

# Machine Learning – Overview

# Main Areas of Artificial Intelligence

- **computer vision**  
(spatial structures, state-of-the-art: Convolutional Neural Networks)
- **natural language processing**  
(sequential structures, state-of-the-art: transformers)
- **automated decision making, robotics**  
(reinforcement learning)



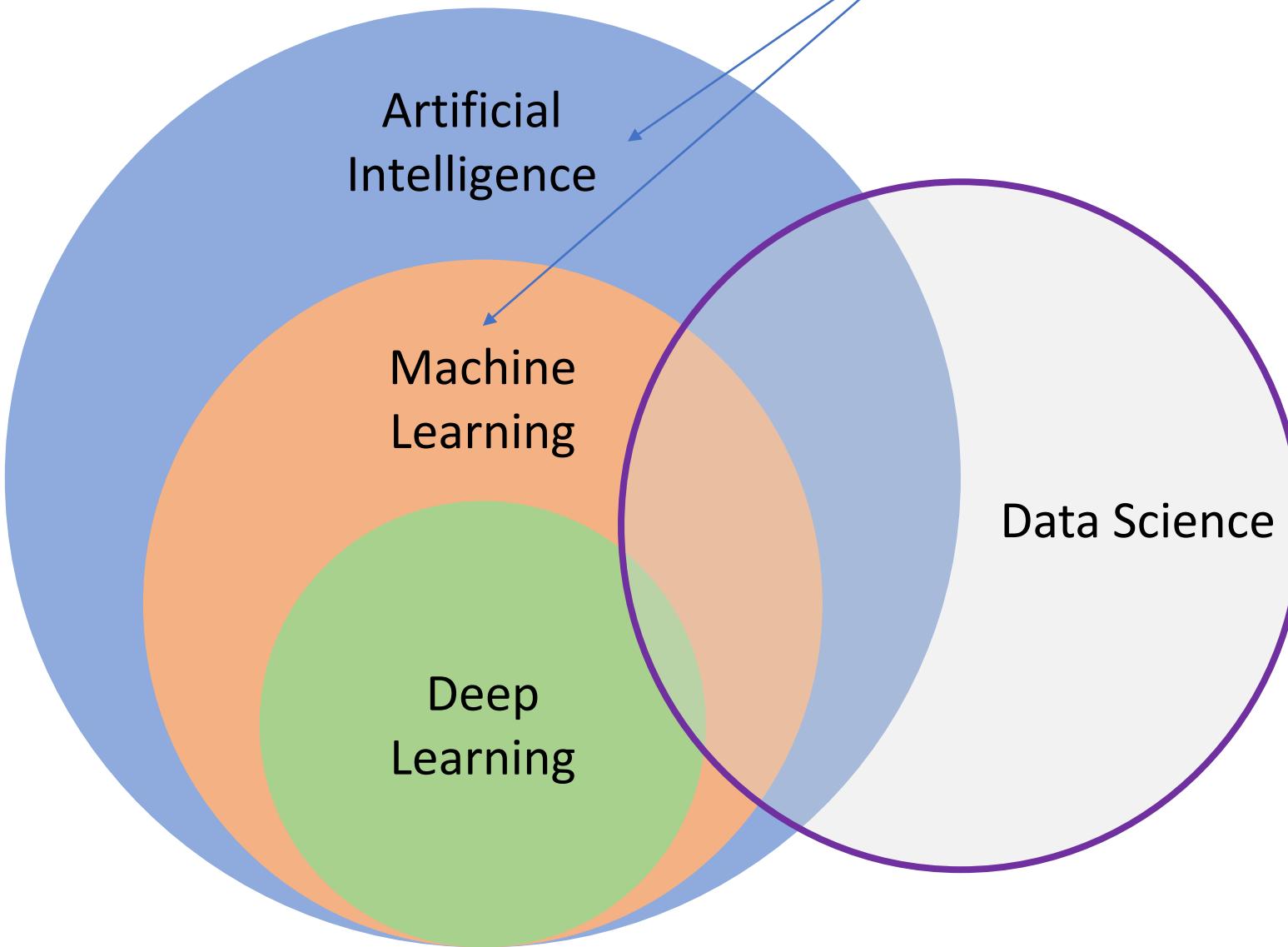
from wikipedia

All of these are enabled by one key ingredient:

- *learning from experience (Machine Learning)*
- also: knowledge representation, automated reasoning (first indices in modern large language models)

agency:  
perception – thought – action

# Buzz Words ...



*Deep Learning:*

special kind of ML  
algorithms using (deep)  
neural networks

*Data Science:*

extract knowledge from  
data (by means of ML,  
among other things)

# Traditional Algorithms and GOFAI

traditional algorithms:

explicit (handcrafted) instructions for each situation



from wikipedia

symbolic AI (aka GOFAI):

use knowledge by means of symbols (as representations), logic, search  
(e.g., expert systems like Deep Blue)

*Public perception is changing over time: A modern chess program, nowadays disparaged as brute computing, would have been considered intelligent in the 50s.*

# ML: Learning from Experience/Data

mainly exploiting statistical dependencies with the aim of **generalization** to new (e.g., future) data (compare with human reasoning by analogies)

training (usually offline optimization):

**ML algorithm + data = explicit algorithm** (to be used at inference time)

→ reduction of complexity and much better generalizability compared to handcrafted algorithms

analogy: Humans do not hit the ground running (storage capacity of DNA limited) but have learning capabilities.

# Supercharging the Scientific Method

use ML and data to replace or enhance explicit methods relying on detailed domain knowledge ([Software 2.0](#))

- overcome our evolutionary limitations in math with clever learning algorithms and collecting data
- immediate impact on many aspects of industry, business, and science, formulated as narrow tasks with strictly defined inputs (aka weak AI)

more imminent than (still philosophical) long-term quest for human-level AI (aka strong AI, AGI), i.e., general-purpose intelligence  
(although recent language models show multi-purpose capabilities)

# Most Famous Applications

recommendations



chatbots



ChatGPT



autonomous driving



translation



assistants (speech recognition)



robotics



OCR



and many more ...

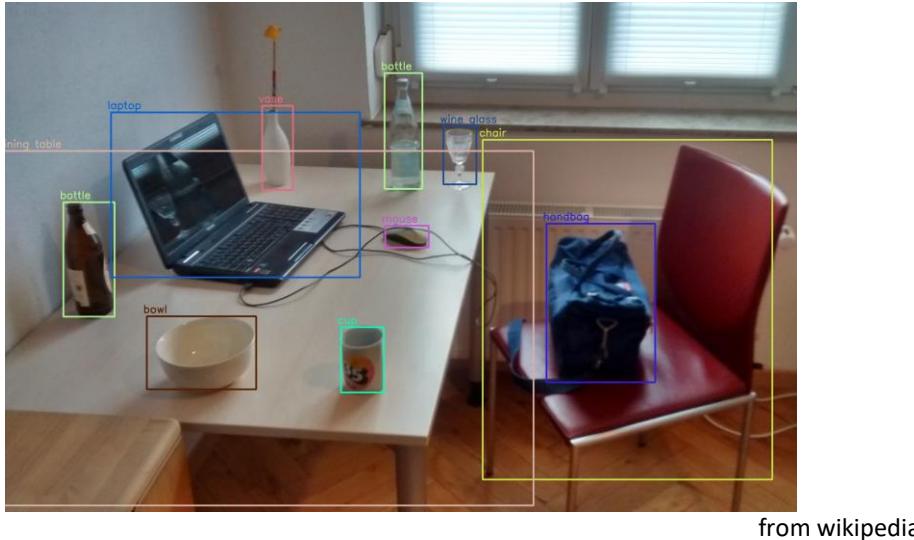
# When to Use ML (= Learning from Data)

## automation

too complex for rules

## complexity / uncertainty

too complex for humans



examples: object recognition, all applications from previous slide

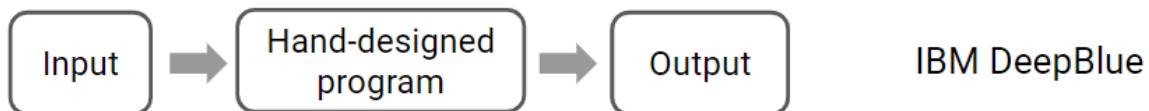
more scientific use cases: medicine (imaging, diagnosis, drug design), particle physics (analysis of collider experiments), material science (material properties and design of new materials), ...



examples: protein structure predictions (AlphaFold), demand forecasting

# Ladder of Generalization

## Rule-based systems



IBM DeepBlue

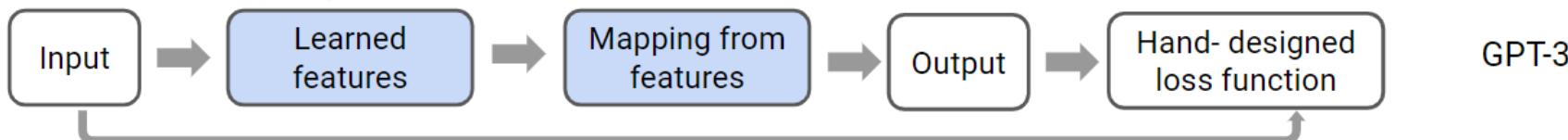
Learnable part of the system

## Classical machine learning



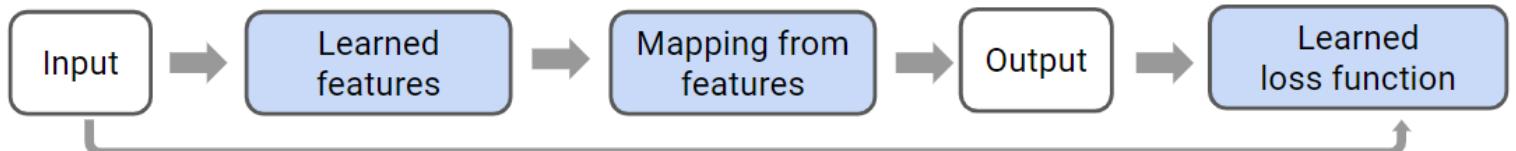
SVM

## Deep learning: (self-)supervised learning



GPT-3

## Deep learning: other RL formulations



???

e.g., ChatGPT (RLHF)

[source](#)

# Generative AI

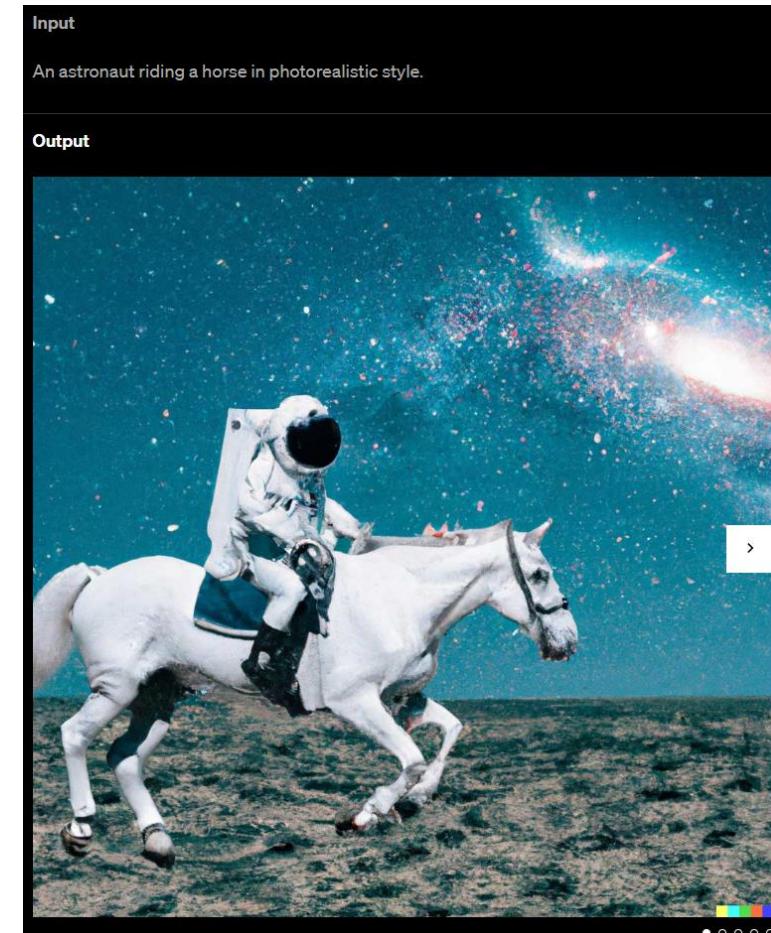
more recently: generative applications

- rather than predictive (or discriminative) ones
- e.g., image generation, conversational AI, new proteins or materials

Depending on the application, there are currently two dominant approaches:

- text generation: large language models (transformer)
- image synthesis: diffusion models

example: DALL-E 2



# Learning Paradigms

# Supervised Learning

**learning by teacher** → usually rather narrow tasks (passive approach)

## Target Quantity

- **known in training:** labeled samples or observations from past
- to be  for unknown cases (e.g., future values)

## Features

- input information that is
- correlated to target quantity
  - known at prediction time



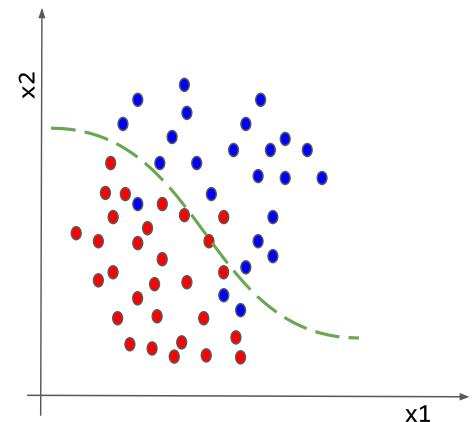
## Example: Spam Filtering

*Classify emails as spam or no spam*

use accordingly **labeled emails as training set**

use information like **occurrence of specific words** or **email length** as **features**

