Introduction to Deep Learning with Watson Studio

Svetlana Levitan, PhD, and David Nichols, PhD
Developer Advocate and Data Scientist
IBM Cloud and Cognitive Software

July 31, 2019

IBM Developer

IBM

Contents

Intro to neural networks

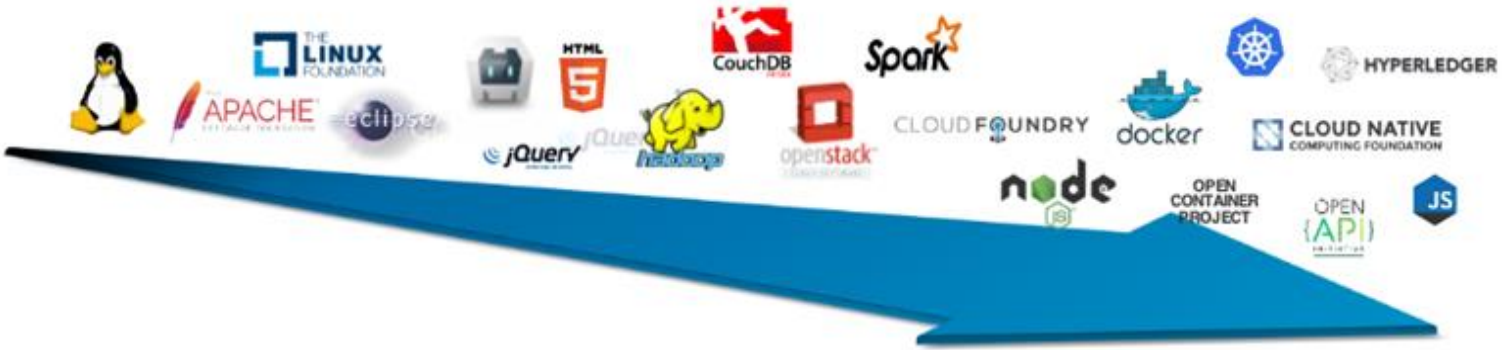
Deep Learning: CNN and RNN

PMML and ONNX for model deployment

AIFairness360 and ART, MAX

Links and resources

IBM's Long History with Open Source and open standards



PMML
Predictive Model Markup Language

ONNX

Center for Open Source Data and AI Technologies

CODAIT aims to make AI solutions dramatically easier to create, deploy, and manage in the enterprise

Relaunch of the Spark Technology Center (STC) to reflect expanded mission

CODAIT

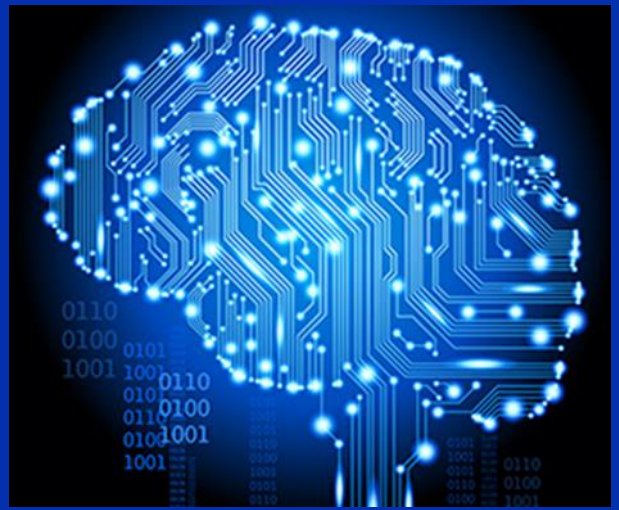
codait.org

codait (French)

= coder/coded

https://m.interglot.com/fr/en/codait

Who uses machine learning today?



Some Applications of Machine Learning

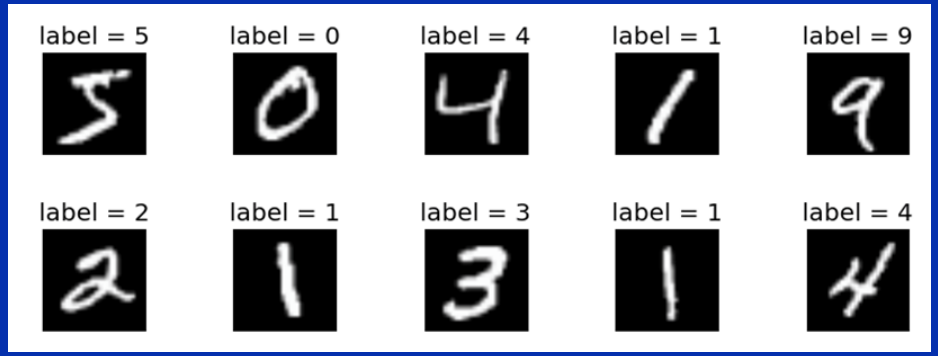
Handwritten digit recognition

Weather forecast

Spam filters for email

Online shopping recommendations

Self-driving car



2011 Watson won Jeopardy
2018 Project Debater

Neural Network Architectures:

Quick Tour

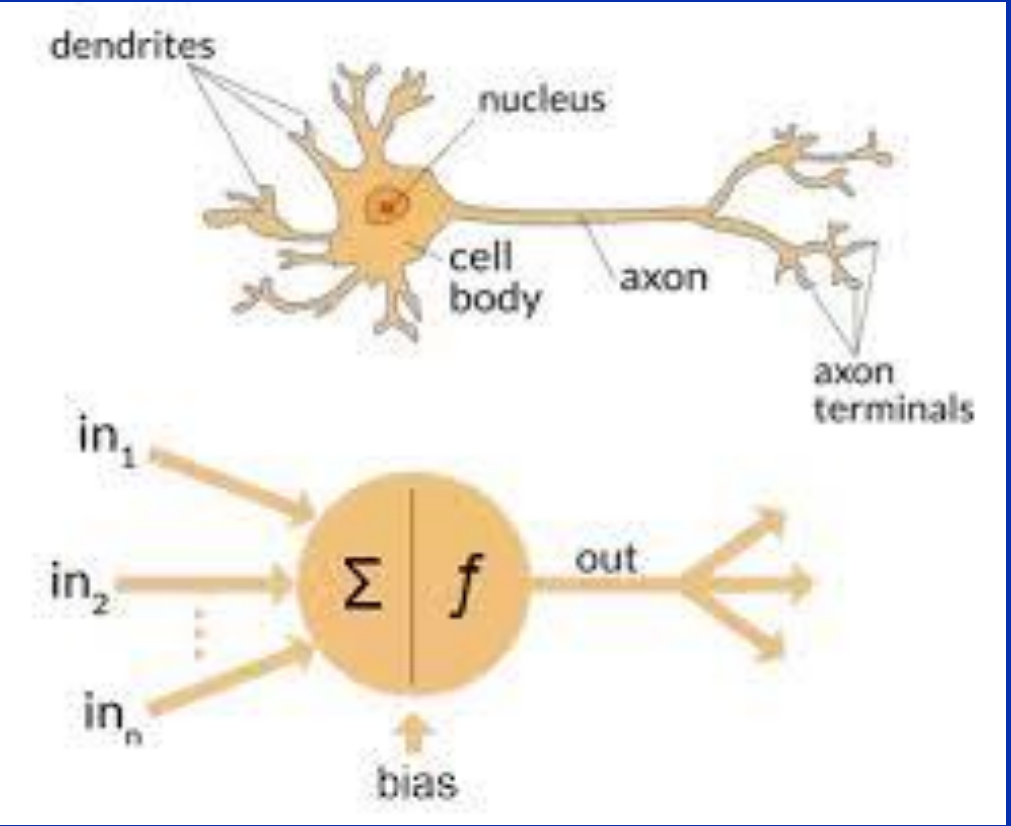
The Elementary Perceptron

1958 Frank Rosenblatt

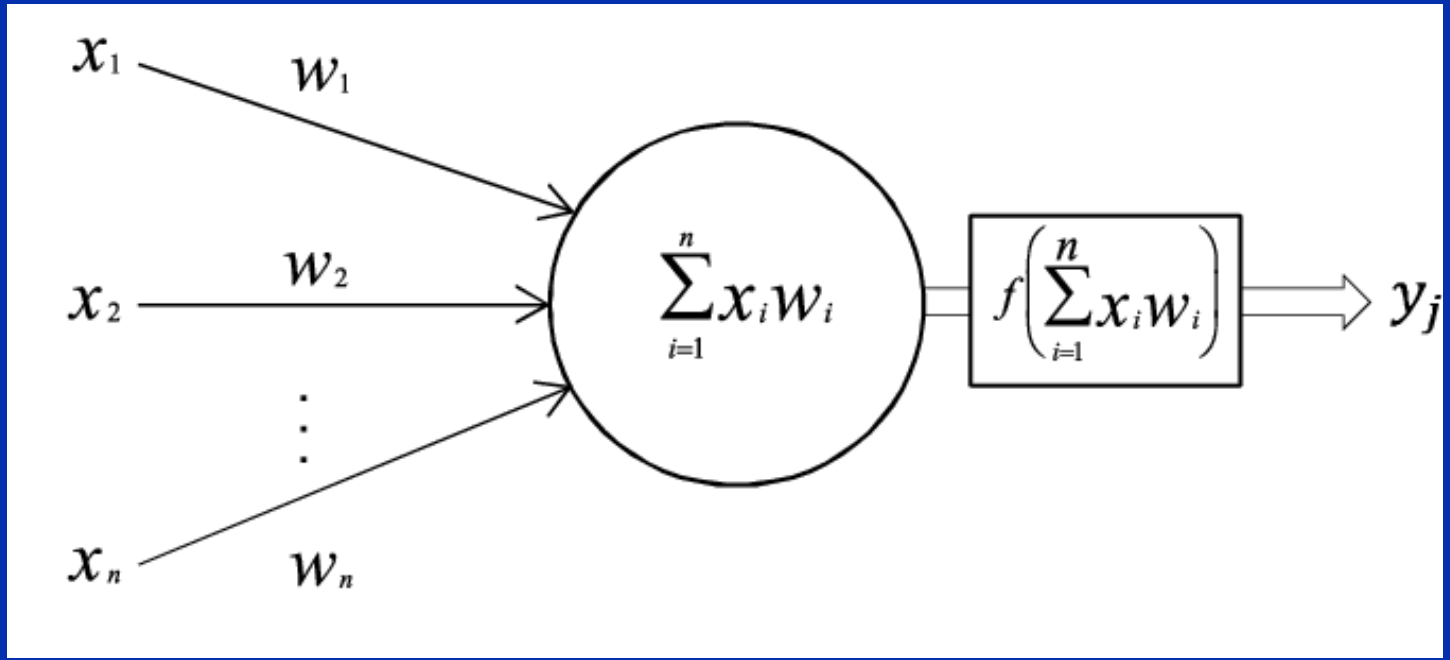
A machine, first implemented in software on IBM 704, later hardware

