k-1}, \mathbf{a}_v^k)$$

↑  
节点 $v$ 第 $k$ 层的特征表示

# 追研究前沿: 贝叶斯深度学习

- ❑ 学习的不是模型每个参数的具体值，而是它的概率分布
- ❑ 可以提供预测结果的不确定性（注：softmax输出是预测结果）





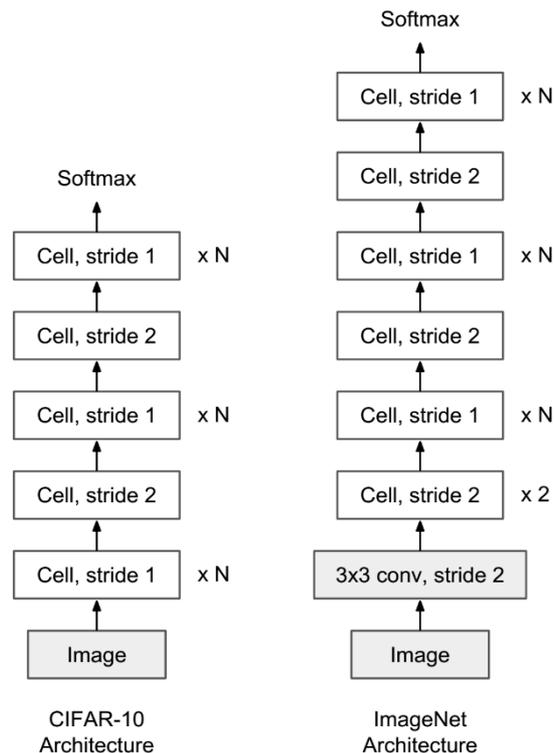
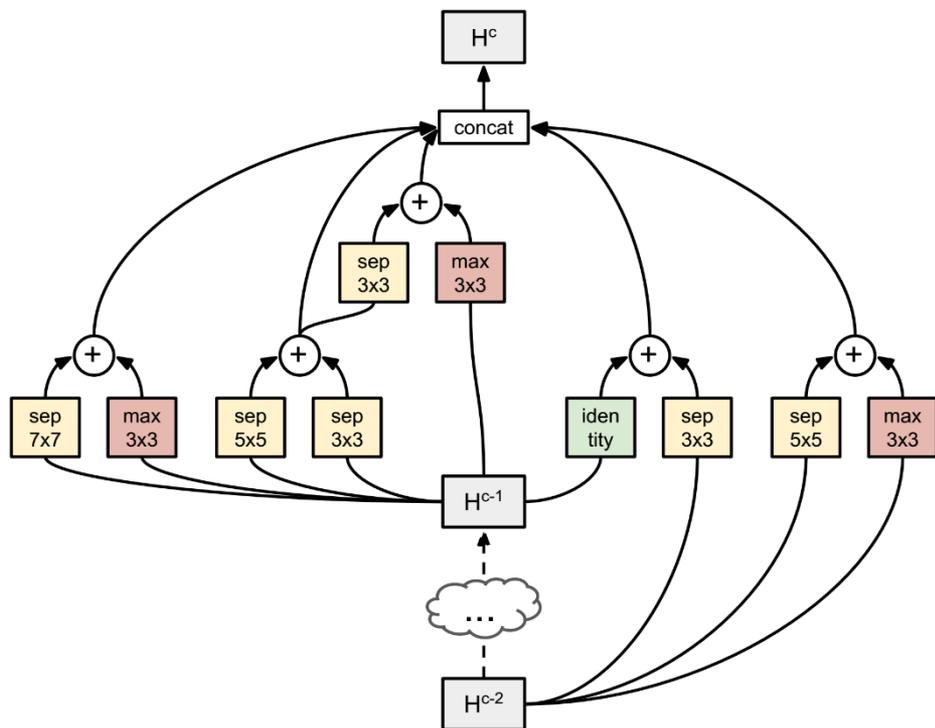
# 追研究前沿: 贝叶斯深度学习

- ❑ 模型训练与预测（方法之一）：Monte Carlo (MC) dropout
  - 在模型每一层加入dropout操作
  - 预测新数据时，仍然使用dropout，得到多次预测结果，统计预测平均值和方差（代表每个预测输出的概率分布）
- ❑ 比非贝叶斯深度学习更加鲁棒（针对输入或参数微小改变）
  - 每次预测：对模型参数进行多次采样得到多个模型
- ❑ 挑战：如何更有效地训练模型

$$P(y|\mathbf{x}, \mathbf{w}) = \frac{p(\mathbf{w}|\mathbf{x}, y)p(\mathbf{w})}{\int p(\mathbf{w}|\mathbf{x}, y)p(\mathbf{w})d\mathbf{w}}$$

# 追研究前沿: 自动机器学习AutoML

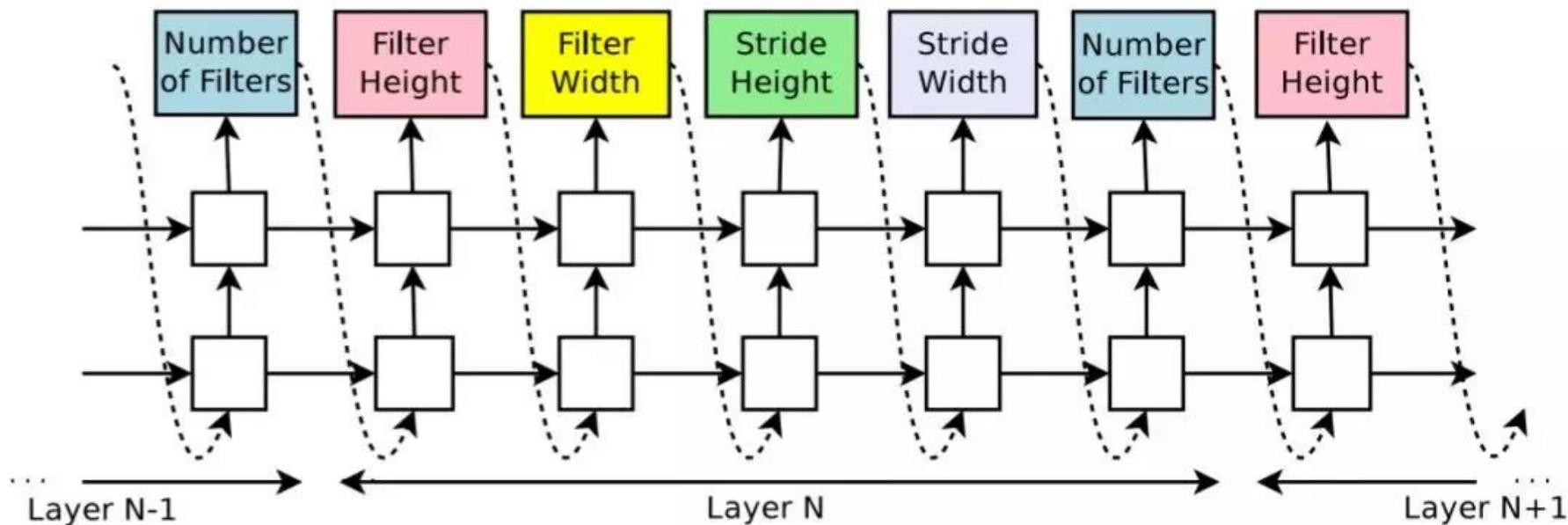
- 深度学习实现了特征提取自动化，但是模型结构需要人设计
- AutoML更加智能: 自动搜索/设计更优的模型结构等超参数



当前AutoML的基本操作模块仍然需要人设计，所以下一步...?

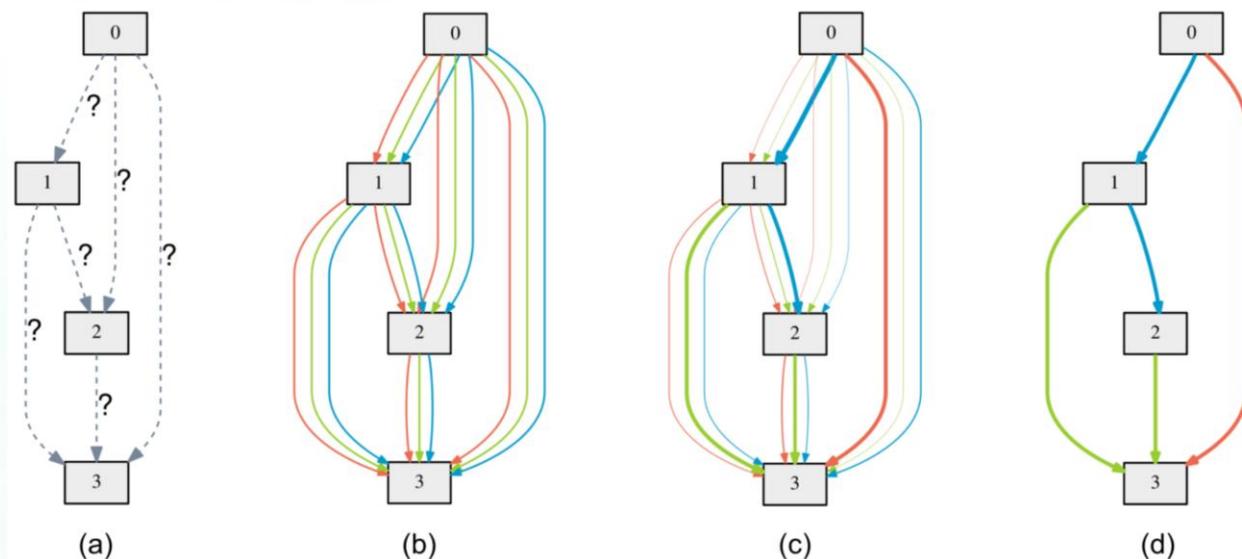
# 追研究前沿: 自动机器学习AutoML

- ❑ NAS(Neural architecture search): 训练元模型寻找模型结构参数
  - (比如) 用一个RNN元模型, 输出一套CNN模型结构参数
  - 用训练数据训练该套参数对应的CNN模型
  - 将CNN性能作为反馈信息, 利用强化学习更新RNN模型参数
  - 重复以上过程



# 追研究前沿：自动机器学习AutoML

- 挑战：如何快速准确评估每次产生的CNN性能
  - 整个训练过程可导，如DARTS (Differential Architecture Search)