**features  $x_1$  and  $x_2$**   
**spam, no spam**



# Reinforcement Learning

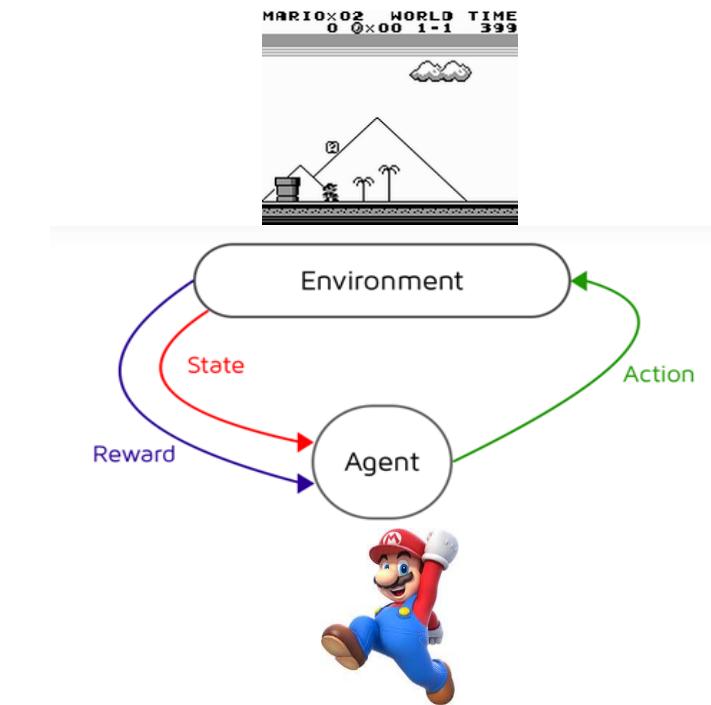
**learning by trial-and-error** (exploration and exploitation)

- goal-based approach → active and more generic than supervised learning (but sparse reward signals)
- receiving feedback from the environment, no supervision
- formalization of sequential decision making (delayed rewards)

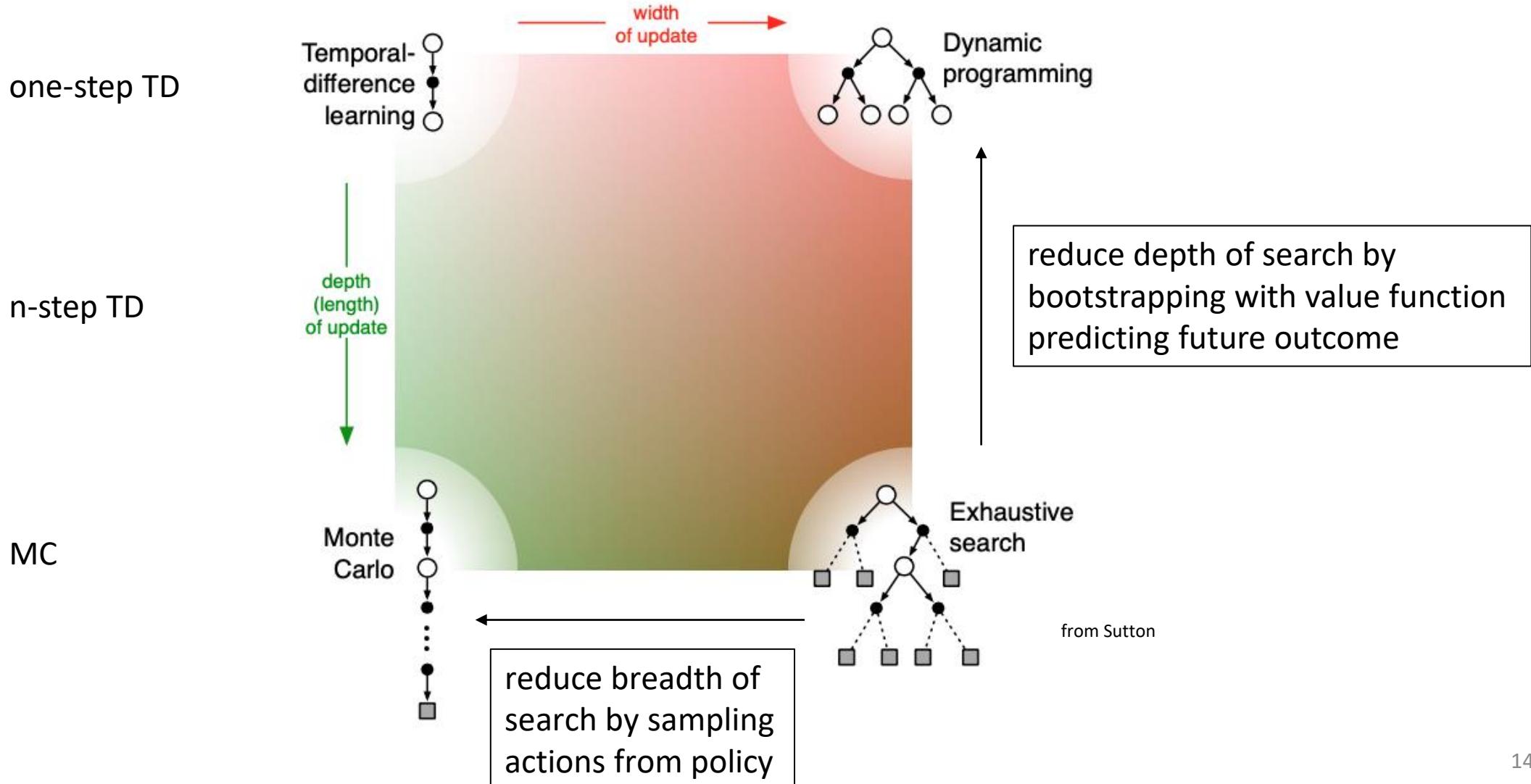
corresponds to search for best action policy to reach a given goal  
(e.g., win a game)

using learning from examples (data) to guide the search

RL setup usually more difficult (e.g., non-differentiable as a whole) than supervised learning one (which can be seen as “generalized optimization”, often of proxy metric)  
but RL can be cast as supervised-learning setup: express rewards by more intricate loss function



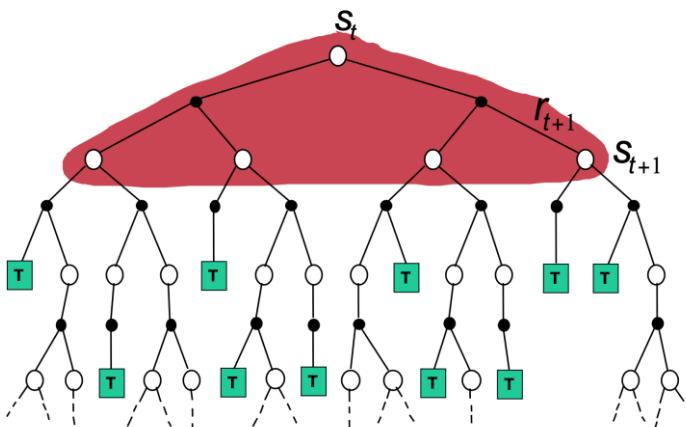
# Reduction of Search Space



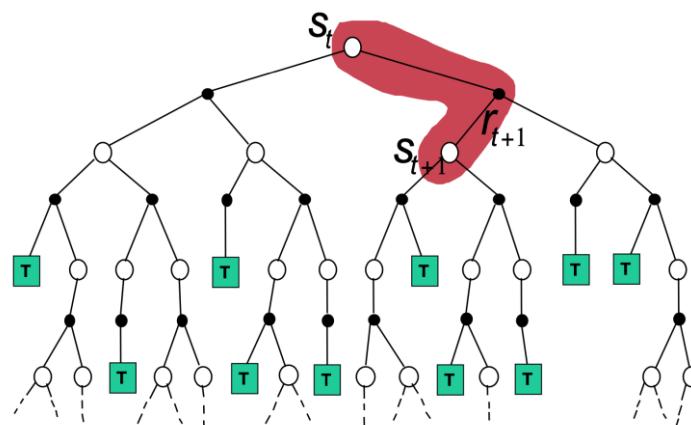
# Main Concepts of Value-Based RL Methods

**bootstrapping:** update estimates of state values based on estimates of values of successor states  
**sampling:** experience of sample sequences (no need for complete knowledge of environment)

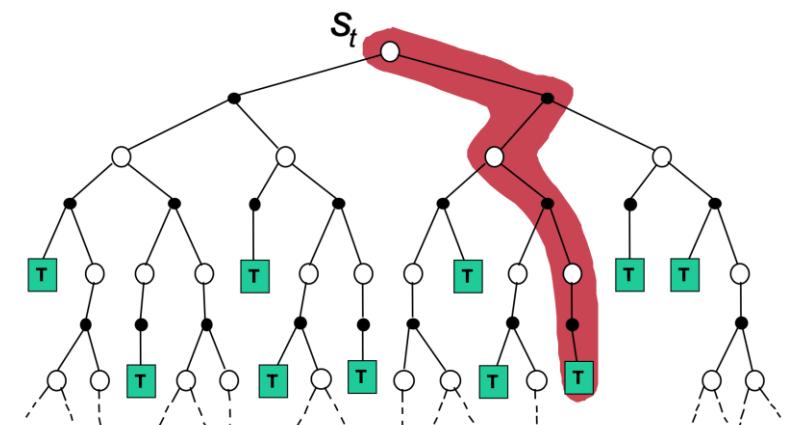
Dynamic Programming



Temporal Difference (TD) Learning



Monte Carlo (MC)



from Sutton

- bootstrapping
- no sampling → model-based  
(transition probabilities needed)

- bootstrapping
- sampling → model-free

- no bootstrapping
- sampling → model-free

# Unsupervised Learning

## learning by observation

no target information → kind of “vague” pattern recognition (but plenty of data)

can be cast as **self-supervised learning**:

- input-output mapping like supervised learning
- but generating labels itself from input information
- learning of semantic feature representations
- e.g., word2vec, BERT, GPT

generative AI as unsupervised learning: generate variations of training data

## How Much Information is the Machine Given during Learning?

### ► “Pure” Reinforcement Learning (**cherry**)

- ▶ The machine predicts a scalar reward given once in a while.

### ► A few bits for some samples

### ► Supervised Learning (**icing**)

- ▶ The machine predicts a category or a few numbers for each input
- ▶ Predicting human-supplied data
- ▶ 10→10,000 bits per sample

### ► Self-Supervised Learning (**cake génoise**)

- ▶ The machine predicts any part of its input for any observed part.
- ▶ Predicts future frames in videos
- ▶ Millions of bits per sample



© 2019 IEEE International Solid-State Circuits Conference

1.1: Deep Learning Hardware: Past, Present, & Future

Y. LeCun

59

## Self-Supervised Learning

- ▶ Predict any part of the input from any other part.

- ▶ Predict the **future** from the **past**.

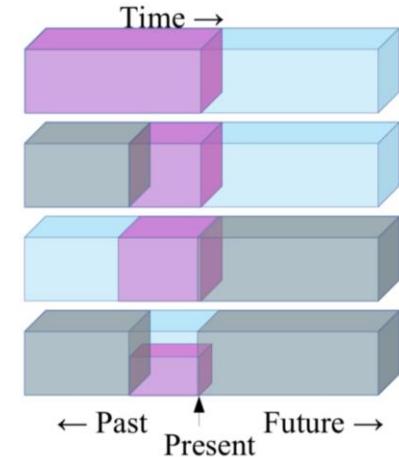
- ▶ Predict the **future** from the **recent past**.

- ▶ Predict the **past** from the **present**.

- ▶ Predict the **top** from the **bottom**.

- ▶ Predict the **occluded** from the **visible**

- ▶ Pretend there is a part of the input you don't know and predict that.



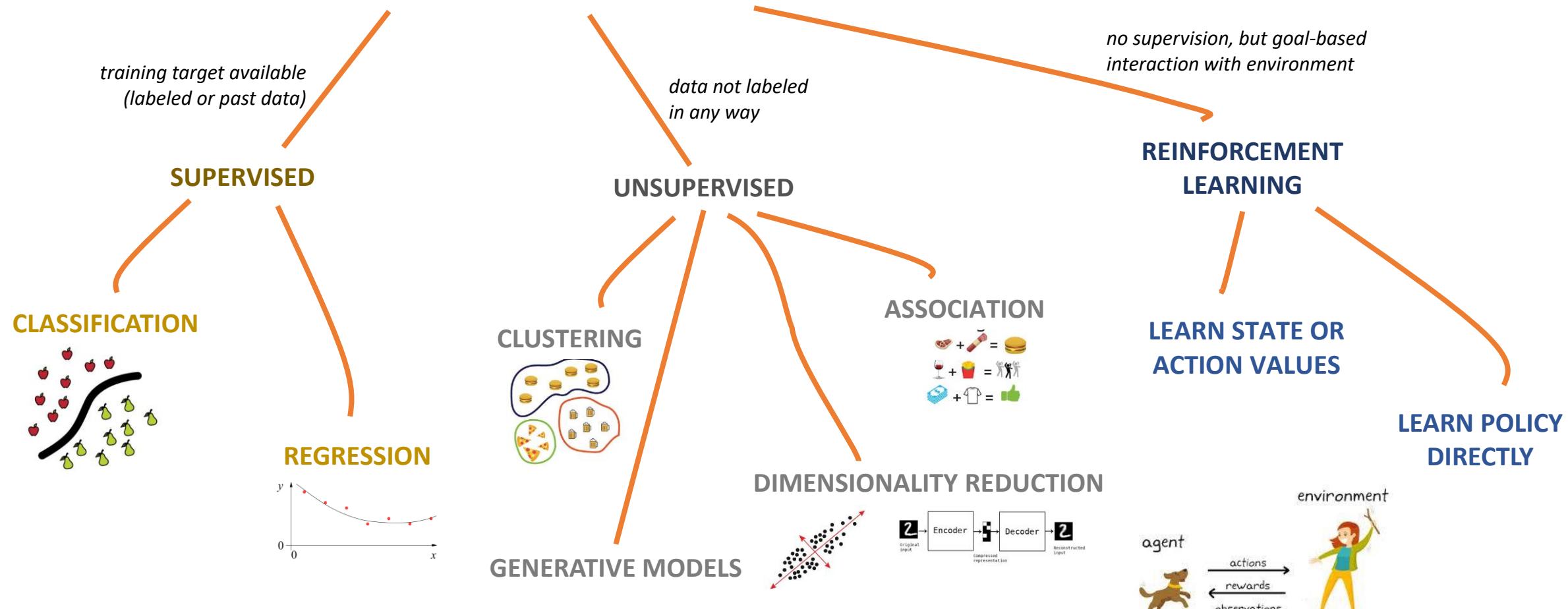
© 2019 IEEE International Solid-State Circuits Conference

1.1: Deep Learning Hardware: Past, Present, & Future

Y. LeCun

58

# MACHINE LEARNING



learning by teacher  
(high-dimensional curve fitting)

learning by observation  
(pattern recognition)

learning by trial-and-error  
(sequential decision making)

unsupervised and reinforcement learning  
can both be cast as supervised-learning

# Fitting and Generalization



... ML ...



