CS 4602

Introduction to Machine Learning

Advanced Deep Networks and Learning Strategies

Instructor: Po-Chih Kuo

Roadmap

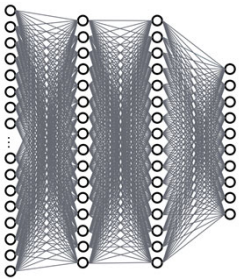
- Introduction and Basic Concepts
- Regression
- Bayesian Classifiers
- Decision Trees
- KNN
- Linear Classifier
- Neural Networks
- Deep learning
- Convolutional Neural Networks
- RNN/Transformer
- Reinforcement Learning
- Model Selection and Evaluation
- Clustering
- Data Exploration & Dimensionality reduction

Learning, learning, learning

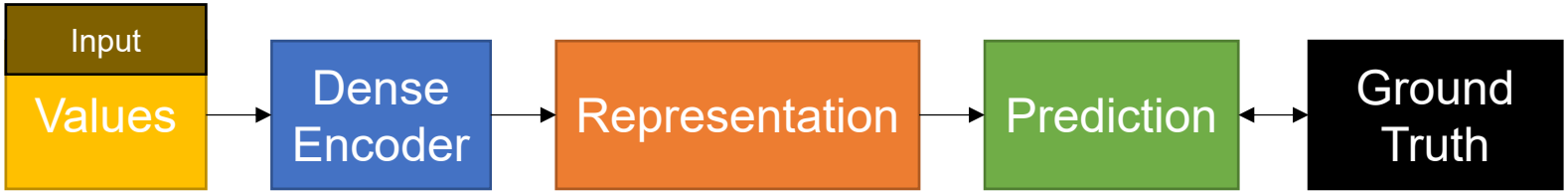
- Supervised learning
  - **FFNNs**
  - **CNNs**
  - **RNNs**
  - **Encoder Decoder**
- Unsupervised learning
  - **Autoencoder**
  - **GAN**
  - **Diffusion model**

  } **Generative AI (GAI)**
- Self-Supervised learning
  - **Large language model**
- Reinforcement learning
- Transfer learning
- Federated learning

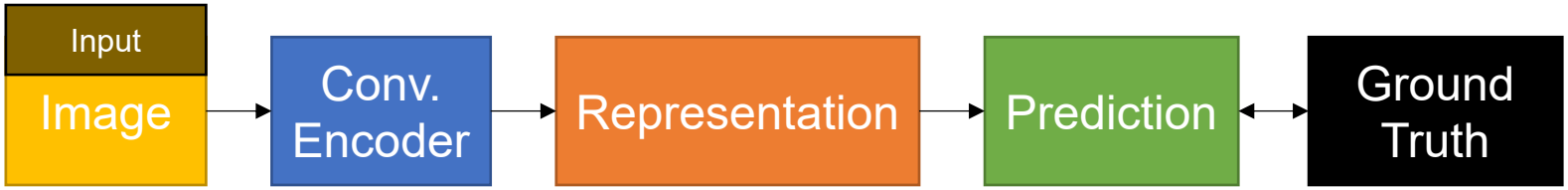
Supervised learning



- **Feed Forward Neural Networks (FFNNs)** - classification and regression based on features.

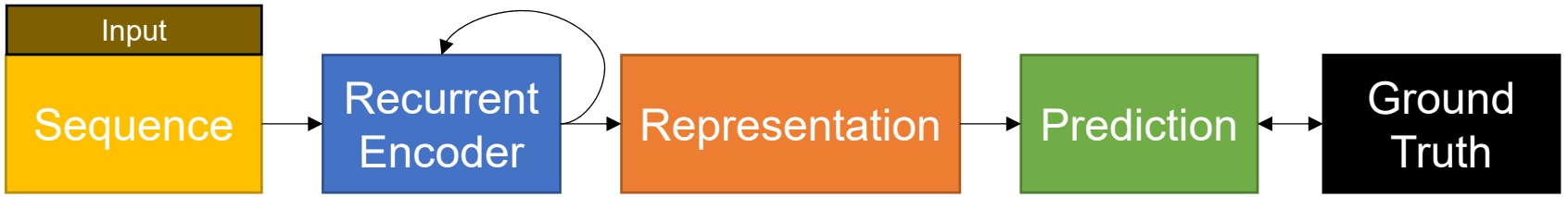


- **Convolutional Neural Networks (CNNs)** - image classification, object detection, video action recognition



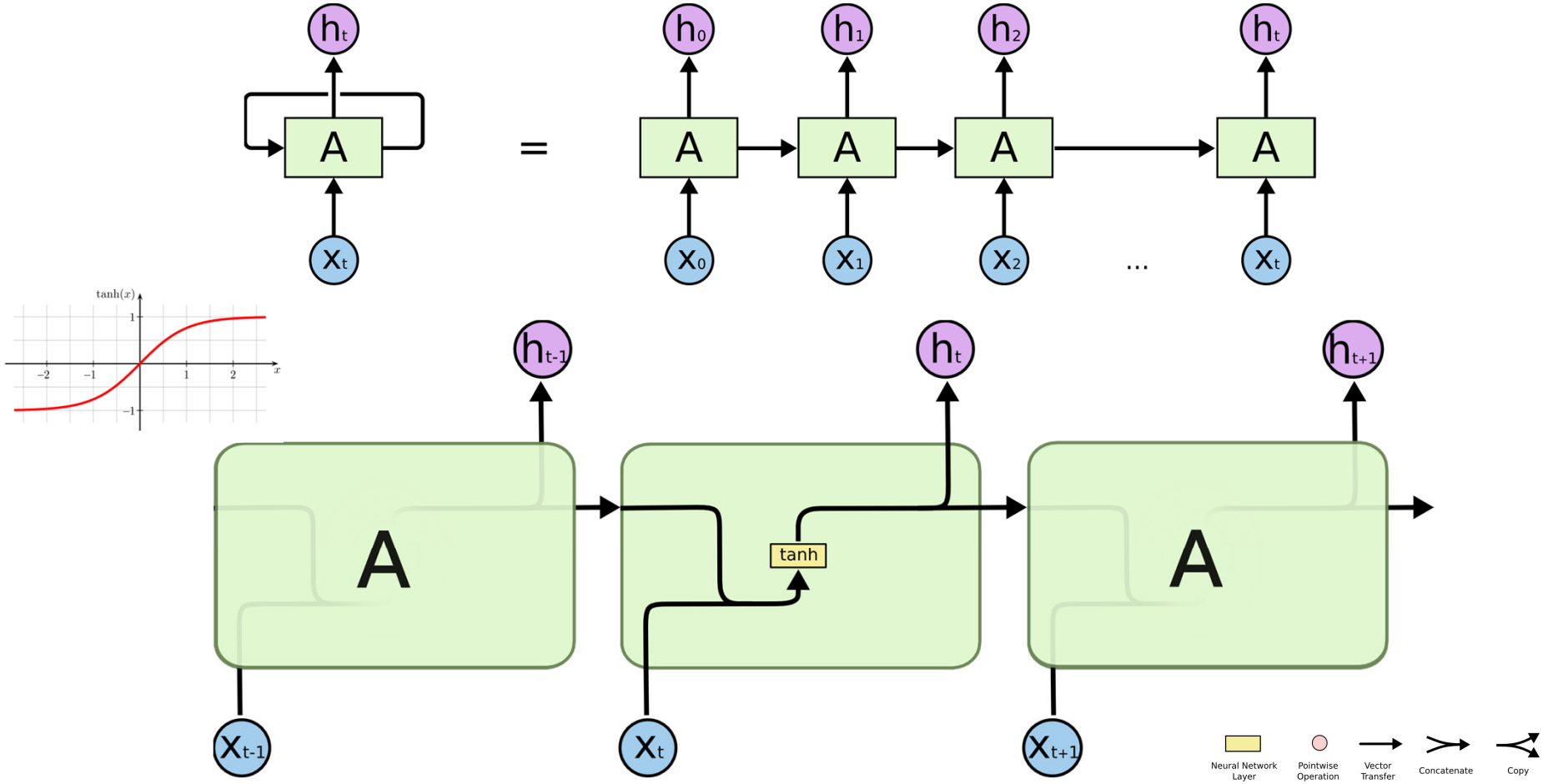
Supervised learning (cont.)

- **Recurrent Neural Networks (RNNs)** - language modeling, speech recognition/generation



- **Encoder Decoder Architectures** - semantic segmentation, machine translation

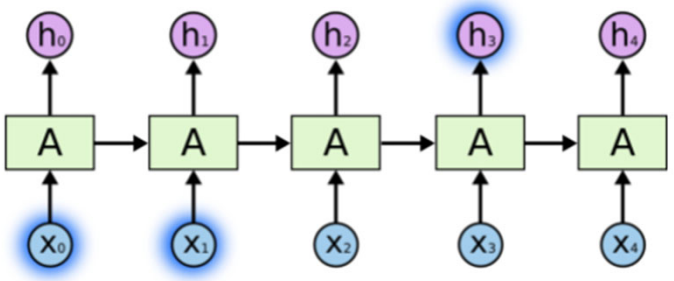
Recurrent Neural Network (RNN)



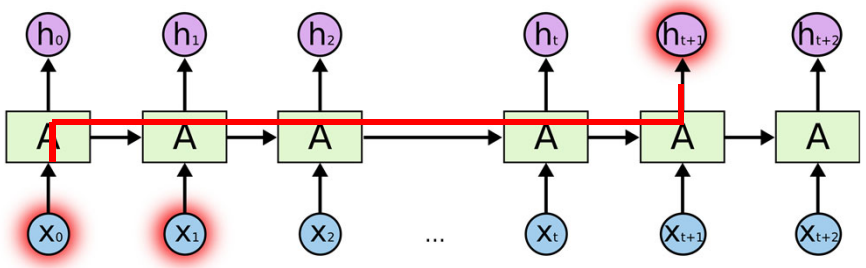
https://colah.github.io/posts/2015-08-Understanding-LSTMs/

Long-Short Term Dependencies

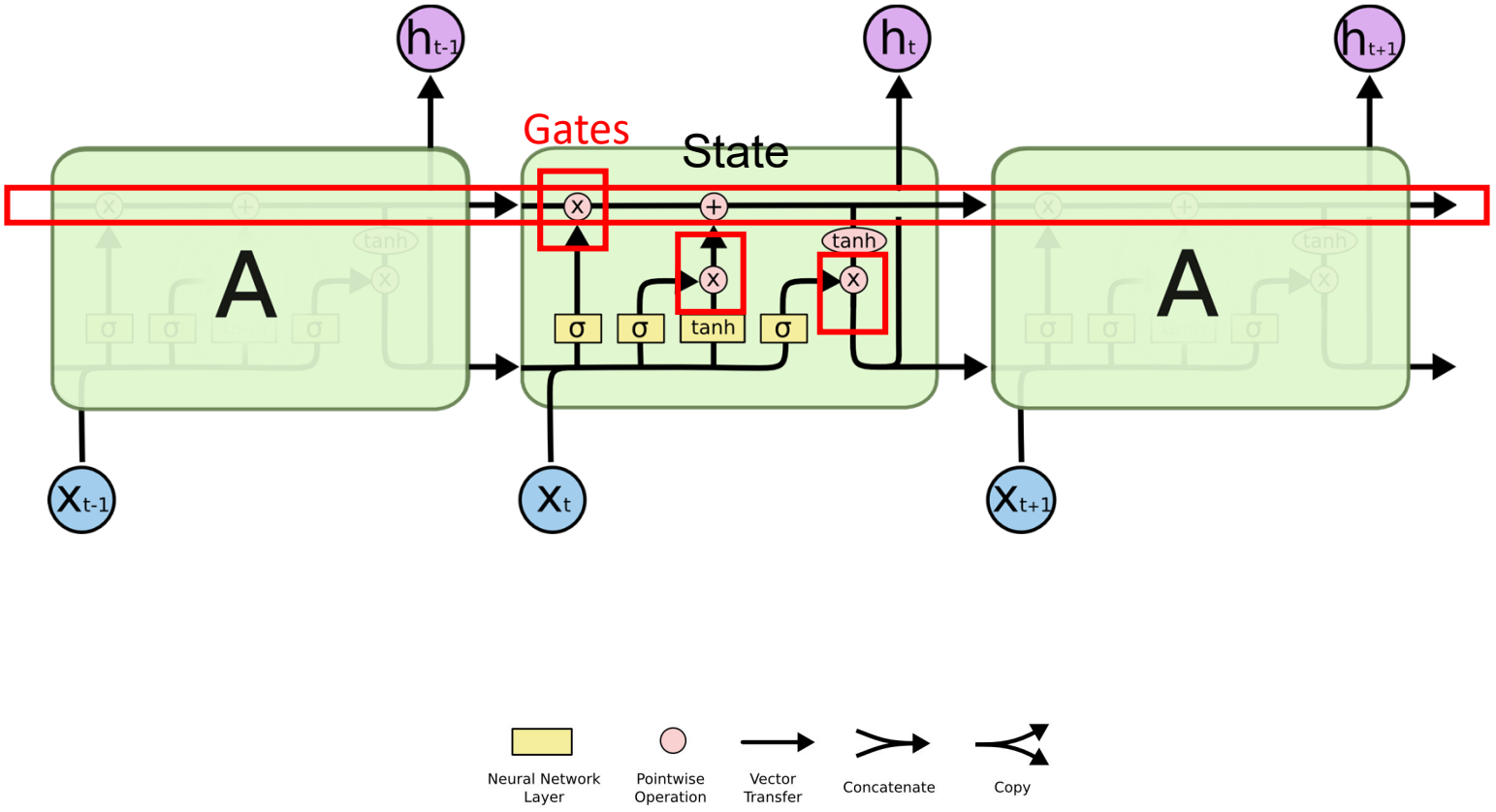
- Short-Term

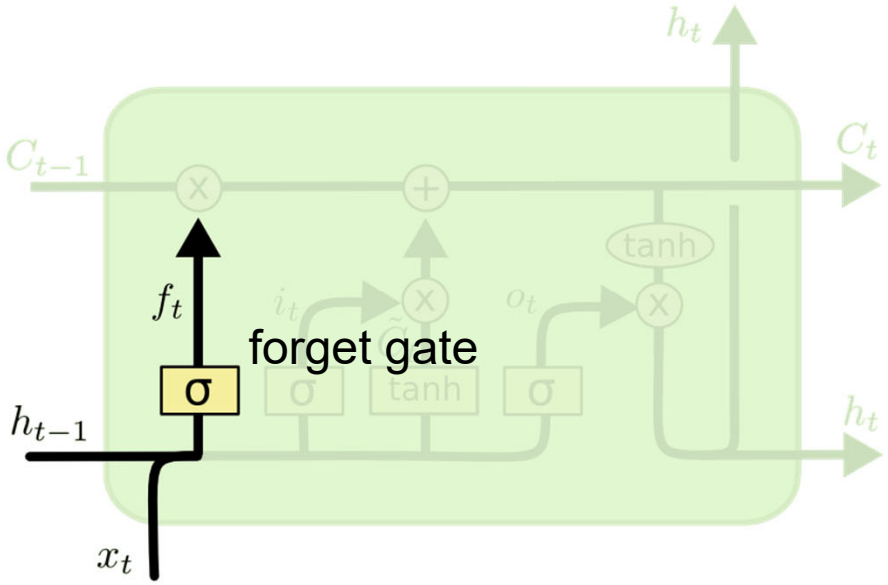


- Long-Term



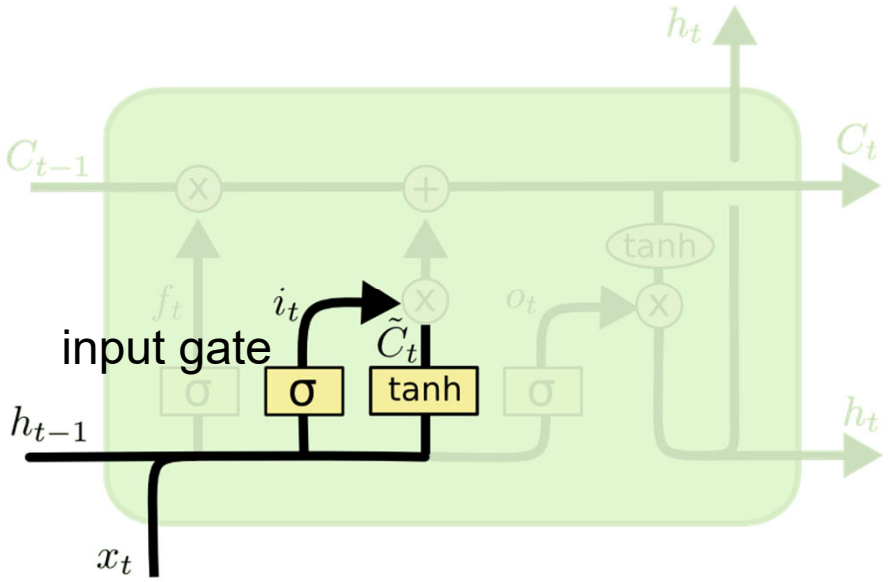
Long-Short Term Memory (LSTM)