颜色：操作（卷积，池化等），粗细：操作的权重，同时优化操作权重和参数

- 每次用更少的训练数据/epochs/卷积个数、更小的输入图象
- AutoML可用于其它任务：数据预处理，数据增广，损失函数等

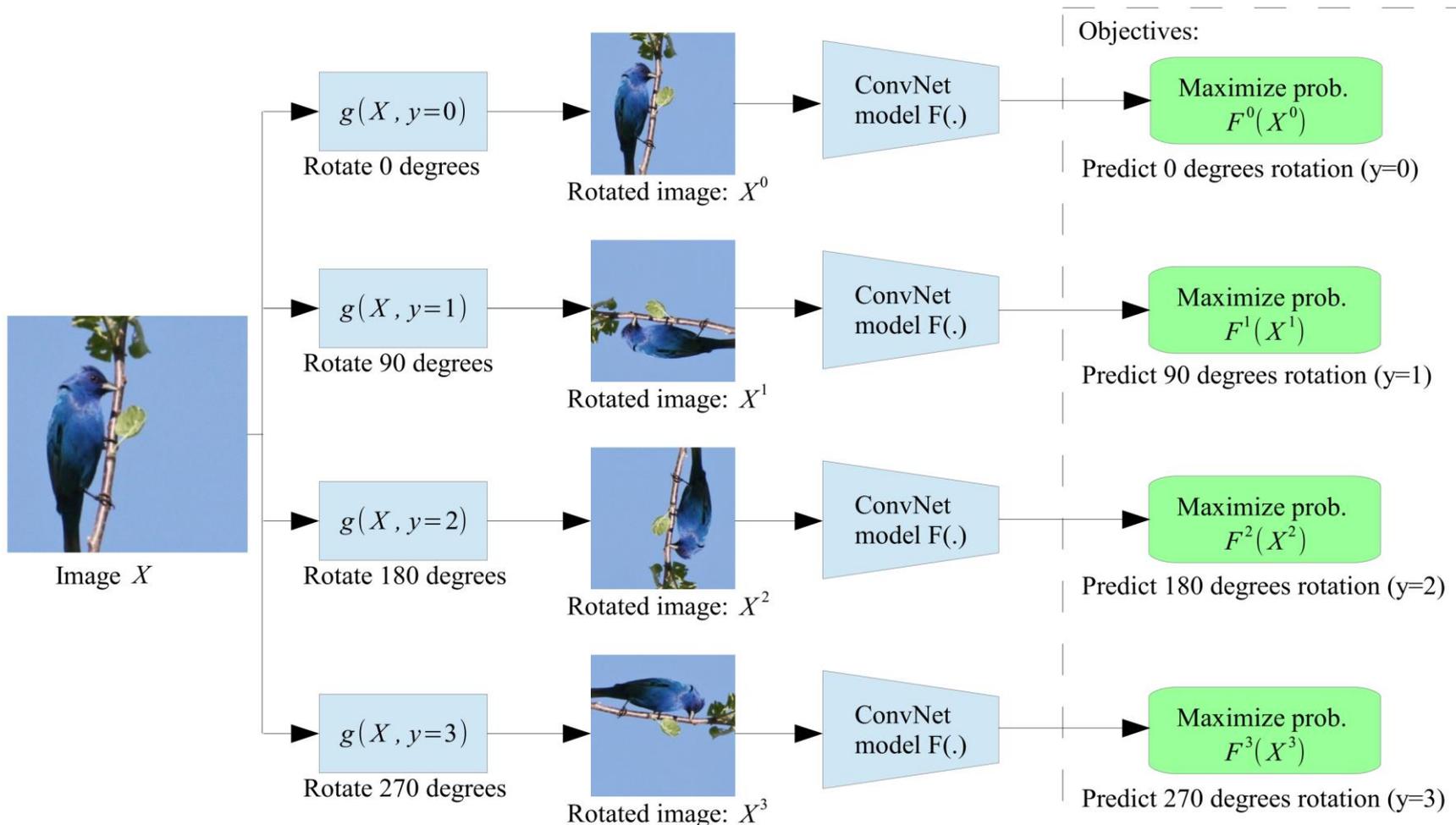


# 追研究前沿: 自监督学习

- 一般步骤:
  - 从每一个无标签数据中, 通过某种方式自动生成一个/组类别标签和对应的数据;
  - 用这些伪标签数据训练神经网络模型;
  - 用训练好的模型实现对原始数据的有效特征提取和表示
- 为什么有效?
  - 模型必须学习到数据中的特征才能实现较好的伪标签预测
- 为什么要进行自监督学习?
  - 为后续(下游)任务提供较好的数据(初始)特征表示
  - 自监督学习可看作迁移学习的第一步进行模型预训练
  - 后续任务所需标注的数据量大大减少

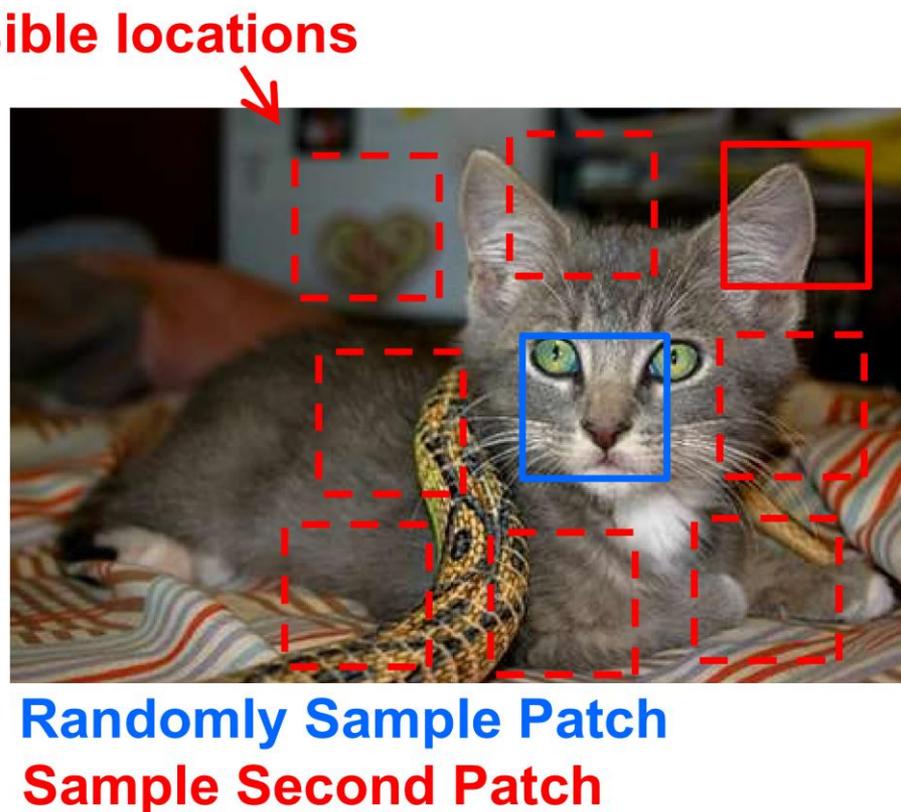
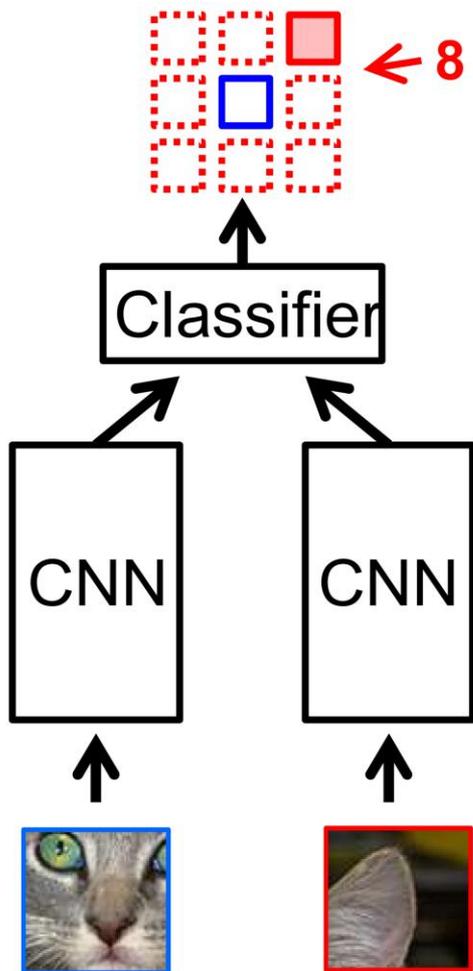
# 追研究前沿: 自监督学习