1969 book by Minsky and Papert →AI winter

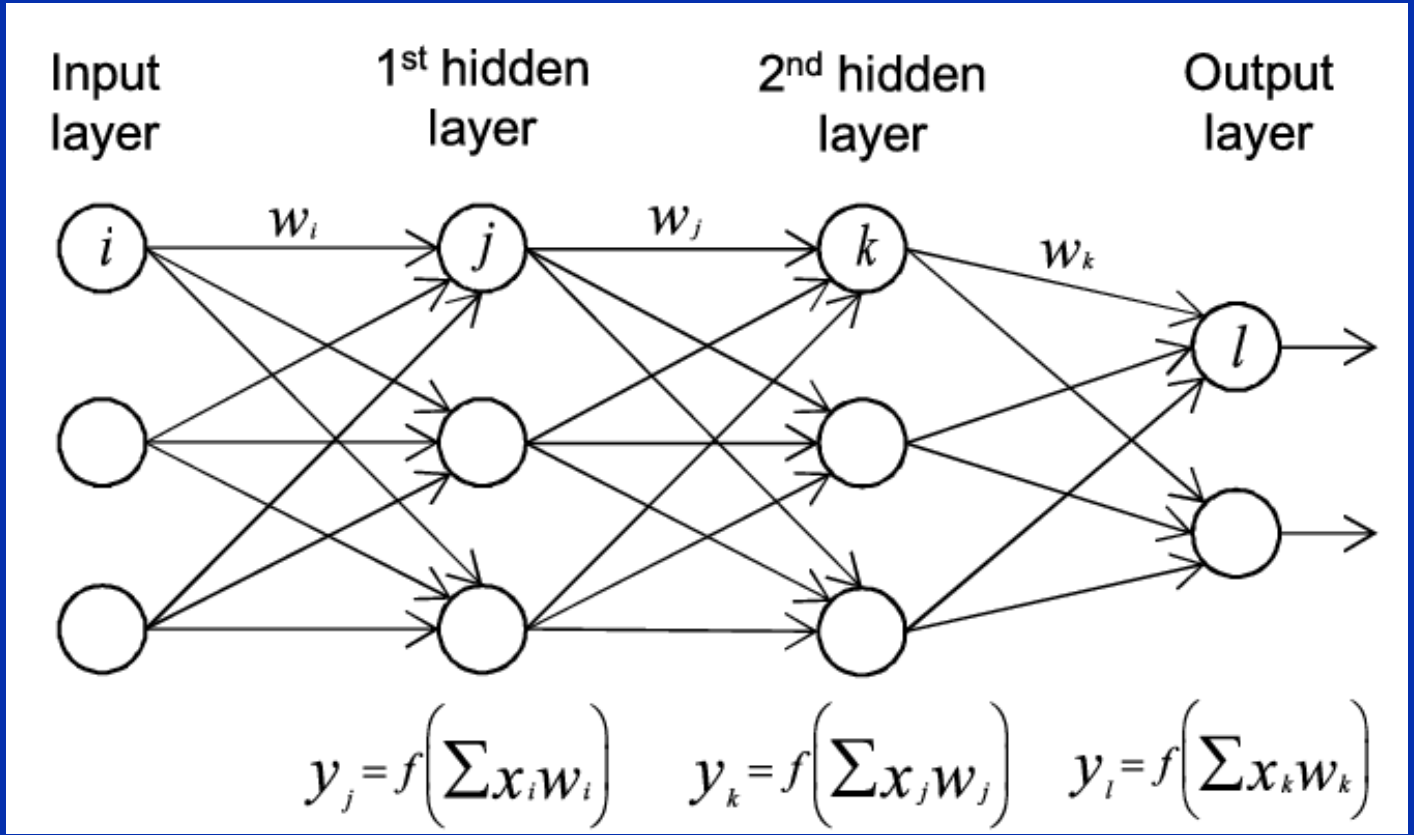
Then MLP = multilayer perceptron



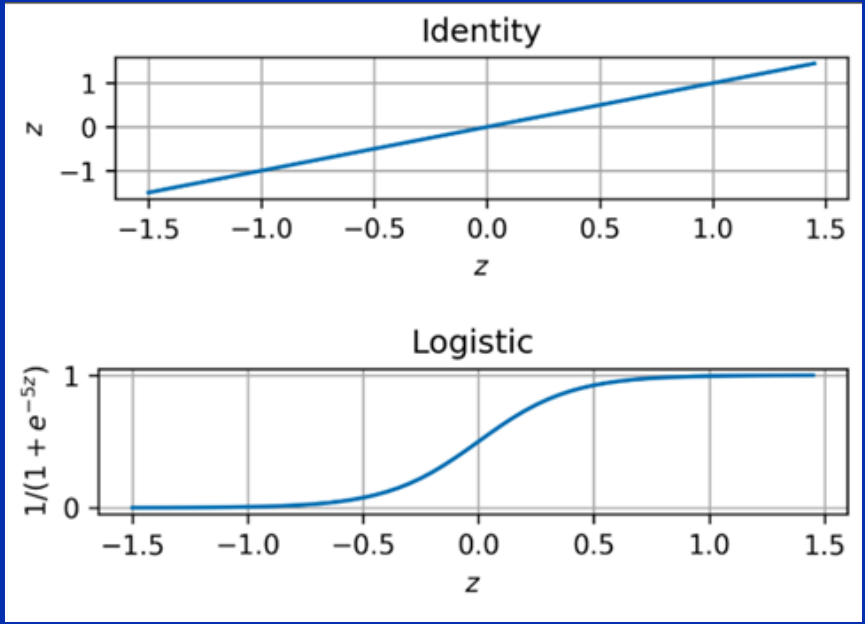
One neuron

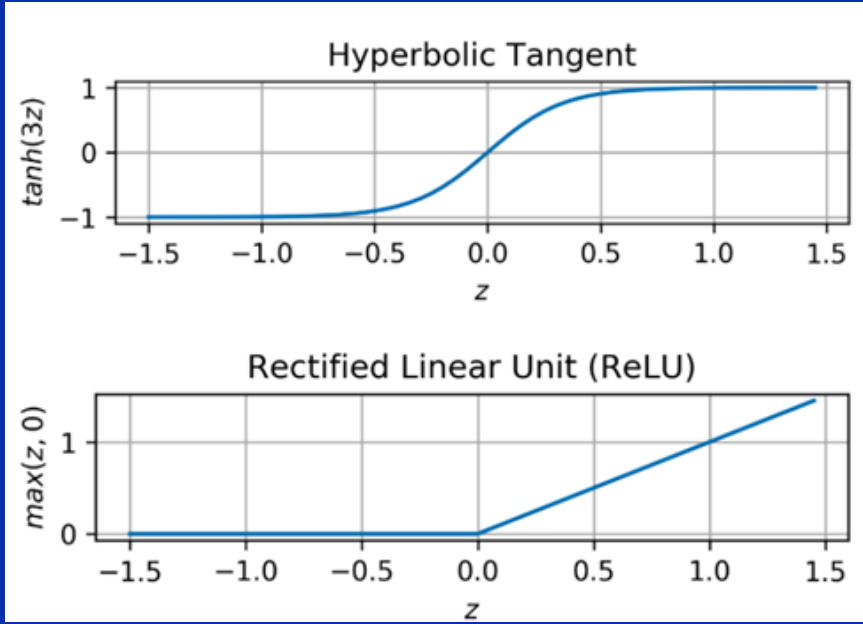


Multi Layer Perceptron

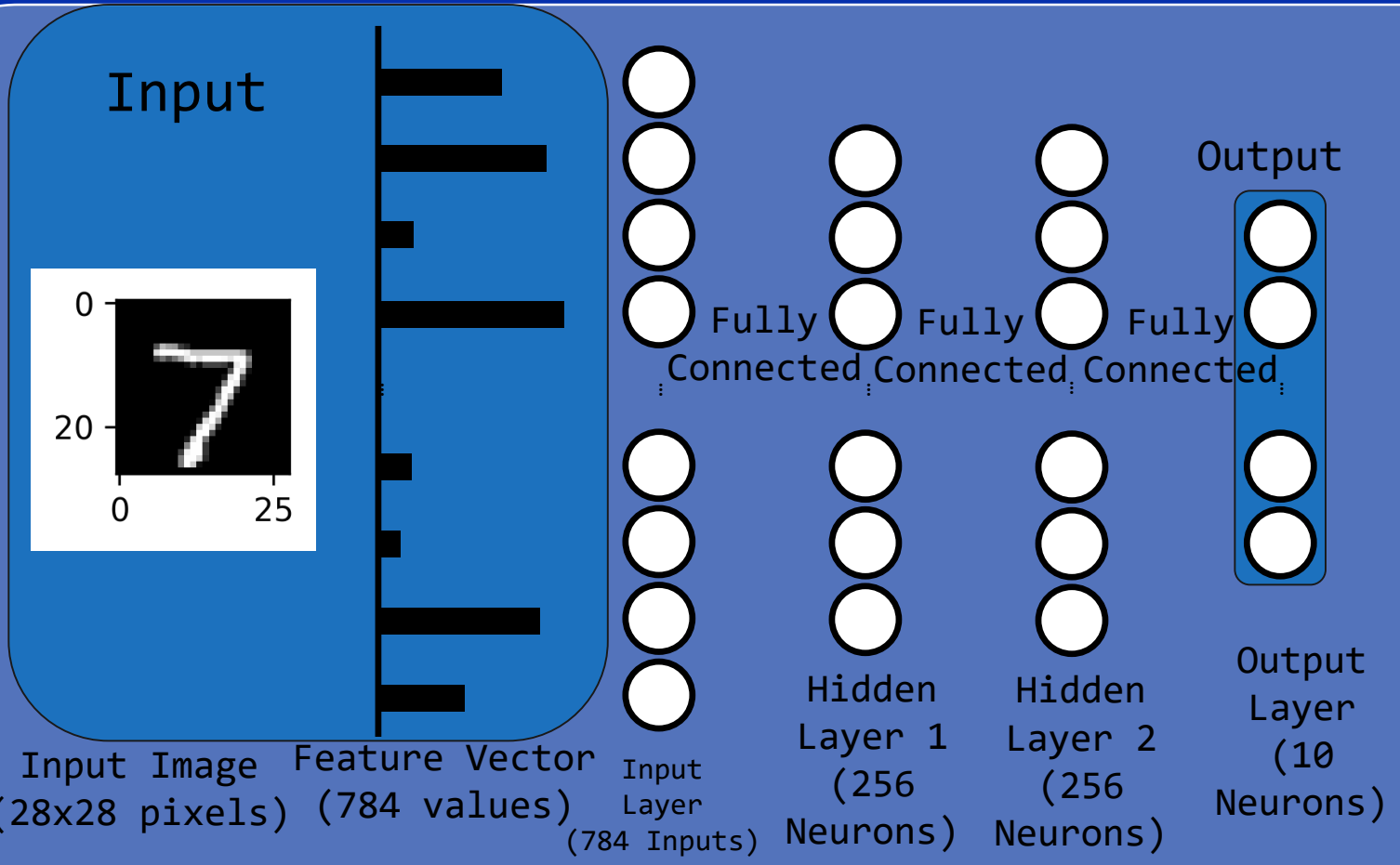


Activation Functions





A Simple Neural Network for Identifying Numbers



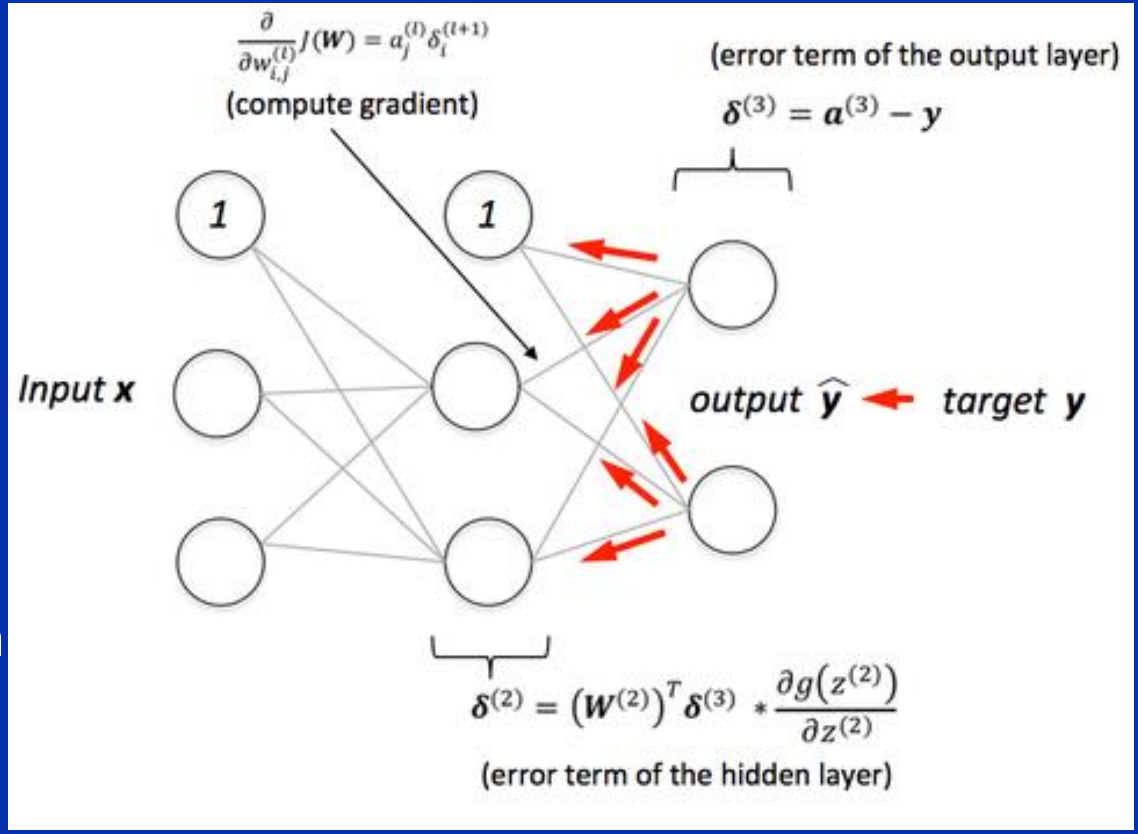
Training Neural Networks with Backpropagation

Initialize weights with small random values

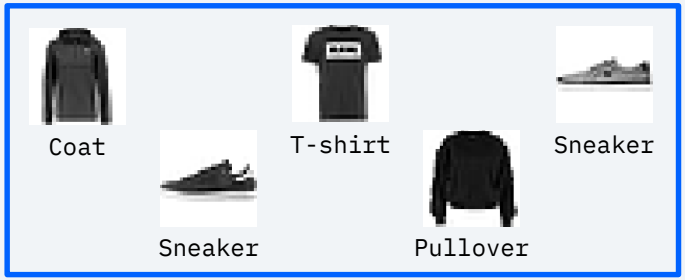
Apply inputs, compute predictions, propagate error back and update weights

Gradient descent methods: Adagrad, Adam, ...