$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] \; + \; b_f\right)$$

forget gate:
1: keep it
0: forget it

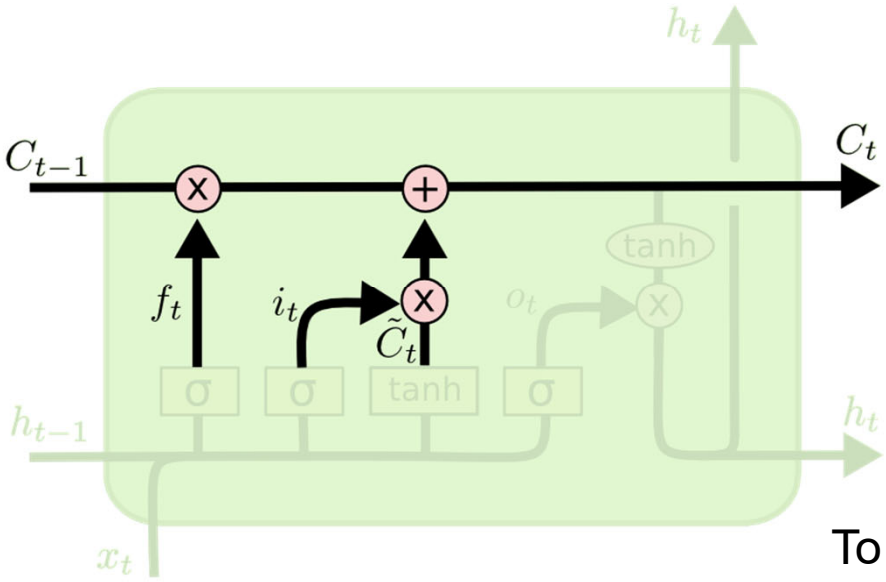


$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] \; + \; b_i\right)$$

$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] \; + \; b_C)$$

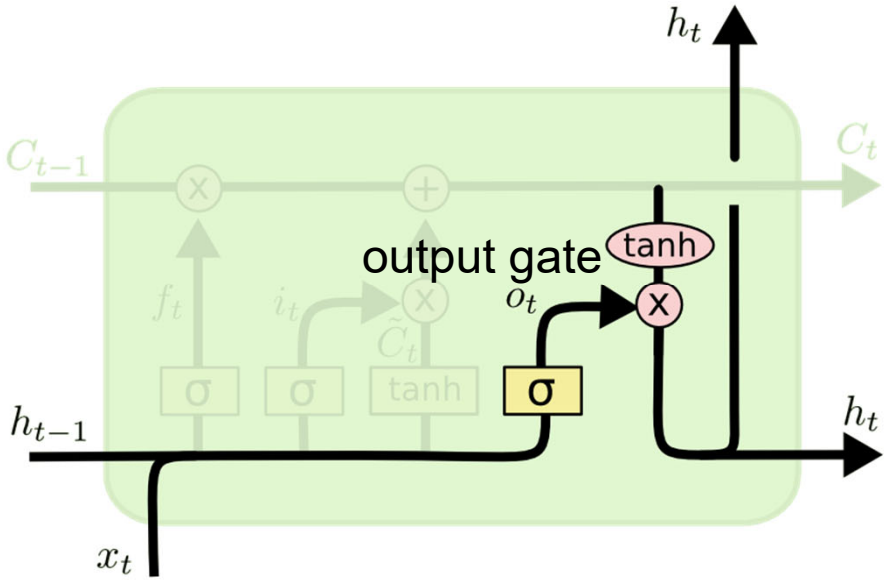
input gate: To decide what new information to store in the cell state.

$\widetilde{C_t}$: new candidate values that could be added to the state.



$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

To update the old cell state, C_{t-1}, into the new cell state C_t

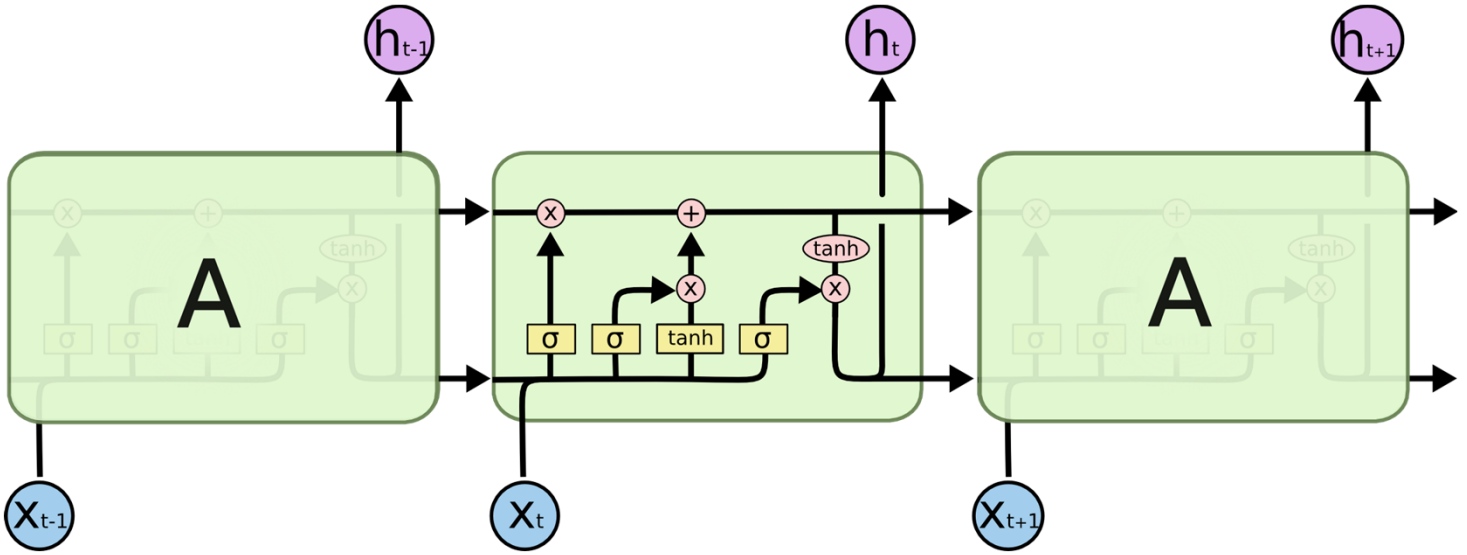


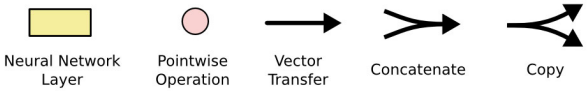
$$o_t = \sigma\left(W_o\left[h_{t-1}, x_t\right] + b_o\right)$$

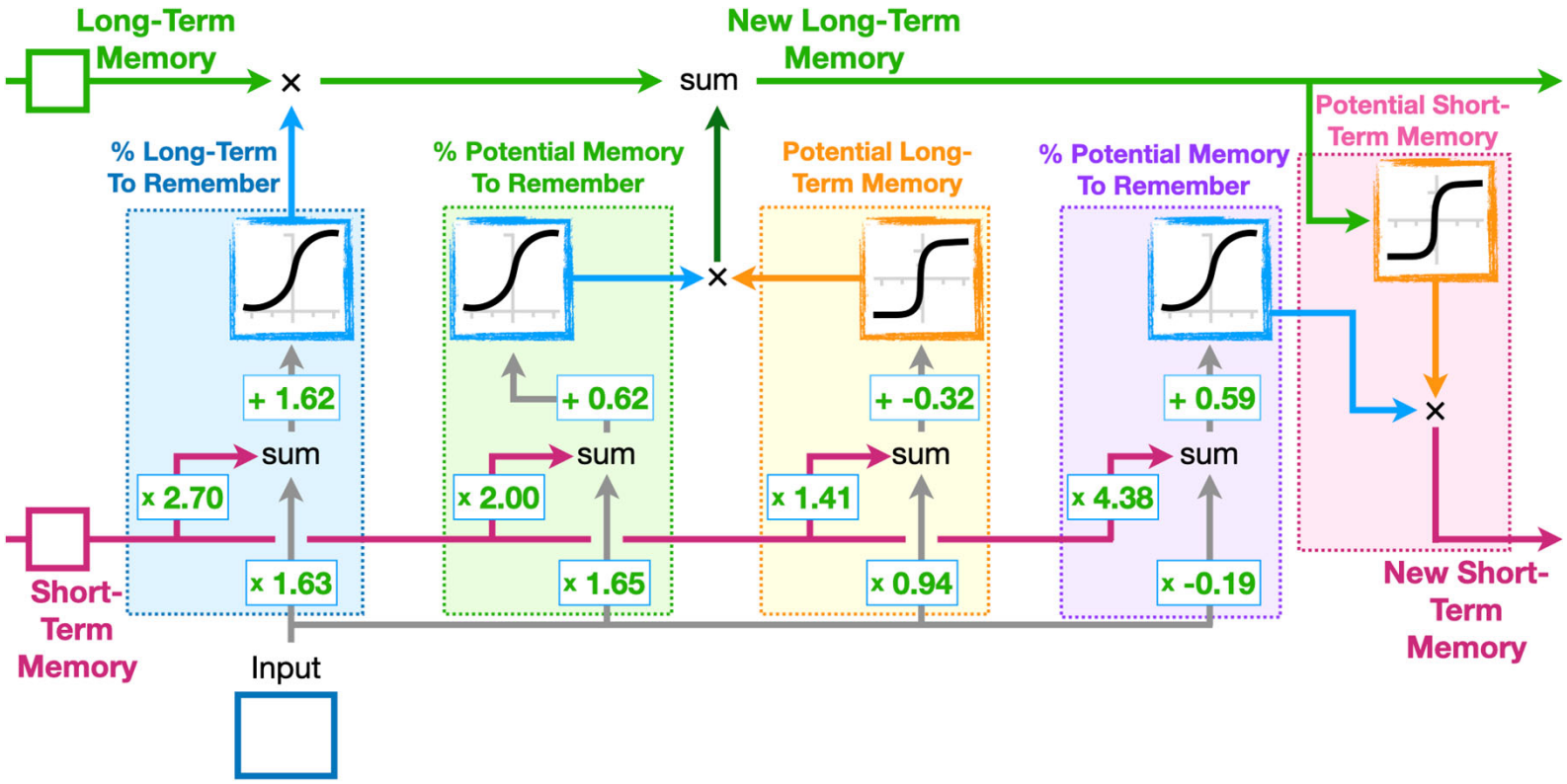
$$h_t = o_t * \tanh\left(C_t\right)$$

To decide the output

LSTM

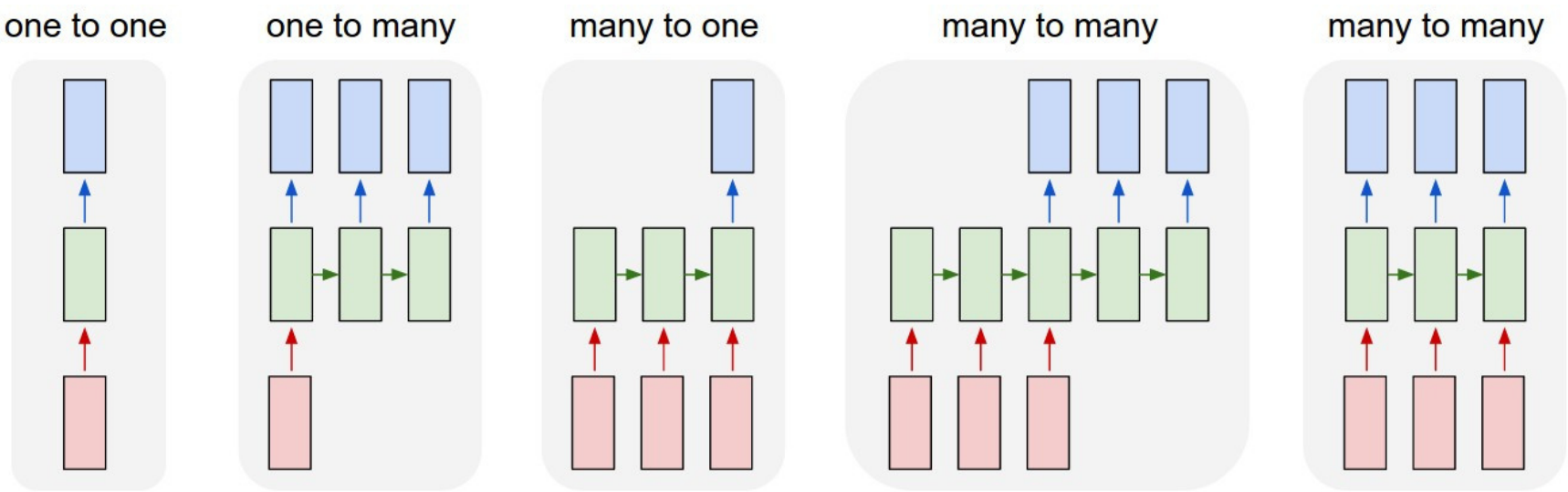

h_{t-1}
h_t
h_{t+1}
A
A
tanh
σ
σ
tanh
σ
X_{t-1}
X_t
X_{t+1}


Neural Network Layer
Pointwise Operation
Vector Transfer
Concatenate
Copy



Ref: https://lightning.ai/lightning-ai/studios/statquest-long-short-term-memory-lstm-with-pytorch-lightning

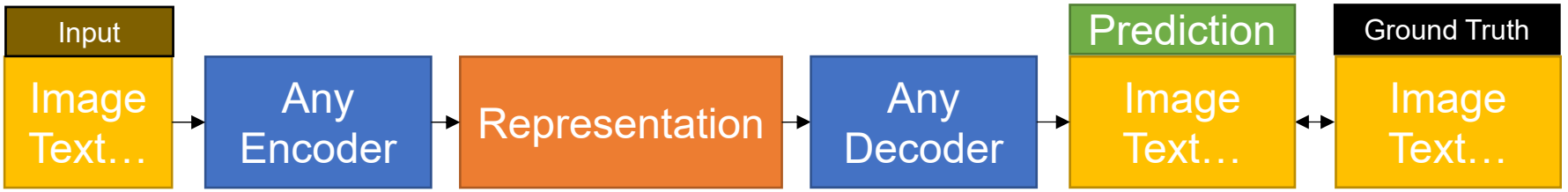
Multi-layer LSTM



Supervised learning (cont.)

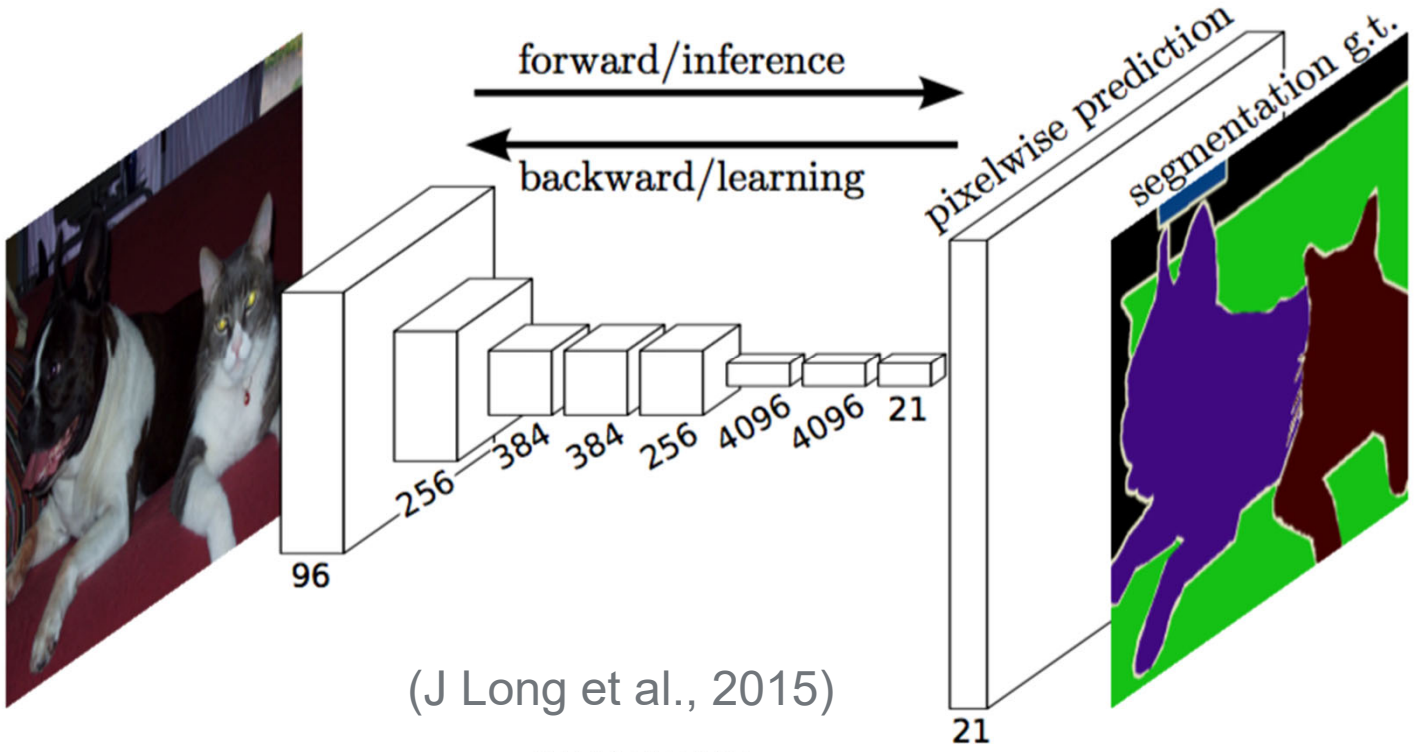
- **Recurrent Neural Networks (RNNs)** - language modeling, speech recognition/generation