## Rotation net: 训练CNN分类器自动判断图像旋转角度



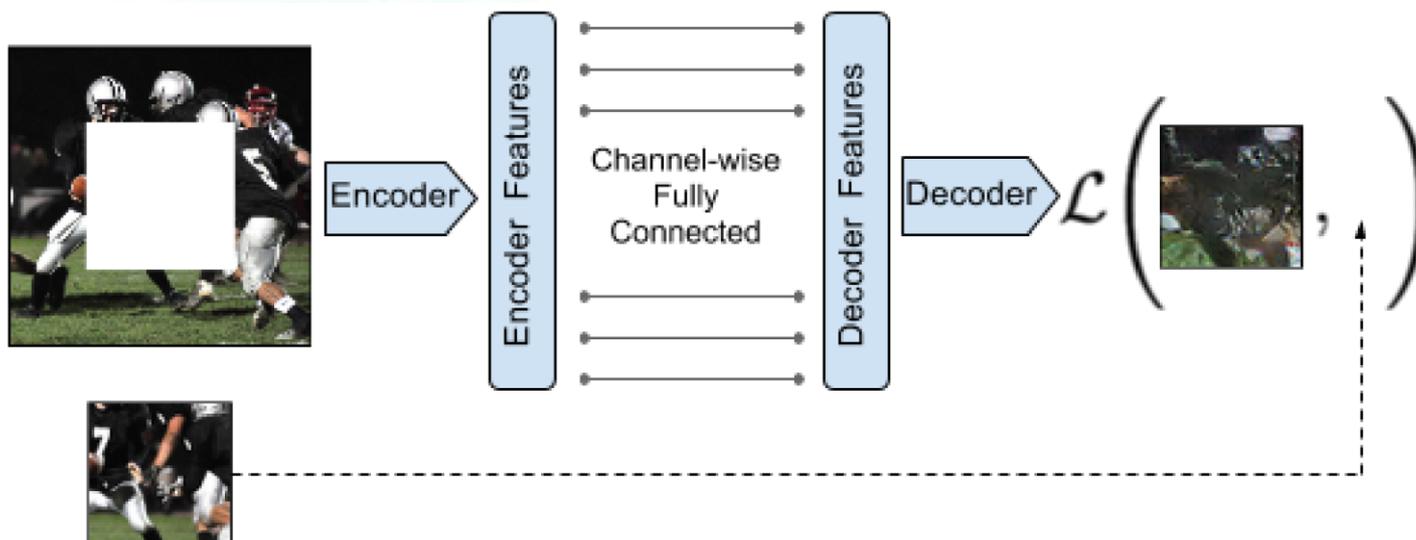
# 追研究前沿: 自监督学习

- Location net: 训练CNN预测两个图像块在原图中的相对位置



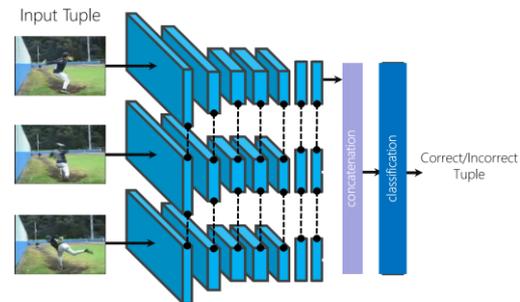
# 追研究前沿: 自监督学习

- Context encoder: 训练自编码器重构遮挡区域

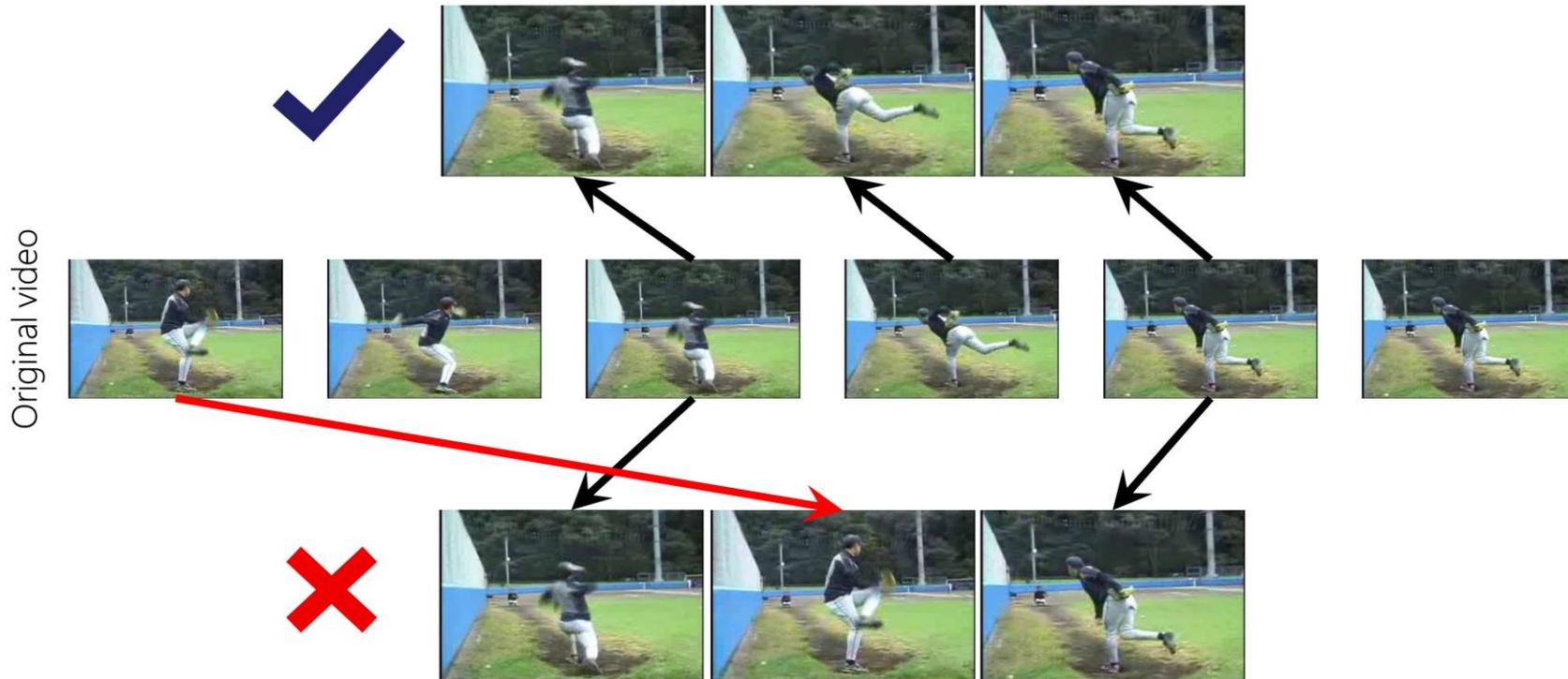


# 追研究前沿: 自监督学习

- Shuffle & Learn: 训练模型判断几张图象出现顺序是否正确



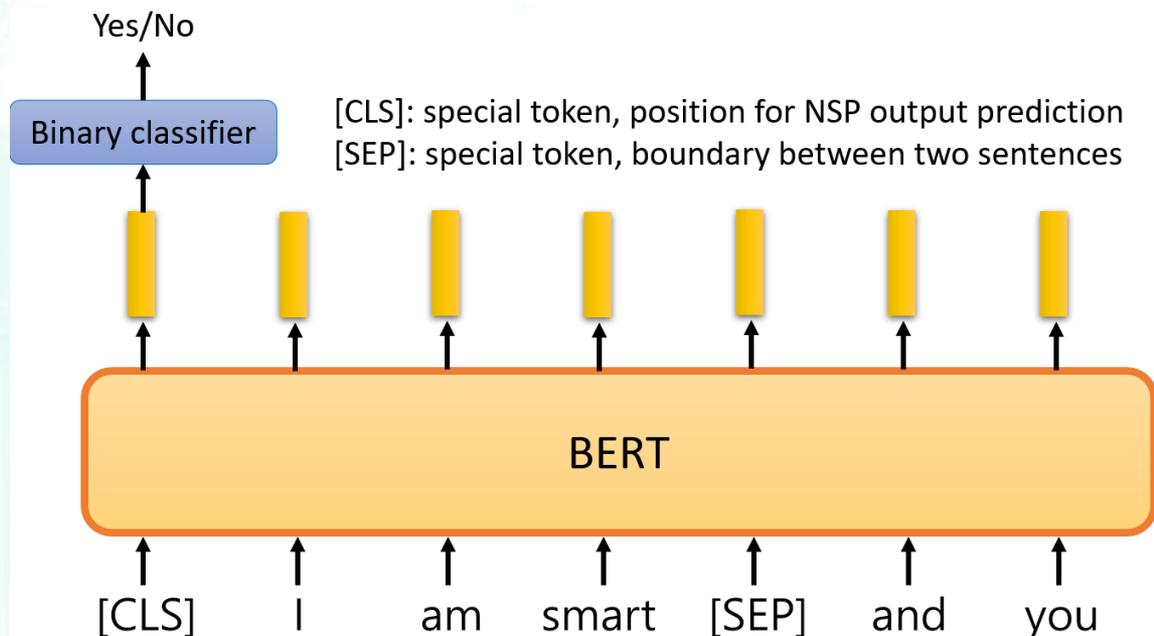
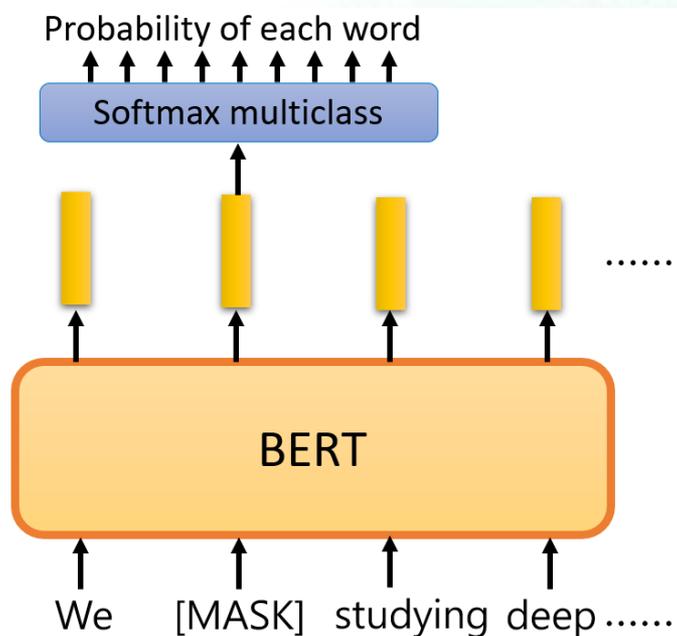
Temporally Correct order



Temporally Incorrect order

# 追研究前沿: 自监督学习

- ❑ BERT任务1: 训练模型预测句子中被遮挡的单词
- ❑ BERT任务2: 预测第二句话紧接第一句话出现是否合理





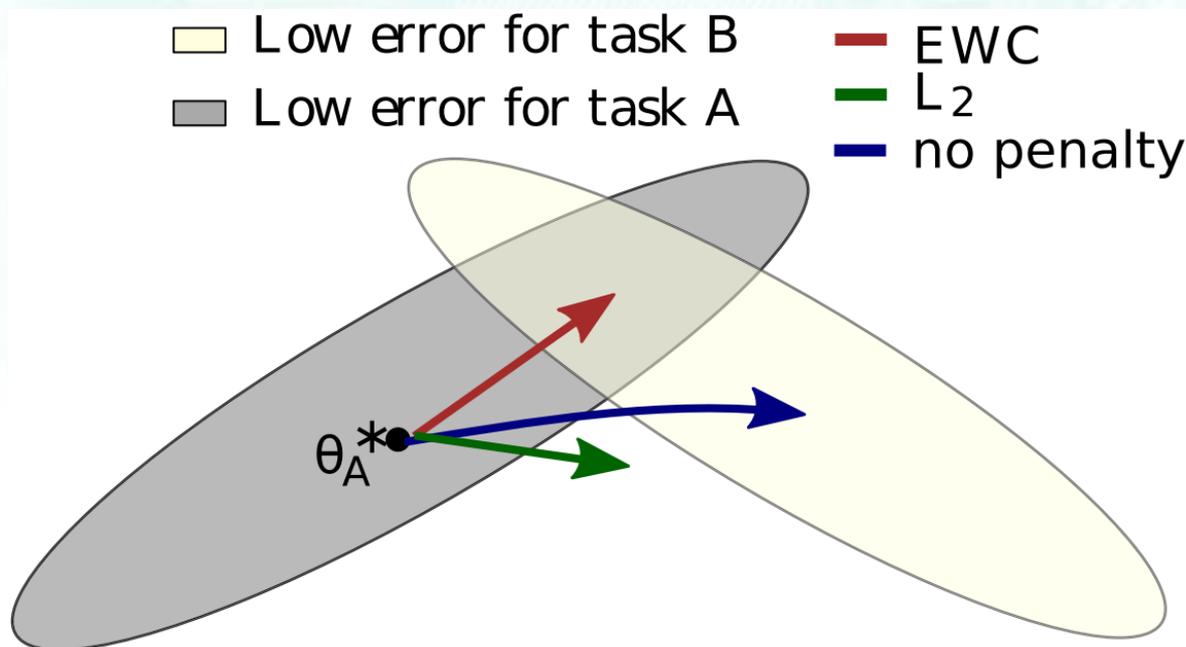
# 追研究前沿:终身学习

- ❑ 人类可以不断学习新知识，但AI模型学新忘旧！
- ❑ 终身学习/持续学习/增量学习：模型逐渐的学习更多的知识（如能做更多的任务、**识别更多的类别**等）
- ❑ 条件限制：学习新类知识时，不用或用很少旧类数据
- ❑ 两种类型：
  - 任务增加型：模型是一个共享特征提取部分的多任务分类器，预测时知道数据来自于哪一个任务（所以应用场景有限）
  - 类别增加型：模型作为单一分类器预测数据类别
- ❑ 核心挑战：学习新类时，如何减少对旧类知识的遗忘！