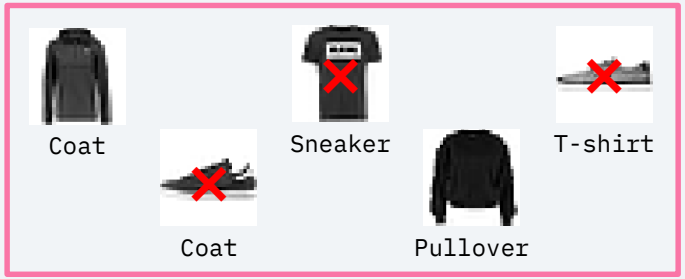
Online or mini-batch or batch

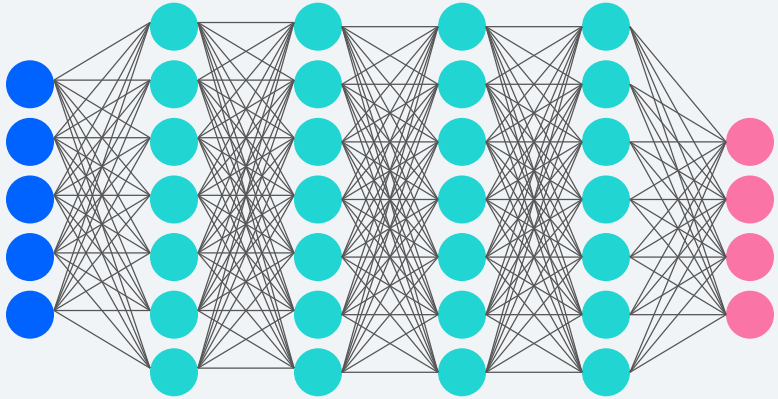


Labeled Training Data



Output Errors



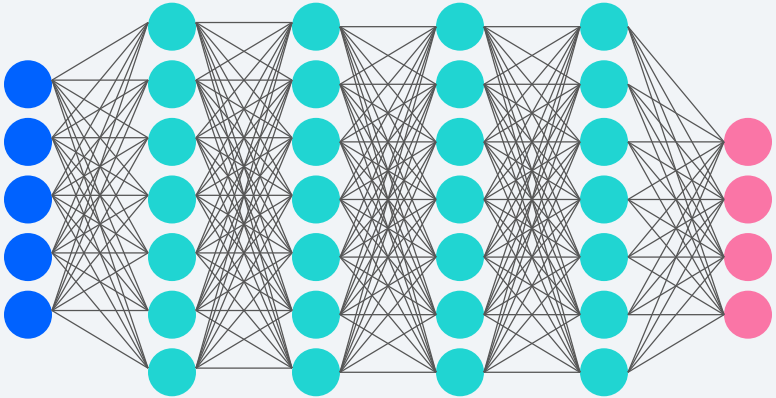


Backpropagation

Fashion-MNIST dataset by Zalando Research, on GitHub <https://github.com/zalandoresearch/fashion-mnist> (MIT License).

Neural Network Inferencing

Input



Output

Sneaker
98%

Fashion-MNIST dataset by Zalando Research, on GitHub <https://github.com/zalandoresearch/fashion-mnist> (MIT License).

Building neural network in SKLearn

```
from sklearn.preprocessing import StandardScaler
scaler = StandardScaler()
# Fit only to the training data
scaler.fit(X_train)

# Now apply the transformations to the data:
X_train = scaler.transform(X_train)
X_test = scaler.transform(X_test)

from sklearn.neural_network import MLPClassifier
mlp = MLPClassifier(hidden_layer_sizes=(256,256),max_iter=500)
mlp.fit(X_train,y_train)

predictions = mlp.predict(X_test)
from sklearn.metrics import classification_report,confusion_matrix
print(confusion_matrix(y_test,predictions))
```

Convolutional neural networks

Convolutional Neural Networks (CNNs)

Widely used in processing of visual images

Photo by Ramdan Authentic

Image representation

Here's the 28 x 28 set of numbers for the digit 7 image:

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	84	185	159	151	60	36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	222	254	254	254	254	241	198	198	198	198	198	198	198	198	170	52	0	0	0	0	0	0
0	0	0	0	0	0	67	114	72	114	163	227	254	225	254	254	254	250	229	254	254	140	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	17	66	14	67	67	67	59	21	236	254	106	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	83	253	209	18	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	22	233	255	83	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	129	254	238	44	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	59	249	254	62	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	133	254	187	5	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	205	248	58	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	126	254	182	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	75	251	240	57	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	19	221	254	166	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	3	203	254	219	35	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	38	254	254	77	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	31	224	254	115	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	133	254	254	52	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	61	242	254	254	52	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	121	254	254	219	40	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	121	254	207	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Convolutional Neural Networks (CNNs)

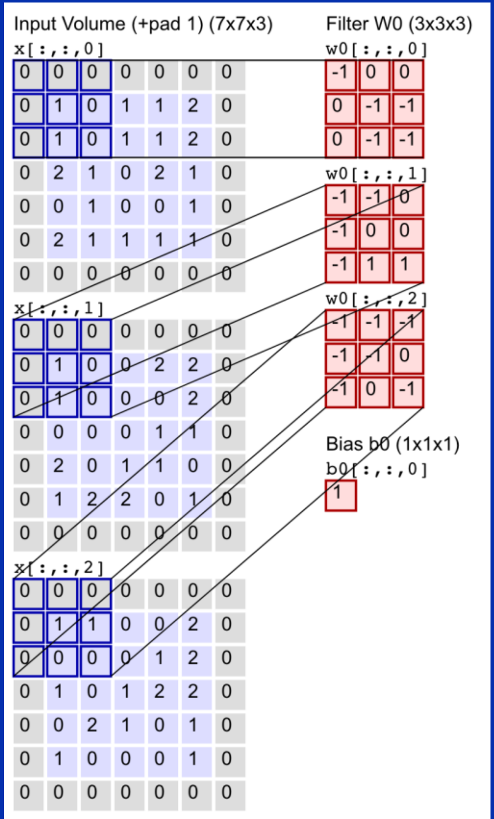
CNNs typically involve use of several types of layers:

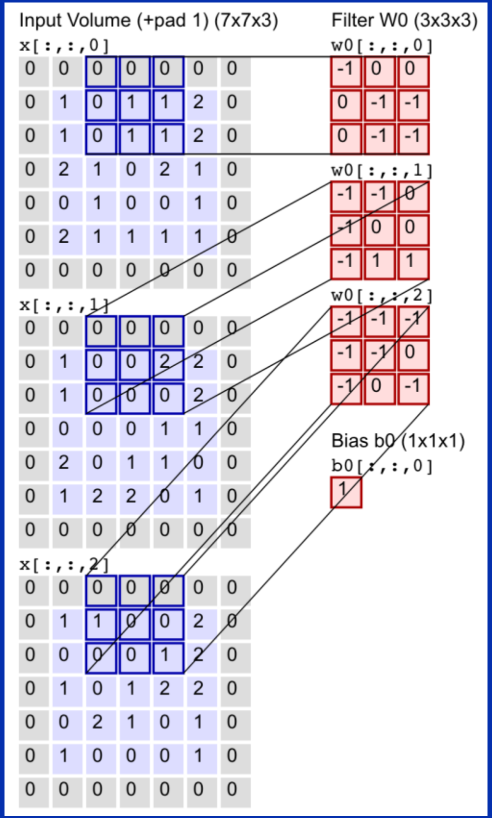
- Convolutional
- Pooling
- Dropout
- Flattening
- Dense (Fully Connected)

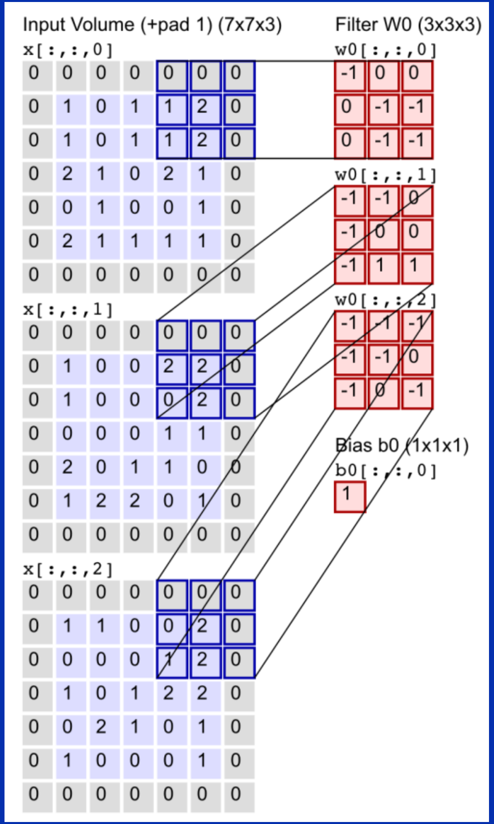
Convolutional filters or kernels

Images on the following four slides are from Stanford University's CS231n Convolutional Networks for Visual Recognition course notes, and are subject to:

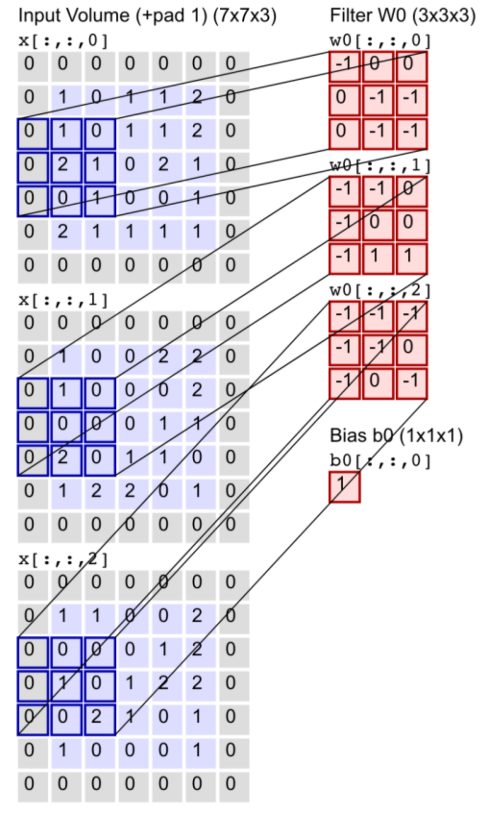
Convolutional filters or kernels

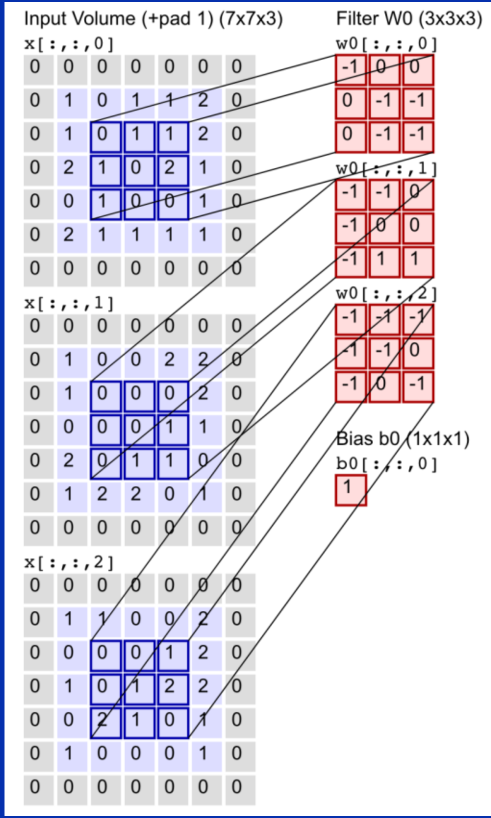


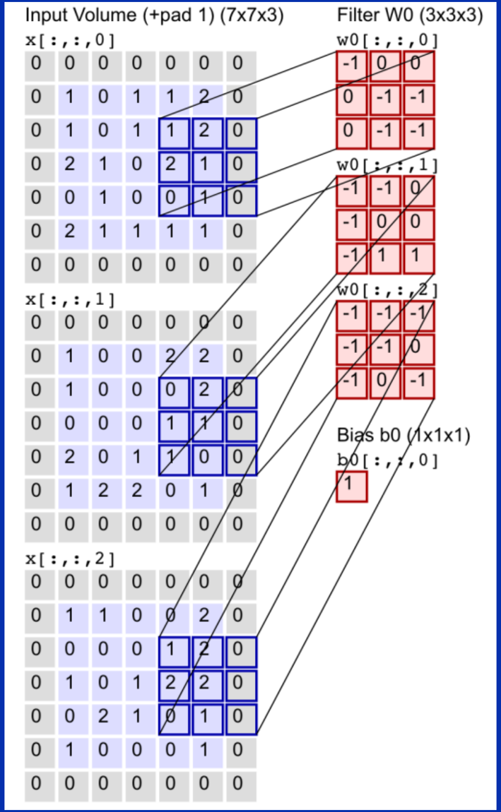




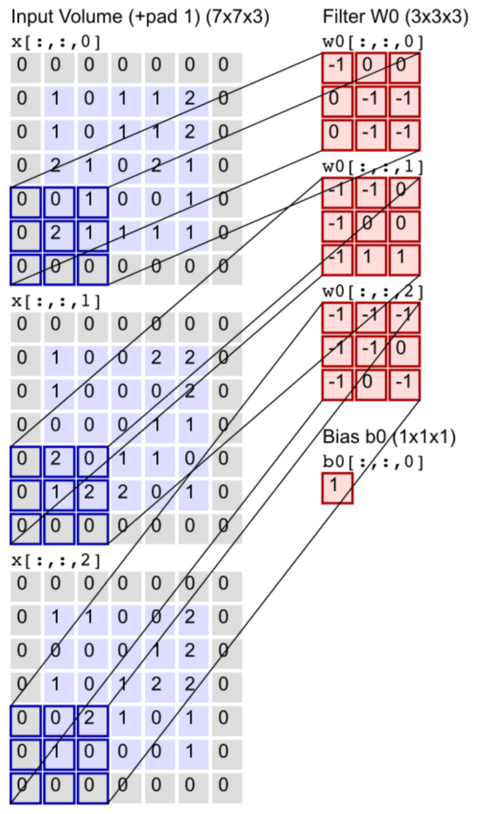
Convolutional filters or kernels

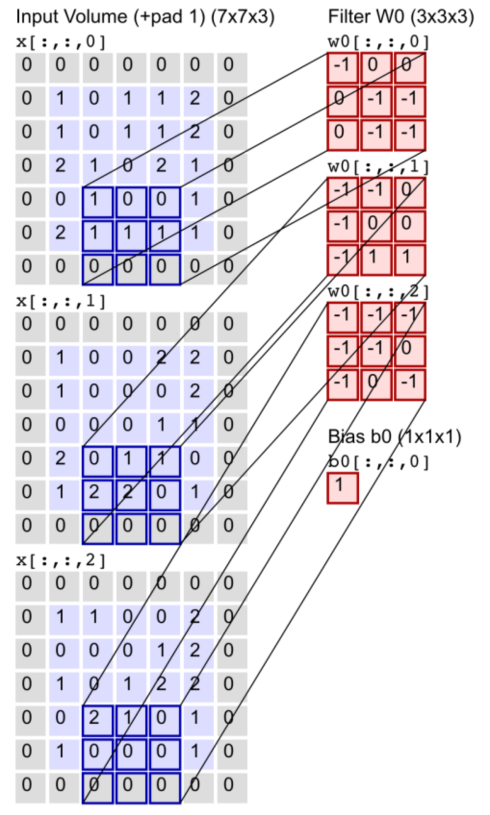


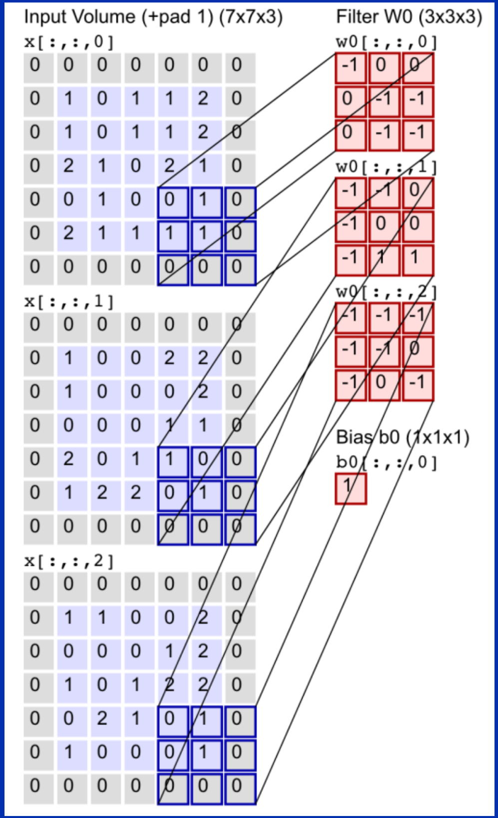




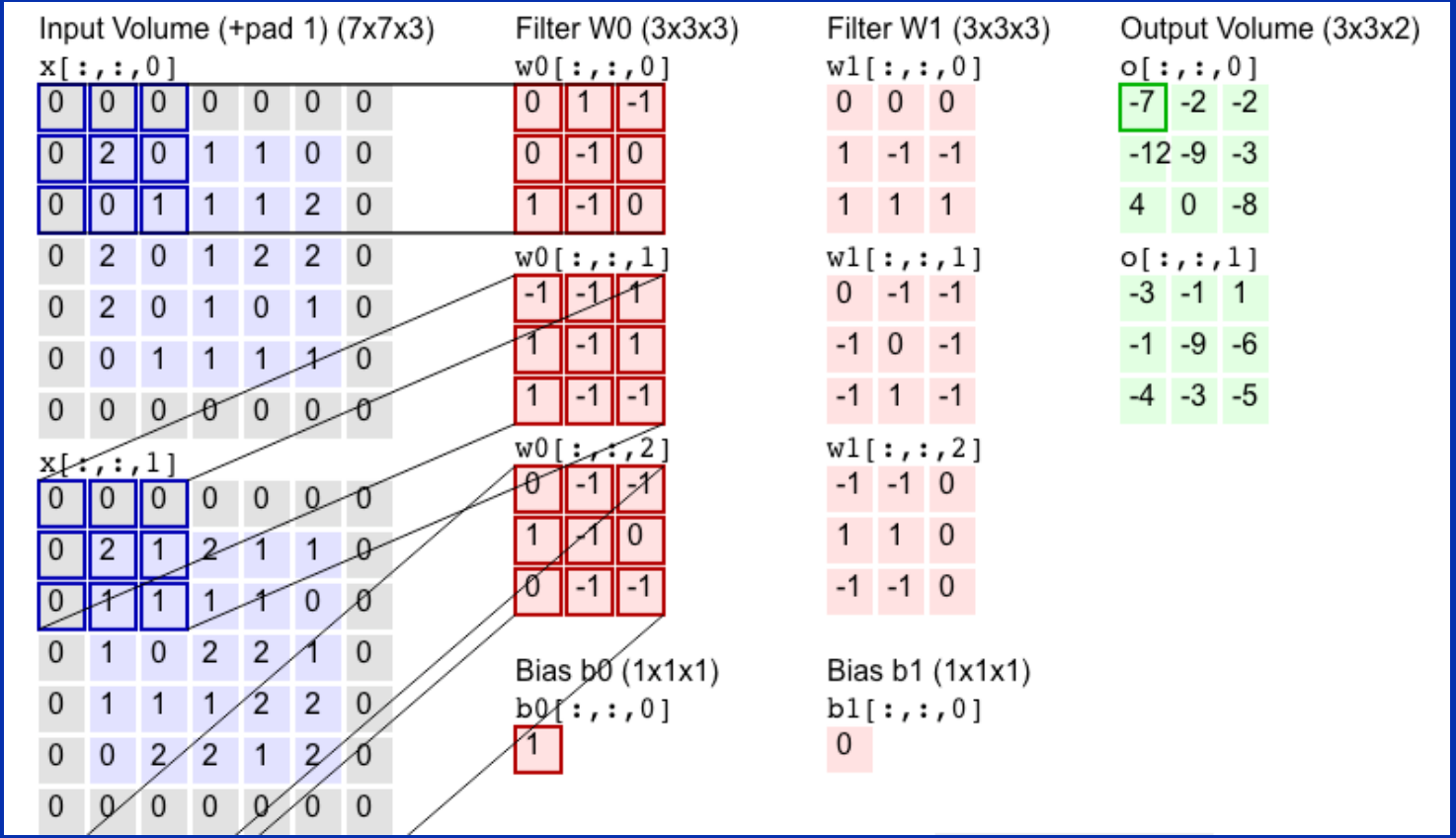
Convolutional filters or kernels







Convolutional layers



Pooling layers

Reduce activation map sizes and serve a regularization function

Most common is a 2 x 2 filter with strides (2,2) and taking the maximum of the four values as the new single value (“max pooling”)