- **Encoder Decoder Architectures** - semantic segmentation, machine translation



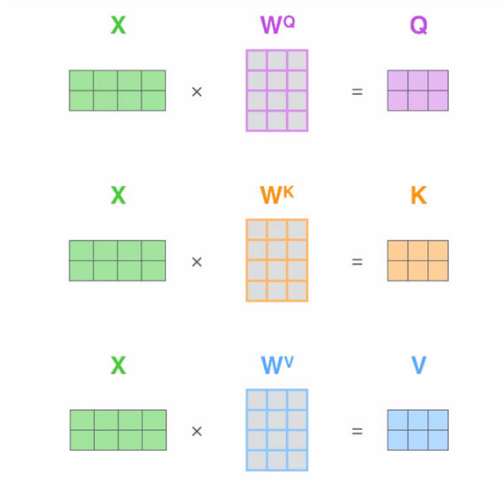
Encoder Decoder

- Fully Convolutional Networks for Semantic Segmentation



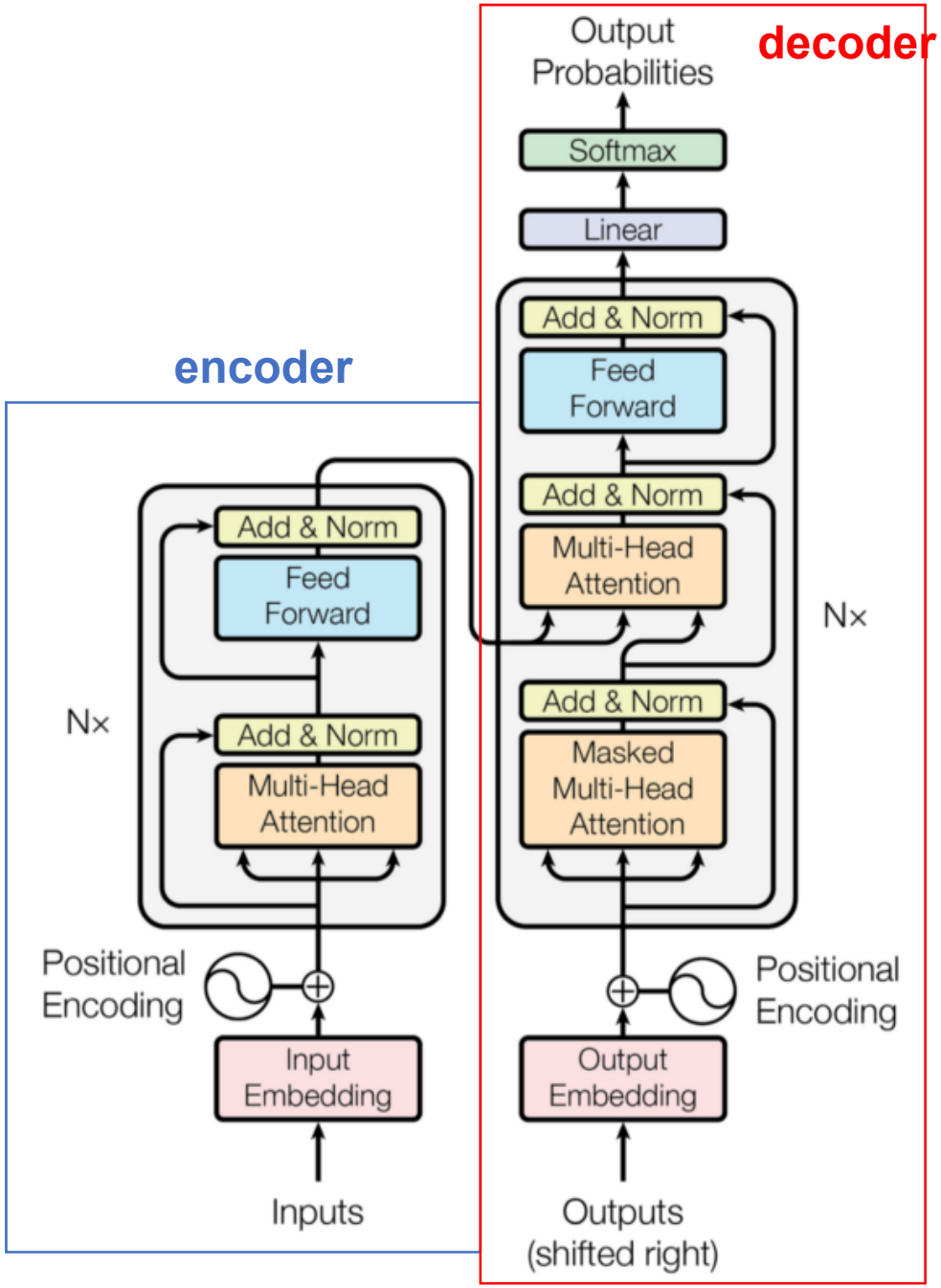
(J Long et al., 2015)

Transformer



Query Key Value

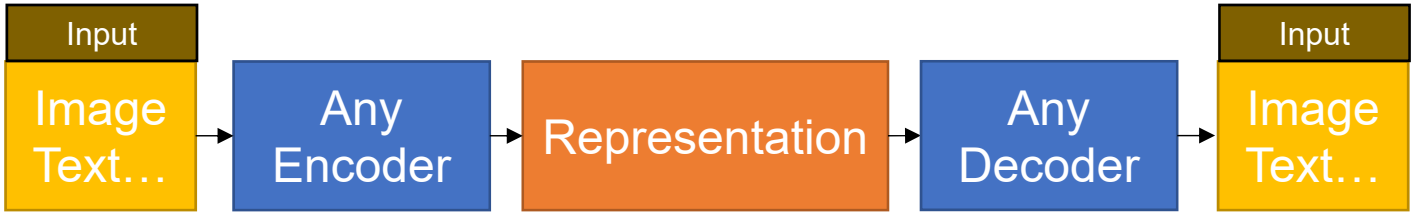
"Attention Is All You Need"



- Further reading: https://theaisummer.com/transformer/

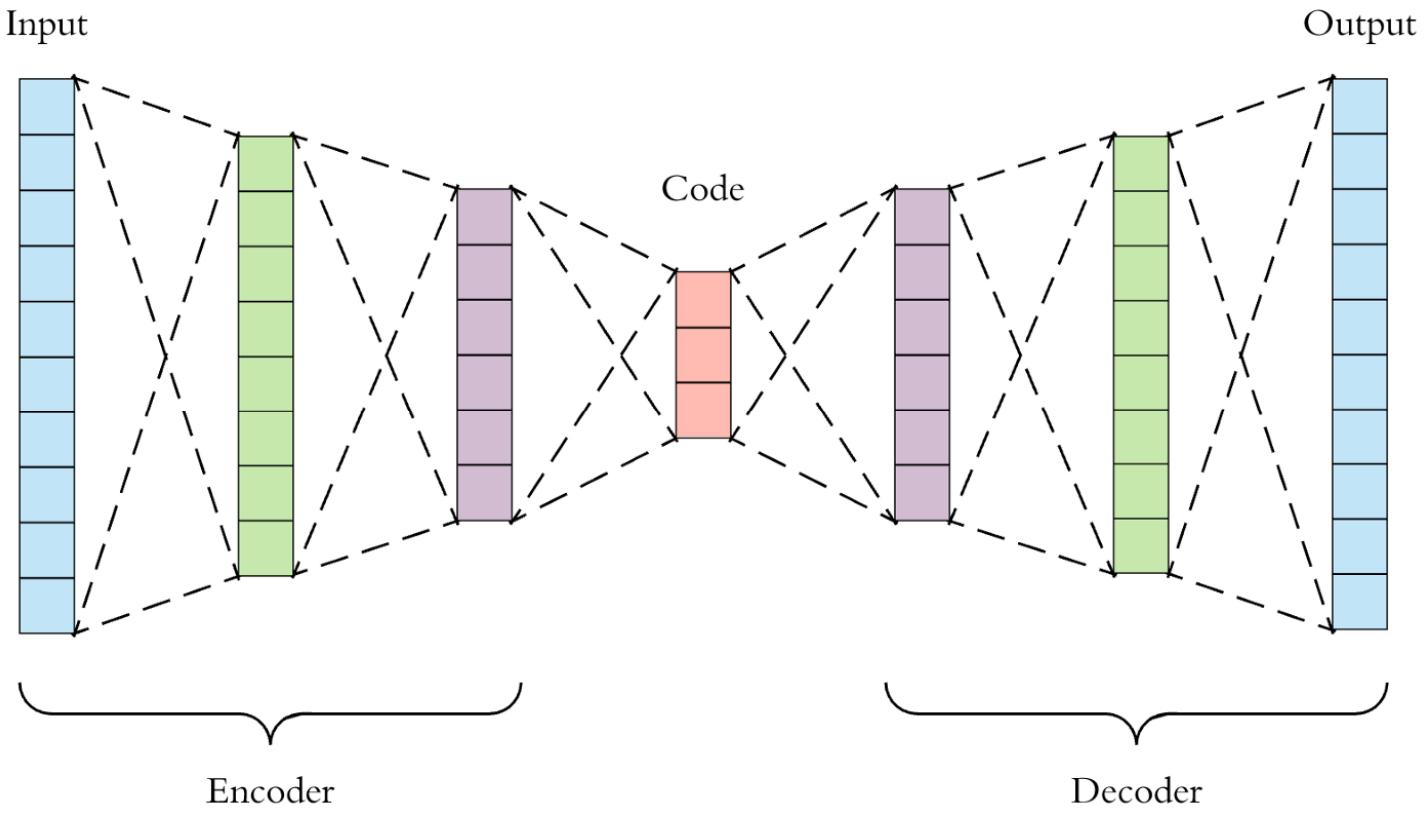
Unsupervised learning

- **Autoencoder** - unsupervised embeddings, denoising

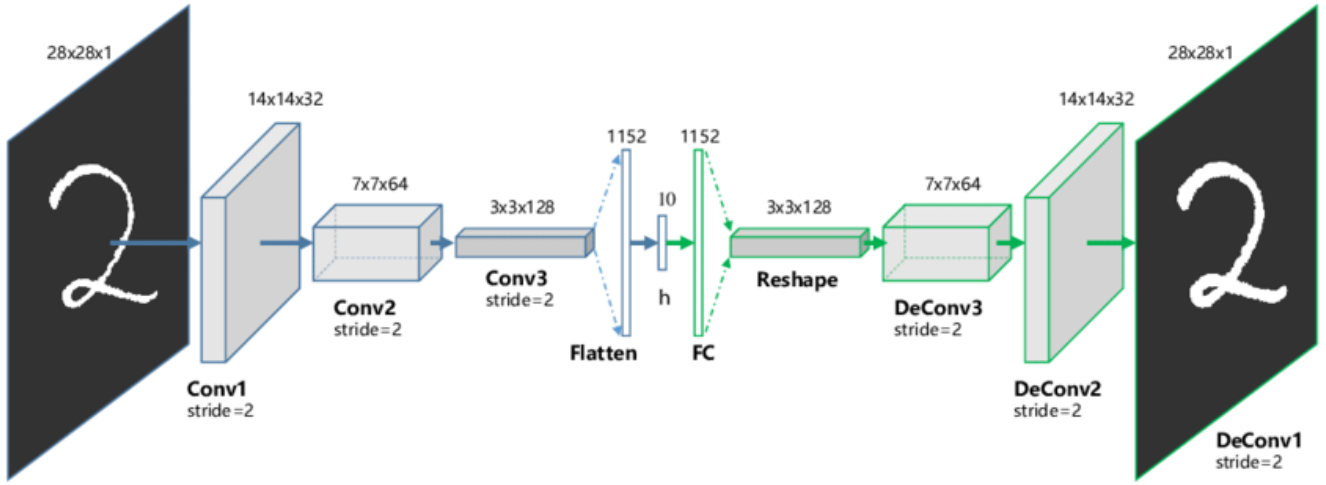


- **Generative Adversarial Networks (GANs)** - generation of realistic images

AutoEncoder

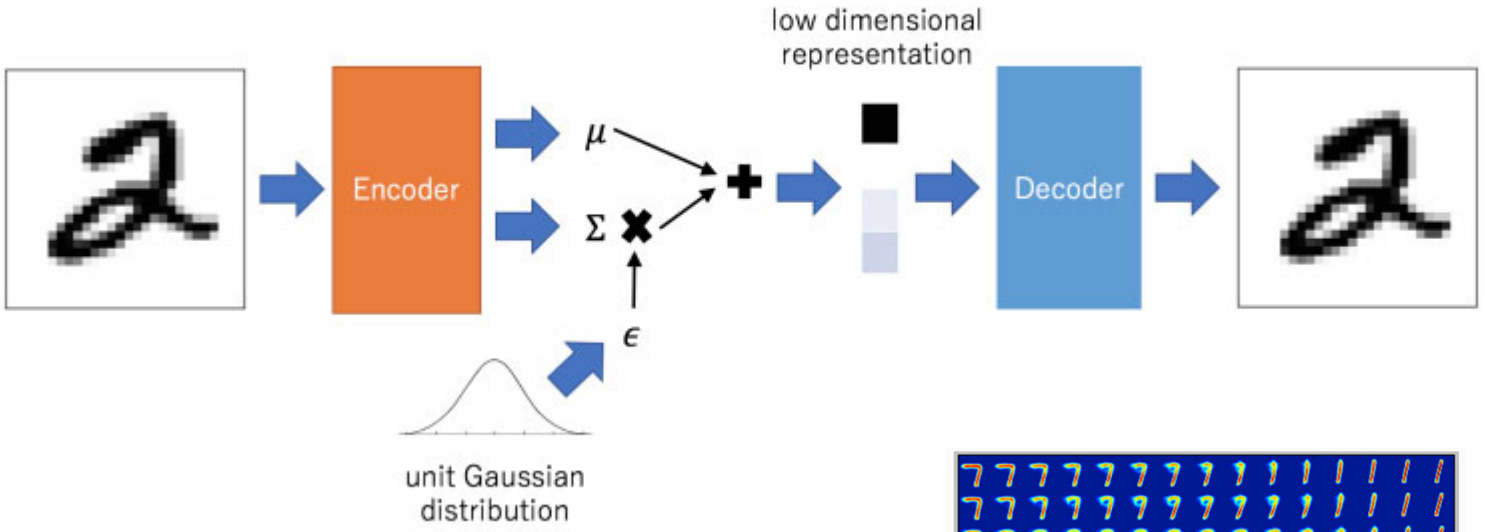


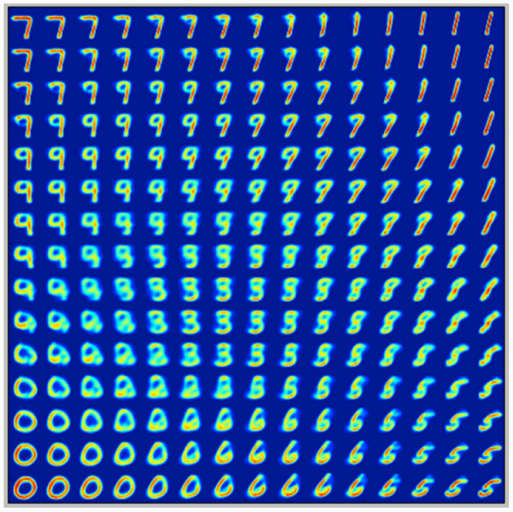
Convolutional AutoEncoder



(Guo et al., 2017)

Variational AutoEncoder (VAE)