# Supervised Learning Scenario

map inputs to output:  $y = f(\mathbf{x})$  (estimated:  $\hat{f}(\mathbf{x})$ )

random variables  $Y$  and  $\mathbf{X} = (X_1, X_2, \dots, X_p)$  ← usually many dimensions

fit train data set of  $(y_i, \mathbf{x}_i)$  pairs

(i.i.d. assumption: random samples from underlying data-generating process)

then apply learned statistical dependencies to test data set

## classification:

categorical target:  $y = 0$  or  $y = 1$  (e.g., image of cat or not), predict probabilities

## regression:

real-valued target:  $Y \in [0, \infty)$  (e.g., demand forecasting) or  $Y \in (-\infty, \infty)$

# Generalization

**generalization** as core of ML:

**empirical risk minimization** (training error) as proxy for minimizing unknown population risk (test error, aka generalization error or out-of-sample error)

generalization gap: difference between test and training error

- **interpolation** to unencountered samples from training environment
- **extrapolation** to testing conditions differing from training environment

curse of dimensionality: many features (dimensions) → lots of data needed to densely sample volume

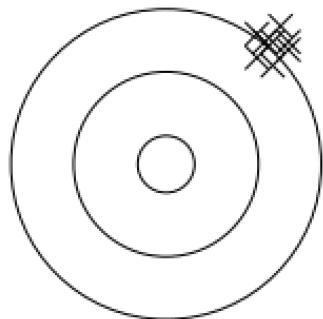
but reality is friendly: most high-dimensional data sets reside on lower-dimensional manifolds (manifold hypothesis) → enabling effectiveness of ML

need for appropriate **inductive bias** (aka learning bias): set of assumptions of a learning algorithm to predict outputs of inputs not encountered during training (“data in disguise”)

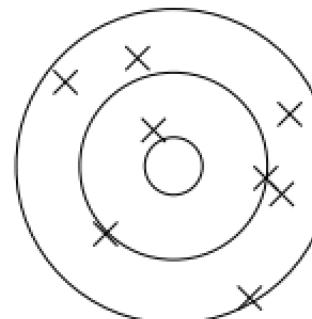
inductive bias comes in many different forms: model design (e.g., linear response), regularization (e.g., convolutions), optimization algorithms, ...

# Bias, Variance, Irreducible Error

think of fitting ML algorithms as repeatable processes with different (i.i.d.) data sets



**bias:**  
due to too simplistic model  
(same for all training data sets)  
“underfitting”



**variance:**  
due to sensitivity to specifics (noise)  
of different training data sets  
“overfitting”

irreducible error (aka Bayes error):

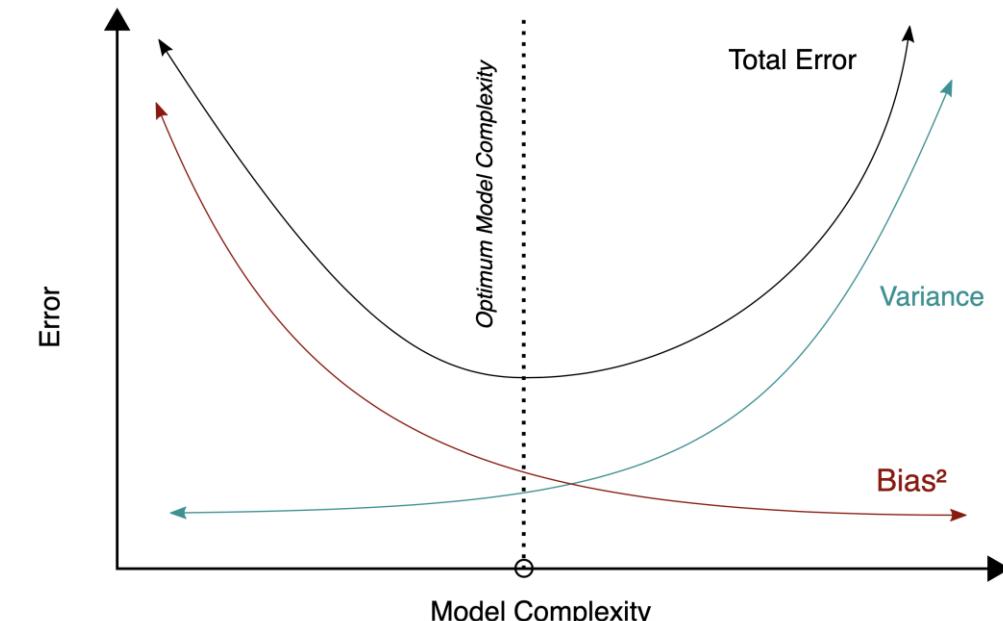
inherent randomness (target generated from random variable following probability distribution)

→ limiting accuracy of ideal model

different potential reasons for inherent randomness (noise): complexity, missing information, ...

# Bias-Variance Tradeoff

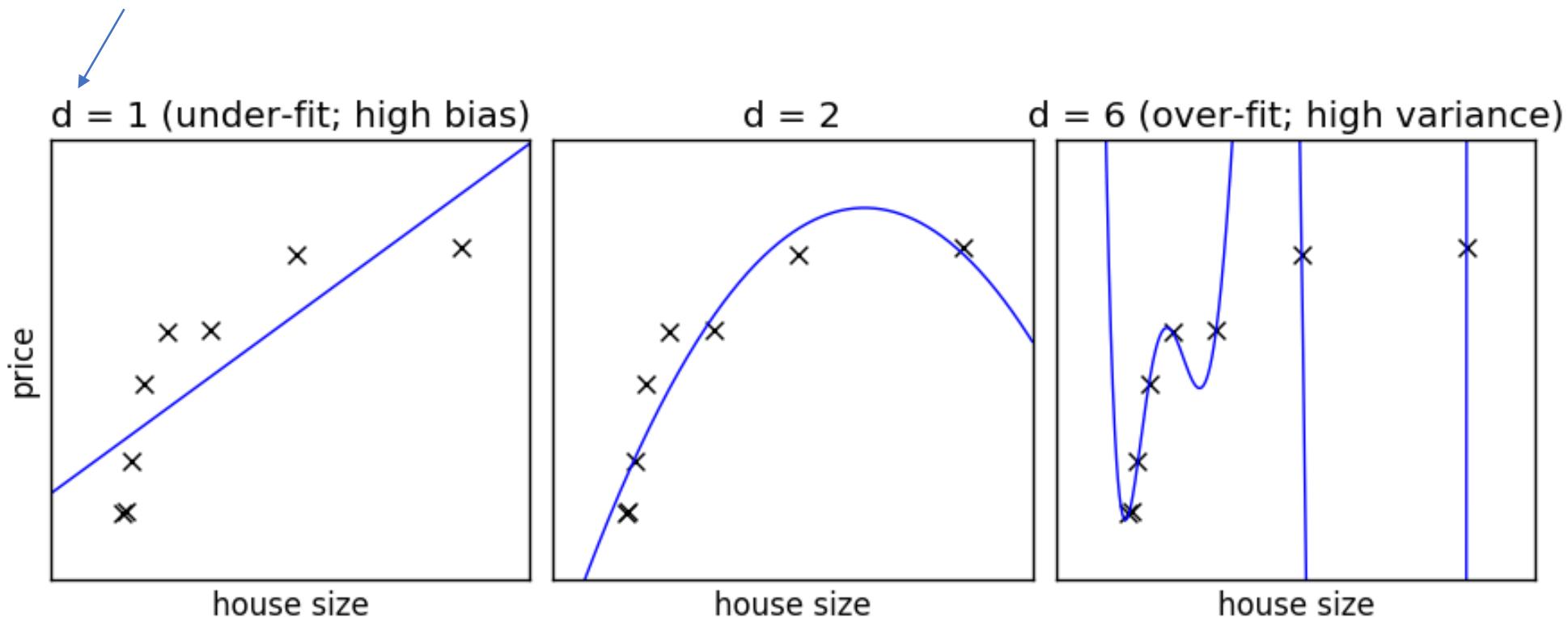
- fundamental concept in classical statistical learning theory
- models of higher complexity have lower bias but higher variance (given the same number of training examples)
- generalization error follows U-shaped curve:  
overfitting once model complexity (number of parameters) passes certain threshold
- overfitting: variance term dominating test error  
→ increasing model complexity increases test error



from wikipedia

# Example: Non-Linear Function Approximation

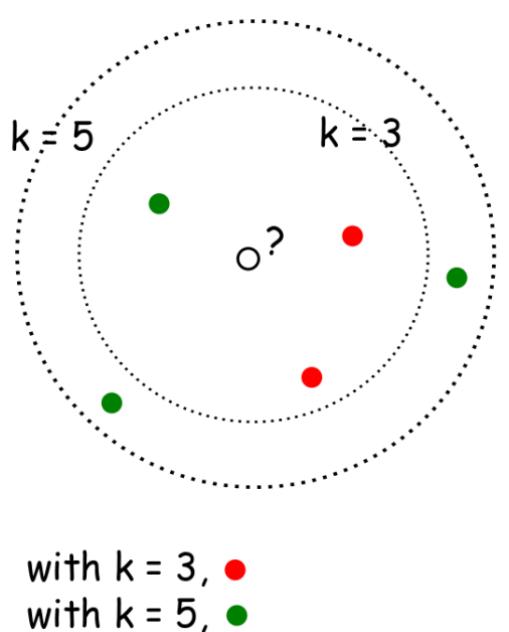
degree of fitted polynomial



from scikit-learn documentation

# Example: k-Nearest Neighbors

- local method, instance-based learning
- non-parametric
- distance defined by metric on  $x$  (e.g., Euclidean)



regression:

$$\hat{f}(x_0) = \frac{1}{k} \sum_{j=1}^k y_j \quad \text{with } j \text{ running over } k \text{ nearest neighbors of } x_0$$

- low  $k$ : low bias but high variance
- high  $k$ : low variance but high bias

$$bias = f(x) - \frac{1}{k} \sum_{j=1}^k y_j$$

$$var = \frac{\sigma^2}{k}$$

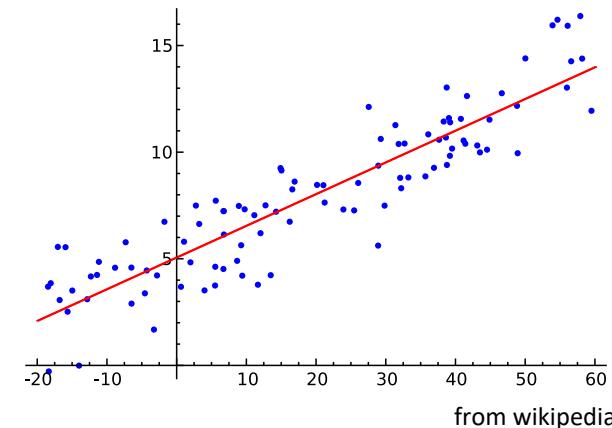
# Linear Regression

fit:

$$y_i = \hat{\alpha} + \sum_{j=1}^p \hat{\beta}_j x_{ij} + \varepsilon_i$$

(model)

error term (noise): reflects assumed data distribution (here: Gaussian with same variance  $\sigma^2$  for all samples)



parameters to be estimated:

- $\hat{\alpha}, \hat{\beta}$

$$\rightarrow \hat{\sigma}^2 = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{f}(x_i))^2$$

(approximating assumed true  $\alpha, \beta, \sigma$ )

predict:

$$\hat{y}_i = E[Y|X = x_i] = \hat{f}(x_i)$$

- conditional mean for squared loss of least squares method
- predict arbitrary quantile by means of quantile loss

$$p(y|x_i) = \mathcal{N}(y; \hat{y}_i, \hat{\sigma}^2)$$

Gaussian

mean

variance  
(reflected  
by  $\varepsilon_i$  in fit)

# General Recipe of Statistical Learning

statistical learning algorithm by combining:

- **model** (e.g., linear function, Gaussian distribution)
- **objective function** (e.g., squared residuals)
- **optimization algorithm** (e.g., gradient descent)
- **regularization** (e.g., convolutions)

# Loss Function

loss function  $L$ : expressing deviation between prediction and target

$$L(y_i, \hat{f}(x_i); \hat{\theta})$$

with  $\hat{\theta}$  corresponding to parameters of model  $\hat{f}(x)$

e.g.,  $\hat{\alpha}, \hat{\beta}$  in linear regression

e.g., squared residuals (for regression problems):

$$L(y_i, \hat{f}(x_i); \hat{\theta}) = (y_i - \hat{f}(x_i; \hat{\theta}))^2$$

# Cost Function

averaging losses over (empirical) training data set:

$$J(\hat{\theta}) = \frac{1}{n} \sum_{i=1}^n L(y_i, \hat{f}(x_i); \hat{\theta})$$

cost function to be minimized according to model parameters  $\hat{\theta}$   
→ objective function

# Cost Minimization

minimize training costs  $J(\hat{\theta})$  according to model parameters  $\hat{\theta}$ :