This reduces the size of the activation map by 75% and helps reduce overfitting

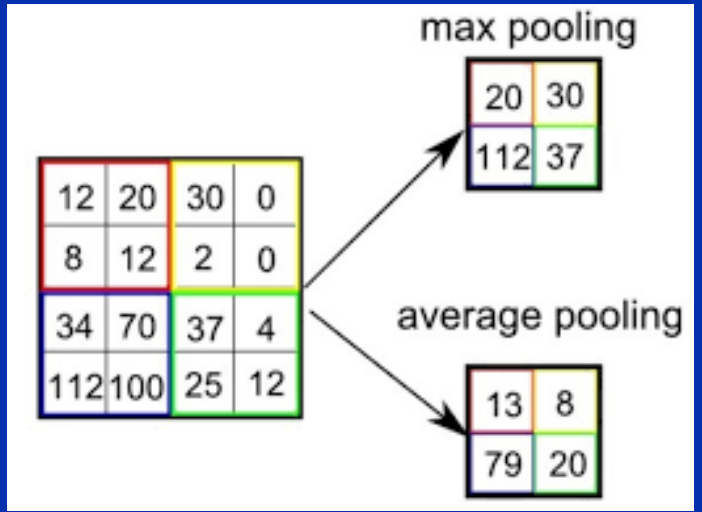
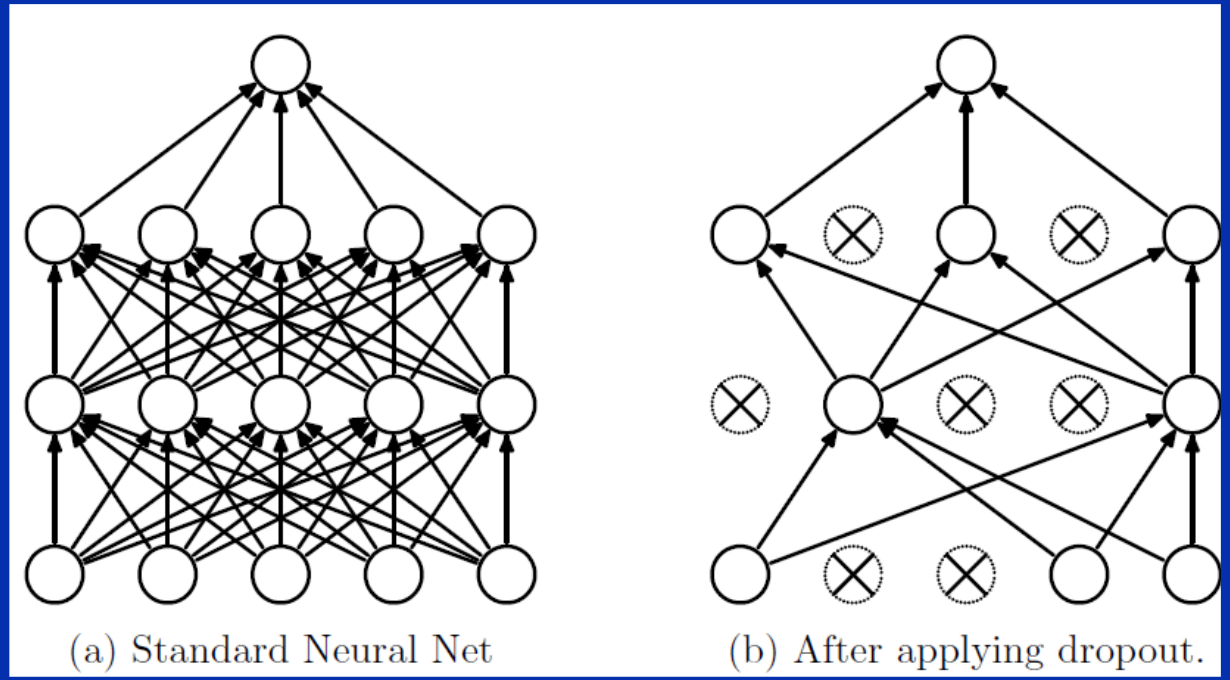


Diagram from quora.com

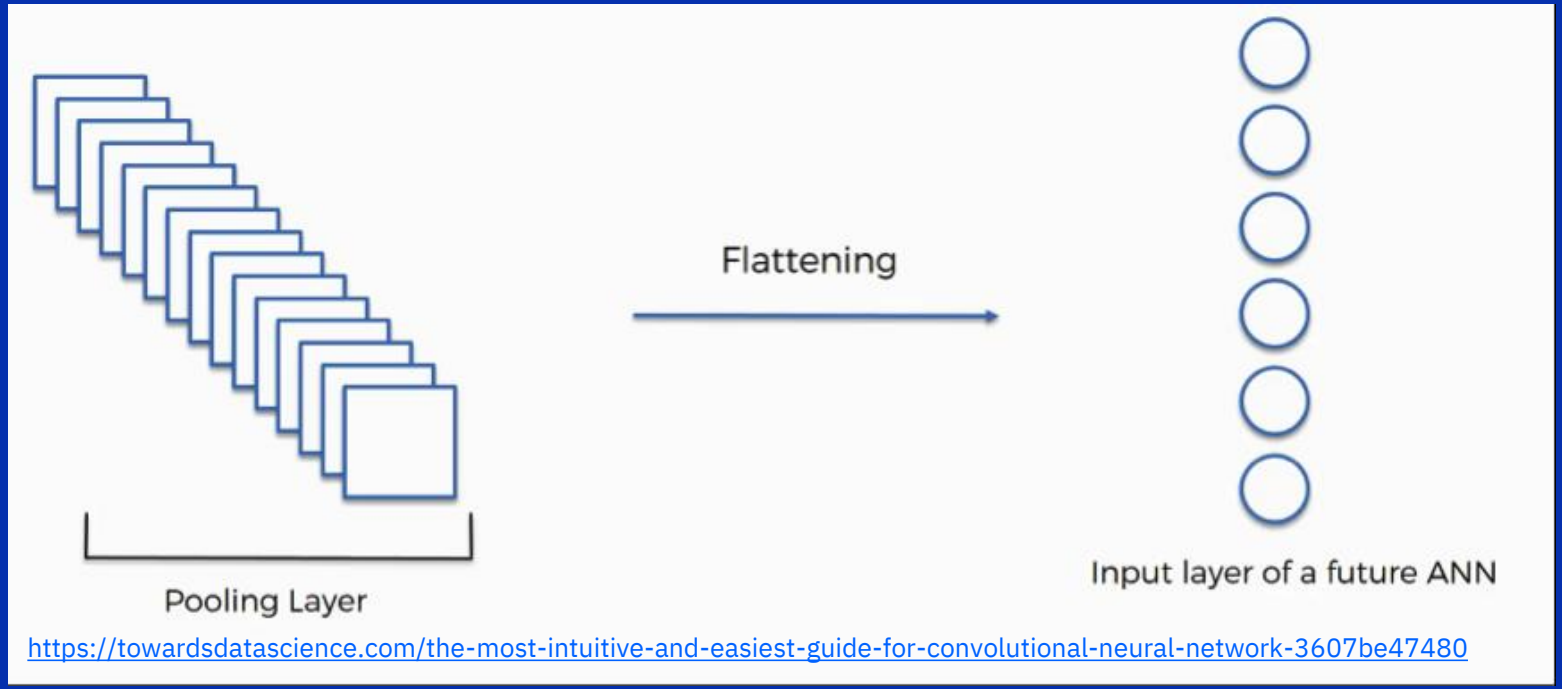
Dropout Layers

Also serve regularization function



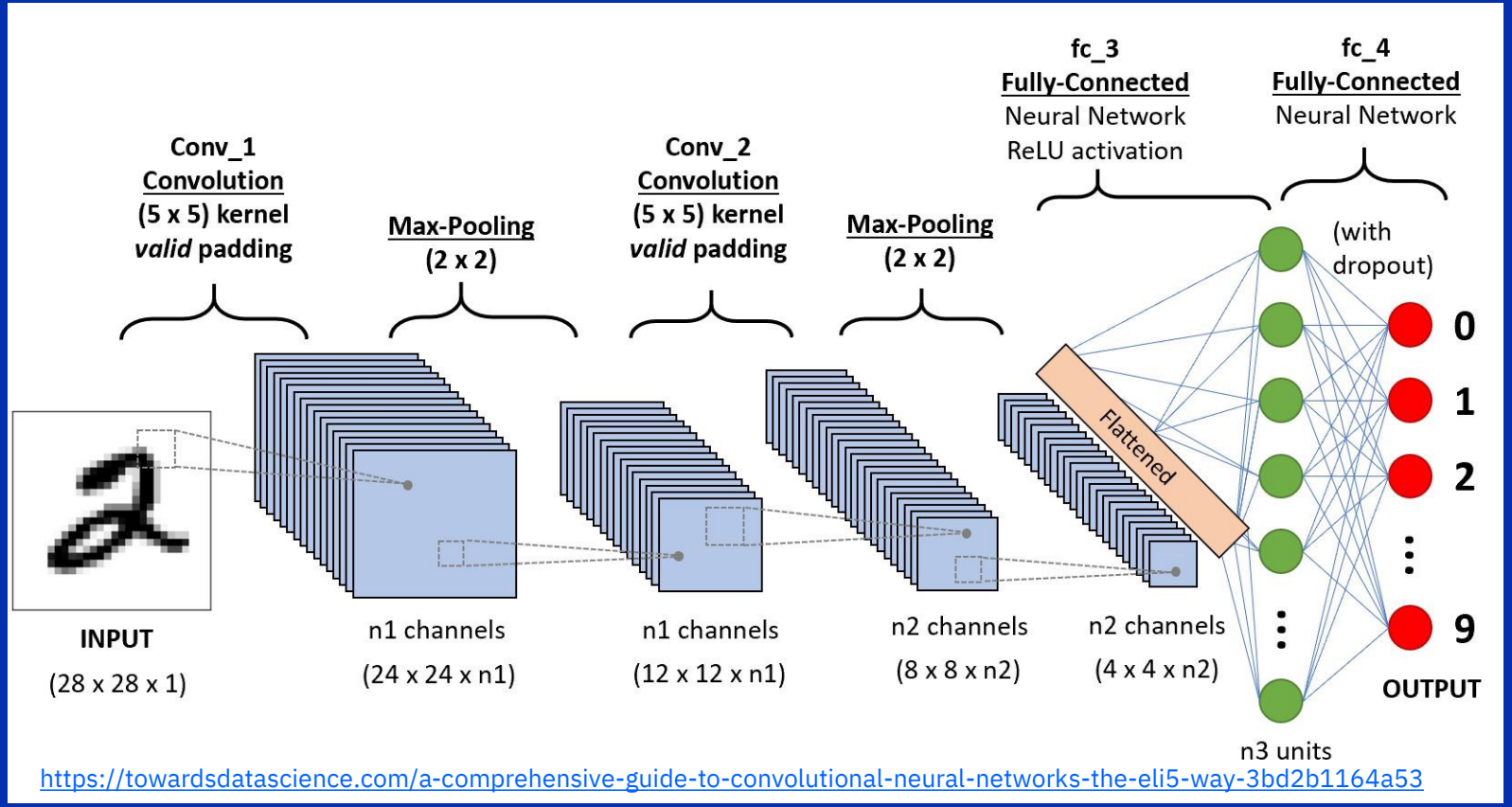
N. Srivastava, G. Hinton, A. Krizhevskiy, I. Sutskever, R. Salahutdinov Dropout: A simple way to prevent neural networks from overfitting. J. of Machine Learning Research 15 (2014) 1929-1958

Flattening layer



https://towardsdatascience.com/the-most-intuitive-and-easiest-guide-for-convolutional-neural-network-3607be47480

Convolutional Neural Networks



https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

Example Time!

Python notebook and flows in

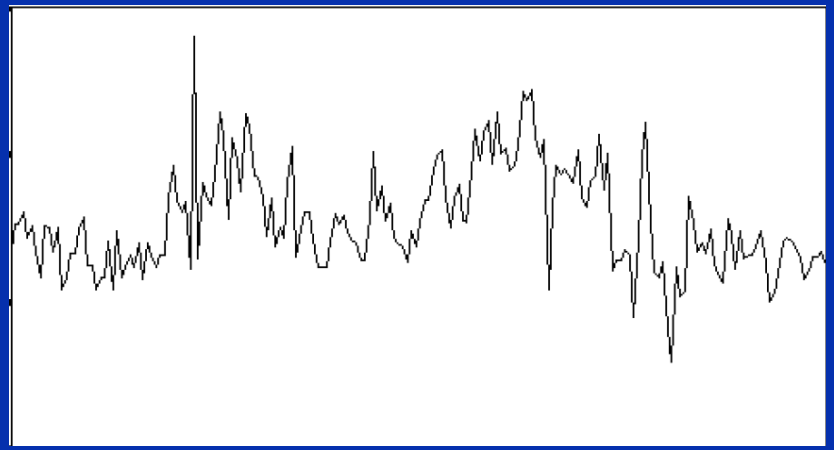
IBM Watson Studio

Recurrent Neural Networks

Recurrent Neural Networks (RNNs)

Some types of data inherently contain sequential aspects, such as:

Time series data



Text data

Great acting! Amazing special effects!
Best movie I've seen in a long time.