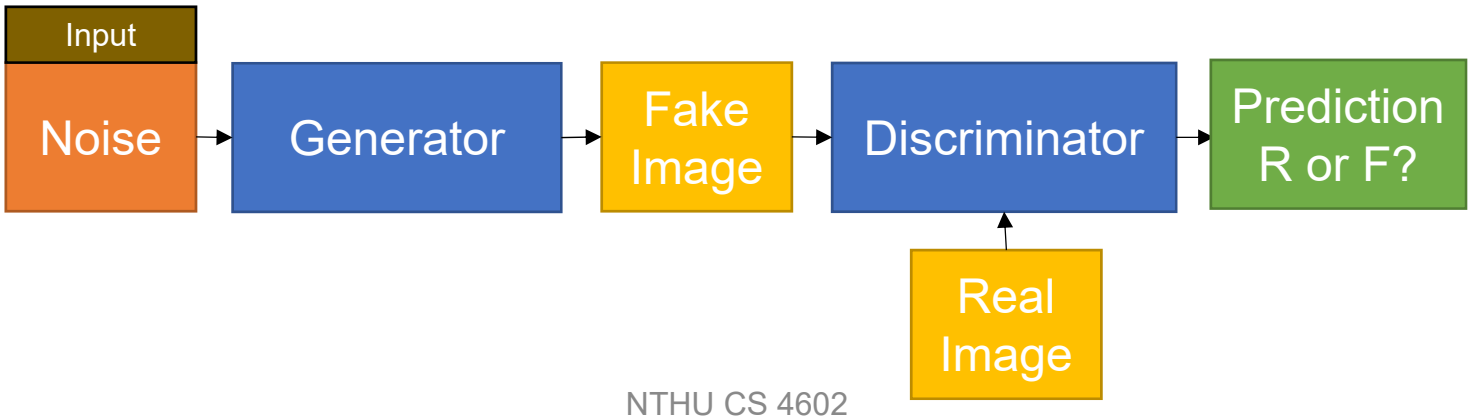




Unsupervised learning

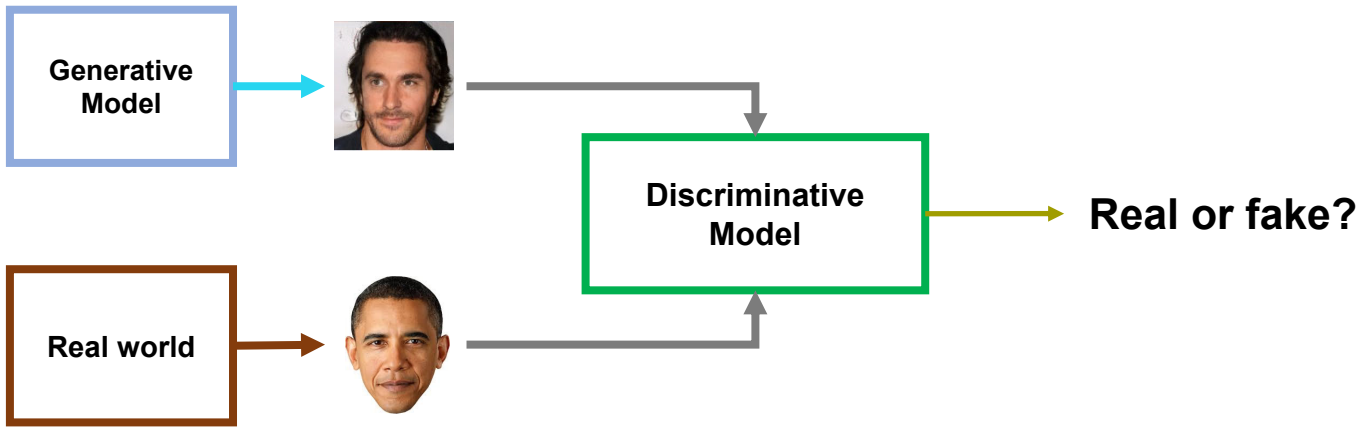
- **Autoencoder** - unsupervised embeddings, denoising

- **Generative Adversarial Networks (GANs)** - generation of realistic images

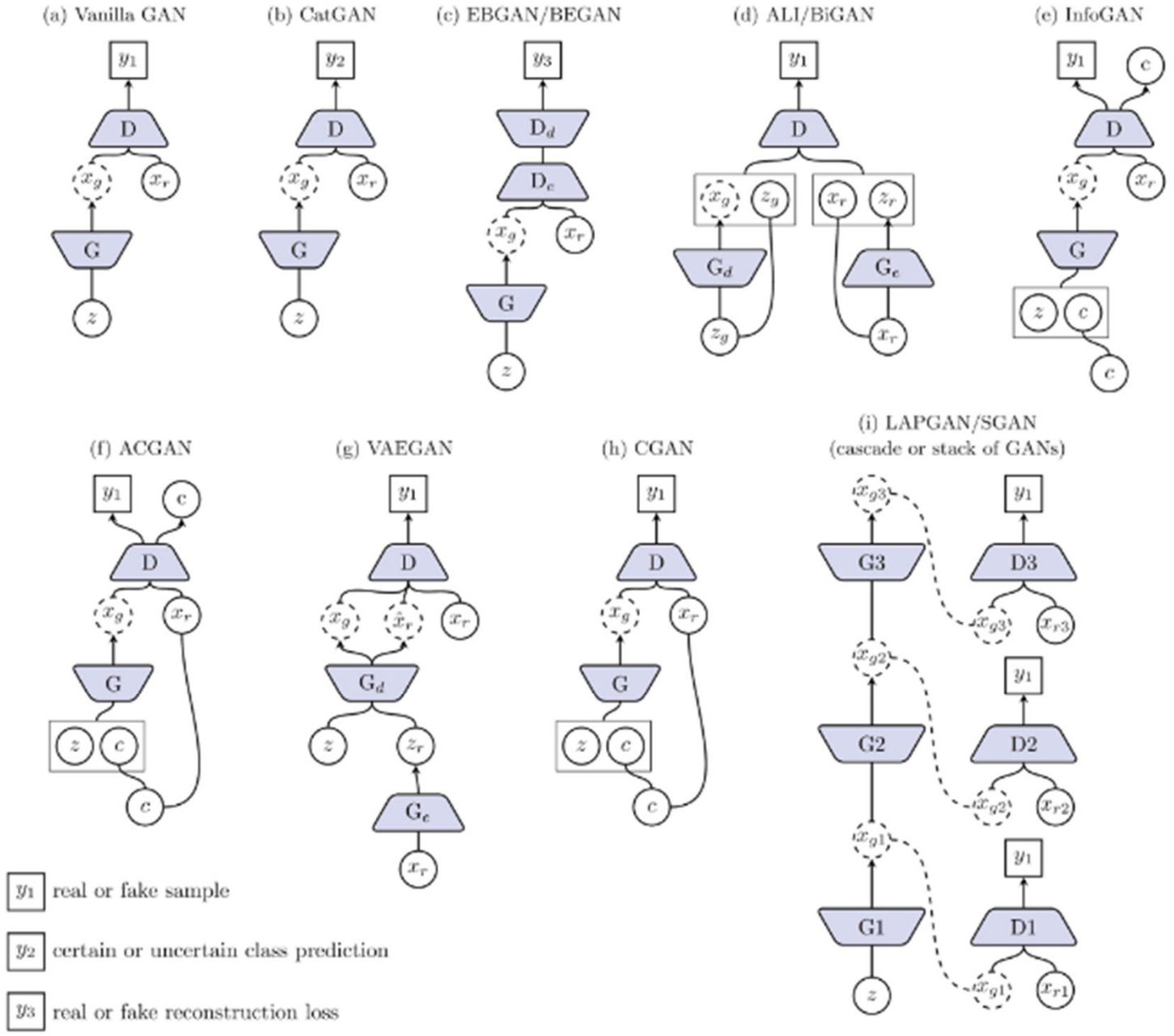


Generative Adversarial Networks (GAN)

- **GAN is the most interesting idea in the last ten years in machine learning.—Yann LeCun, Director, Facebook AI**

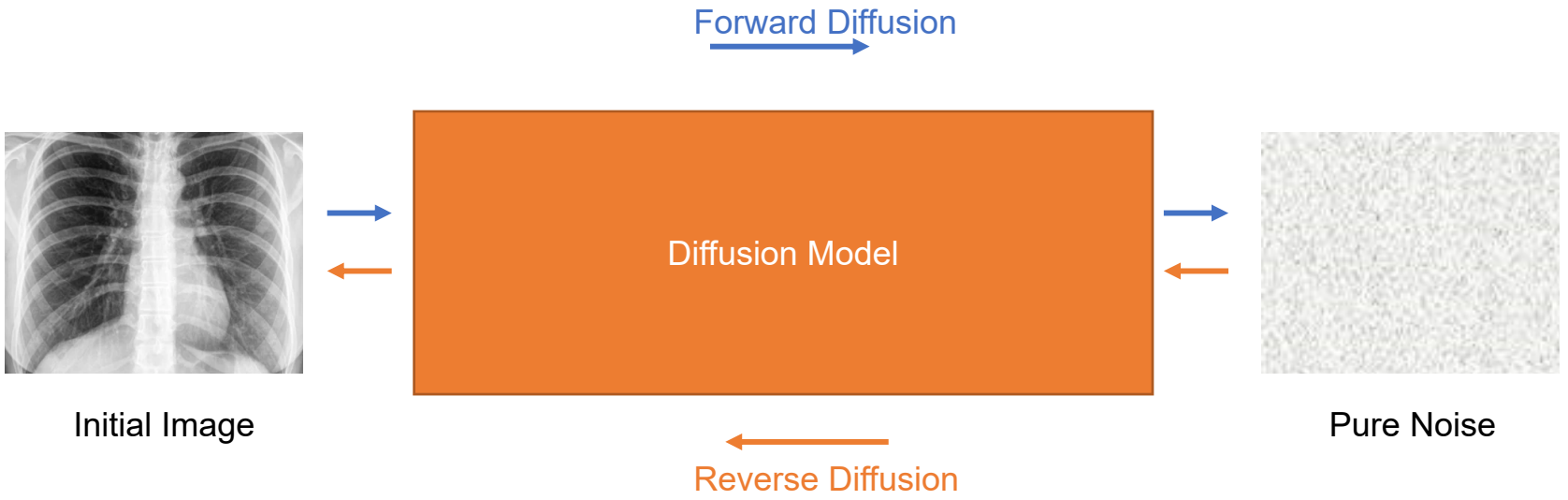


(Karras et al., 2018)



"Generative adversarial network in medical imaging: A review", 2019

Diffusion Models

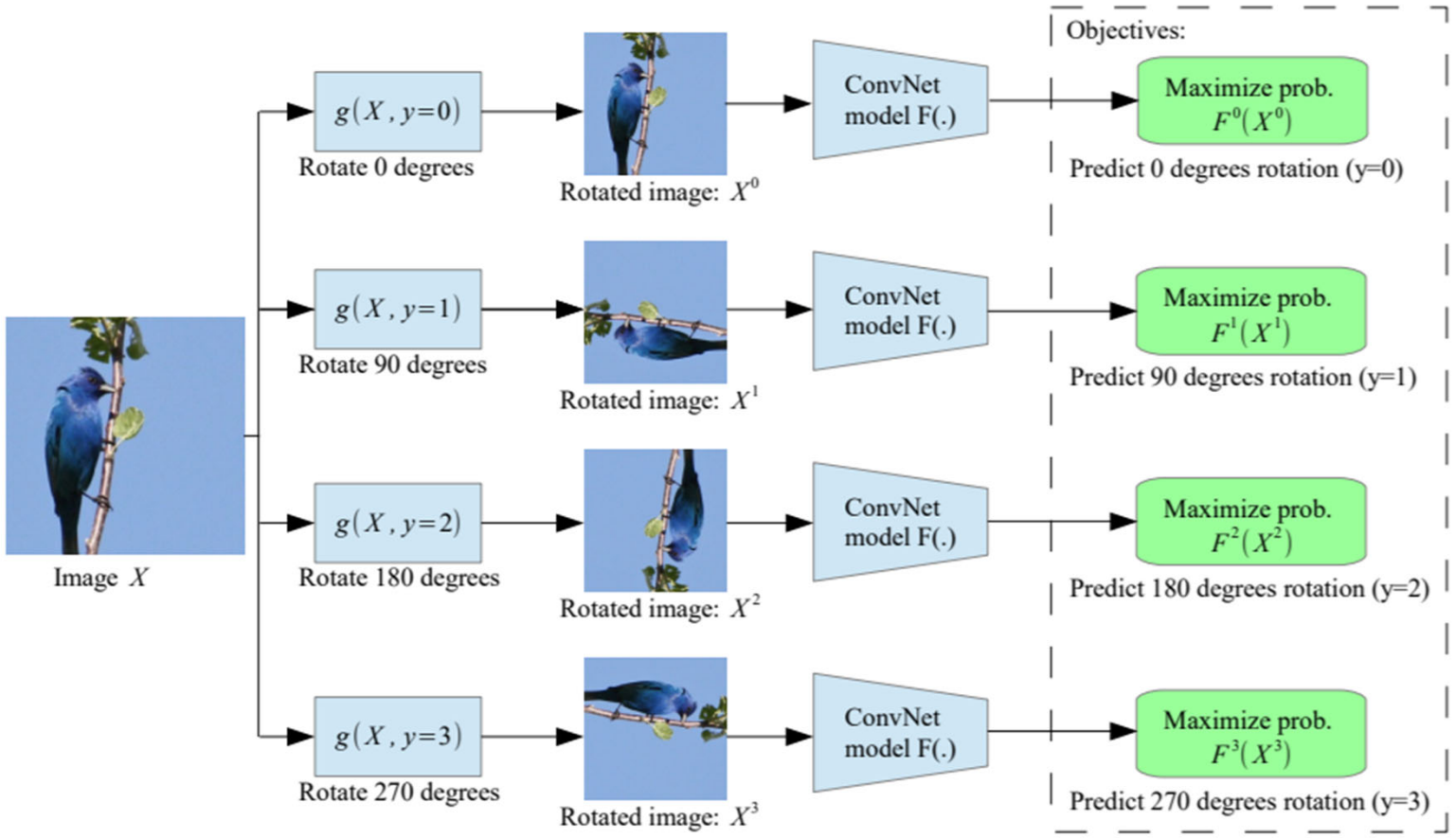


What makes a good generative AI

Self-Supervised Learning (SSL)

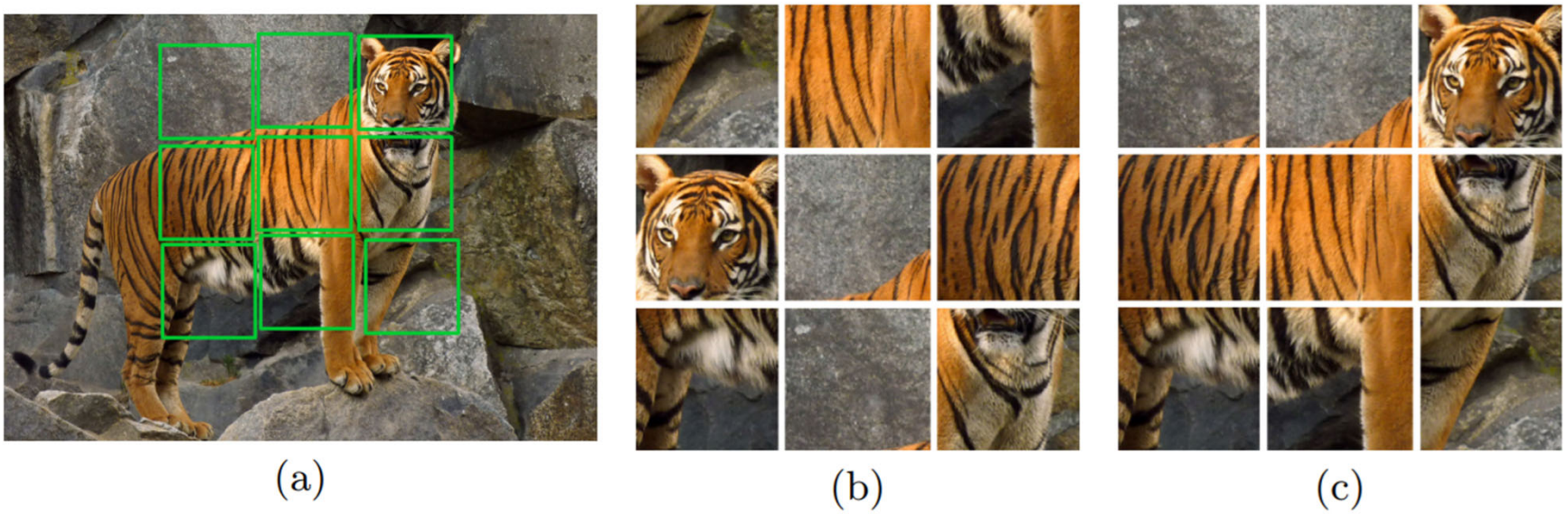
- A representation learning method where a supervised task is created out of the unlabelled data.
- Self-supervised learning is used to reduce the data labelling cost and leverage the unlabelled data pool.
- Some of the popular methods:
  - Rotation
  - Jigsaw Puzzle