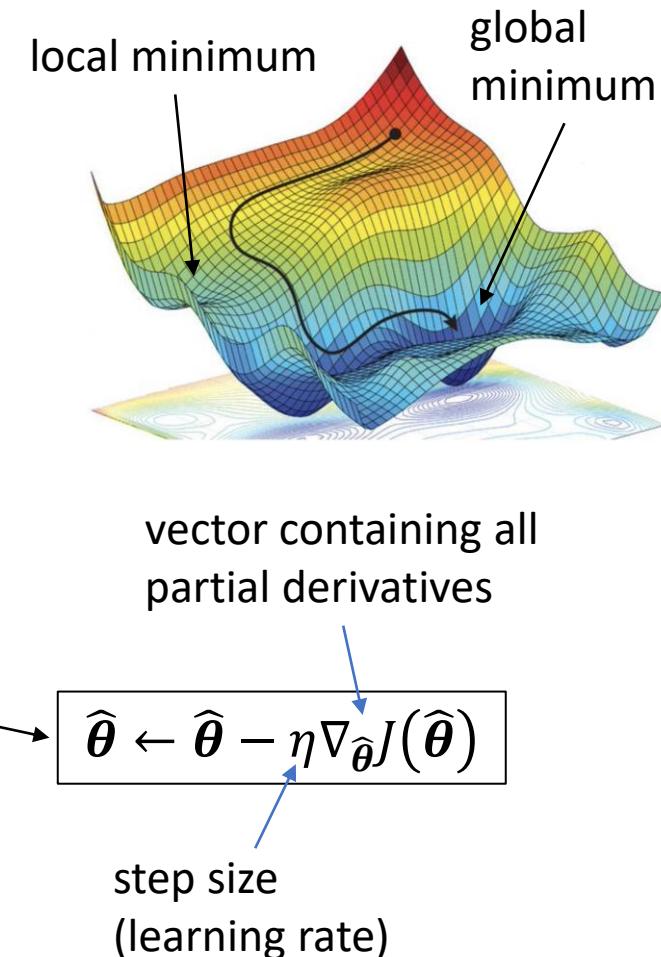
$$\nabla_{\hat{\theta}} J(\hat{\theta}) = 0$$

e.g., for mean squared error (aka least squares method):

$$\nabla_{\hat{\theta}} \frac{1}{n} \sum_{i=1}^n (y_i - \hat{f}(x_i; \hat{\theta}))^2 = 0$$

analytical solution for linear regression: ordinary least squares

in general: iterative, numerical optimization (e.g., **gradient descent**)



**maximum likelihood estimation** (minimization of  $D_{KL}$  between probability distributions of true data-generating process and model: *make the model distribution match the empirical distribution*):

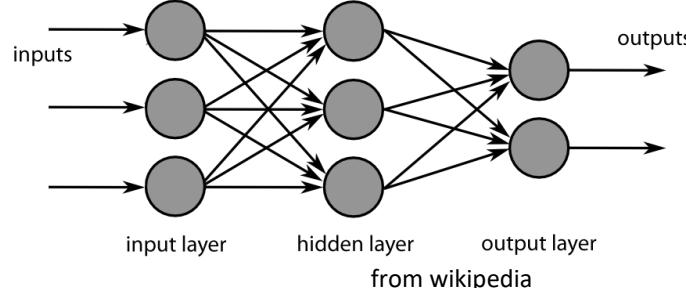
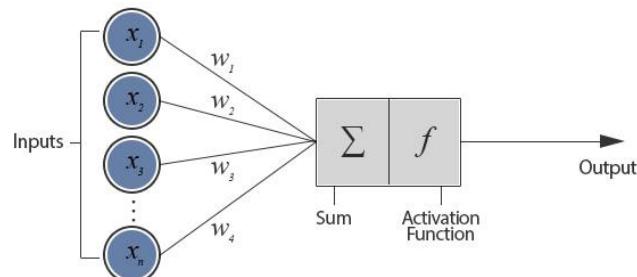
special objective function, estimate mode of assumed model distribution

# Algorithmic Families

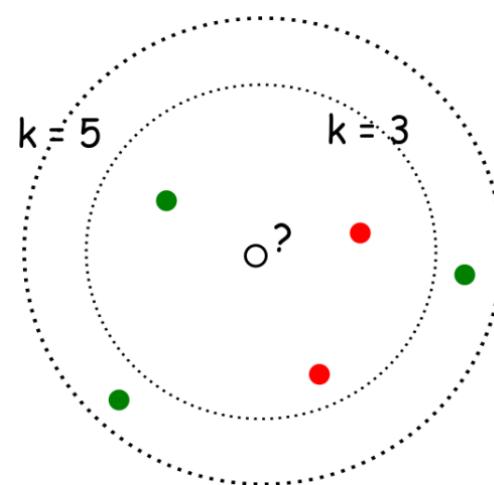
## linear (parametric) models

- linear regression
- Generalized Linear Models
- Generalized Additive Models

**neural networks:** non-linear just by means of activation functions



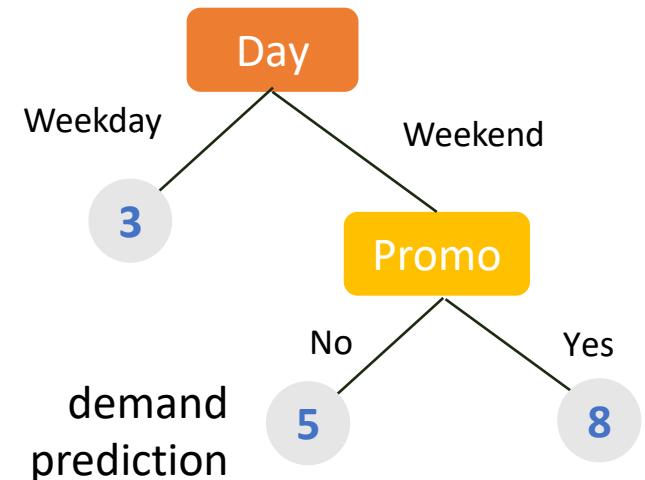
## nearest neighbors (local methods, instance-based learning) – non-parametric models



with  $k = 3$ , ●  
with  $k = 5$ , ●

**kernel/support-vector machines:** linear model (maximum-margin hyperplane) with kernel trick

## decision trees: rule learning



## often used in ensemble methods

- bagging: random forests
- boosting: gradient boosting

Most ML algorithms (even unsupervised and RL) can be described by the general recipe of combining models, costs, optimization, and regularization methods.

including non-linear models like neural networks (backpropagation), support-vector machines (hinge loss in soft-margin SVM), or decision trees (impurity functions)

Most powerful ML algorithms are compound, with rather simple (often linear) building blocks. → reductionism with complex interactions

To generalize well, one needs to find a method with an appropriate inductive bias for the task at hand (e.g., suitable objective function or regularization method like convolutional layers).

# Deep Learning

# Recap: Goal of ML

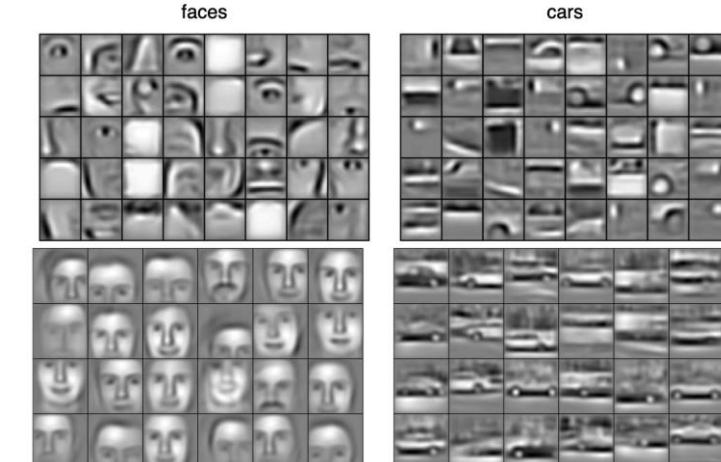
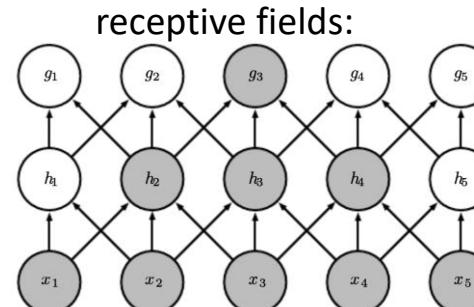
generalization from optimization on training data set (approximation of true data generating probability distribution by empirical risk minimization)

- fitting: complex function approximation
- for generalization: learning of good abstraction/representation of data/concepts

→ deep learning methods (neural networks with many layers) optimal candidates

e.g., convolutional neural networks (CNN) can learn hierarchical representation by means of many convolutional and pooling layers

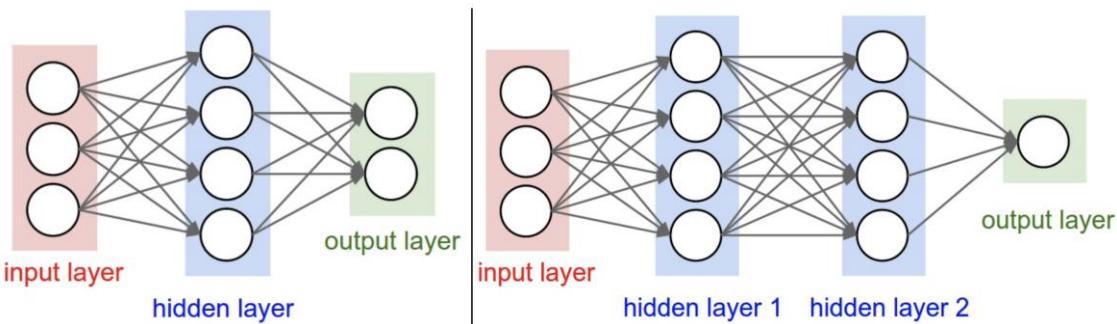
the deeper the better:  
accuracy, hierarchical representation (many aspects of nature hierarchical)



[source](#)

# Multi-Layer Perceptron (MLP)

fully-connected feed-forward network with at least one hidden layer



toward deep learning: add hidden layers

more layers (depth) more efficient than just  
more nodes (width): less parameters needed  
for same function complexity

classification:

- logistic regression in hidden nodes
- cross-entropy loss:  $L_i(y_i, \hat{f}(\mathbf{x}_i); \hat{\mathbf{w}}) = -\sum_{k=1}^K y_{ik} \log \hat{f}_k(\mathbf{x}_i; \hat{\mathbf{w}})$
- several output nodes  $k$  for multi-classification
- softmax output function:  $g_k(\mathbf{t}_i) = \frac{e^{t_{ik}}}{\sum_{l=1}^K e^{t_{il}}}$

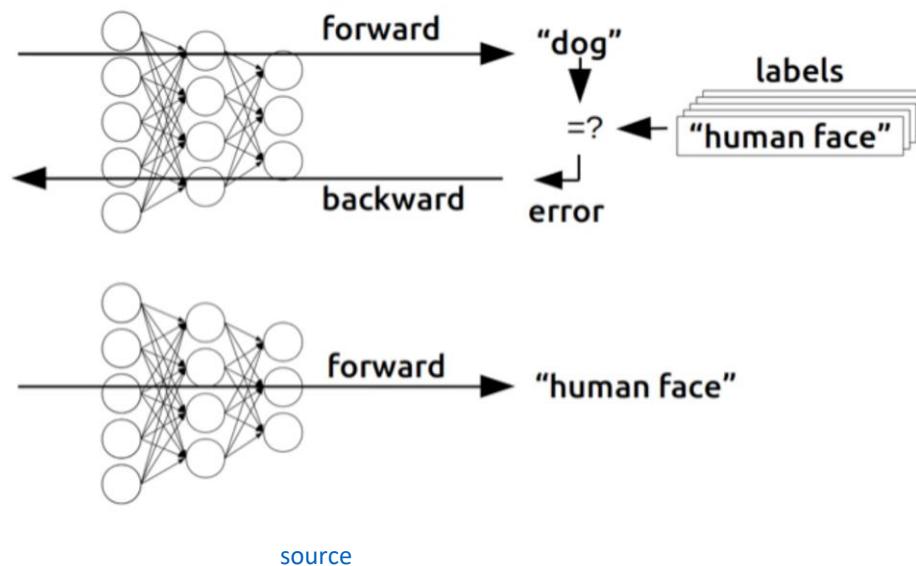
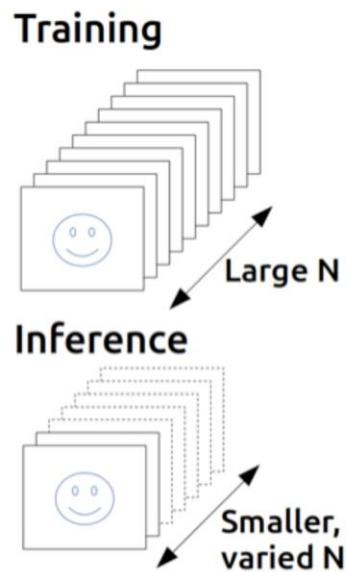
regression:

- squared error loss
- identity output function
- usually just one output node

# Learning Mechanism: Back-Propagation

back-propagation of errors (gradients of cost function according to weights) through layers via chain rule of calculus (avoiding redundant calculations of intermediate terms)

each node exchanges information only with directly connected nodes → enables efficient, parallel computation

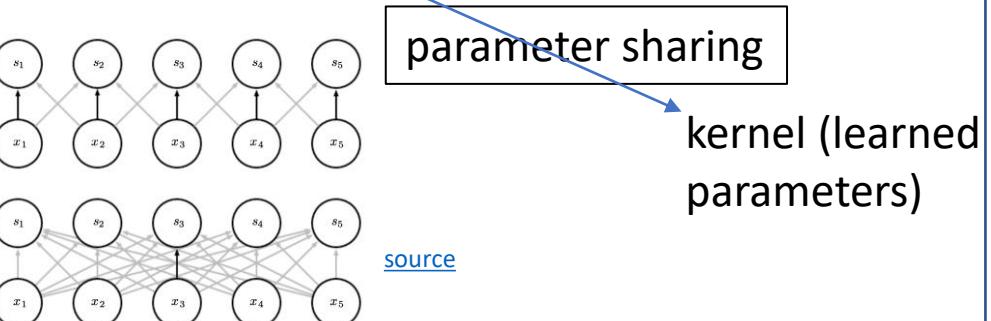


- forward pass: current weights fixed, predictions computed
- backward pass: errors computed from predictions and back-propagated → weights then updated according to loss gradients (via gradient descent)