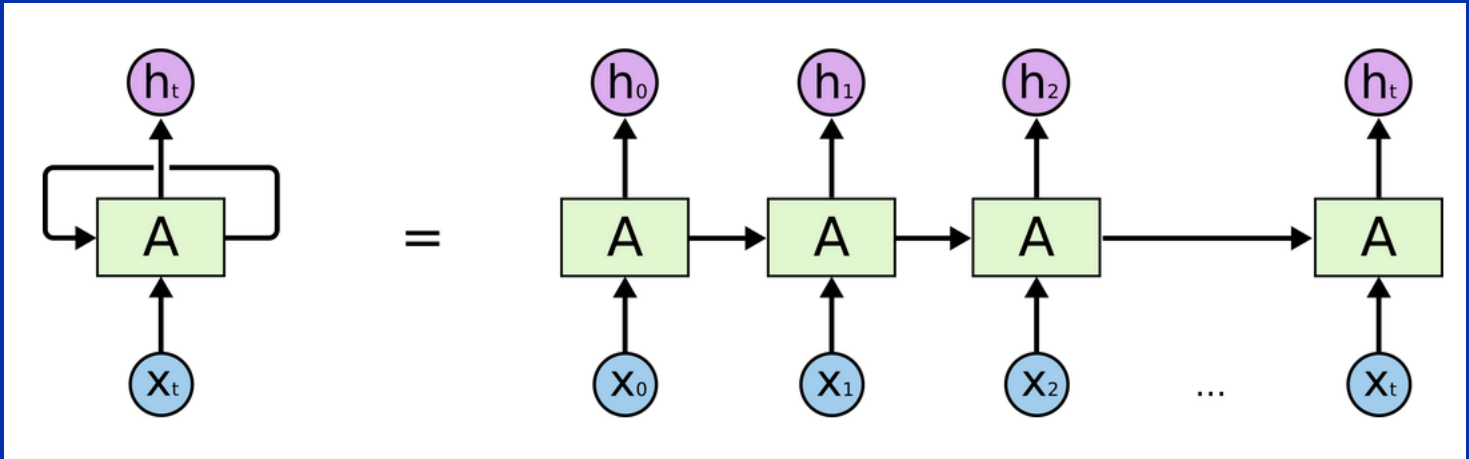
Who let that guy get hold of a camera?
What a mess! I could have had a nice nap
if the noises weren't so irritating.

Recurrent Neural Networks (RNNs)

RNN structures typically include the following types of layers:

- Embedding (if analyzing text data)
- Recurrent
- Fully connected or dense

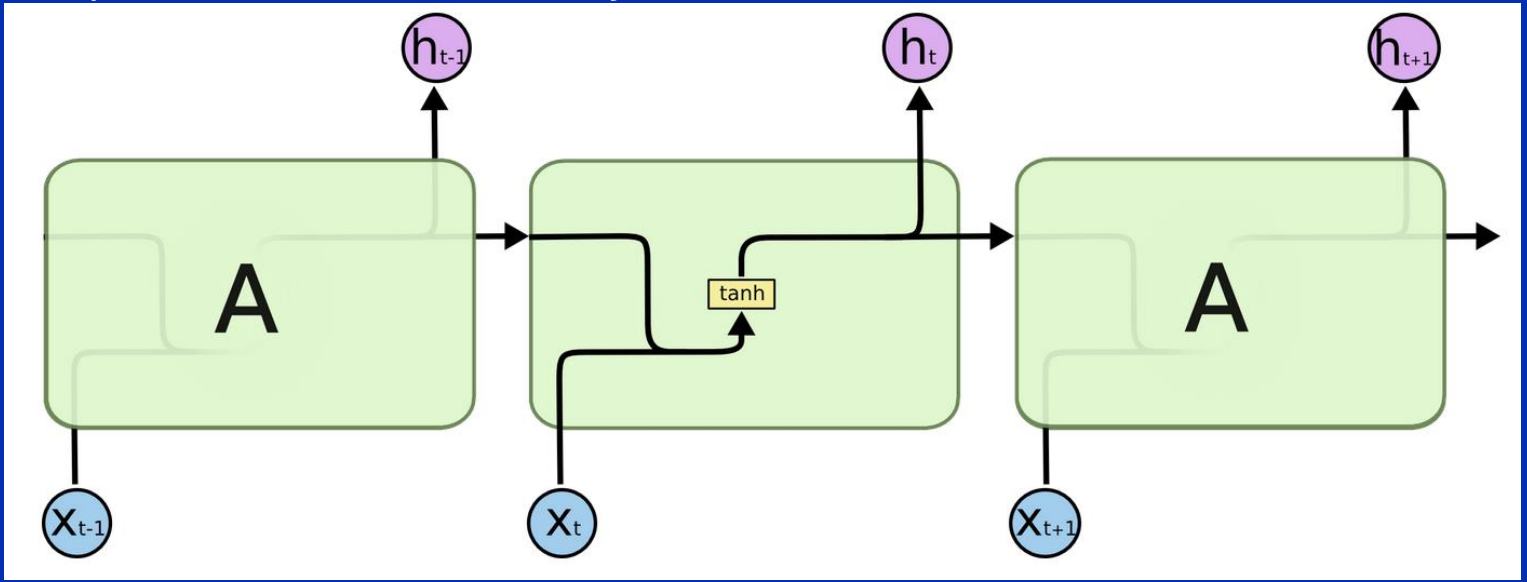
Recurrent Neural Networks (RNNs)



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

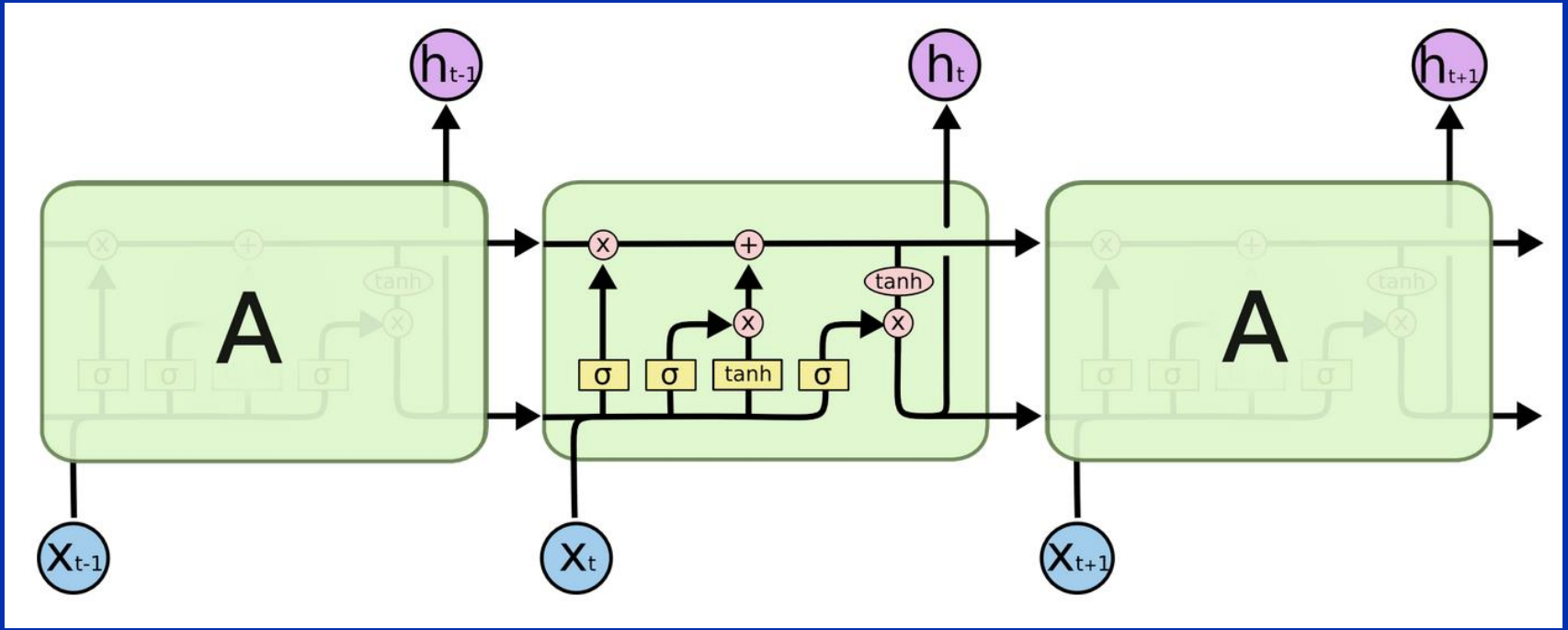
Recurrent Neural Networks (RNNs)

Simple recurrent network layer structure



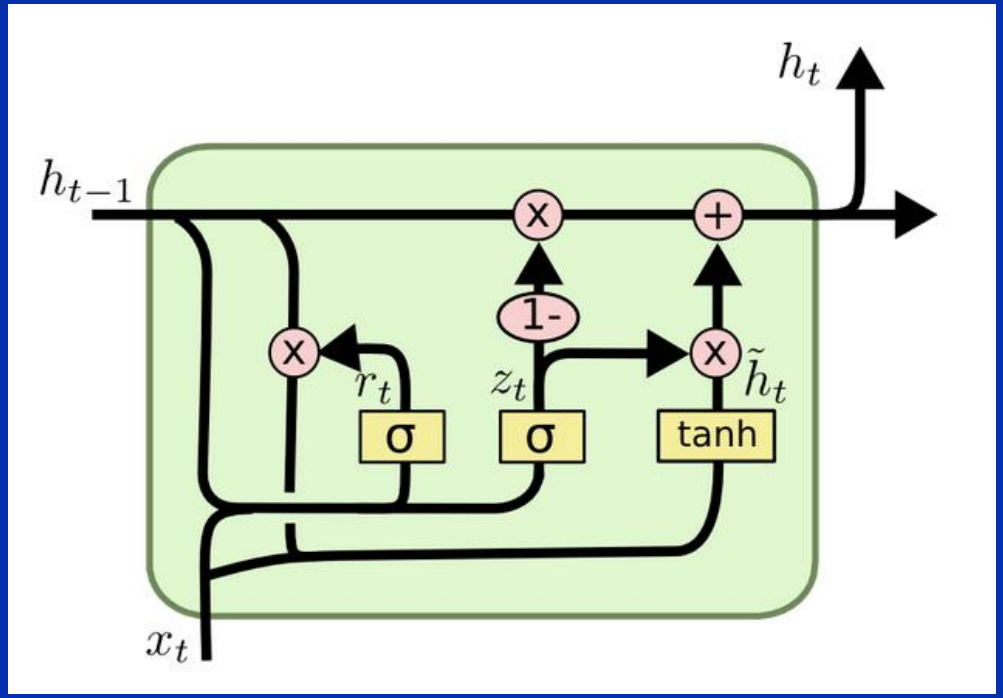
https://colah.github.io/posts/2015-08-Understanding-LSTMs/

Long Short-Term Memory (LSTM) RNNs



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

Gated Recurrent Unit (GRU) RNNs



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

Example Time!

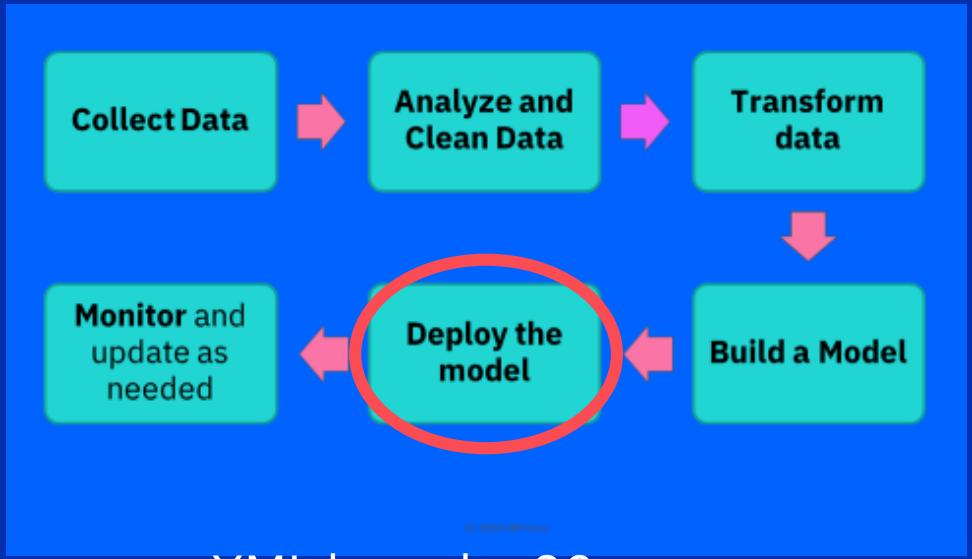
RStudio in IBM Watson Studio

Model deployment

Model deployment

Challenges:

- Different Teams
- Different environments
- Need to keep data prep steps



Solutions: open standards

PMML: Predictive Model Markup Language – XML based, >20 years

PFA: Portable Format for Analytics, JSON based, ~5 years

ONNX: Open Neural Network eXchange, Protobuf, < 2 years

Or Docker containers

What are PMML and PFA?