# 追研究前沿: 终身学习

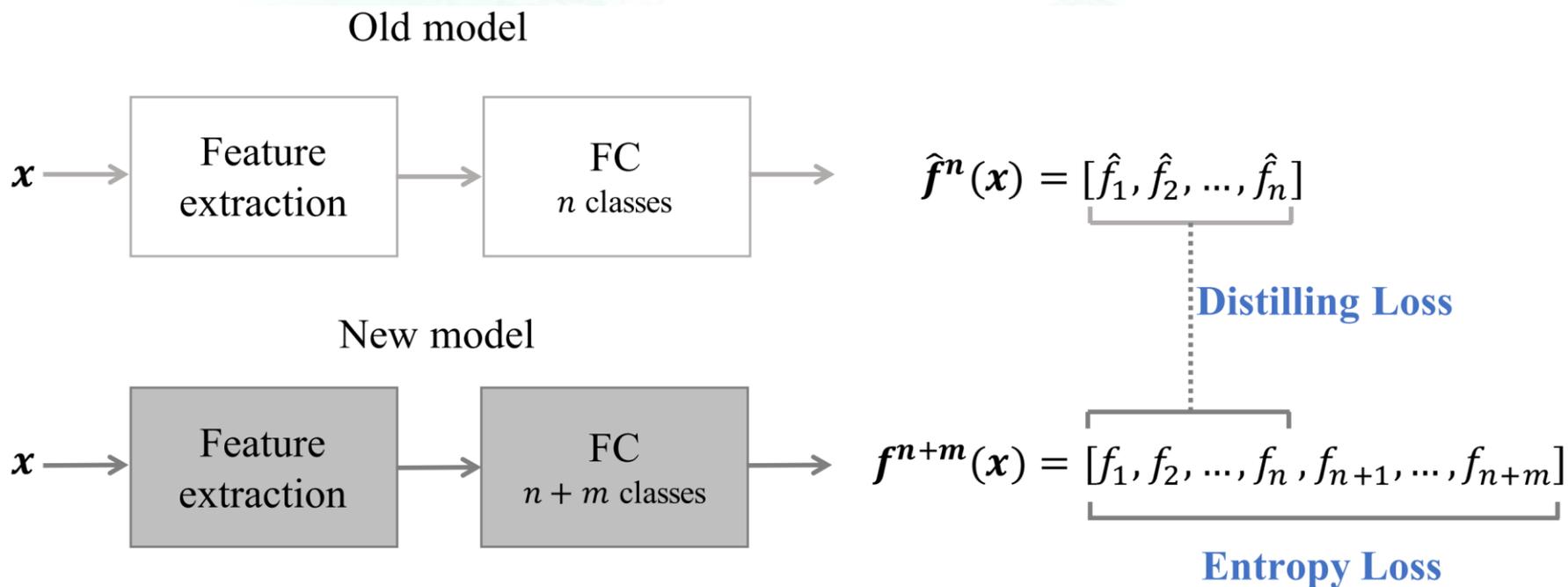
- 基于正则化训练的方法: 更新模型学习新任务/新类时, 通过加入正则化项, 尽量少改变对旧任务/旧类重要的模型参数
- 对应假设: 旧知识体现在分类器模型的参数里

$$\mathcal{L}(\theta) = \mathcal{L}_B(\theta) + \sum_i \frac{\lambda}{2} F_i(\theta_i - \theta_{A,i}^*)^2$$