Rotation



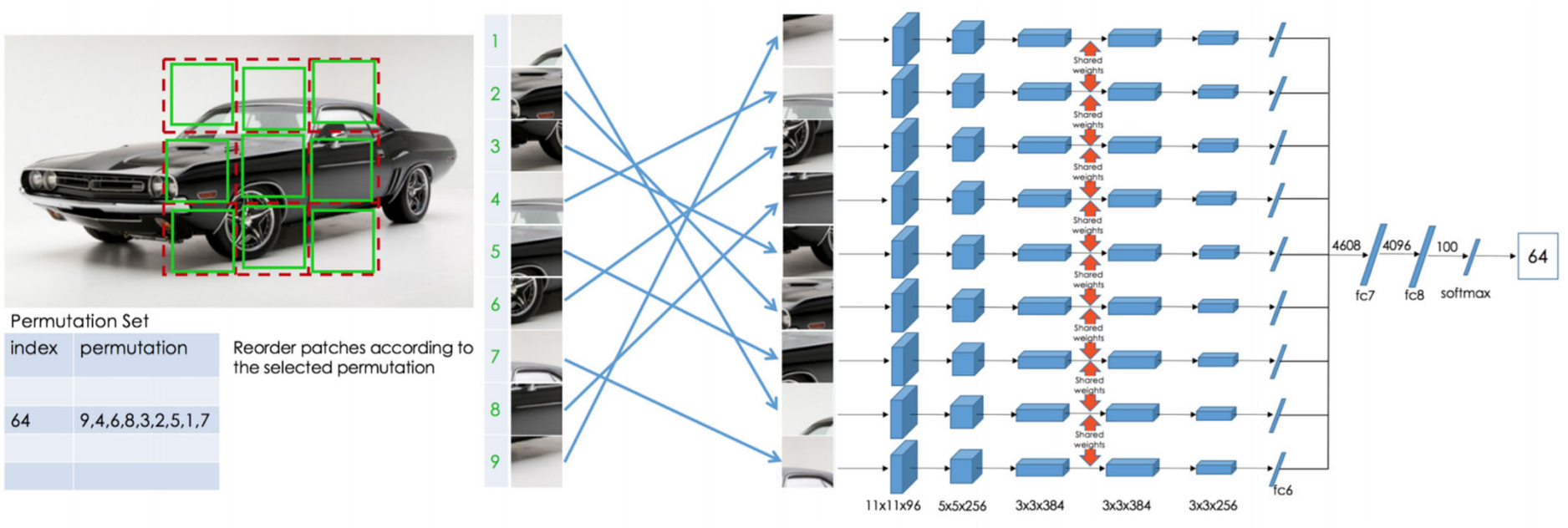
Unsupervised Representation Learning by Predicting Image Rotations https://arxiv.org/pdf/1803.07728.pdf

Jigsaw Puzzle



Unsupervised Learning of Visual Representations by Solving Jigsaw Puzzles https://arxiv.org/abs/1603.09246

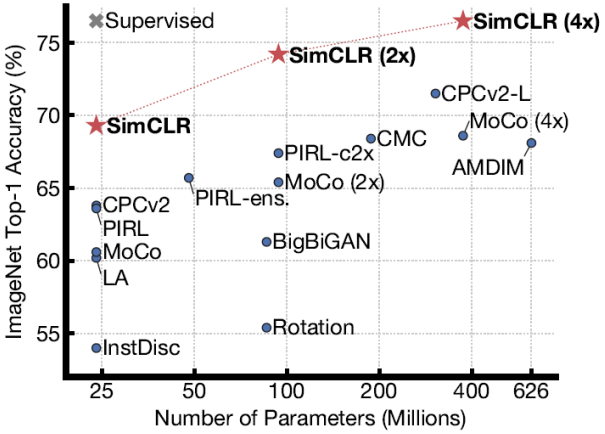
Learning the right positions

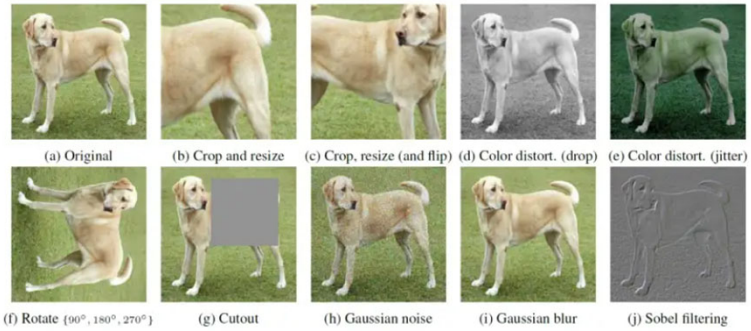


Given 9 tiles, there are $9! = 362{,}880$ possible permutations.

SSL + Contrastive Learning

- SimCLR: A Simple Framework for Contrastive Learning of Visual Representations





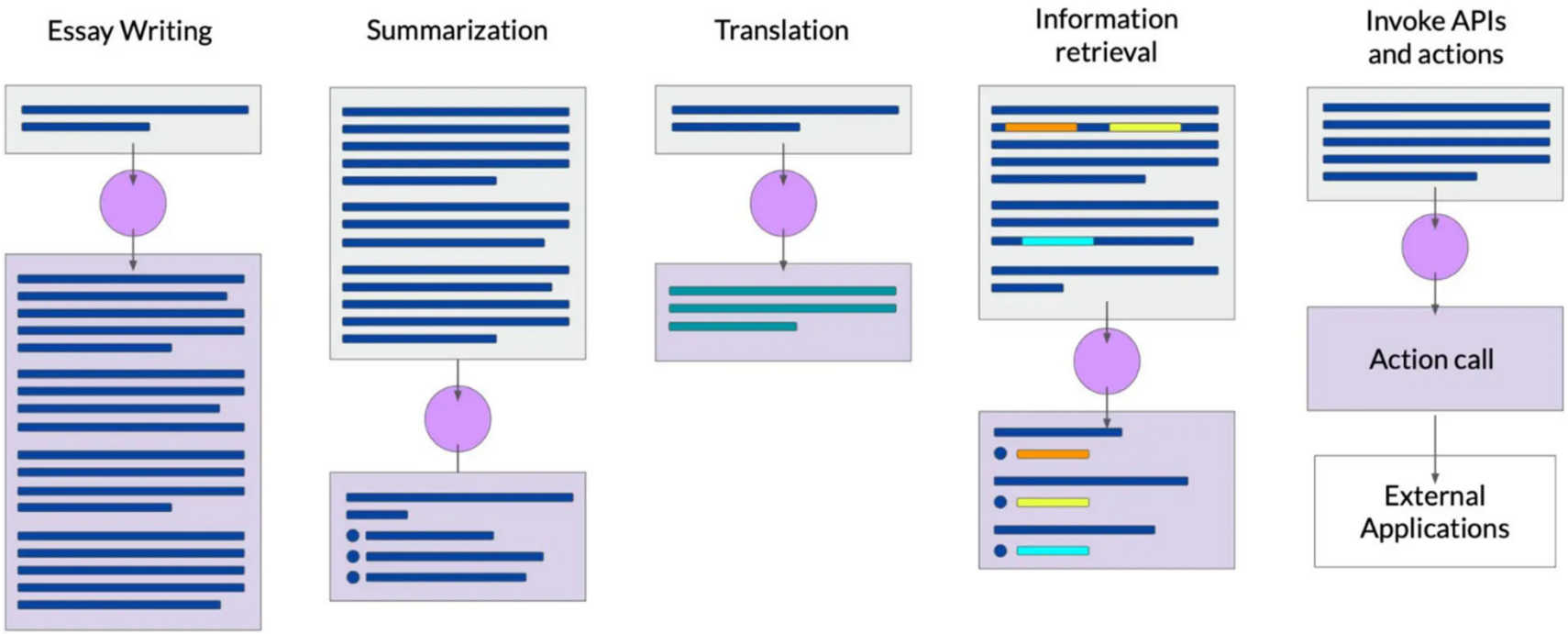
GIF for SimCLR (from Google AI Blog)

What about LLM (Large Language Model)?

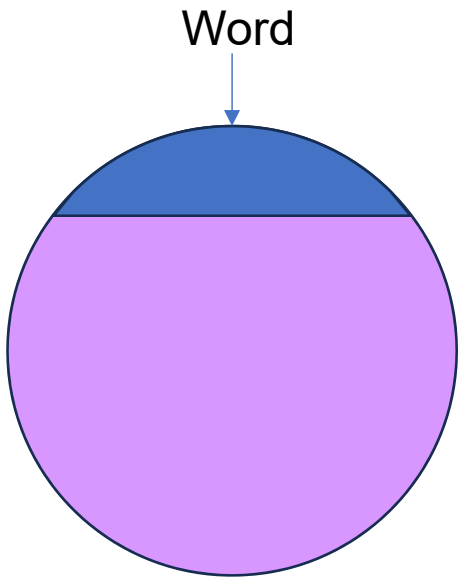
NLP (Natural Language Processing) + Transformer + Self-supervised Learning

Language Model	Description	Is it "Large"?	Emergence
Bag-of-Words Model	Represents text as a set of unordered words, without considering sequence or context.	No	1950s-1960s
N-gram Model	Considers groups of N consecutive words to capture sequence.	No	1950s-1960s
Hidden Markov Models (HMMs)	Represents language as a sequence of hidden states and observable outputs.	No	1980s-1990s
Recurrent Neural Networks (RNNs)	Processes sequential data by maintaining an internal state, capturing context of previous inputs.	No	1990s-2010s
Long Short-Term Memory (LSTM) Networks	Extension of RNNs that captures longer-term dependencies in sequences.	No	2010s
Transformers	Neural network architecture that processes sequences of variable length using a self-attention mechanism.	Yes	2017-Present

What problem to solve



Source: DeepLearning.AI


Word

Word Embeddings

- Represent words with vectors
- Words with similar meaning tend to occur in similar contexts:
  - The cat meowed at me for food.
  - The kitten meowed at me for treats.
- If we use vectors to encode tokens we can attempt to store this meaning.
  - Vectors are the basic inputs for many ML methods.
  - Tokens that are similar in meaning can be positioned as neighbors in the vector space using the right mapping functions.

How to convert words into vectors?

- Initial idea: Let's count the frequency of the words!

Document	the	cat	sat	in	hat	with
the cat sat	1	1	1	0	0	0
the cat sat in the hat	2	1	1	1	1	0
the cat with the hat	2	1	0	0	1	1

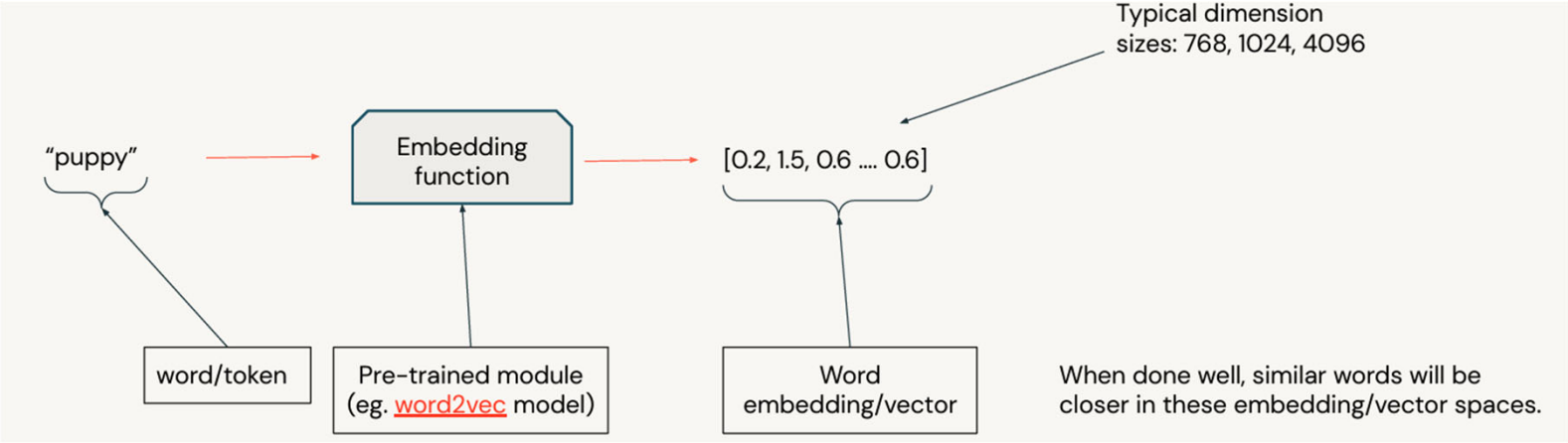
We now have length-6 vectors for each document:

- 'the cat sat' → [1 1 1 0 0 0]
- 'the cat sat in the hat' → [2 1 1 1 1 0]
- 'the cat with the hat' → [2 1 0 0 1 1]

SPARSITY!

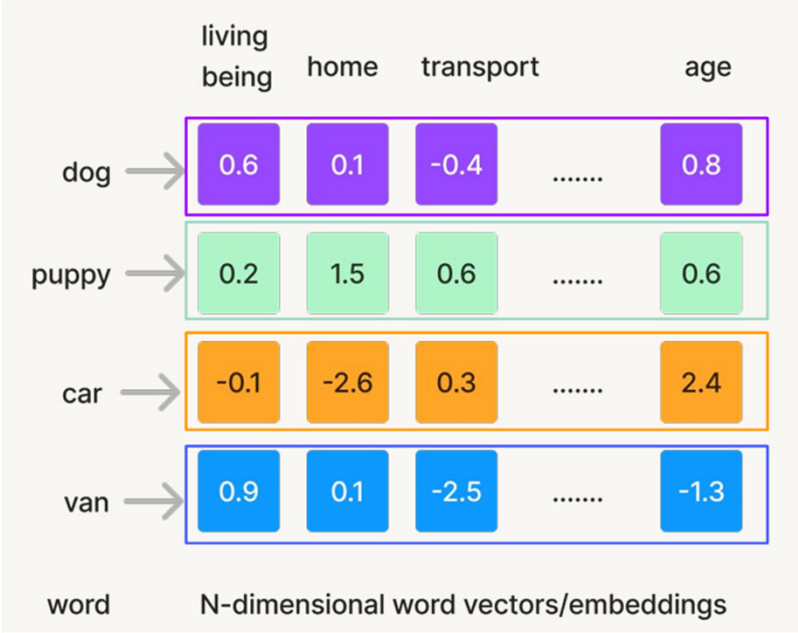
Creating dense vector representation

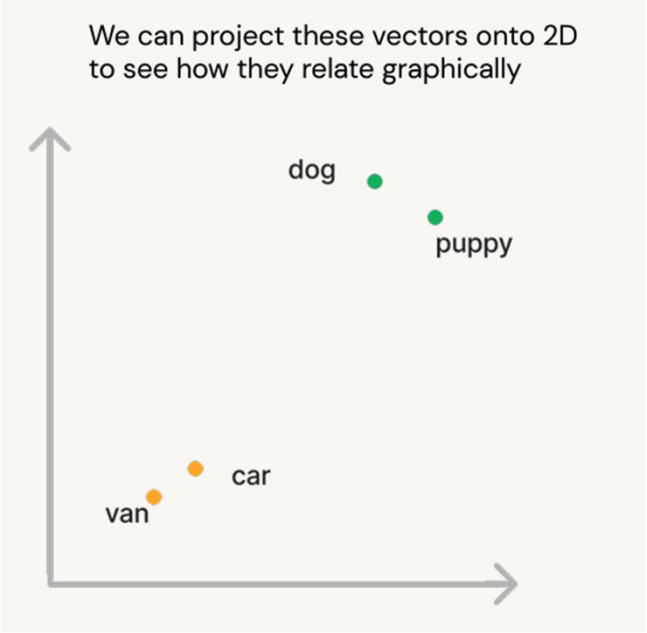
- New idea: Let's give each word a vector representation and use data to build our embedding space.

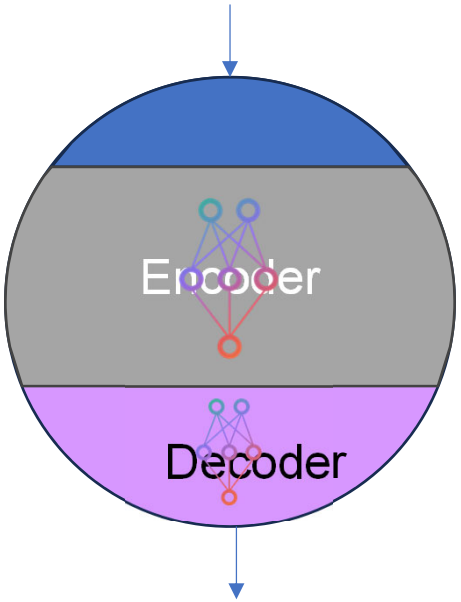


Dense vector representations

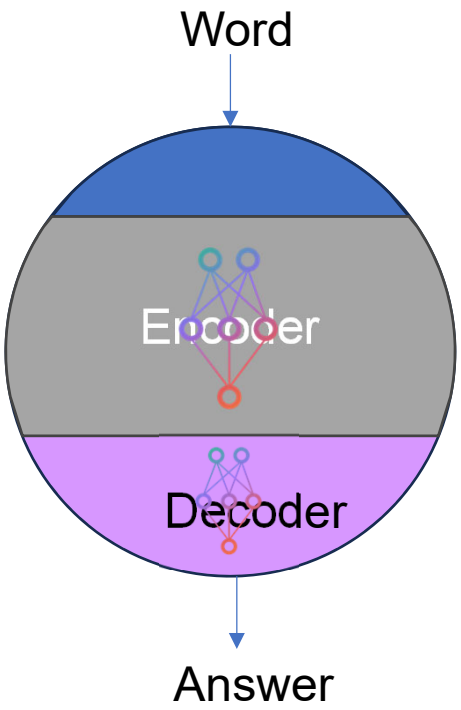
- Visualizing common words using word vectors.