**CNN** in short: local connections, shared weights, pooling, many layers

# Convolutional Neural Networks

## convolutional vs fully-connected layer:



0	2	15	0	11	10	0	0	1	9	3	0	0
0	0	4	6	10	26	255	255	171	95	33	0	25
0	10	151	238	255	245	245	253	255	225	225	10	0
0	14	170	255	255	244	254	253	245	255	253	124	0
0	98	255	255	255	251	241	111	141	135	215	251	285
13	217	243	255	255	232	229	57	2	0	10	237	255
16	229	252	255	249	12	0	7	7	0	0	237	255
0	61	245	252	25	12	9	9	3	0	236	243	255
0	87	252	250	248	17	0	12	1	252	255	248	14
0	13	111	255	255	245	255	182	181	245	242	240	19
1	0	1	51	251	255	241	254	255	245	251	12	7
0	0	4	0	55	251	255	246	254	253	250	11	0
0	0	4	97	255	255	255	248	257	252	244	255	18
0	22	208	252	246	251	241	10	0	255	245	255	194
0	111	255	252	255	18	24	0	6	0	255	232	250
0	218	252	250	157	7	11	0	0	2	255	255	120
0	173	255	255	101	9	20	0	13	0	13	255	251
0	101	251	251	255	230	98	55	10	11	217	248	253
0	18	144	255	255	247	255	255	249	255	252	255	17
0	0	23	11	215	255	252	248	255	242	248	241	12
0	0	6	1	5	253	235	255	257	247	37	0	4
0	0	5	0	0	0	0	0	0	1	0	6	0

## source

many images  
(training examples),  
potentially with  
several channels

several kernels  
producing several  
feature maps

several kernels producing several feature maps

down-sampling by convolutions and pooling

flatten dimensions for final classification or regression

highly regularized form of feed-forward neural networks

The diagram illustrates the concepts of convolution, translation equivariance, locality, and spatial inductive bias.

**convolution:** A central concept where a smaller input grid (3x3) is processed by a kernel (3x3). The stride is indicated as  $S=1$ .

- input:** The original input grid.
- Striding in CONV:** Shows how a stride of 2 would skip every other input unit.
- locality:** A box labeled "locality" with a blue line connecting it to the input grid.
- translation equivariance:** A box labeled "translation equivariance" with a blue line connecting it to the input grid.
- spatial inductive bias:** A box labeled "spatial inductive bias" with a blue line connecting it to the input grid.

Detailed description: The diagram shows a 4x4 input grid being processed by a 3x3 kernel. The stride is  $S=1$ , meaning each kernel unit processes one input unit. A callout "Striding in CONV" shows a 2x2 stride example where the kernel only processes every second input unit. A box labeled "locality" points to the input grid, indicating that only nearby input units are considered. A box labeled "translation equivariance" also points to the input grid, suggesting that the output is invariant to shifts in the input. A box labeled "spatial inductive bias" points to the input grid, indicating that the model can learn spatial patterns.

## translation invariance

max pooling:

The diagram shows a 4x4 input tensor (X) with values:

1	0	2	3
4	6	6	8
3	1	1	0
1	2	2	4

A vertical axis labeled **X** and a horizontal axis labeled **Y** indicate the spatial dimensions. An arrow points from the input tensor to a 2x2 output tensor (Y) with values:

6	8
3	4

The label "Single depth slice" is positioned above the input tensor.

from wikipedia

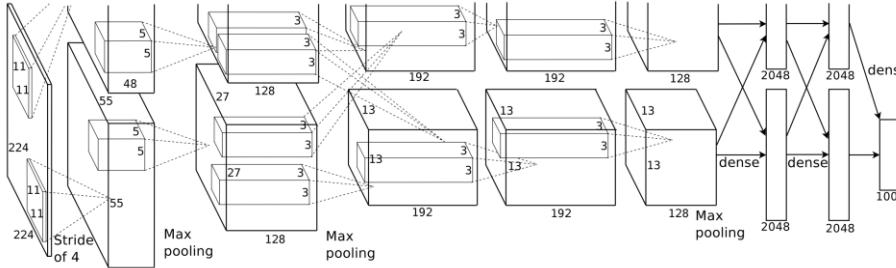
# Rise of Deep Learning

a little bit oversimplified:

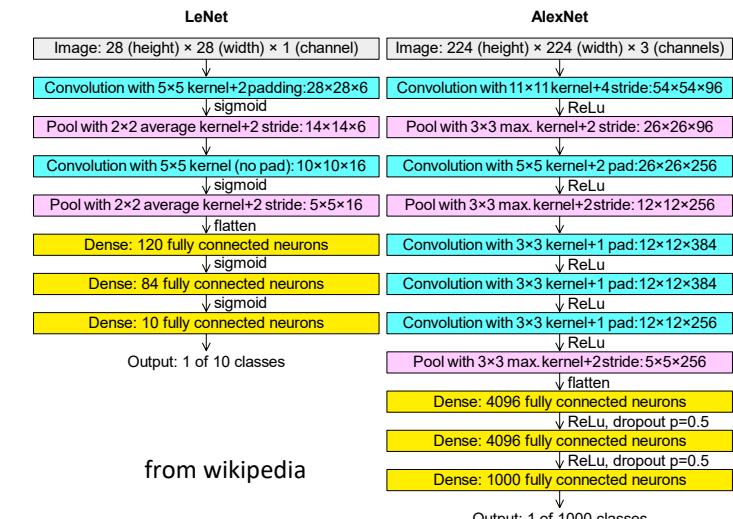
deep learning = lots of training data + parallel computation + smart algorithms

AlexNet:

ImageNet (with data augmentation) + GPUs (allowing more layers) + ReLU, dropout  
(pivotal moment for deep learning: ImageNet challenge 2012)



source



from wikipedia

37

# Training Subtleties of Deep Neural Networks

optimization and regularization difficult

- non-convex optimization problem (e.g., local vs global minima, saddle points), easily overfitting
- many hyperparameters to tune

many methods to get it working in practice (despite partly patchy theoretical understanding)

optimization

- activation and loss functions
- weight initialization
- stochastic gradient descent
- adaptive learning rate
- batch normalization

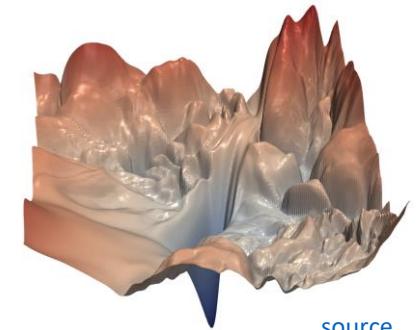
explicit regularization

- weight decay
- dropout
- data augmentation
- weight sharing

implicit regularization

- early stopping
- batch normalization
- stochastic gradient descent

typical loss surface:



[source](#)

# Large Language Models (LLM)

natural language processing: dealing with sequential structures (e.g., text)  
examples:

- machine translation (sequence-to-sequence model)
- sentiment classification
- chat bot (conversational AI)

context awareness via **embeddings** and (formerly) recurrent neural networks  
**(RNN)** or (nowadays) **self-attention**

LLMs: **transformer** models with hundreds of billions of parameters

# Embeddings

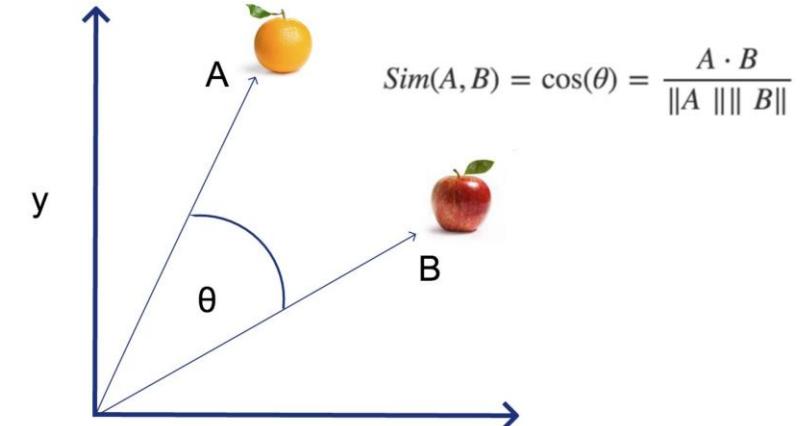
representation of entities by vectors

similarity between embeddings by, e.g., cosine  
similarity → semantic similarity

most famous application: word embeddings  
→ associations (natural language processing)

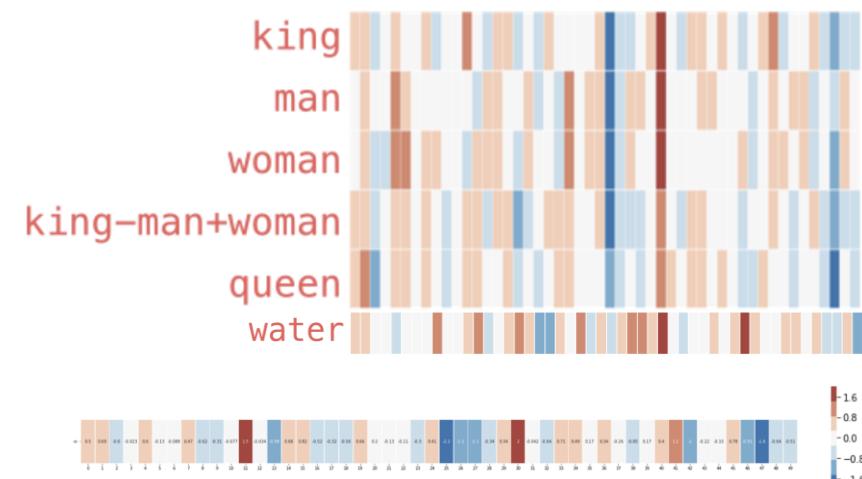
but general concept: embeddings of  
(categorical) features (e.g., products in  
recommendation engines)

learned via co-occurrence (e.g., [word2vec](#))



but also direction of difference  
vectors interesting (analogies):

king – man + woman ≈ queen



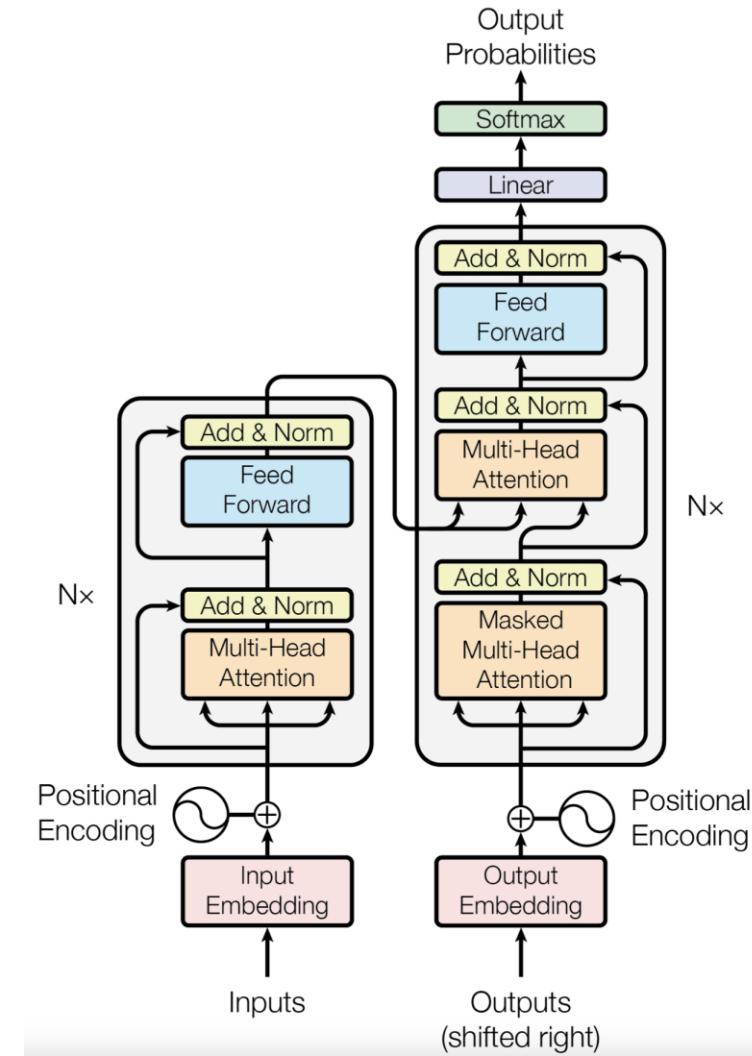
[source](#)

# Transformer

attention is all you need: getting rid of RNNs  
replaced by multi-headed self-attention (implemented  
with matrix multiplications and feed-forward neural  
networks)

- allowing for much more parallelization
- allowing for bigger models (more parameters)

better long-range dependencies thanks to shorter path  
lengths in network (less sequential operations)