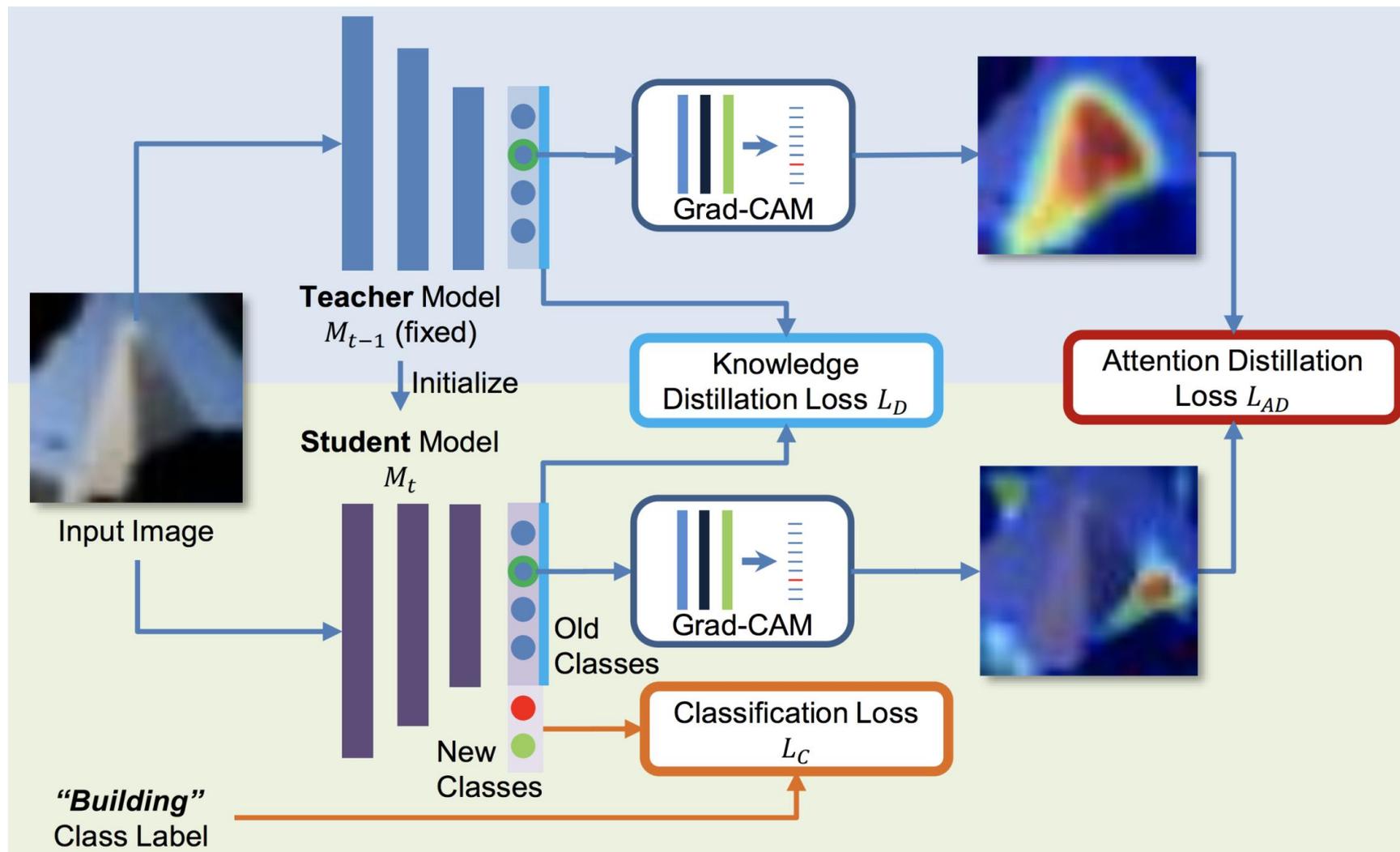
# 追研究前沿: 终身学习

- ❑ 知识蒸馏法: 针对 (新旧) 数据在旧分类器的输出响应, 让新分类器对应的输出部分有相似的响应
- ❑ 对应假设: 旧知识体现在分类器对数据的响应上



# 追研究前沿: 终身学习

- 知识蒸馏也可以基于卷积层输出（得到的注意力分布）





# 探未解之谜

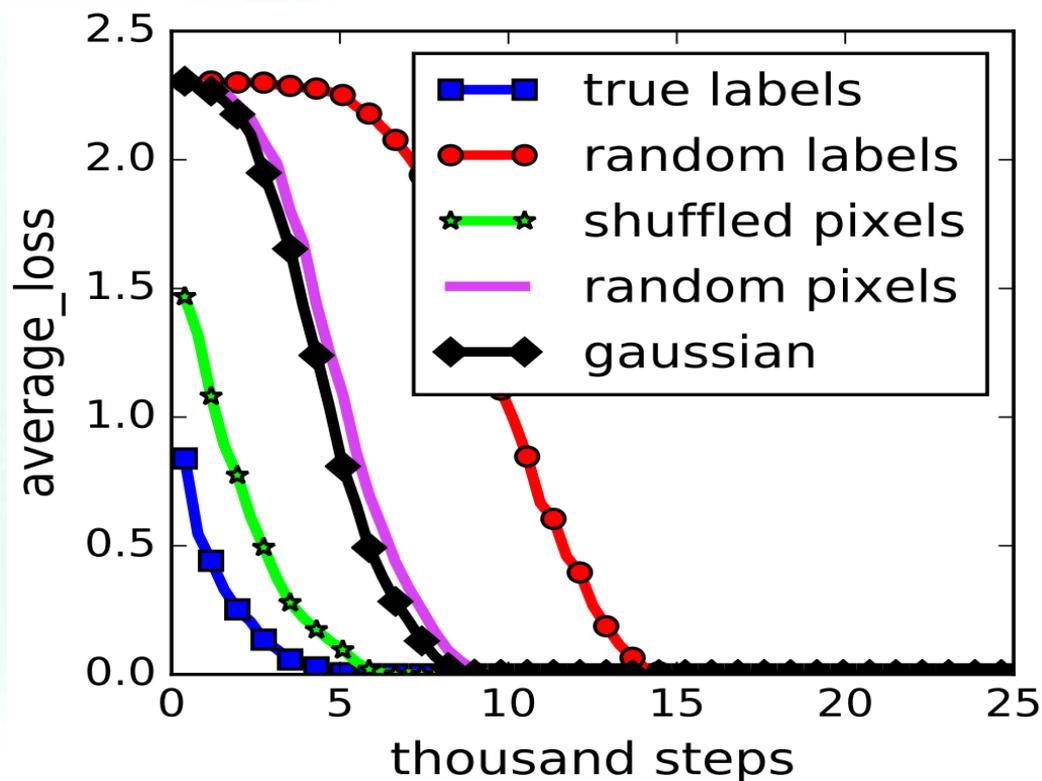
---

还有很多问题没答案，甚至没思路！



# 探未解之谜：为什么神经网络没有过拟合？

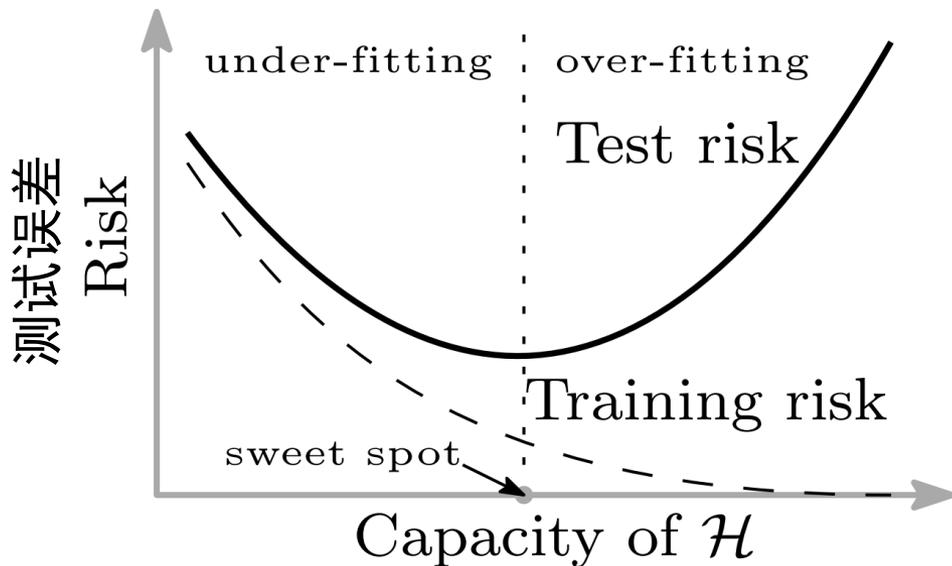
- ❑ CNN在标签随机打乱的数据甚至噪音数据上能被训练到误差为0.
- ❑ 即使加上正则项或dropout等操作，CNN也有类似表现！



**揭示：** CNN在分类任务中表现好，可能不是因为各种正则化，而是来自于CNN对所有训练数据的记忆。

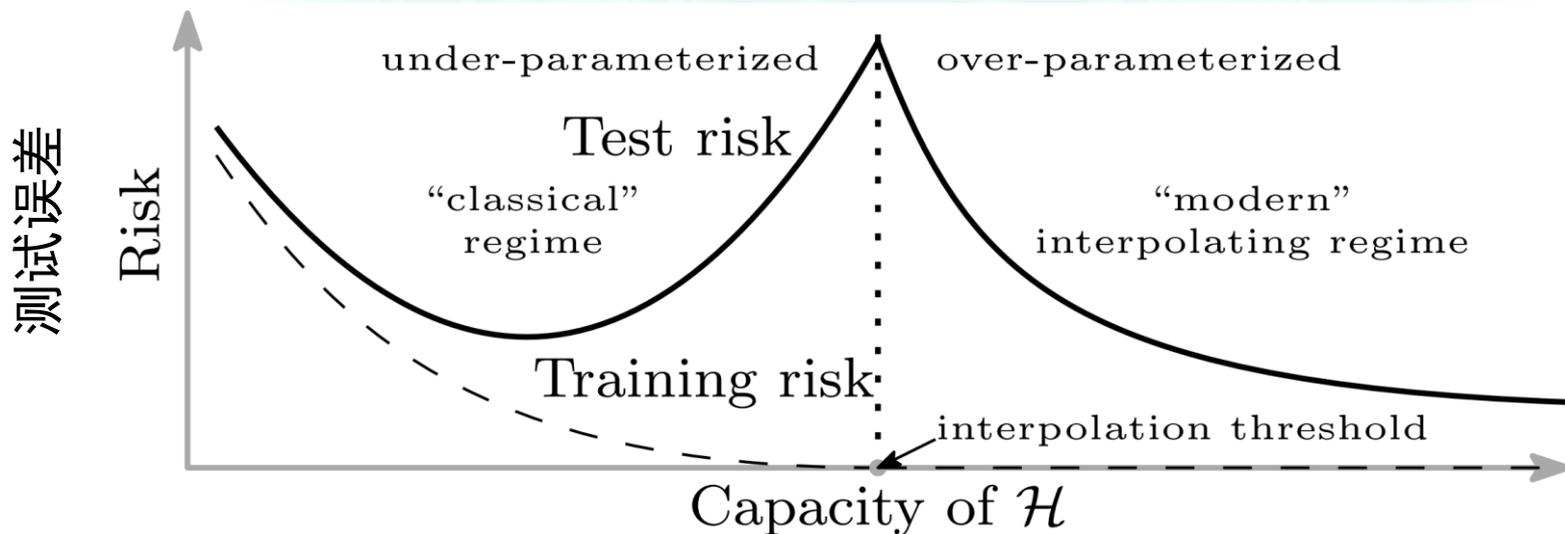


# 探未解之谜：传统机器学习理论不再适用？



← 传统机器学习理论

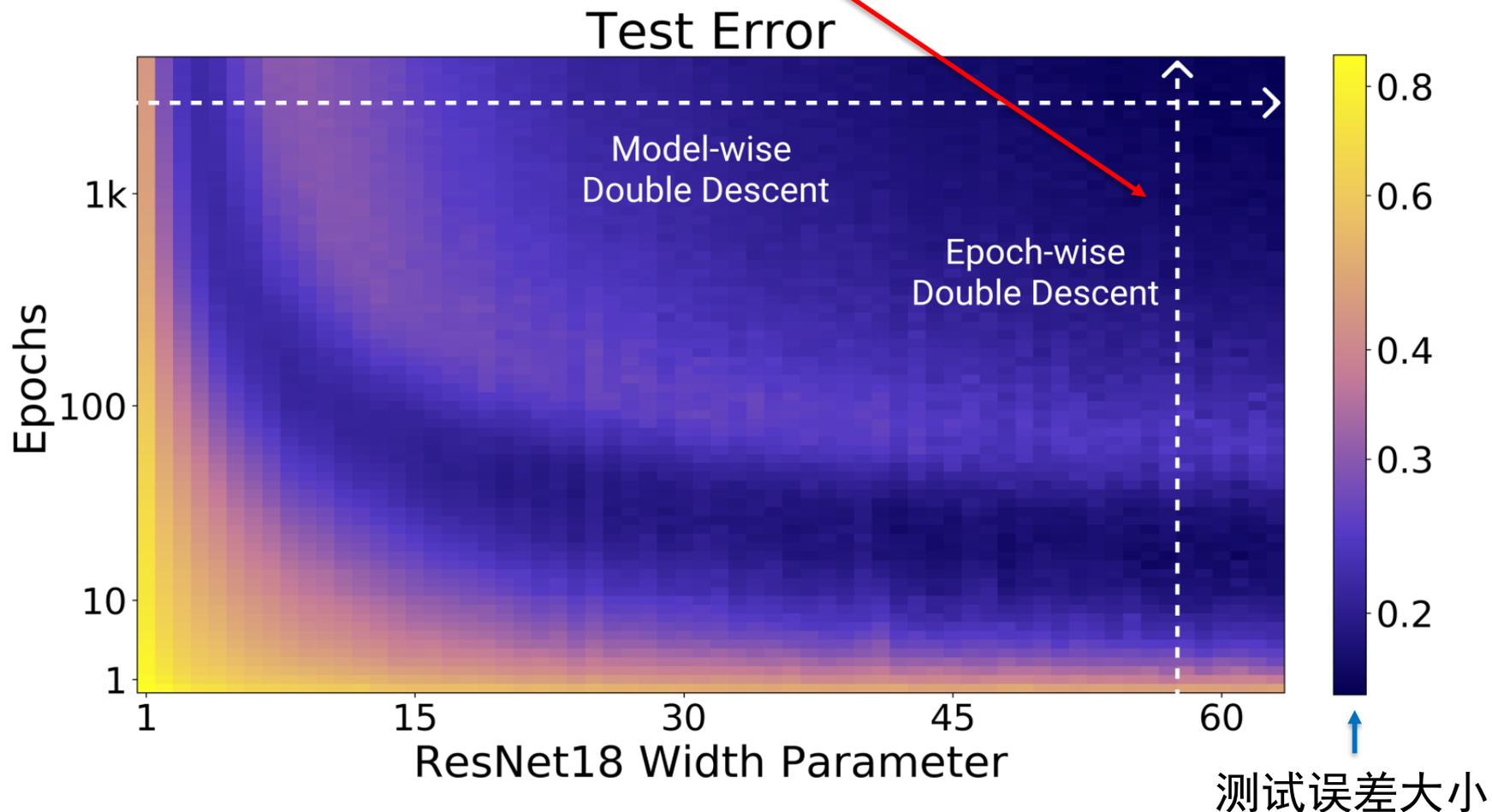
模型真实表现  
(当训练模型时early stop或不用正则化项)





# 探未解之谜：传统机器学习理论不再适用？

- 测试误差的Double descent现象不仅发生在模型尺寸/复杂度变化时，也发生在**训练次数变化时**！





# 探未解之谜：但是，小网络一定没大网络好？

## □ 实验

- Step 1: 基于随机初始化训练一个大神经网络A
- Step 2: 通过对大网络剪枝得到一个性能与A接近的小网络B
- Step 3: 用大网络里（对应小网络B的结构）的原始随机初始化，重新训练一个有同样结构的小网络B'
- Step 4: (结果发现) B' 的性能不差于原始大网络A

彩票假说 (Lottery ticket hypothesis)：任意一个随机初始化的大网络中存在一个小网络，当用同样的对应初始化参数和最多同样多次训练小网络后，小网络的性能不亚于大网络的性能。

## Why?

# 探未解之谜：鲁棒性/安全性

- 模型的鲁棒性很差：在任一图像中加入特定的人眼感觉不到的特定噪音（对抗噪音），会导致模型的性能急剧下降！



“panda”  
57.7% confidence

正常图像

+ .007 ×



对抗噪音

=



“gibbon”  
99.3 % confidence

对抗样本



# 探未解之谜：鲁棒性/安全性

- 模型攻击基本思路：如果知道模型参数，通过梯度上升法改变原始输入图像，使模型对更改后的图像（对抗样本）预测错误

目标：找到一个与原图像 $\mathbf{x}$ 接近的对抗样本，使损失函数 $L$ 的输出增加

$$L(\boldsymbol{\theta}, \tilde{\mathbf{x}}, y) \approx L(\boldsymbol{\theta}, \mathbf{x}, y) + (\tilde{\mathbf{x}} - \mathbf{x})^T \nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{x}, y)$$

$\boldsymbol{\theta}$ : model parameter;  $y$ : label of input  $\mathbf{x}$ ;  $\tilde{\mathbf{x}}$ : perturbed input