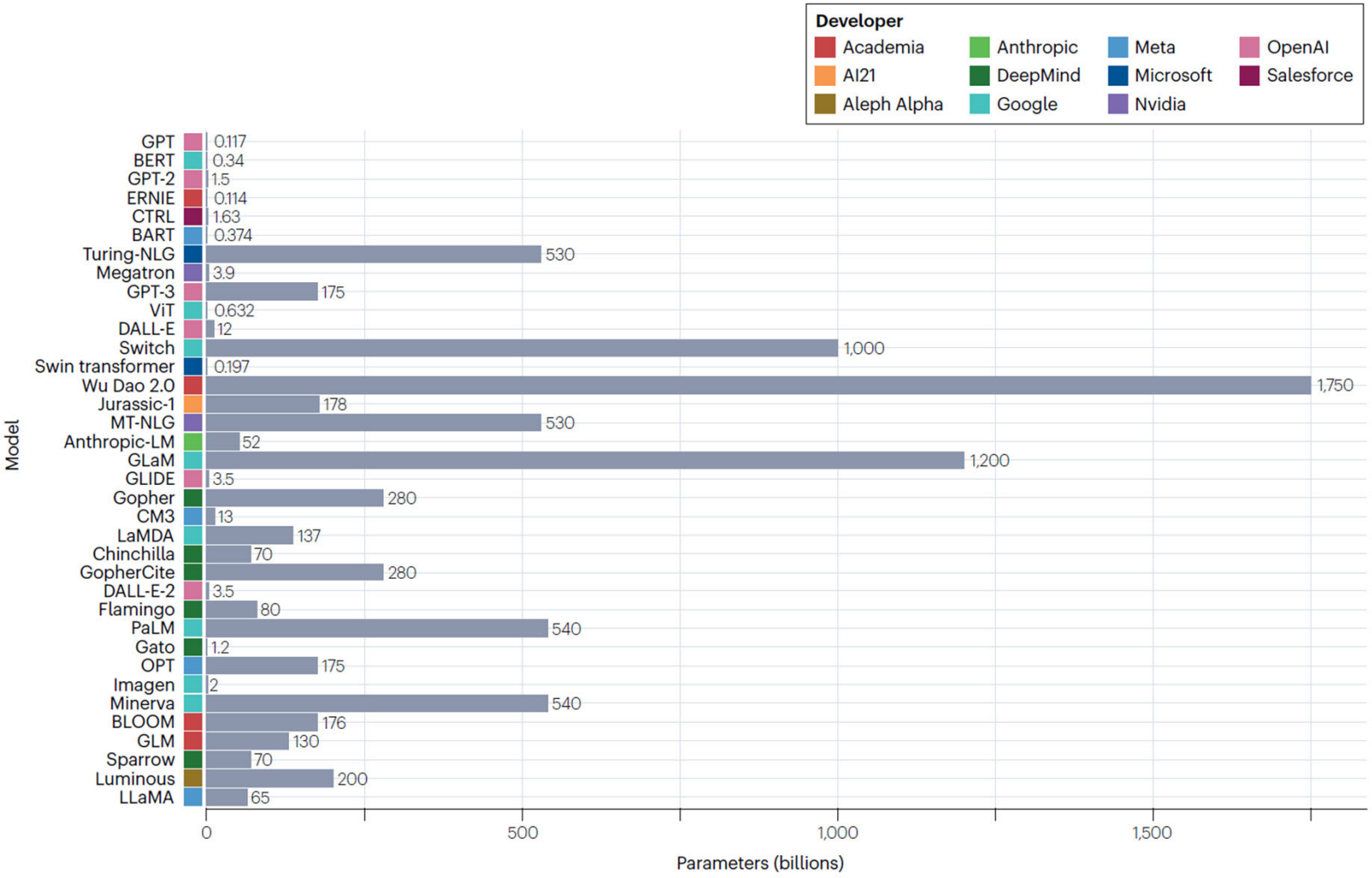


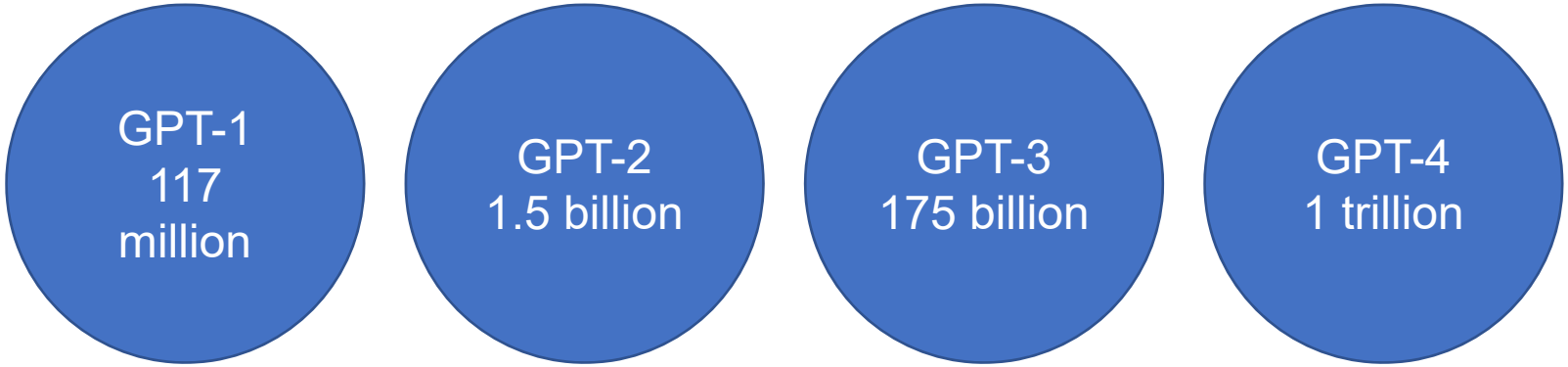

Encoder
Decoder

How to train your model?



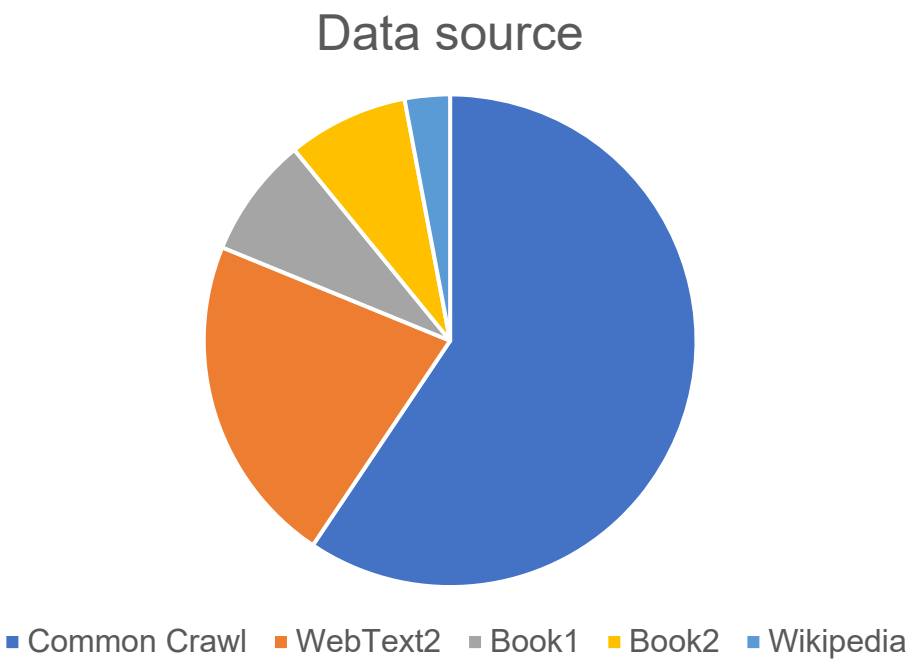
Parameters of LLM




GPT-1
117
million
GPT-2
1.5 billion
GPT-3
175 billion
GPT-4
1 trillion

We need data!

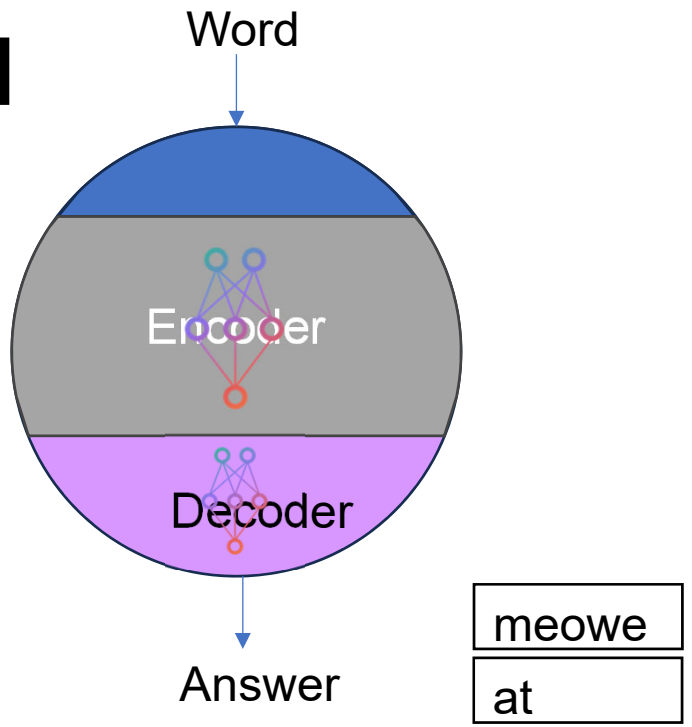
GPT-3



How to train your model?

The kitten [redacted] at me for treats.

The kitten meowed [redacted] me for treats.

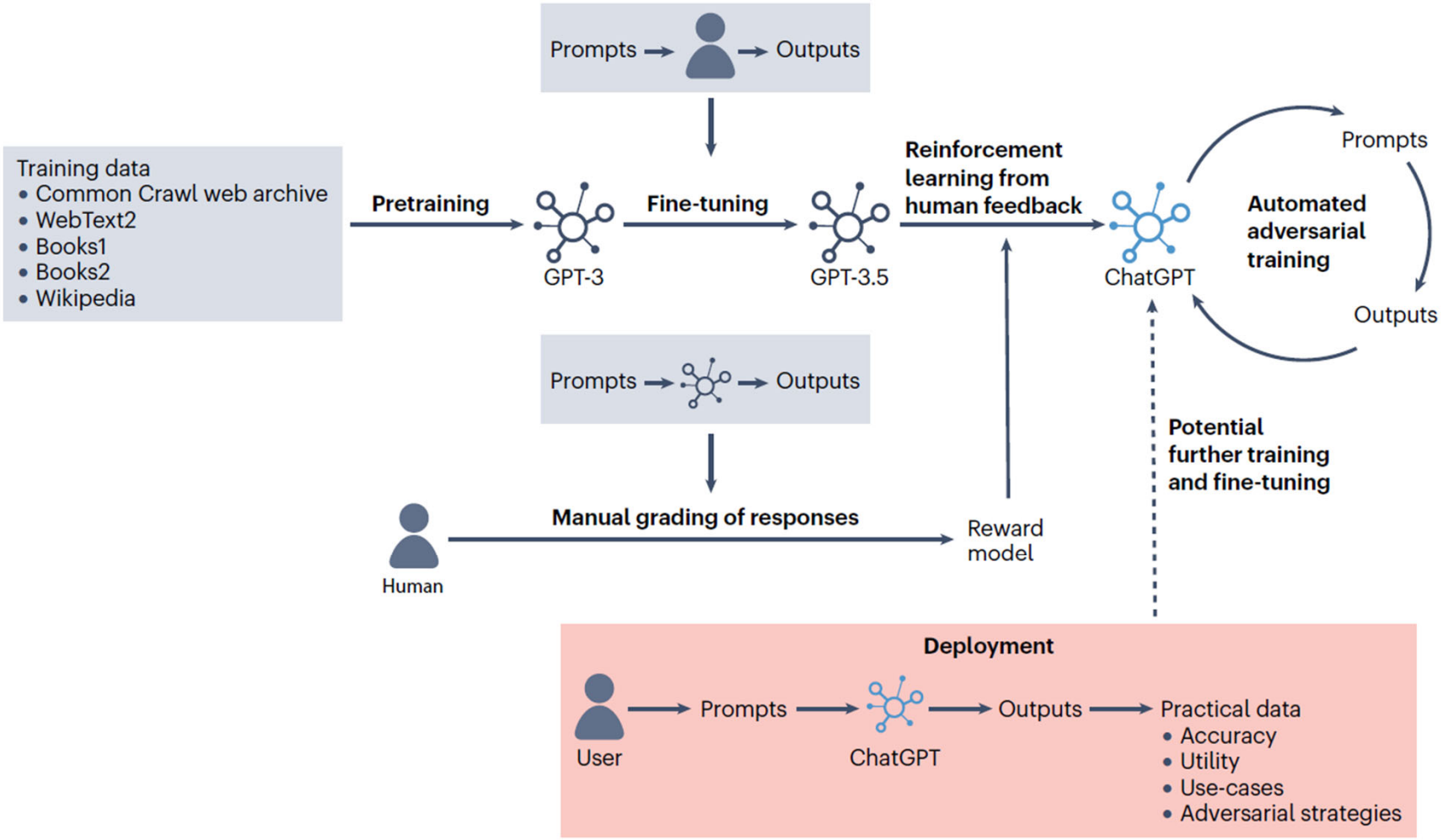


Training schemata

- Masked language modeling
  - cloze tasks: predicting masked tokens in a sequence
- Permuted language modeling
  - language modeling with randomly sampled input tokens
- Denoising autoencoding
  - Recovering undistorted inputs after intentional corruption
- Next-sentence prediction
  - Distinguishing whether sentences are contiguous or not.
- Examples
  - Gato, DALL-E, Enhanced Language Representations with Informative Entities (ERNIE), Bidirectional Encoder Representations from Transformers (BERT) and Bidirectional and Auto-regressiveTransformers (BART)

From LLM to generative AI chatbot

- Fine-tuning involved exposing GPT-3 to prompts and responses produced by human researchers acting the part of an application user and AI assistant
- **Reinforcement learning from human feedback' (RLHF)** was conducted using a reward model trained on data generated by human graders tasked with ranking GPT-3.5 responses to a set of queries.


Prompts
Outputs
Training data
• Common Crawl web archive
• WebText2
• Books1
• Books2
• Wikipedia
Pretraining
GPT-3
Fine-tuning
GPT-3.5
Reinforcement learning from human feedback
ChatGPT
Prompts
Automated adversarial training
Outputs
Prompts
Outputs
Potential further training and fine-tuning
Manual grading of responses
Human
Reward model
Deployment
User
Prompts
ChatGPT
Outputs
Practical data
• Accuracy
• Utility
• Use-cases
• Adversarial strategies

Reinforcement Learning

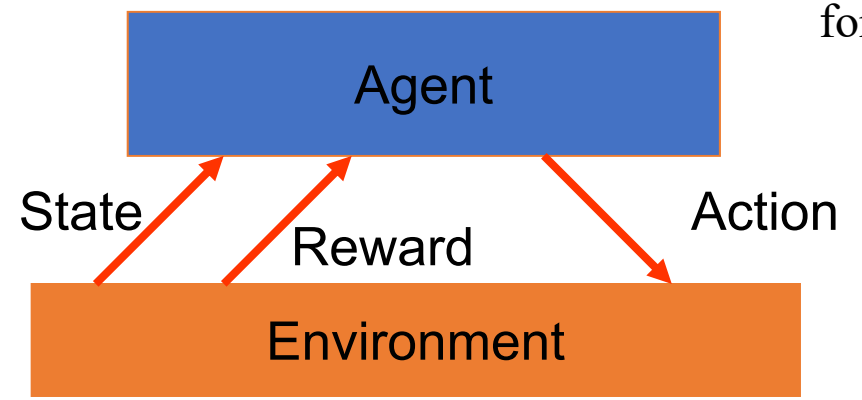
- **Deep Reinforcement Learning** - game playing, robotics in simulation, self-play, neural architecture search

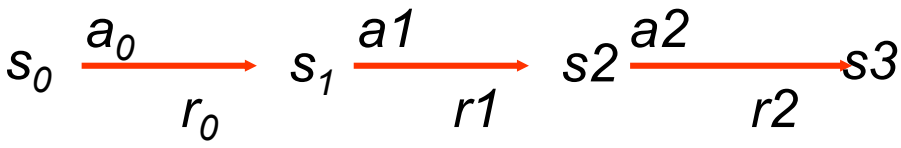
Reinforcement Learning

- Supervised Learning: Immediate feedback (labels provided for every input).
- Unsupervised Learning: No feedback (no labels provided).
- Reinforcement Learning: Delayed scalar feedback (a number called reward).
- RL deals with agents that must sense & act upon their environment.
- Examples:
  - A robot cleaning the room and recharging its battery
  - Robot-soccer
  - Modeling the economy through rational agents
  - Learning how to fly a helicopter
  - Scheduling planes to their destinations