XML and JSON for model exchange and deployment

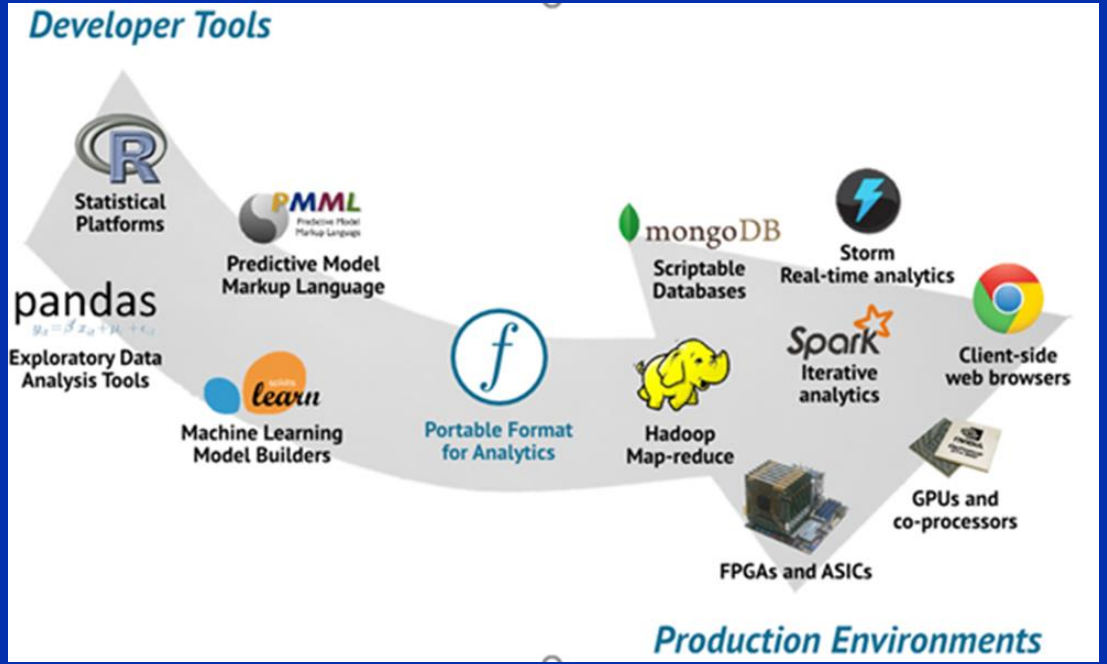
PMML 0.7 in 1997, 1.1 in 2000, 4.4 in 2019