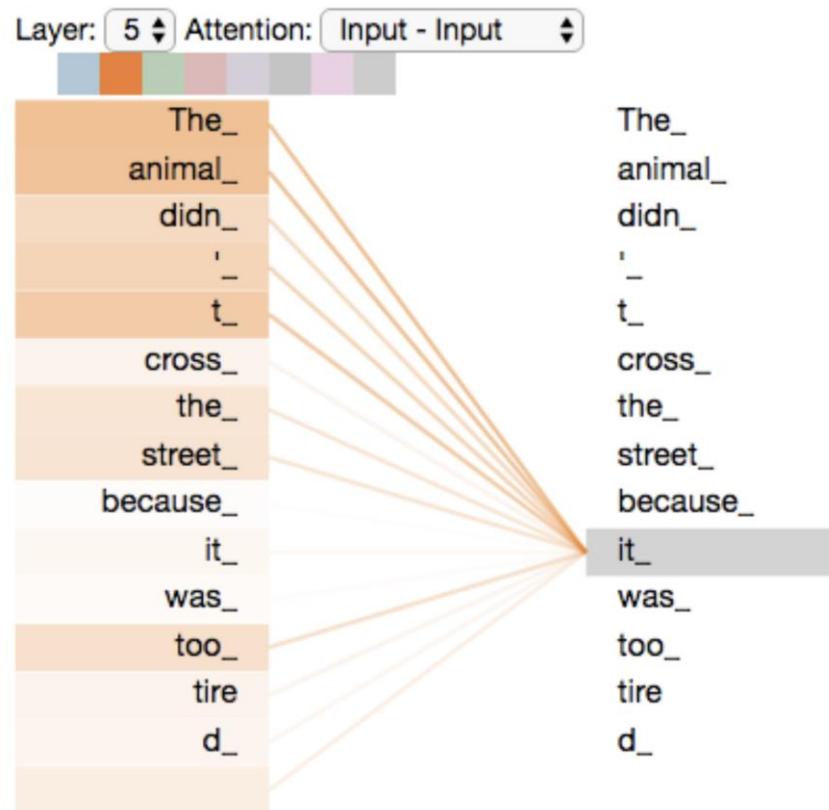


[source](#)

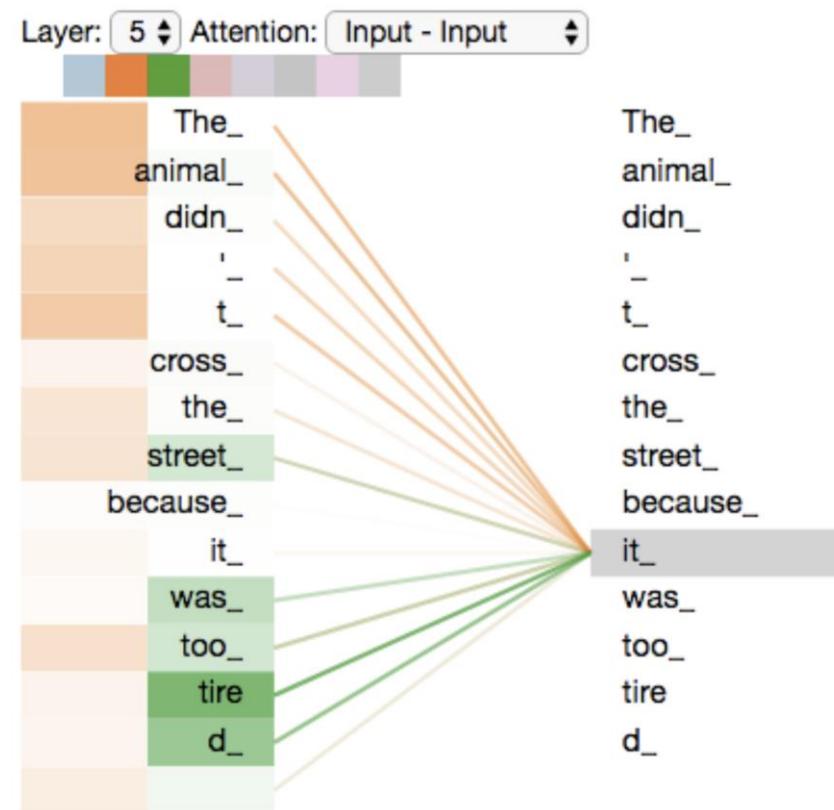
# Self-Attention

computational complexity  
quadratic in length of input (each token attends to each other token)

evaluating other input words in terms of relevance for encoding of given word



multi-head attention: several attention layers running in parallel (considering different aspects of input)

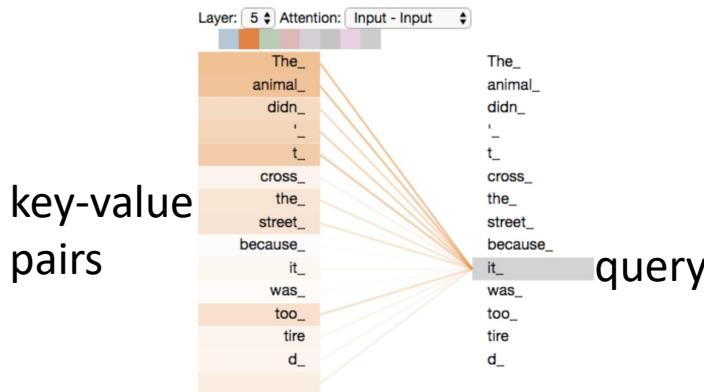


source

# Scaled Dot-Product Attention

3 abstract matrices created from inputs (e.g., word embeddings) by multiplying inputs with 3 different weight matrices

- query Q
- key K
- value V



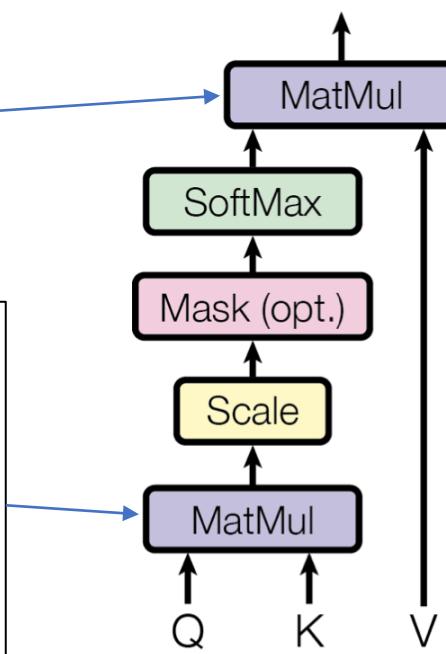
filtering: multiplication of attention probabilities with corresponding key word values

scoring each of the key words (context) with respect to current query word: multiplication of inputs (in contrast to inputs times weights in neural networks)

softmax not scale invariant: largest inputs dominate output for large inputs (more embedding dimensions  $d_k$ )

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

Scaled Dot-Product Attention

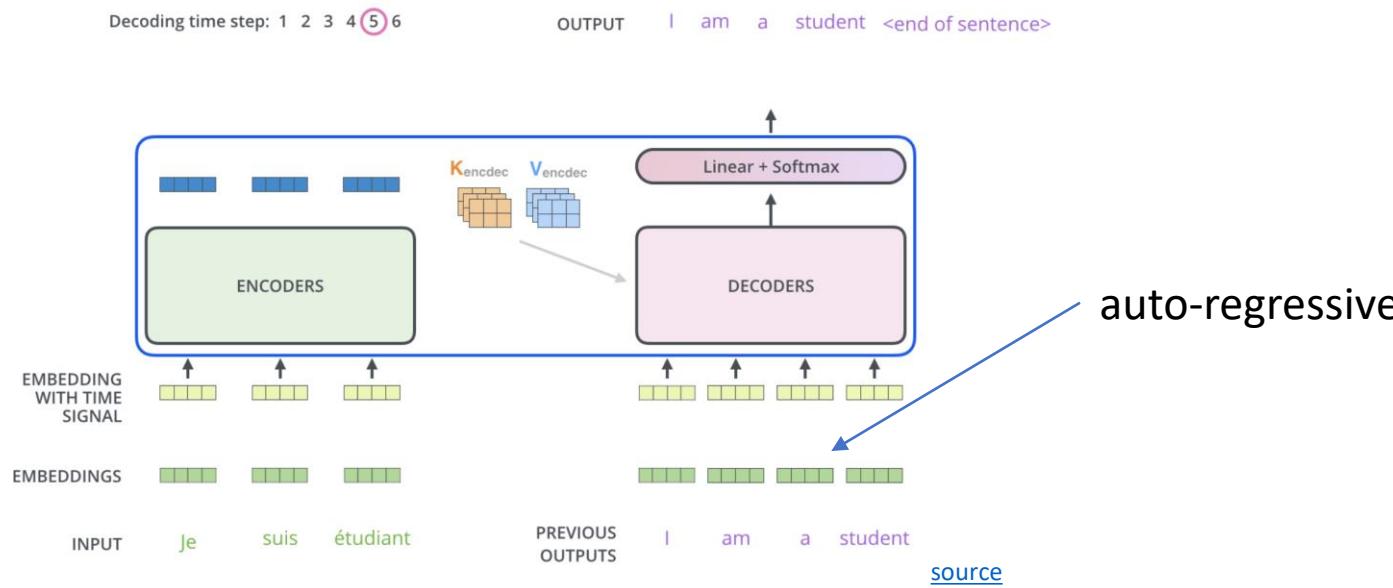


[source](#)

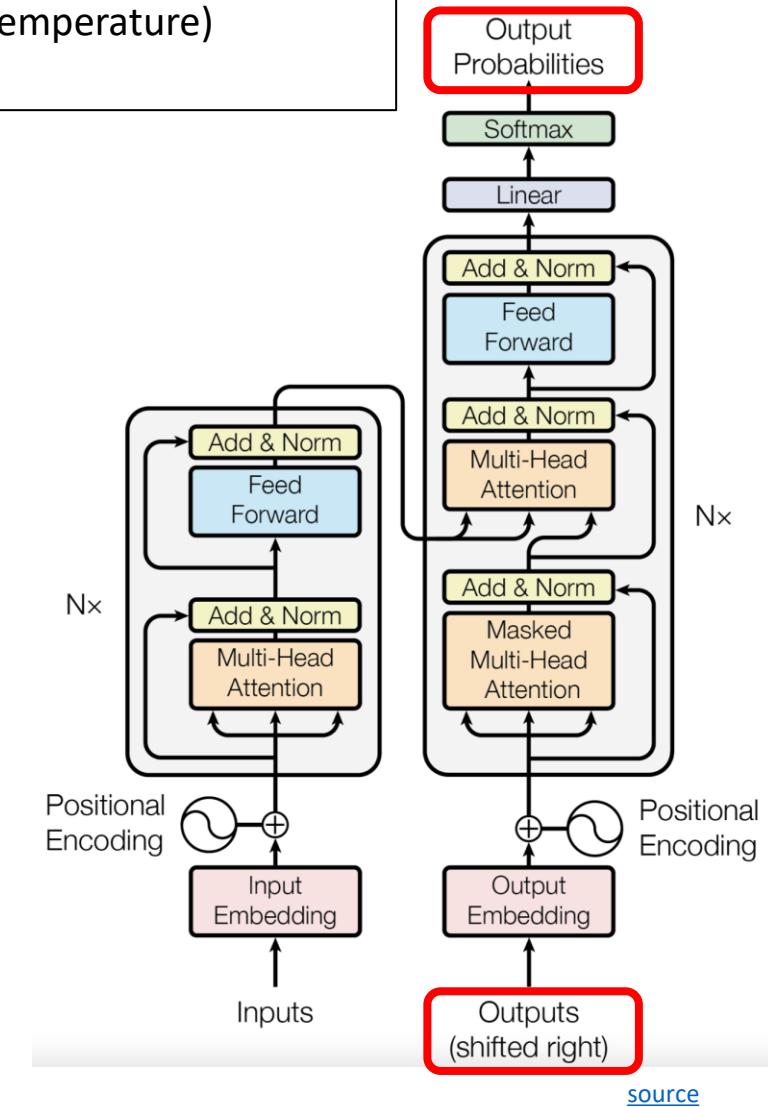
# Sequence Completion

- greedily picking the one with highest probability
- pick according to probabilities (degree of randomness controlled by softmax temperature)
- beam search

for each step/token (iteratively), choose one output token to add to decoder input sequence → increasing uncertainty



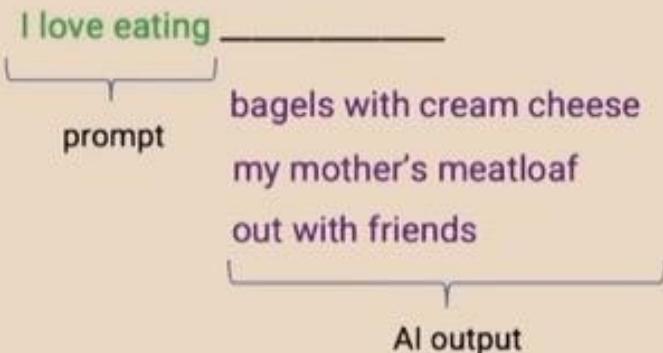
prompt: externally given initial sequence for running start and context on which to build rest of sequence ([prompt engineering](#))



[source](#)

# This decade: Generative AI

## Text generation process



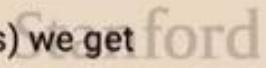
## How it works

Generative AI is built by using supervised learning ( $A \rightarrow B$ ) to repeatedly predict the next word.

*My favorite food is a bagel with cream cheese and lox.*

Input (A)	Output (B)
My favorite food is a	bagel
My favorite food is a bagel	with
My favorite food is a bagel with	cream

When we train a very large AI system on a lot of data (hundreds of billions of words) we get a Large Language Model like ChatGPT.