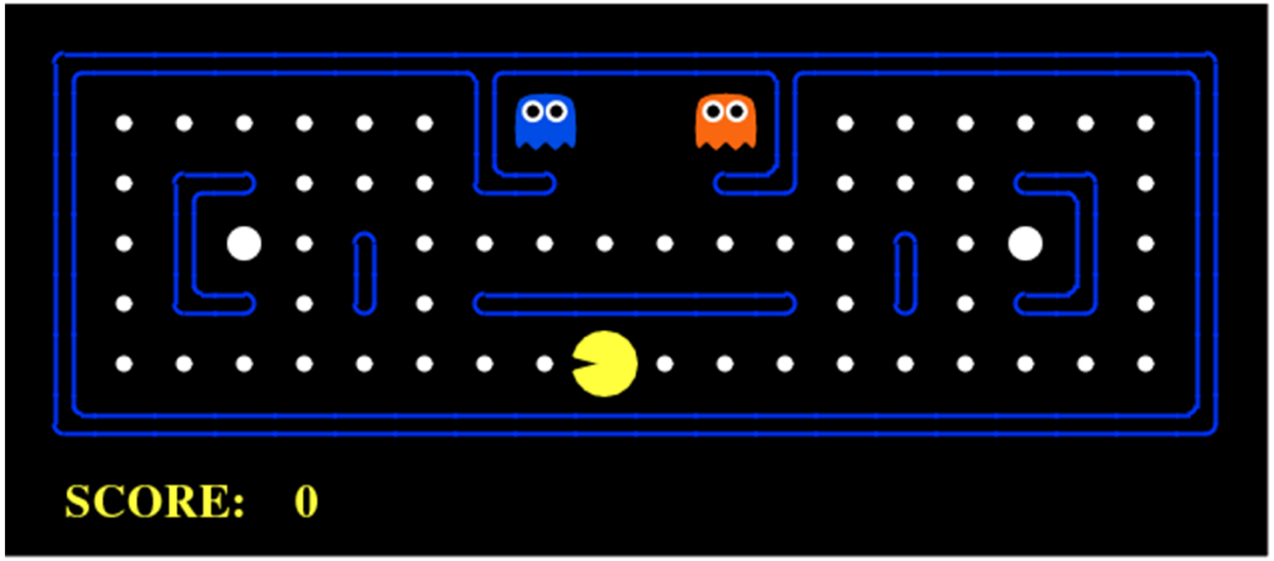
The Big Picture

- S– set of states
- A– set of actions
- T(s,a,s') = P(s'|s,a)– the probability of transition from *s* to *s'* given action *a*
- R(s,a)– the expected reward for taking action *a* in state *s*





Your action influences the state of the world which determines its reward


SCORE: 0

The Task

- To learn an optimal *policy* that maps states of the world to actions of the agent. I.e., if this patch of room is dirty, I clean it. If my battery is empty, I recharge it.

$$\pi : S \rightarrow A$$

- What is it that the agent tries to optimize?
  - the total discounted future reward:

$$V^{\pi}(s_t) = r_t + \gamma r_{t+1} + \gamma^2 r_{t+2} + \ldots$$
$$= \sum_{i=0}^{\infty} \gamma^i r_{t+i}, 0 \leq \gamma < 1$$

Note: immediate reward is worth more than future reward.

Value Function

- Let's say we have access to the optimal value function that computes the total future reward $V^*(s)$

- The optimal policy $\pi^*(s)$ is chosen by maximizing:

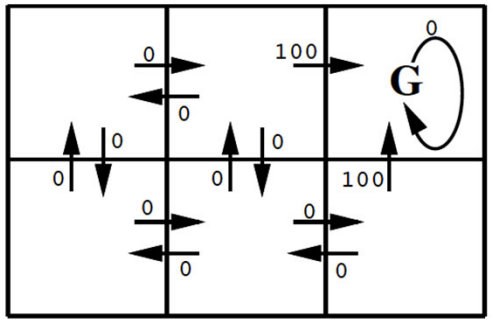
$$\pi^*(s) = \arg\max_a \left[r(s,a) + \gamma V^*(\delta(s,a)) \right]$$

- We assume that we know what the reward will be if we perform action "a" in state "s": $r(s,a)$

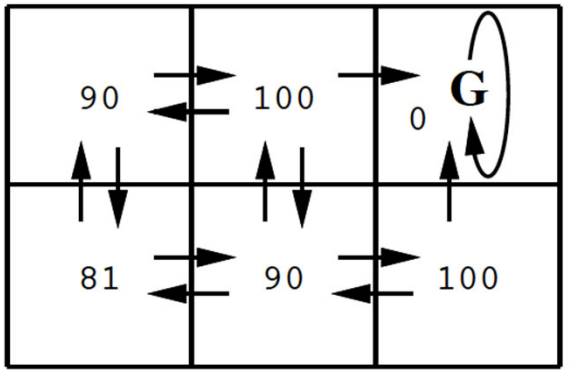
- We also assume we know what the next state of the world will be if we perform action "a" in state "s":

$$s_{t+1} = \delta(s_t, a)$$

Example: Find your way to G

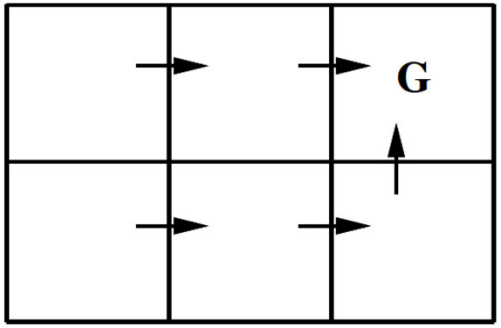


$r(s, a)$ (immediate reward) values



$V^*(s)$ values

$\gamma = 0.9$



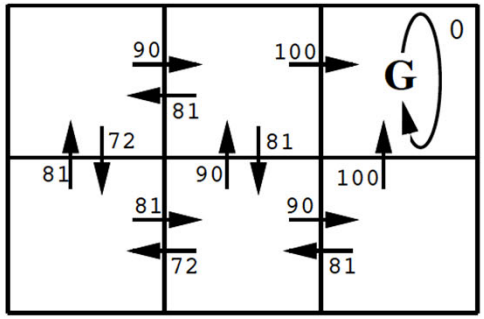
One optimal policy

Q-Function

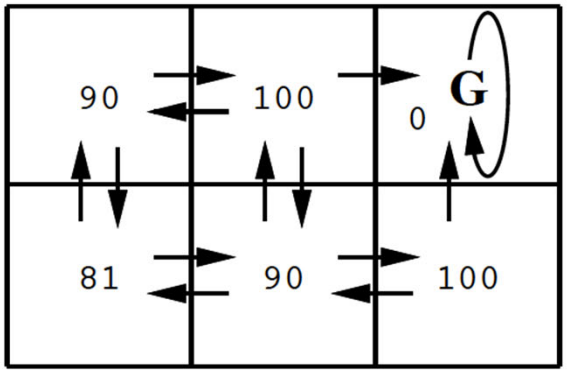
- One approach to RL to estimate V*(s). $V^*(s) \leftarrow \max_a \left[r(s,a) + \gamma V^*(\delta(s,a)) \right]$
- However, this approach requires you to know r(s,a) and δ(s,a).
- We need a function that directly learns good state-action pairs, i.e. what action should I take in this state. We call this Q(s,a).
- Given Q(s,a) it is now trivial to execute the optimal policy, *without knowing r(s,a) and δ(s,a).* We have:

$$\pi^*(s) = \arg\max_a Q(s,a)$$

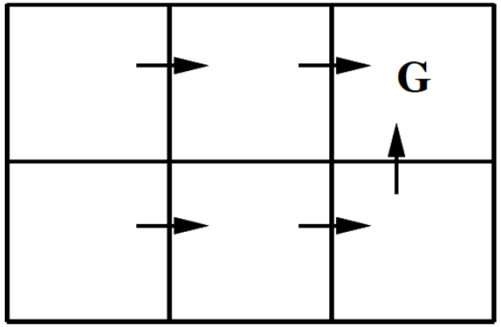
$$V^*(s) = \max_a Q(s,a)$$



$Q(s, a)$ values



$V^*(s)$ values



One optimal policy

$$\pi^*(s) = \arg\max_a Q(s,a)$$

$$V^*(s) = \max_a Q(s,a)$$

Q-Learning

$$Q(s,a) \equiv r(s,a) + \gamma V^*(\delta(s,a))$$
$$= r(s,a) + \gamma \max_{a'} Q(\delta(s,a),a')$$

- This still depends on r(s,a) and δ(s,a).
- However, imagine the robot is exploring its environment, trying new actions as it goes.
- At every step it receives some reward "r", and it observes the environment change into a new state s' for action a.
  How can we use these observations, (s,a,s',r) to learn a model?

$$\hat{Q}(s,a) \leftarrow r + \gamma \max_{a'} \hat{Q}(s',a') \quad s' = s_{t+1}$$

- This equation continually estimates Q at state s consistent with an estimate of Q at state s'**: temporal difference (TD-Q) learning**.
- Do an update after each state-action pair.

3 steps in Q-learning

1. Agent starts in a state (s_1) takes an action (a_1) and receives a reward (r_1)
2. Agent selects action by referencing Q-table with highest value (max) OR by random (epsilon, ε)
3. Update q-values

Initialized

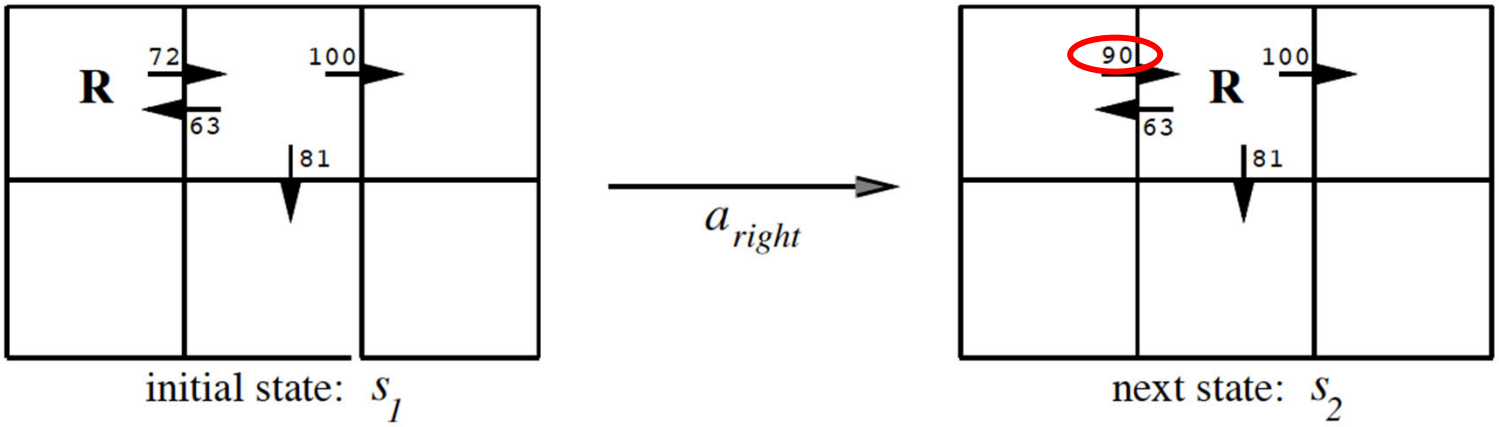
Q-Table		Actions					
		South (0)	North (1)	East (2)	West (3)	Pickup (4)	Dropoff (5)
States	0	0	0	0	0	0	0
	. . .	. . .	. . .	. . .	. . .	. . .	. . .
	327	0	0	0	0	0	0
	. . .	. . .	. . .	. . .	. . .	. . .	. . .
	499	0	0	0	0	0	0

Training

Q-Table		Actions					
		South (0)	North (1)	East (2)	West (3)	Pickup (4)	Dropoff (5)
States	0	0	0	0	0	0	0
	. . .	. . .	. . .	. . .	. . .	. . .	. . .
	328	-2.30108105	-1.97092096	-2.30357004	-2.20591839	-10.3607344	-8.5583017
	. . .	. . .	. . .	. . .	. . .	. . .	. . .
	499	9.96984239	4.02706992	12.96022777	29	3.32877873	3.38230603

https://en.wikipedia.org/wiki/Q-learning

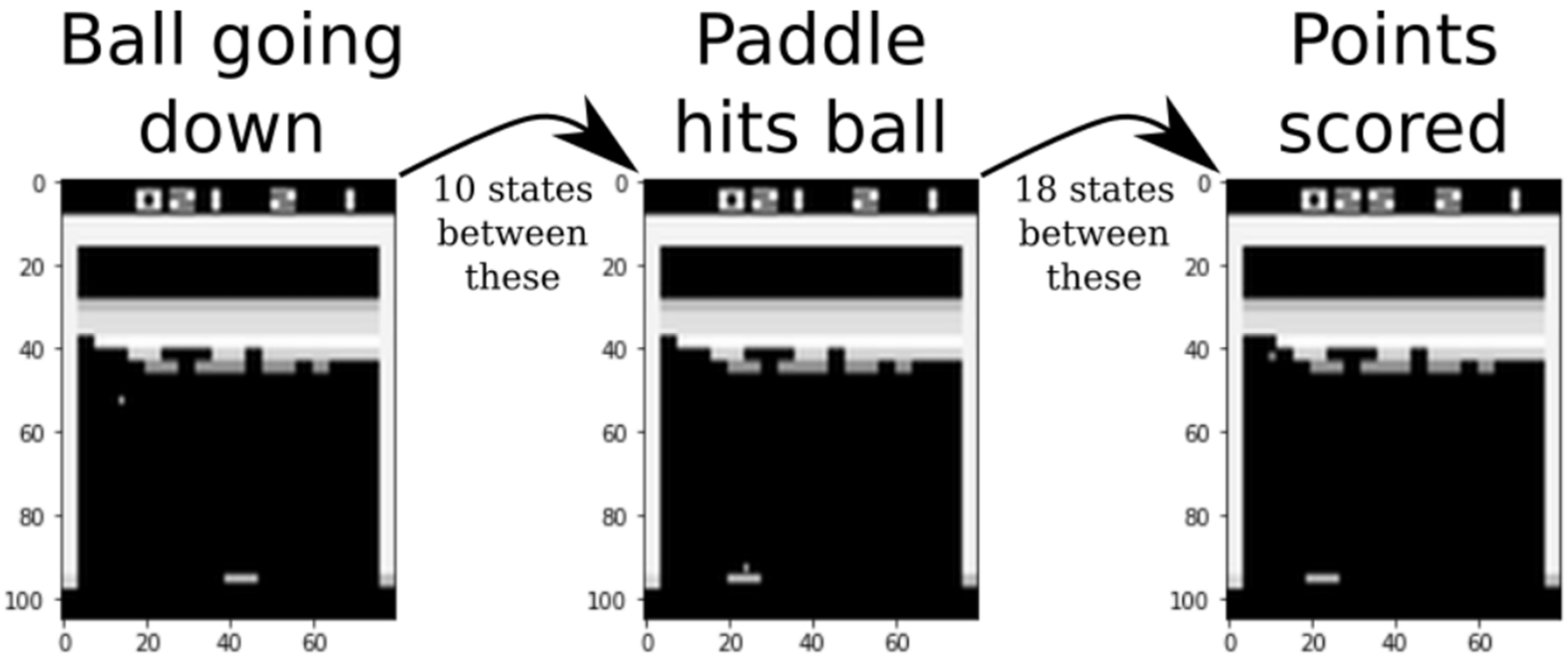
Example Q-Learning



$$\hat{Q}(S_1, a_{right}) \leftarrow r + \gamma \max_{a'} \hat{Q}(S_2, a')$$
$$\leftarrow 0 + 0.9 \max(63, 81, 100)$$
$$\leftarrow 90$$

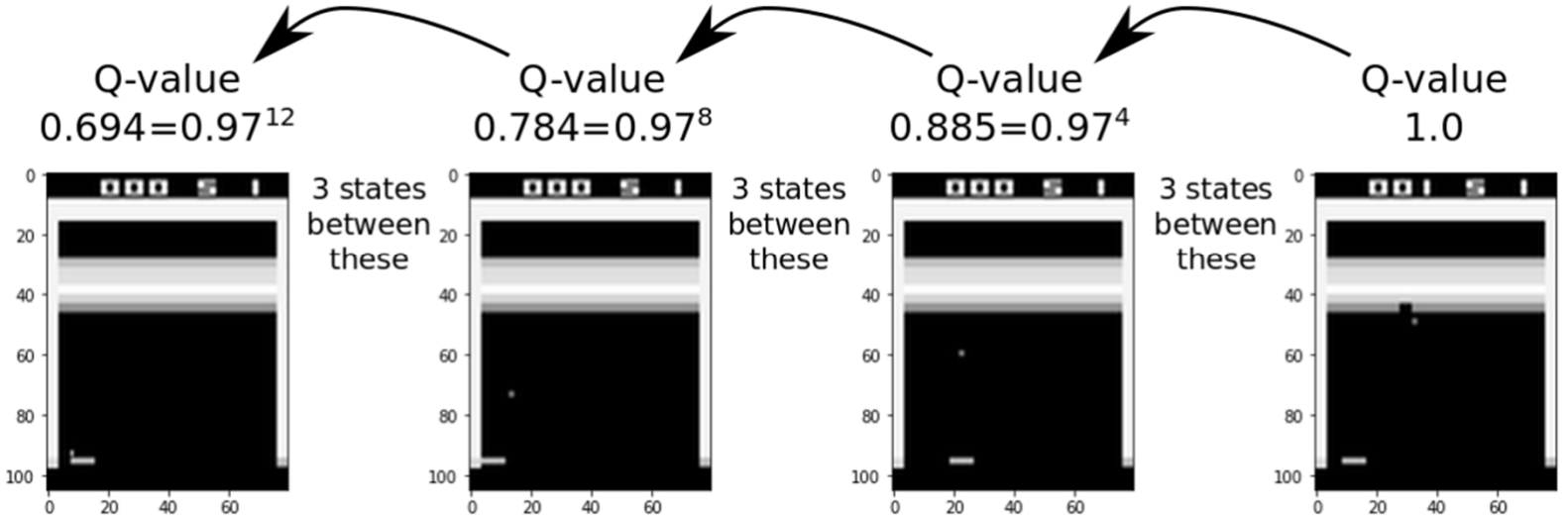
Q-learning propagates Q-estimates 1-step backwards