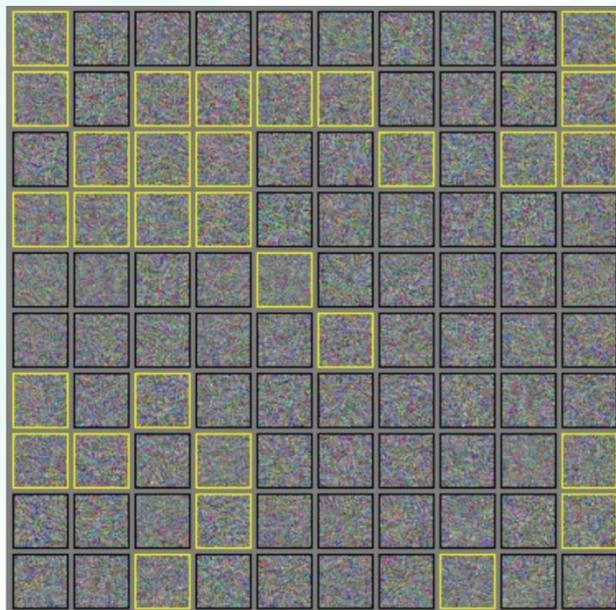
$$\begin{aligned} \arg \max_{\tilde{\mathbf{x}}} & L(\boldsymbol{\theta}, \mathbf{x}, y) + (\tilde{\mathbf{x}} - \mathbf{x})^T \nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{x}, y) \\ \text{s.t.} & \|\tilde{\mathbf{x}} - \mathbf{x}\|_{\infty} < \epsilon \end{aligned}$$

最优解：Fast Gradient Sign Method (FGSM)

$$\tilde{\mathbf{x}} = \mathbf{x} + \epsilon \text{sign}(\nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{x}, y))$$

# 探未解之谜：鲁棒性/安全性

- ❑ 模型攻击基本思路：如果知道模型参数，通过梯度上升法改变原始输入图像，使模型对更改后的图像（对抗样本）预测错误
- ❑ 对模型攻击，可以让分类器准确率降到10%以下！
- ❑ 也可以让模型将噪音图像误认为特定一类物体！



FGSM方法让模型将以上黄色框内图像识别为“Airplane”！



# 探未解之谜：鲁棒性/安全性

- ❑ 即使不知道待攻击模型的参数，也可以通过攻击其它（已知模型参数）模型产生对抗样本，用这些样本攻击目标！黑盒攻击！
- ❑ 黑盒攻击更常见；白盒攻击（知道待攻击模型参数）更厉害！

## 如何防御这些攻击？

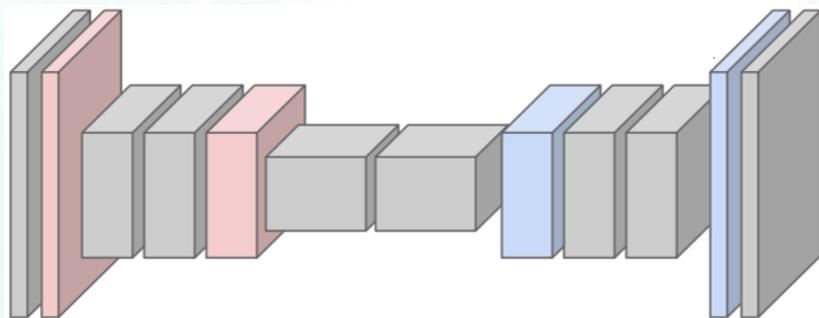
- ❑ 训练模型时将对抗样本纳入训练数据 → 难于有效防御多种不同的攻击方法
- ❑ 设计模型使得对抗样本难于产生 → 不能对训练好的模型进行防御；容易被新方法攻击
- ❑ 设法去除对抗样本中的（对抗）噪音

↓

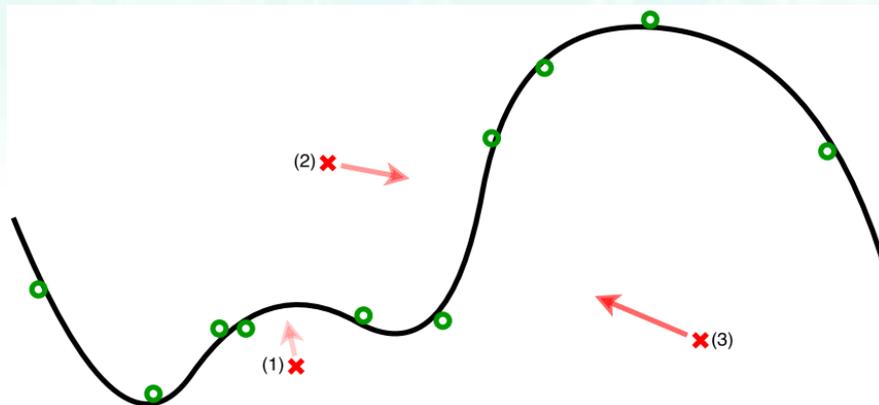
不用考虑分类器的结构与训练；  
不用考虑攻击方法的类型

# 探未解之谜：鲁棒性/安全性

- ❑ 去除噪音方法一：利用正常数据训练自编码器
- ❑ 对新的正常数据，自编码器输出与输入（几乎）一样
- ❑ 对于对抗样本，自编码器输出一个与输入接近的正常数据



编码器将含噪音的图像投影到正常图像的分布区域：

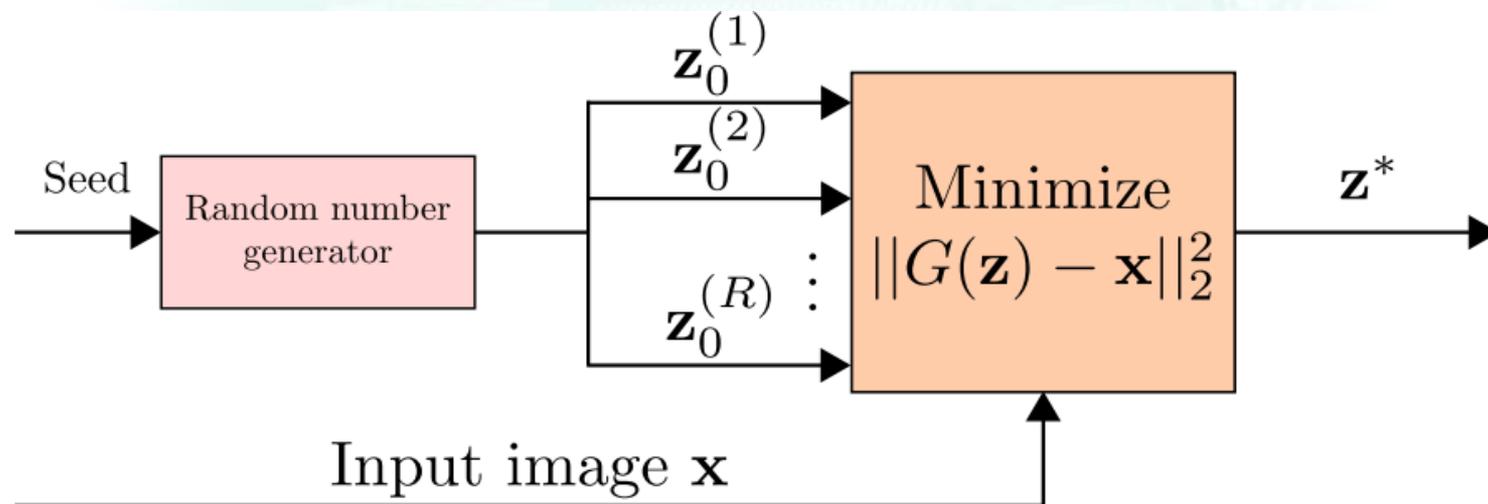


# 探未解之谜：鲁棒性/安全性

- ❑ 去除噪音方法二：利用正常数据训练GAN
- ❑ 对新的数据，用GAN中的生成器重构出相似的数据

$$\mathbf{z}^* = \arg \min_{\mathbf{z}} \|G(\mathbf{z}) - \mathbf{x}\|_2^2$$

- ❑ 对重构数据的类型进行预测



重构时的多个seeds共同使用增加了攻击模型的难度！



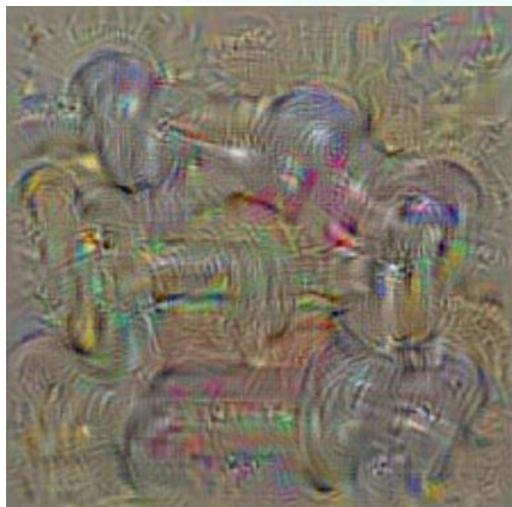
# 探未解之谜：模型可解释性

- 深度学习模型是个“黑盒子”？
  - 只有预测结果，没有预测详细过程
  - 原因：模型是一个复杂非线性变换
  
- 为什么要打开这个黑盒子？
  - 低于人类表现时：帮助人们发现模型的不足
  - 与人类表现持平：增加人们对模型预测的信任感
  - 超过人类表现：教人类如何更好地预测

# 探未解之谜：解释模型特定输出神经元

- 从输入端寻找可解释性：对于训练好的模型，寻找最佳输入图像  $\mathbf{I}$ ，使得特定pre-softmax输出  $f_c(\mathbf{I})$  最大