Andrew Ng



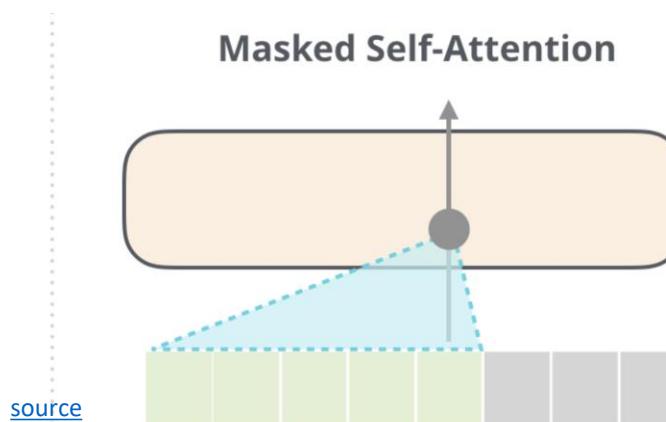
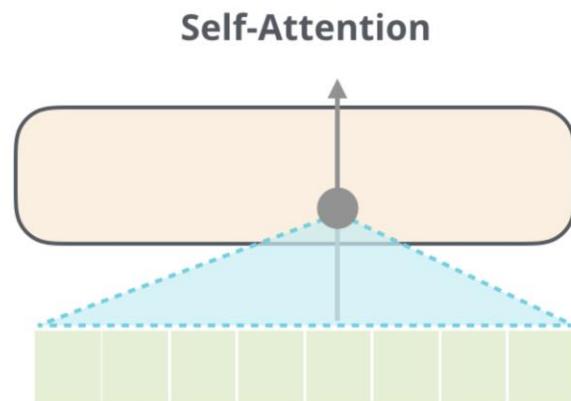
# Typical Transformer Architectures for LLMs

**encoder-decoder** LLMs: sequence-to-sequence, e.g., machine translation

**encoder-only** LLMs:

- representation learning (and subsequent fine-tuning)
- training: prediction of masked words
- incorporate context of both sides of token

example: Google's [BERT](#)  
(Bidirectional Encoder Representations from Transformers)



source

**decoder-only** LLMs:

- text generation (potentially in-context only), e.g., chat bot
- training: next-word prediction
- output one token at a time (auto-regressive: consuming its own output)

examples: OpenAI's [GPT](#)  
(Generative Pre-trained Transformer), Meta's [Llama2](#)

[GPT-4 capabilities](#)

# Multi-Task Learning of LLMs

compositional nature of deep learning allows transfer learning in a semi-supervised way (also prominent for CNNs in computer vision):

- self-supervised **pre-training** (e.g., next-word prediction) on massive data sets (foundation models like GPT or BERT)
- subsequent supervised **fine-tuning** on specific tasks and (usually much smaller) data sets (by adapting parameters or/and adding layers )

the new paradigm:

**in-context** learning as alternative to fine-tuning: only using information fed into LLM via input prompt, no parameter updates (typically decoder-only)

typical prompt: instructions, context (potentially retrieved externally from, e.g., knowledge-base embeddings), query, output indicator  
with (few-shot) or without (zero-shot) providing explicit examples

[prompt engineering](#)

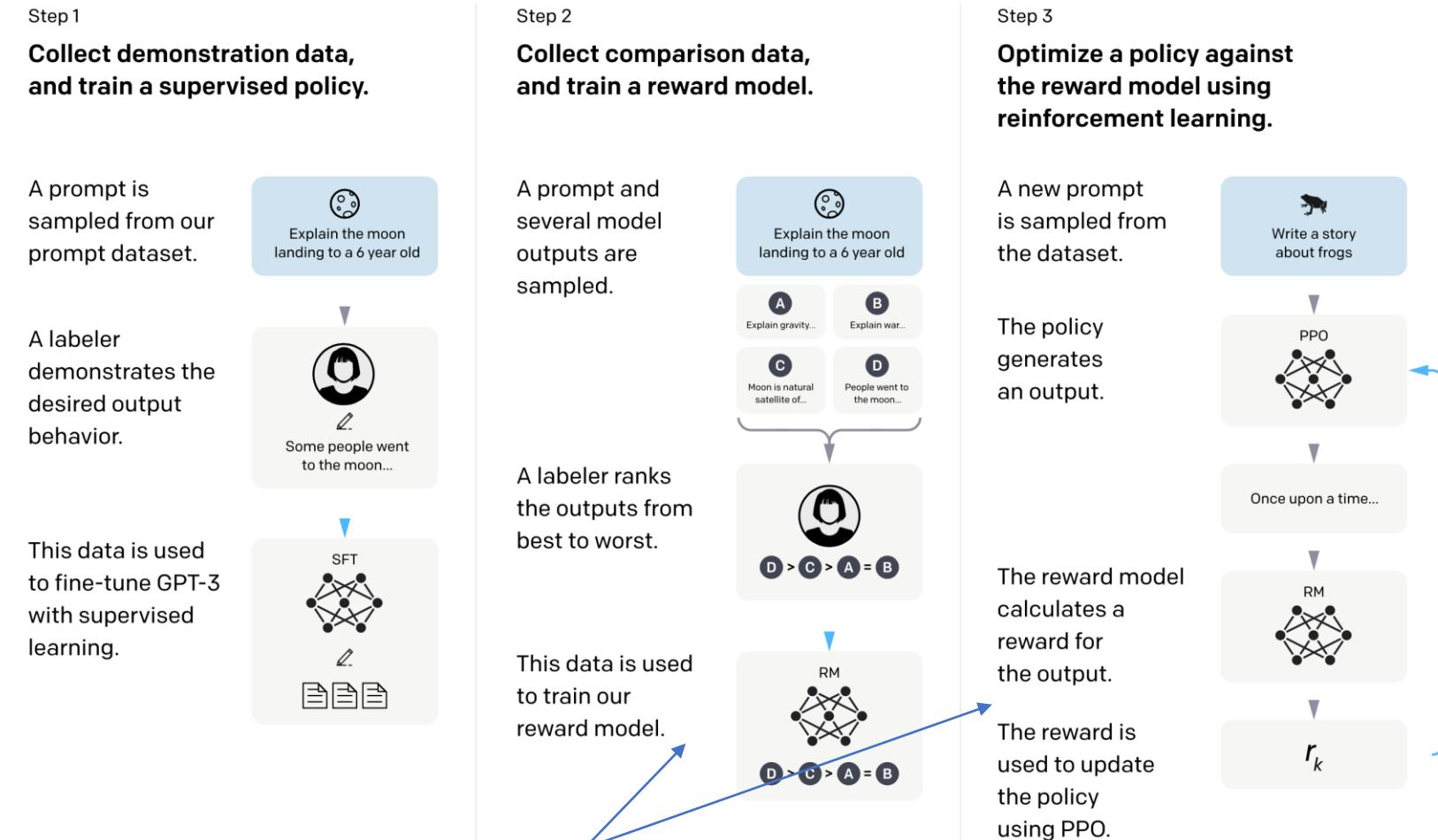
# Conversational AI: RL from Human Feedback

example for supporting large language models (transformers) with RL

used in famous ChatGPT

goal: improve alignment with user intentions

→ learn from human preferences



RL looks at reward of text output passages as a whole (rather than token-level loss in supervised learning)

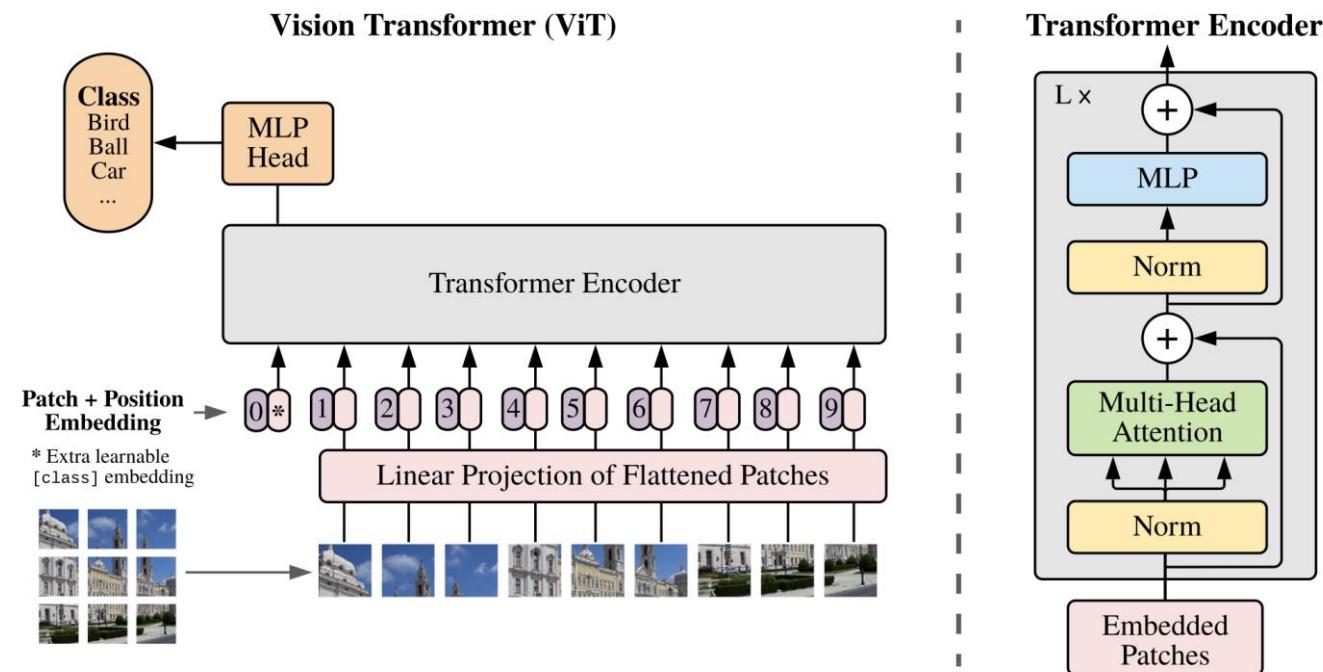
# Transformer for Vision

formulation as sequential problem:

- split image into patches and flatten → use as tokens
- produce linear embeddings and add positional embeddings

processing by transformer encoder:

- pre-train with image labels
- fine-tune on specific data set

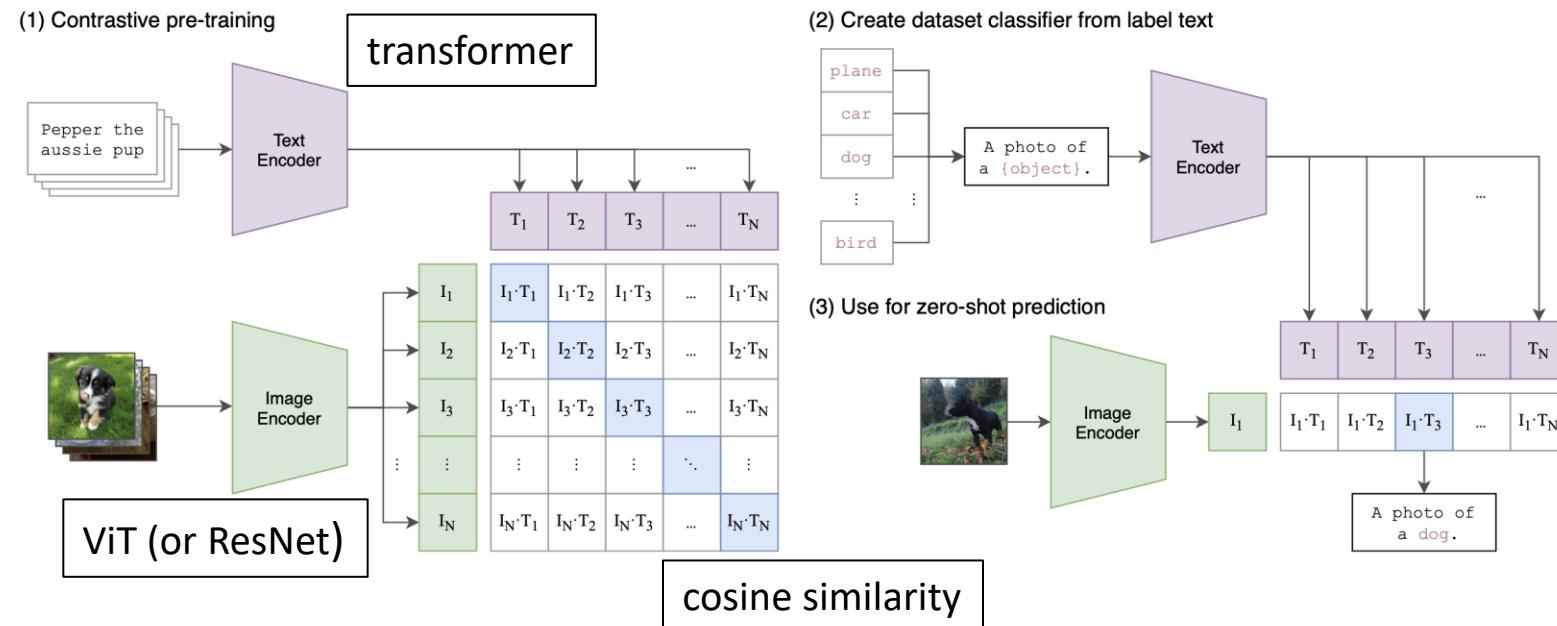


source

# Combination of Vision and Text: Multi-Modality

example: [CLIP](#) (Contrastive Language-Image Pre-training)

- learn image representations by predicting which caption goes with which image (pre-training)
- zero-shot transfer (e.g., for object recognition)



multi-purpose (multi-modal and multi-task) models as next generalization step of ML (e.g., Google's [Pathways](#))

transformers good candidate (universal and flexible architecture, little task-specific inductive bias)

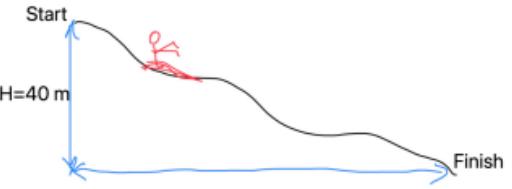
# Google's Gemini:



## Prompt

Here's a solution to a Physics problem by a student.

23. A skier slides down the frictionless slope as shown. What is the skier's speed at the bottom?



Solution:

The conservation of energy means that the energy of the skier is same at the beginning and at the end.

$$\text{Start: } E = mgL$$

$$\text{End: } E = \frac{1}{2}mv^2$$

$$\Rightarrow mgL = \frac{1}{2}mv^2$$

$$\Rightarrow v = \sqrt{2gL} = \sqrt{2 \times 9.81 \times 80} = 39.6 \text{ m}\cdot\text{s}^{-1}$$

Try to reason about the question step by step.