Example: Atari Breakout

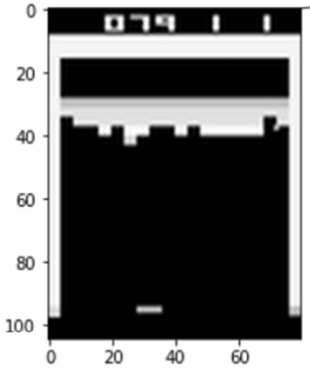


https://colab.research.google.com/github/Hvass-Labs/TensorFlow-Tutorials/blob/master/16_Reinforcement_Learning.ipynb#scrollTo=CT6gxbxIJ-V_

$$Q(s_t, a_t) \leftarrow \underbrace{r_t}_{\text{reward}} + \underbrace{\gamma}_{\text{discount}} \cdot \underbrace{\max_a Q(s_{t+1}, a)}_{\text{estimate of future rewards}}$$

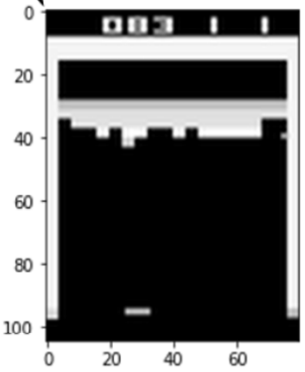


State *t*



One step in game

State *t+1*



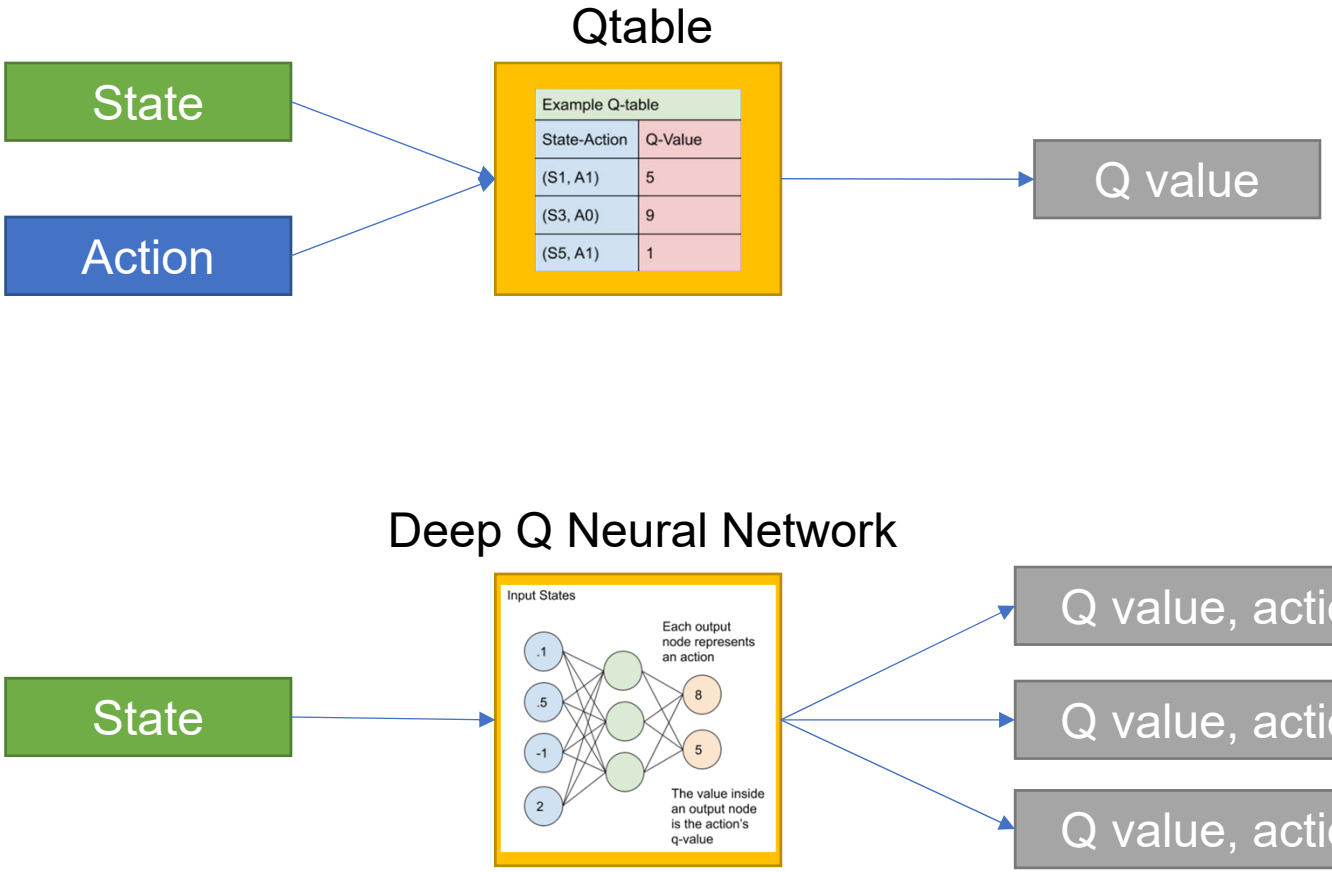
Action:	Q-Values:
====	======
NOOP	**2.900** (Action Taken)
FIRE	2.622
RIGHT	2.078
LEFT	2.266
RIGHTFIRE	2.183
LEFTFIRE	2.780

Update Q-Value
1+0.97x1.830=2.775

Action:	Q-Values:
====	======
NOOP	1.814
FIRE	1.777
RIGHT	1.825
LEFT	1.697
RIGHTFIRE	**1.830** (Max Value)
LEFTFIRE	1.740

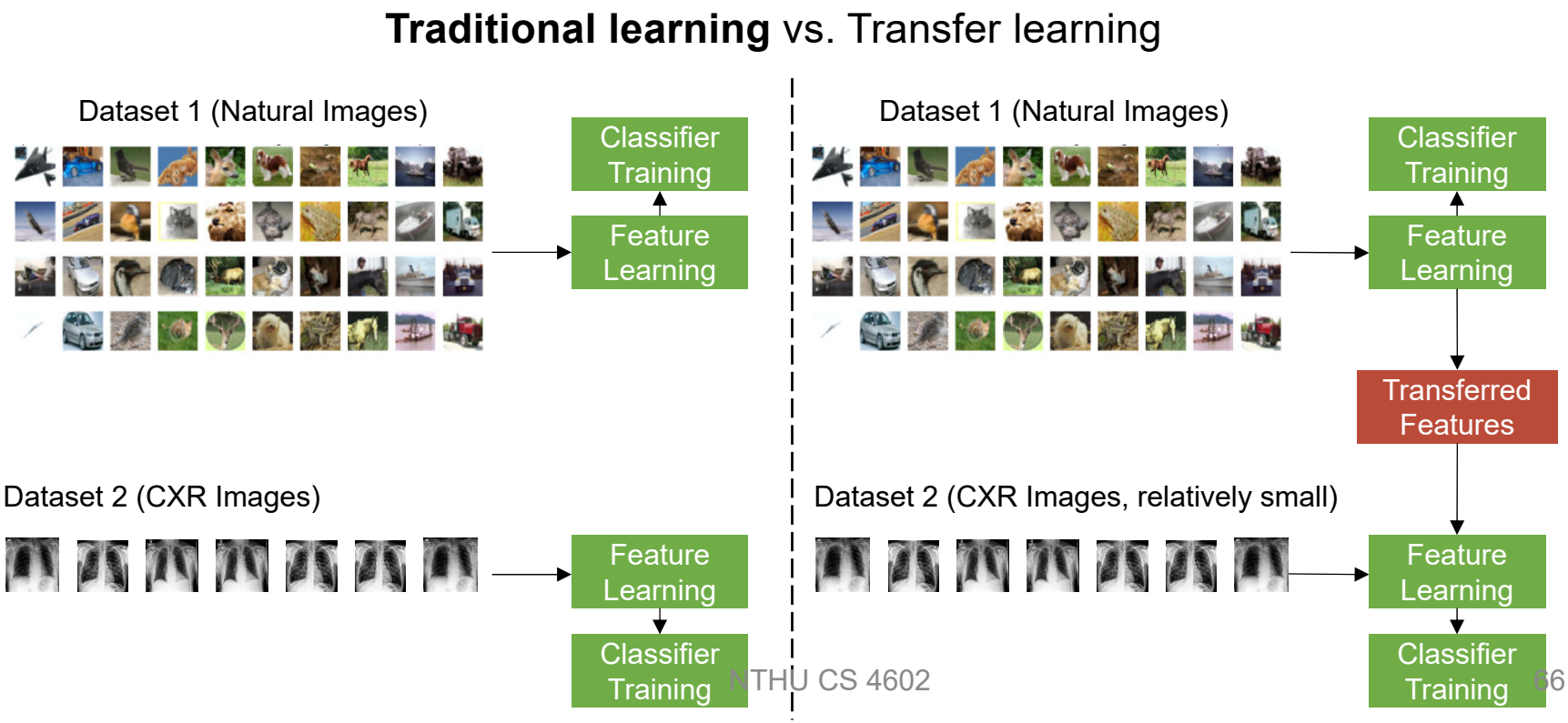
$$Q(state_t, NOOP) \leftarrow \underbrace{r_t}_{\text{reward}} + \underbrace{\gamma}_{\text{discount}} \cdot \underbrace{\max_a Q(state_{t+1}, a)}_{\text{estimate of future rewards}} = 1.0 + 0.97 \cdot 1.830 \simeq 2.775$$

RL + DL = Deep Q-Network (DQN)

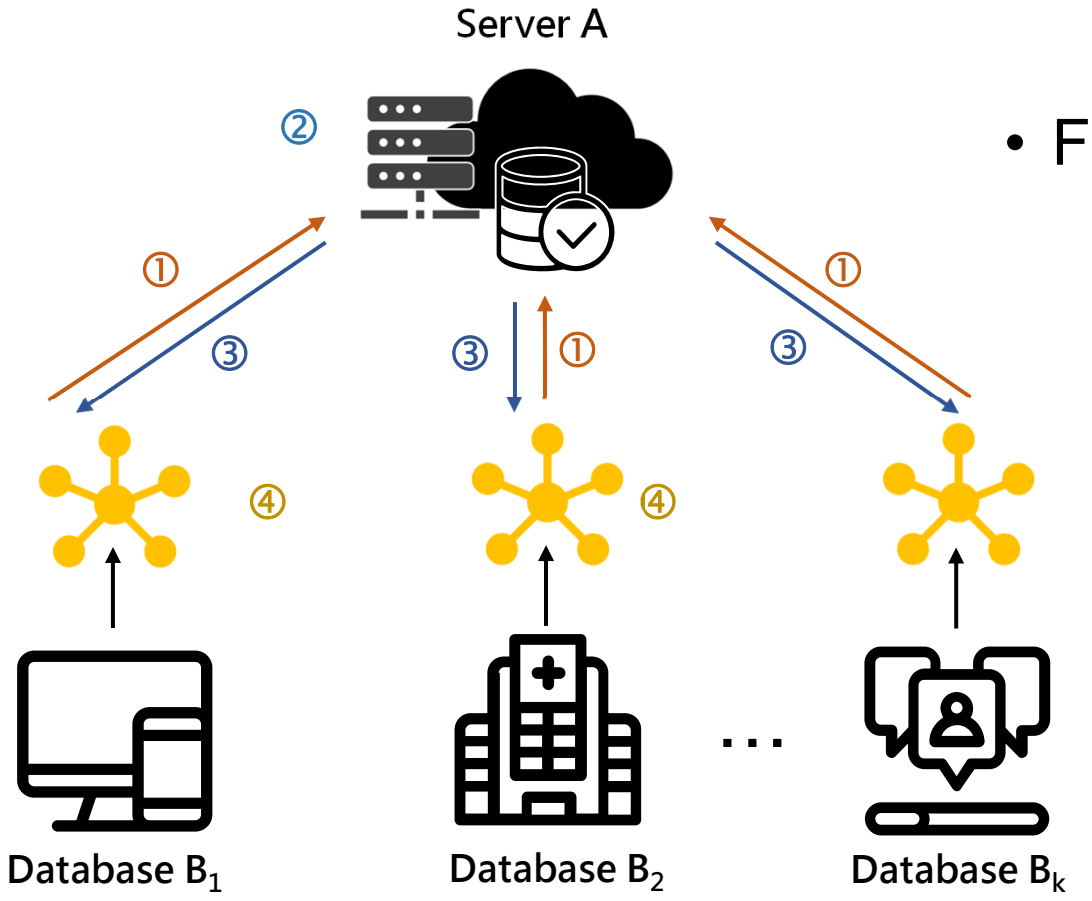


Transfer learning

- Improvement of learning for new task through the transfer of knowledge from similar task that has been trained.



Federated learning



- Federated Learning Steps

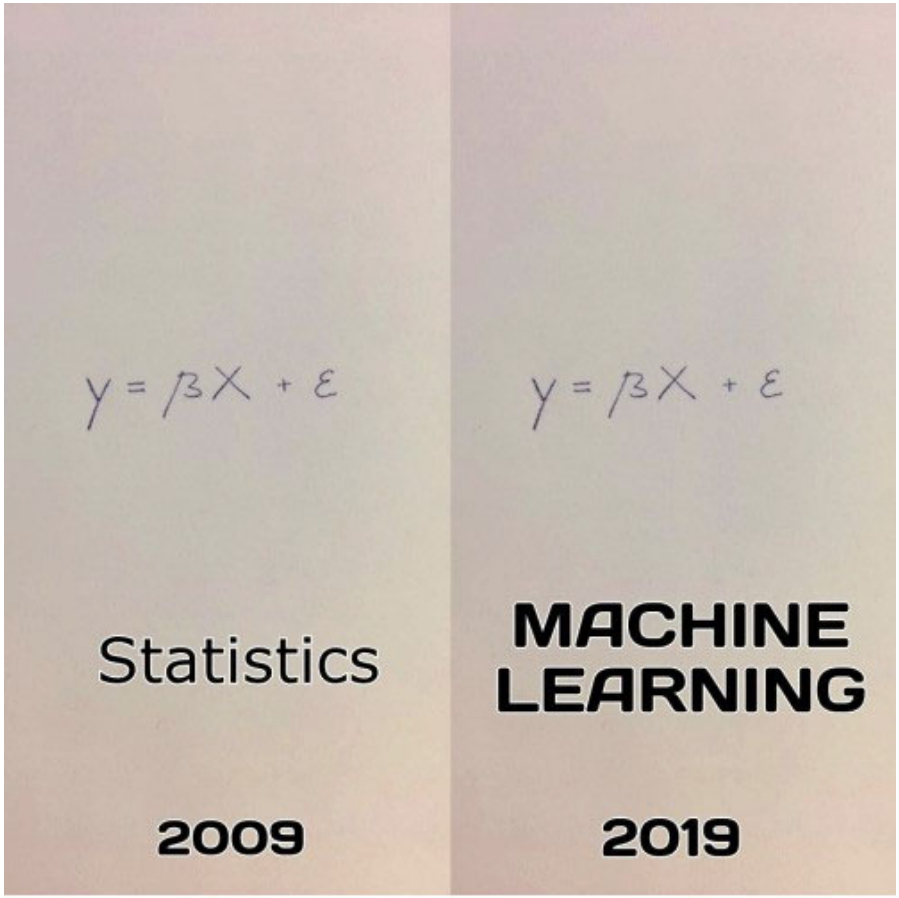
① Sending encrypted gradients
② Secure aggregation
③ Sending back model updates
④ Updating models

Konečný, Jakub, et al. "Federated learning: Strategies for improving communication efficiency." *arXiv preprint arXiv:1610.05492* (2016).

Learning, learning, learning

- Supervised learning
  - **FFNNs**
  - **CNNs**
  - **RNNs**
  - **Encoder Decoder**
- Unsupervised learning
  - **Autoencoder**
  - **GAN**
- Self-Supervised learning
- Reinforcement learning
- Transfer learning
- Federated learning

Questions?



#10yearchallenge