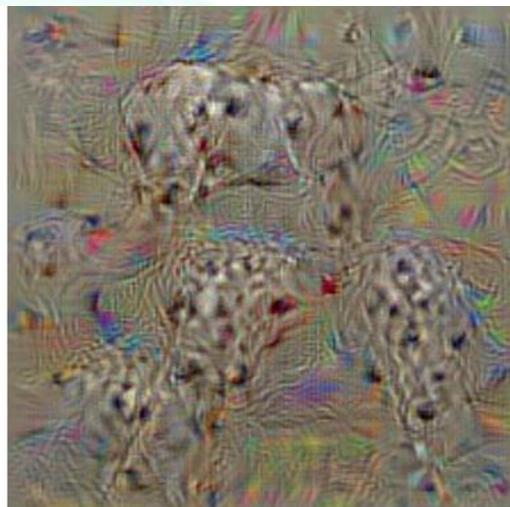
$$\arg \max_{\mathbf{I}} f_c(\mathbf{I}) - \lambda \|\mathbf{I}\|^2$$



dumbbell



cup

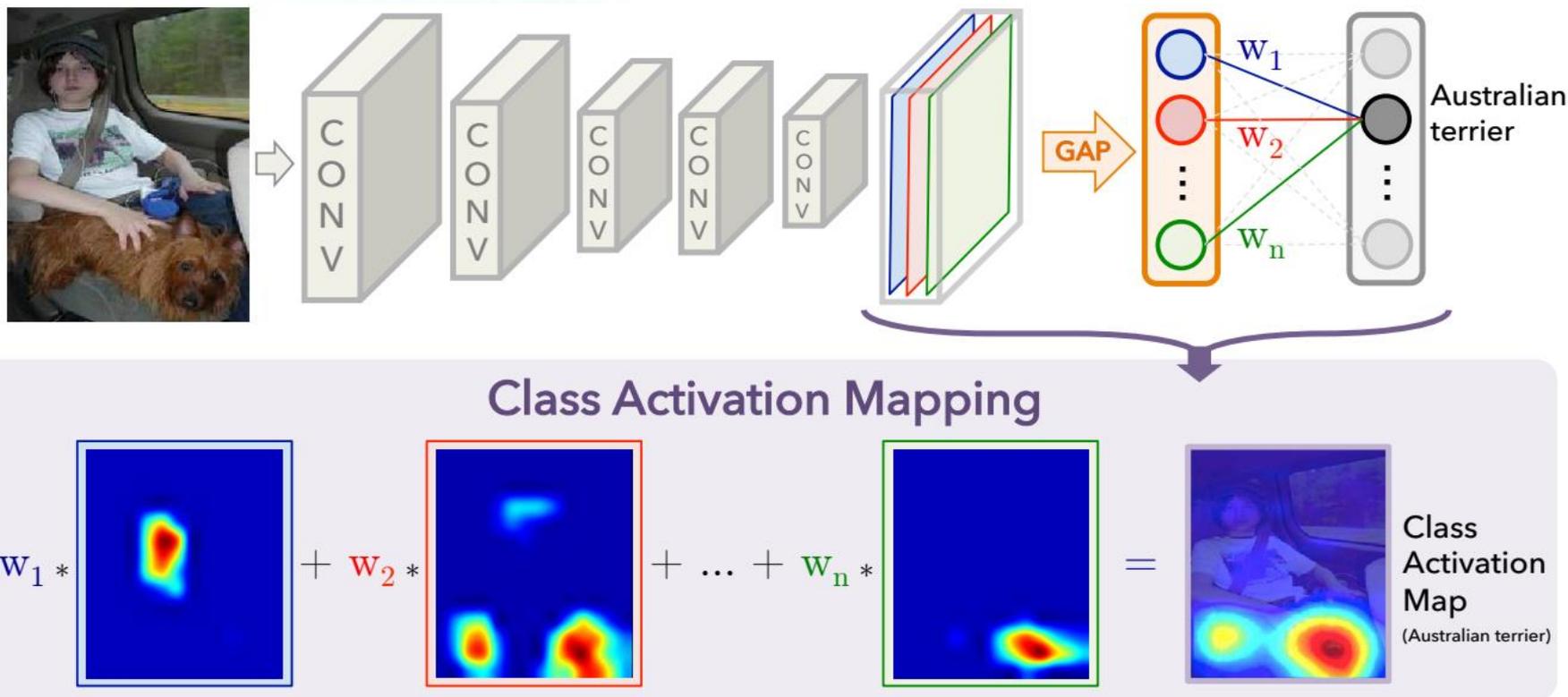


dalmatian

一定程度上帮助人们理解每个输出神经元在关注什么样的视觉特征，但无法解释对真实图像预测时模型在关注什么。

# 探未解之谜：解释模型的每次预测

- 从靠近输出端寻找可解释性：最后卷积层输出特征图的特定线性组合可解释模型预测时关注的图像区域





# 探未解之谜：解释模型的每次预测

Pre-softmax

GAP: global average pooling for channel k

$$S_c = \sum_k w_k^c \sum_{x,y} f_k(x,y) = \sum_{x,y} \sum_k w_k^c f_k(x,y)$$

Class activation map (CAM) for class c

$$M_c(x,y) = \sum_k w_k^c f_k(x,y)$$

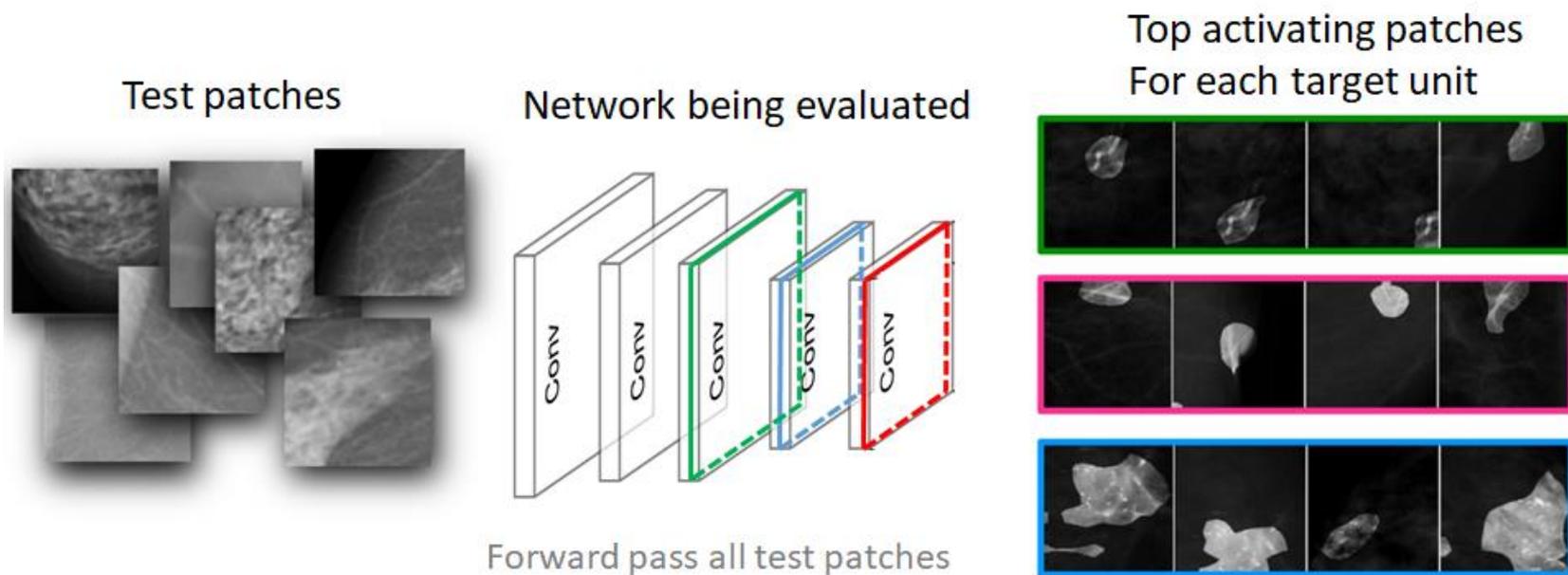
Weighted feature maps

Importance of activation at (x,y) for class c

$$S_c = \sum_{x,y} M_c(x,y)$$

# 探未解之谜：解释模型的每次预测

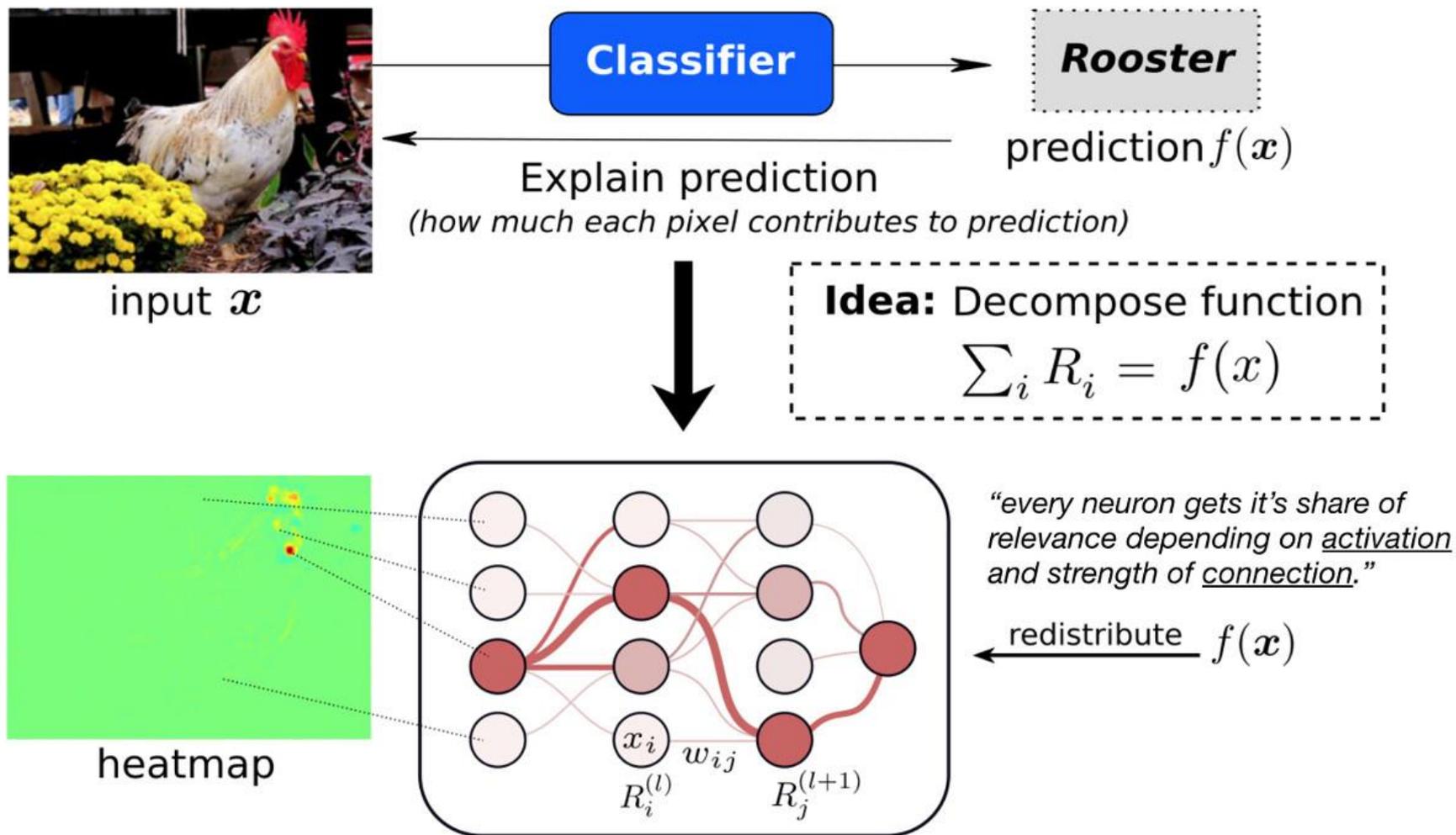
- 特定卷积核的可解释性：通过大量输入图像，收集并描述特征图中激活区域对应的图像信息，理解卷积核所对应的视觉特征