Did the student get the correct answer? If the solution is wrong, please explain what is wrong and solve the problem.

Make sure to use LaTeX for math and round off the final answer to two decimal places.



## Response

The student did not get the correct answer. The student made a mistake in the calculation of the potential energy at the start of the slope. The potential energy at the start of the slope is given by  $mgh$ , where  $m$  is the mass of the skier,  $g$  is the acceleration due to gravity, and  $h$  is the height of the slope. The student used the length of the slope,  $L$ , instead of the height,  $H$ , in the calculation of the potential energy.

The correct solution is:

The conservation of energy means that the total energy of the skier is the same at the beginning and at the end of the slope.

At the start of the slope, the skier has only potential energy, which is given by  $mgh$ .

At the end of the slope, the skier has only kinetic energy, which is given by  $\frac{1}{2}mv^2$

Therefore, we can write:

$$mgh = \frac{1}{2}mv^2$$

Cancelling out the mass  $m$  on both sides, we get:

$$gh = \frac{1}{2}v^2$$

Solving for  $v$ , we get:

$$v = \sqrt{2gh}$$

Substituting the given values, we get:

$$v = \sqrt{2 \times 9.81 \times 40} = 28.01 \text{ m/s}$$

Therefore, the skier's speed at the bottom of the slope is 28.01 m/s.

# Generative Models

# Generative vs Discriminative Models

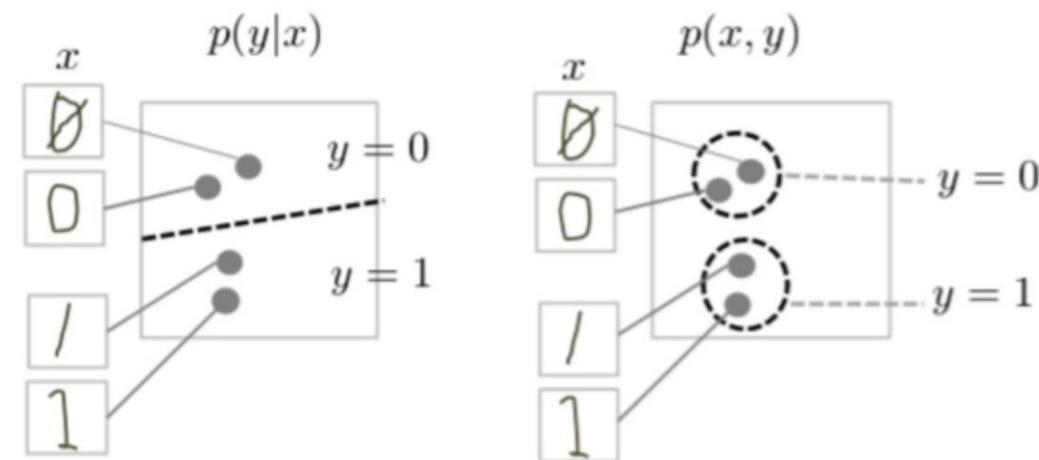
generative models: predict joint probability  
 $P(Y, X)$  (what allows to create new data samples) or directly generate new data samples

or just  $P(X) \rightarrow$  unsupervised (or self-supervised) learning

discriminative models: predict conditional probability (or probability distribution for regression)  $P(Y|X)$  or directly output (label for classification, real value for regression)

task of generative models more difficult: model full data distribution rather than merely find patterns in inputs to distinguish outputs

discriminative model      generative model



[source](#)

# Data Generation

generative models can be used for discriminative tasks (although potentially inferior to direct discriminative methods)

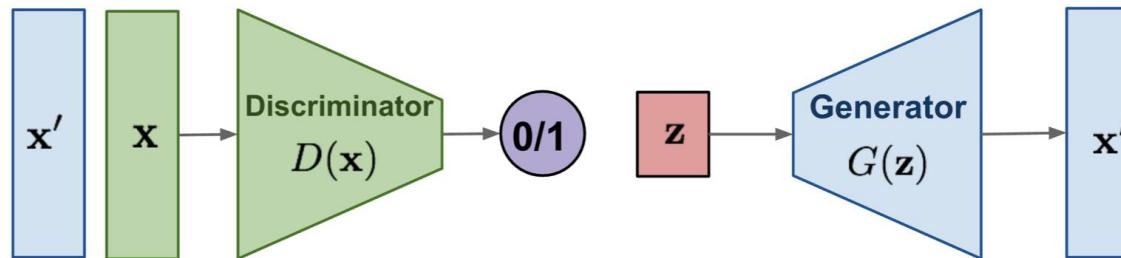
but generative methods do more than discriminative ones: model full data distribution

→ allows generation of new data samples (can be images, text, [video](#), [audio](#), code like SQL or Python, proteins, materials, time series, structured data, ...)

large (auto-regressive) language models examples of generative models

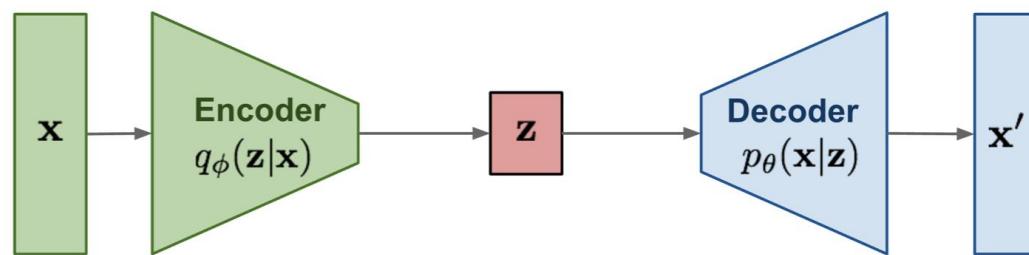
# Different Types of Generative Models

**GAN:** Adversarial training



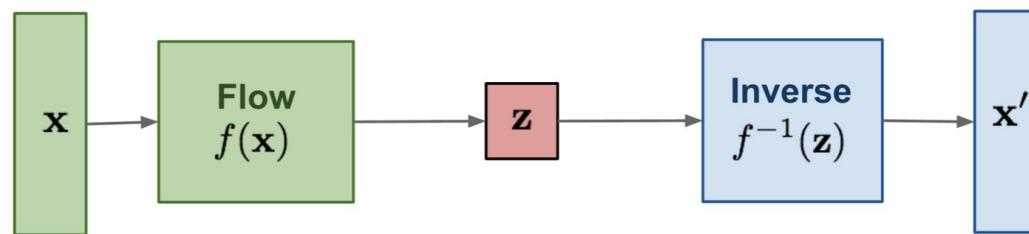
two neural networks playing a zero-sum game

**VAE:** maximize variational lower bound



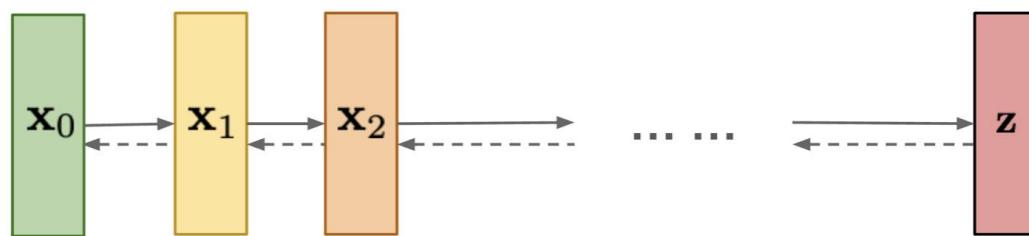
learn variational distribution (not just replicating inputs)

**Flow-based models:** Invertible transform of distributions



more complex distributions by applying change-of-variable technique (need for specialized architecture)

**Diffusion models:** Gradually add Gaussian noise and then reverse



chain of denoising autoencoders

# Conditioning

as discussed so far, generative methods give no control over what kind of data is generated (limited usability)

→ need for conditional approach (e.g., conditioning on describing text, for example by means of CLIP)

example GANs:

transform usual GAN to conditional model by feeding extra information  $y$  (e.g., class labels) as additional input layer into both generator and discriminator

$$L(\mathbf{x}_i) = E_{\mathbf{x} \sim p_r(x)}[\ln D(\mathbf{x}_i|y_i)] + E_{\mathbf{x} \sim p_g(x)}[\ln(1 - D(\mathbf{x}_i|y_i))]$$

G: minimize, D: maximize

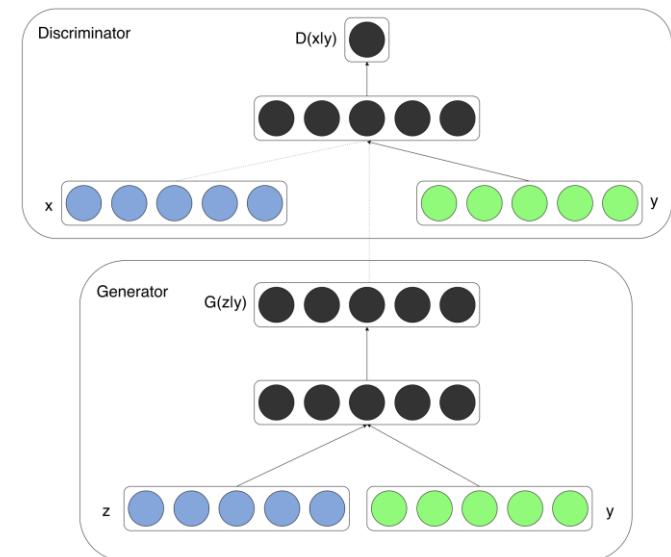
tradeoff between diversity (unconditioned)  
and fidelity (guidance)

similar idea as softmax temperature in auto-regressive LLMs



[source](#)

guided diffusion: “Pembroke Welsh corgi”



[source](#)

# Multi-Modal Generative Models

example: generate images from text descriptions

[DALL-E](#) (blend of WALL-E and Salvador Dalí): decoder-only transformer auto-regressively modeling text and image tokens as single data stream

TEXT PROMPT

an armchair in the shape of an avocado....

AI-GENERATED IMAGES

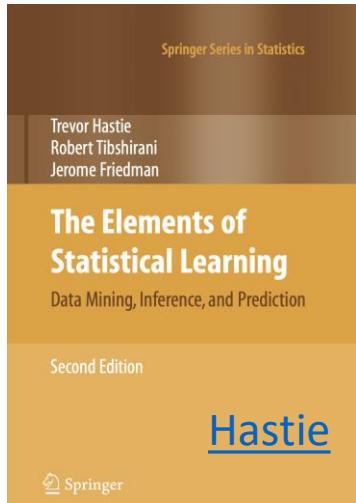


[source](#)

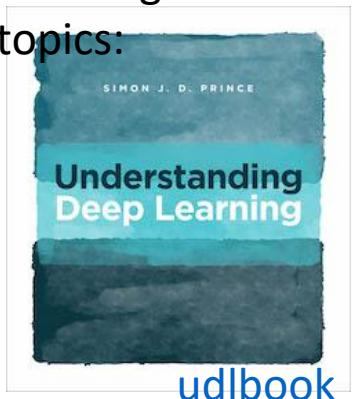
[DALL-E 2](#): image generation (diffusion) conditioned on CLIP embeddings

# Literature

foundations of ML:



covering newer topics:



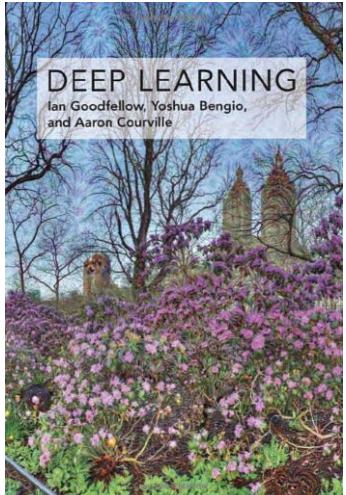
[udlbook](#)

a few seminal papers:

- [back-propagation](#): one of the founding moments of deep learning
- [CNN](#): neural networks work
- [AlexNet](#): deep learning takes over
- [transformer](#): SOTA

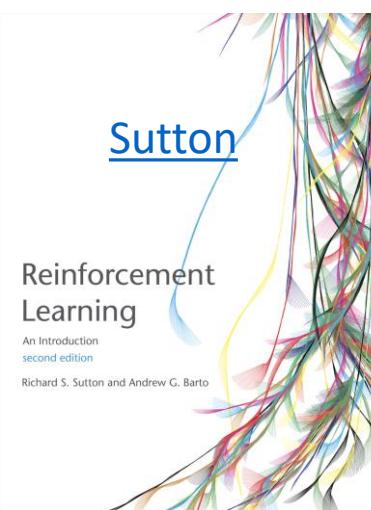
foundations of deep learning:

<https://www.deeplearningbook.org/>



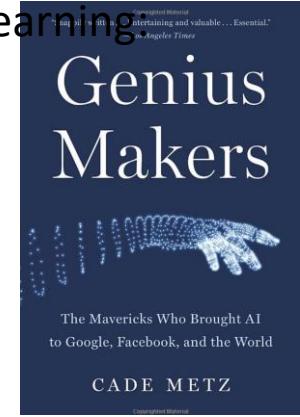
[The Little Book of Deep Learning](#)

overview of reinforcement learning:

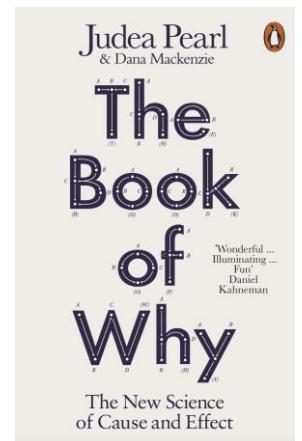


[Sutton](#)

historical overview of deep learning:



gentle but genuine introduction to causality:



# Some Philosophical Thoughts

computational theory of mind: mind from matter

just scaling up current methods (e.g., LLMs) enough to achieve general intelligence? or additional methods needed?

agency via goal-based approaches? (is reward enough?)

emergent capabilities of complex systems difficult to foresee: emotions or consciousness occurring as emergent capabilities?