激活特定卷积核的图像区域往往与某一类的（疾病）特征相关；预测新图象时，激活的卷积核可解释模型在关注什么（疾病）特征。

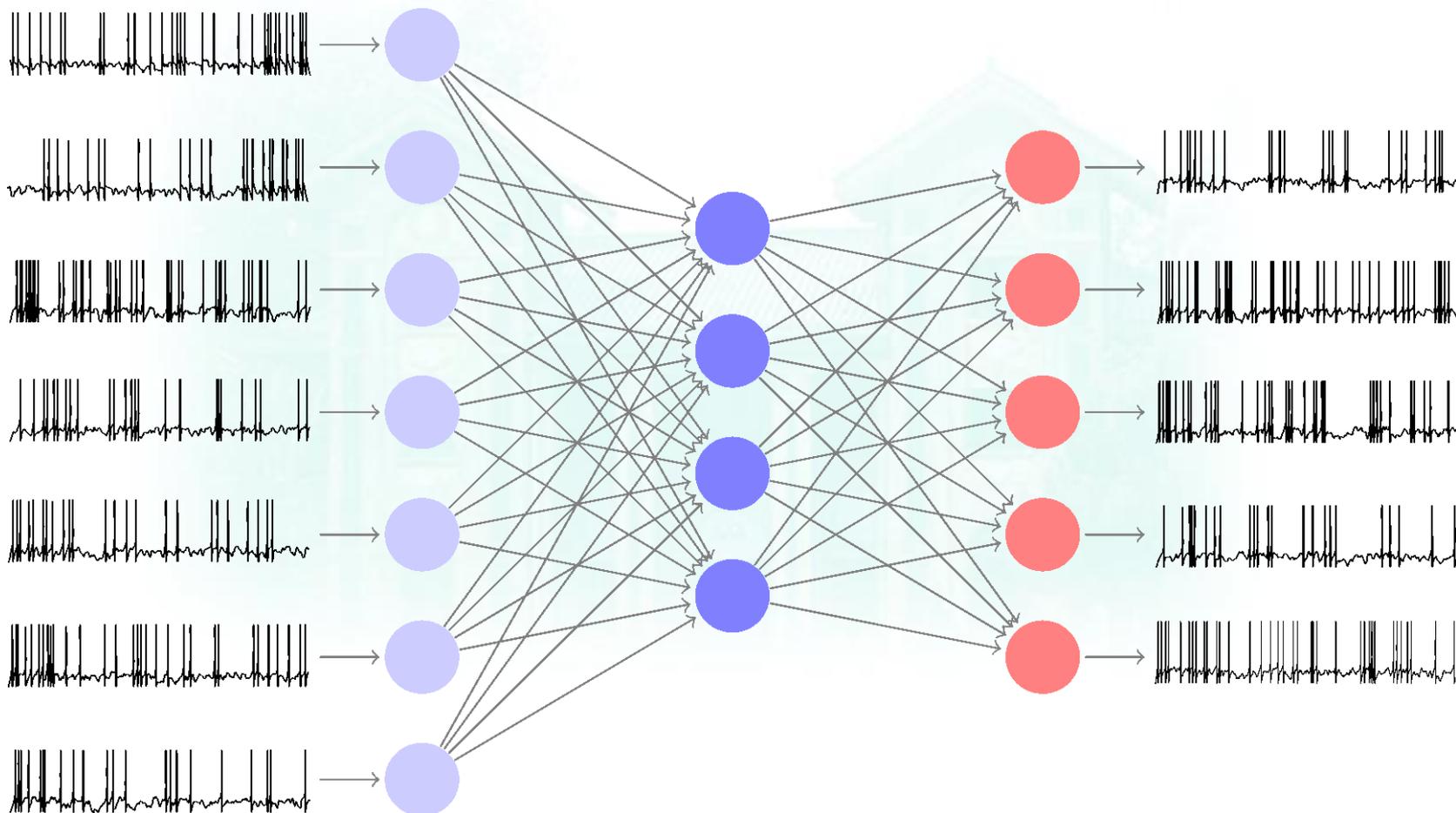
# 探未解之谜：解释模型的每次预测

- LRP (Layer-wise relevance propagation): 将特定输出一层层分解到输入端，得到每个像素的共享大小



# 探未解之谜：脉冲神经网络

- ❑ 人类大脑神经元活动：脉冲序列；如何学习和更新？
- ❑ Spiking neural network: 更像大脑神经元，但有监督训练较困难





# 探未解之谜：认知与推理

- ❑ 深度学习目前解决的是Perceptual AI问题
- ❑ 还不具有真正认知和推理能力 (Cognitive AI)
  - 目前：基于大数据建立的输入-输出统计关系
  - 失效：少见/极端情况下犯简单错误
  
- ❑ 探索方向
  - 基于符号的逻辑推理：No?
  - 将推理过程嵌入模型？
  - 如何连接认知与推理？

# 探未解之谜：伦理与公平

## □ AI伦理

- 安全可控 (AI-人类)：如何确保AI机器人/算法绝对可控？
- 人机融合：半人半机，思想决策被AI影响/控制
- AI武器 (国家-国家/团体/个体)：谁决定谁能/不能使用，如何有效限制；AI蜜蜂寻找攻击特定目标…
- 自动驾驶事故 (公司-个体)：AI算法提供商，汽车制造商，出租公司，乘客各负什么责任？保护乘客还是行人？
- AI导致失业：谁之错？如何用AI帮助失业者？



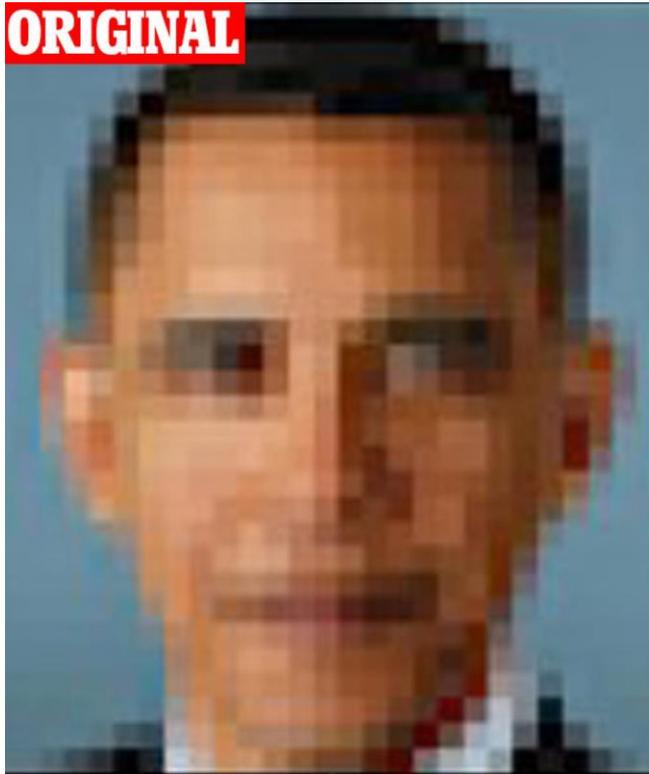
超越了技术本身，需要多学科、多职能部门参与

# 探未解之谜：伦理与公平

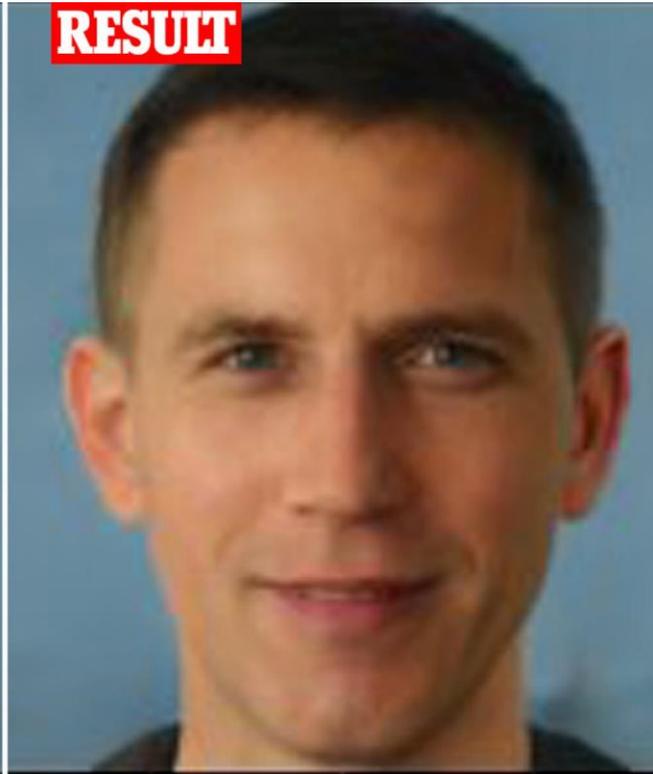
## □ AI公平

- 算法偏见：人脸识别算法对白种人性能好，对黑种人差！
- 如何保证不同性别、地区、民族、国家的人们能同等接受AI的教育或利用AI帮助学习、工作和生活？

**ORIGINAL**



**RESULT**





# 评大众观点

- ❑ 深度学习只不过是调参
- ❑ 没新意，只是数据更多、计算更快
- ❑ 深度学习只是工具和工程方法
- ❑ 深度学习需要大数据和人工标注
- ❑ 深度学习发展已经到顶
- ❑ 深度学习真正落地应用的例子很少

模型算法创新  
思想百花齐放  
安全解释之谜  
前沿挑战多样  
产业应用井喷  
莫学无畏儿郎

- ❑ AI理解你的所思所想
- ❑ 机器翻译已超越人类翻译
- ❑ AI将很快超越人类智能

哗众取宠  
以偏概全  
难越天堑



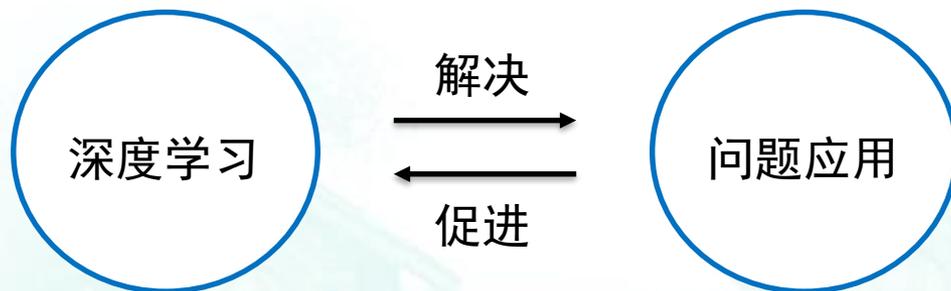
# 讨论

- 将来AI/DL会有那些可能或不可能的突破；什么应用场景可能或不可能有AI参与？给出理由



# 结论

## 深度学习与应用



- 深度学习的研究大大促进了AI的发展与应用
- 深度学习是一种思想，而不仅仅是一类方法
- 还有很多问题和挑战需要被攻克



# 最终：人类的还是AI的？

---

## 人-机鸿沟 (The Human-AI Gaps) :

真认知 (Conscious)

真情绪 (Emotional)

真体验 (Embodiment)

真生死 (Limited life)