Used by >30 companies and OS packages

dmg.org/pmml

PFA – small math programming language

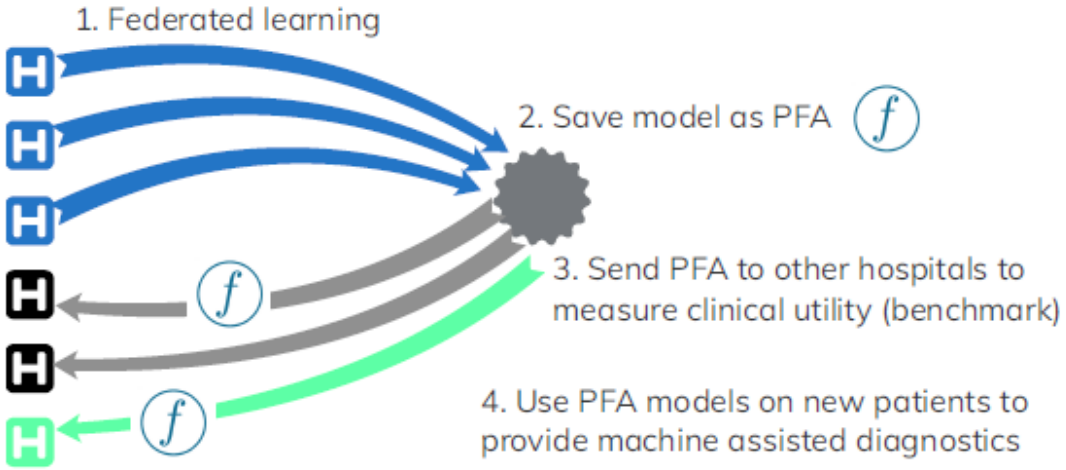
dmg.org/pfa



Use of PMML and PFA in medical applications

Human Brain Project

Ludovic Claude,
CHUV
Lausanne,
Switzerland



ONNX: Open Neural Network eXchange

Since 2017

Protobuf

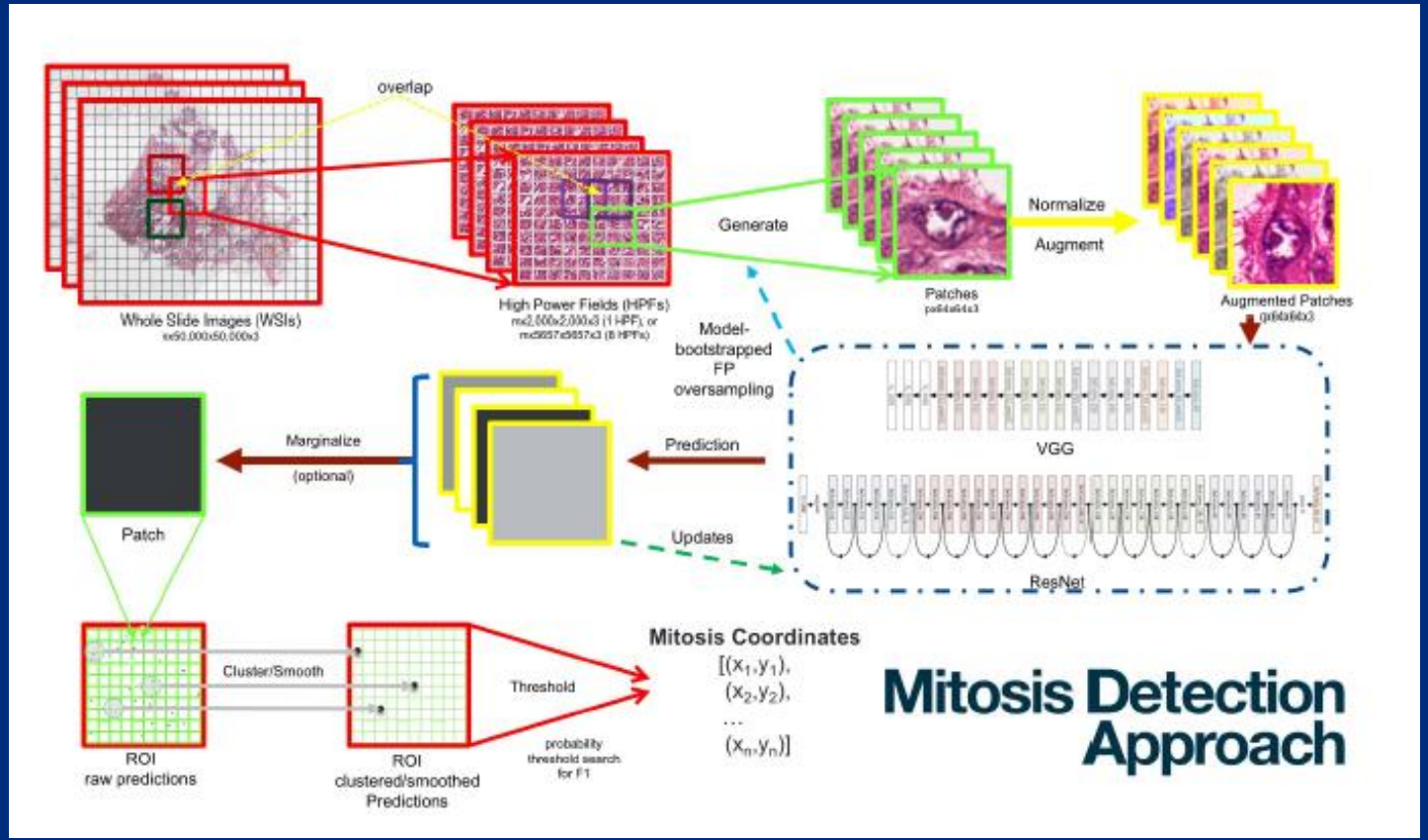
Covers DL and traditional ML

Active work by many companies

Using ONNX in medical image processing: potential applications

MAX

ibm.biz/
model-exchange

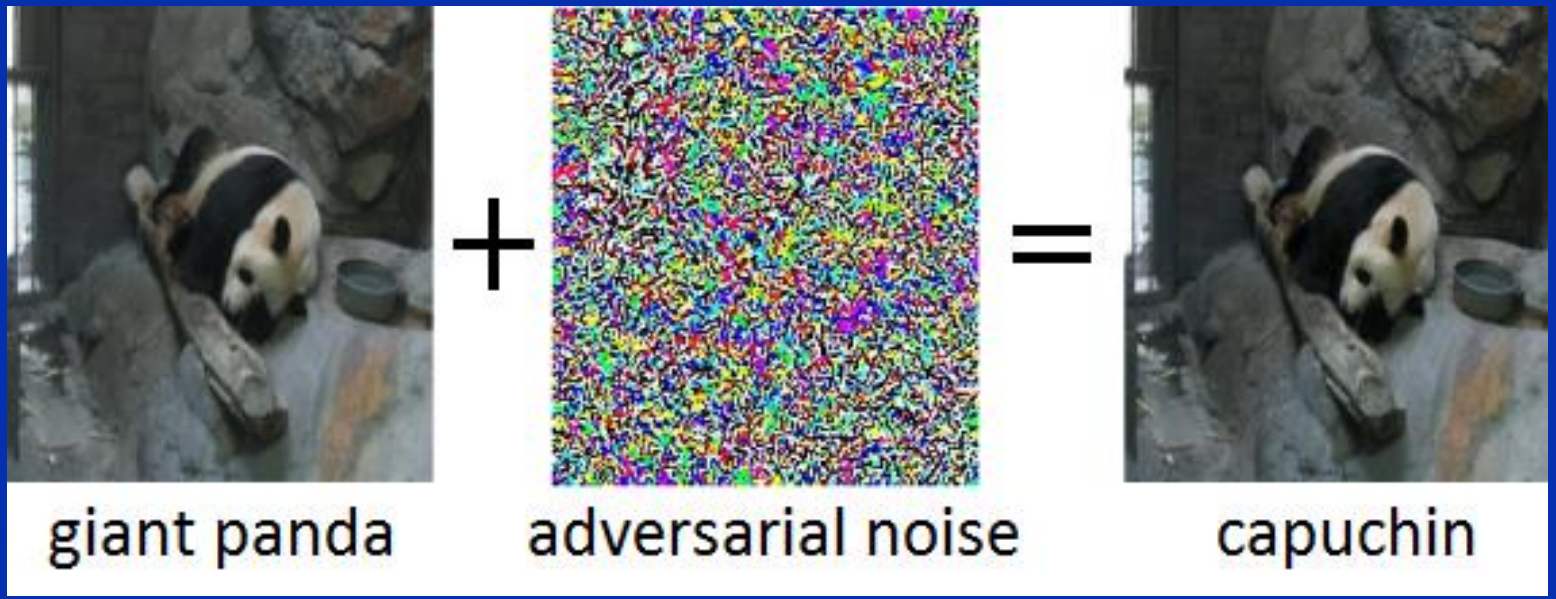


Adversarial Robustness

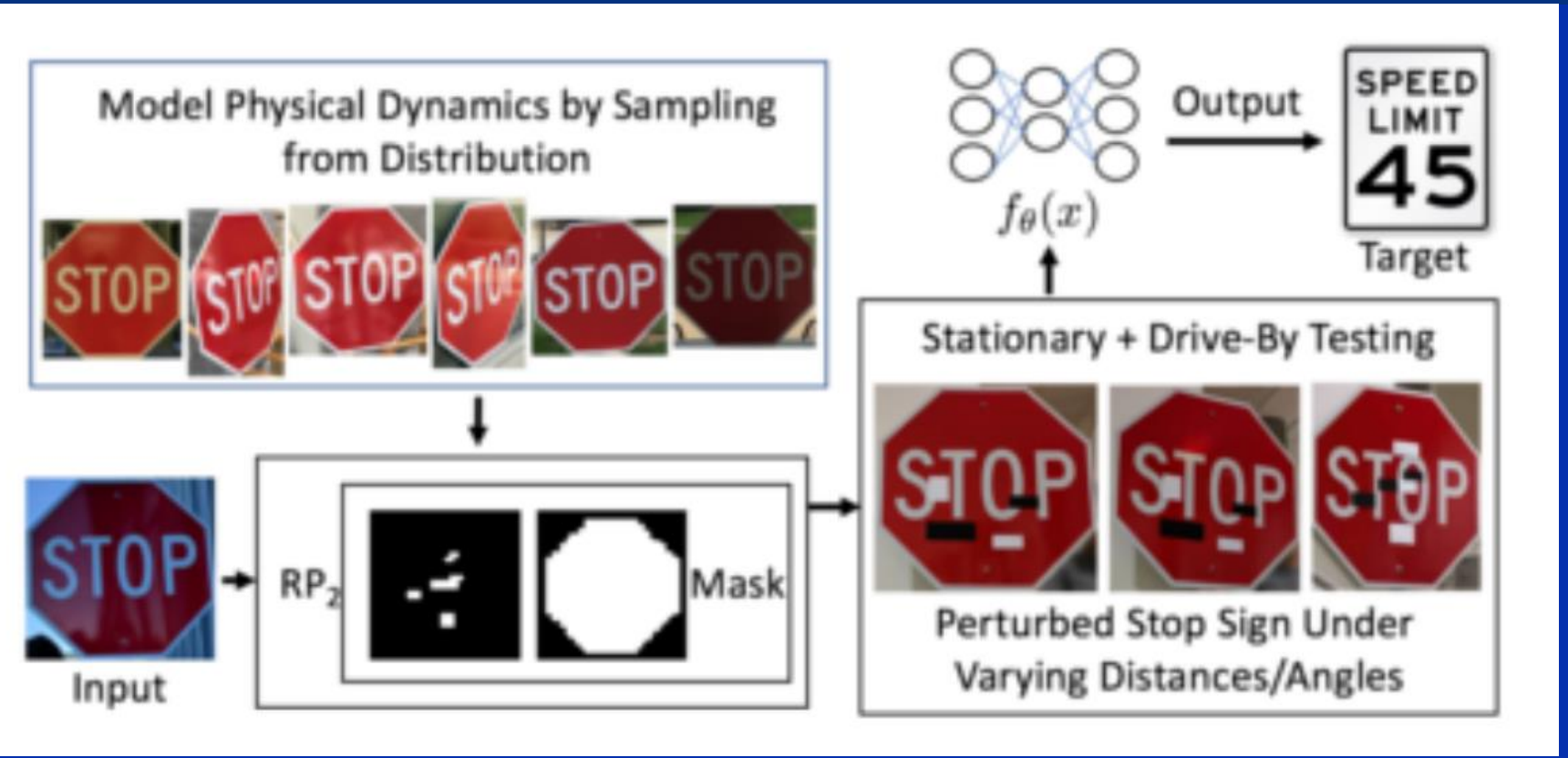
Deep learning and adversarial attacks

Deep Learning models are now used in many areas

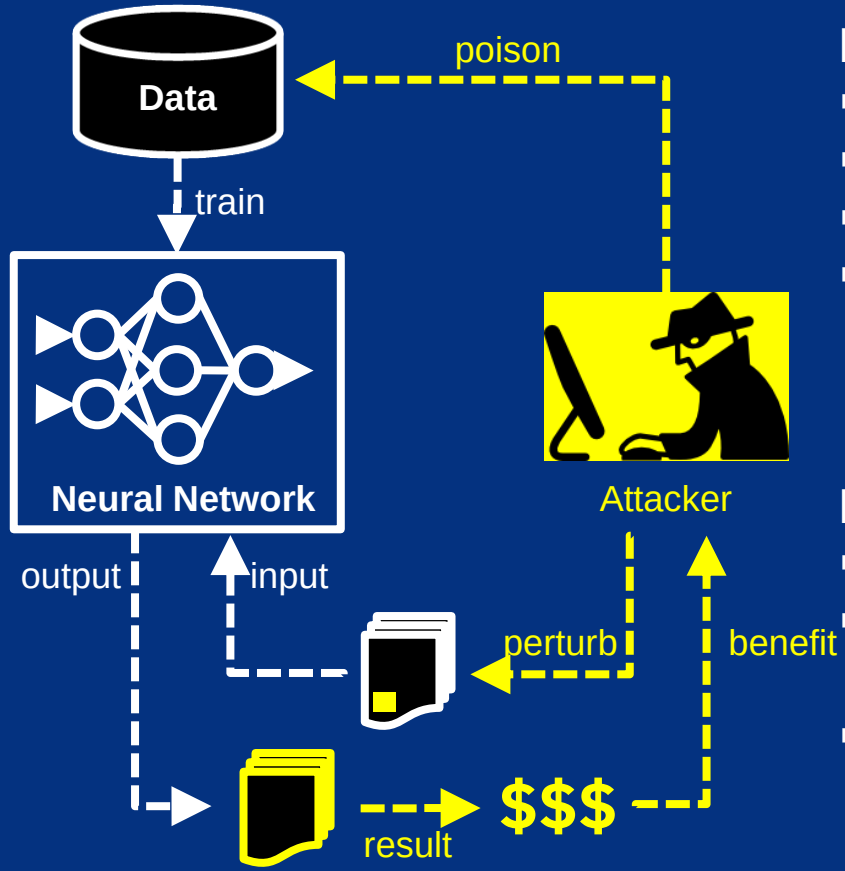
Can we trust them?



Scarier example



Adversarial Threats to AI



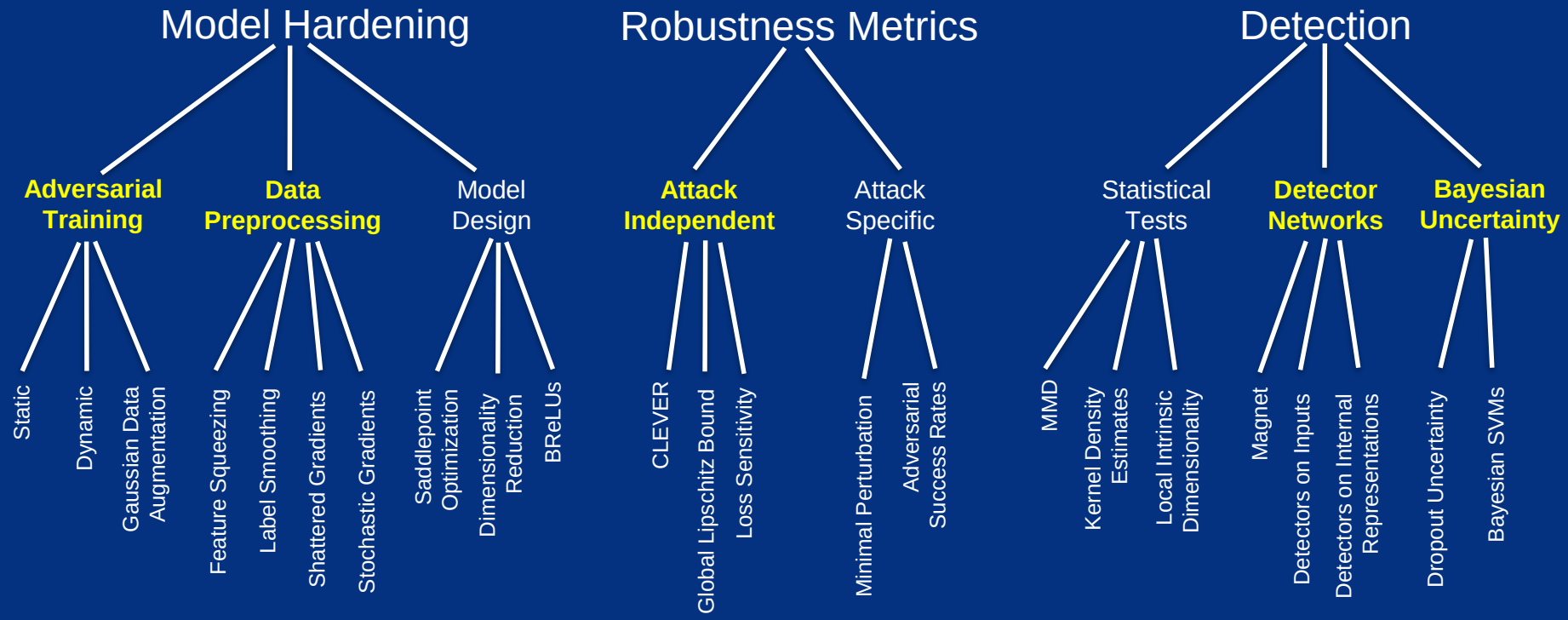
Evasion attacks

- Performed at test time
- Perturb inputs with crafted noise
- Model fails to predict correctly
- Undetectable by humans

Poisoning attacks

- Performed at training time
- Insert poisoned sample in training data
- Use backdoor later

How to defend?
Taxonomy of defenses

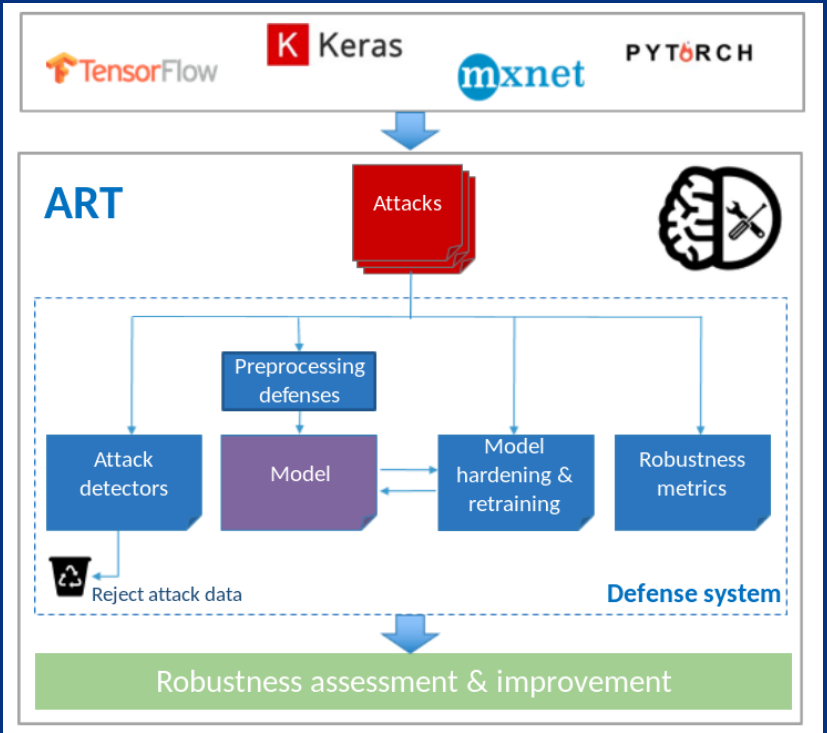


The Adversarial Robustness Toolbox (ART)

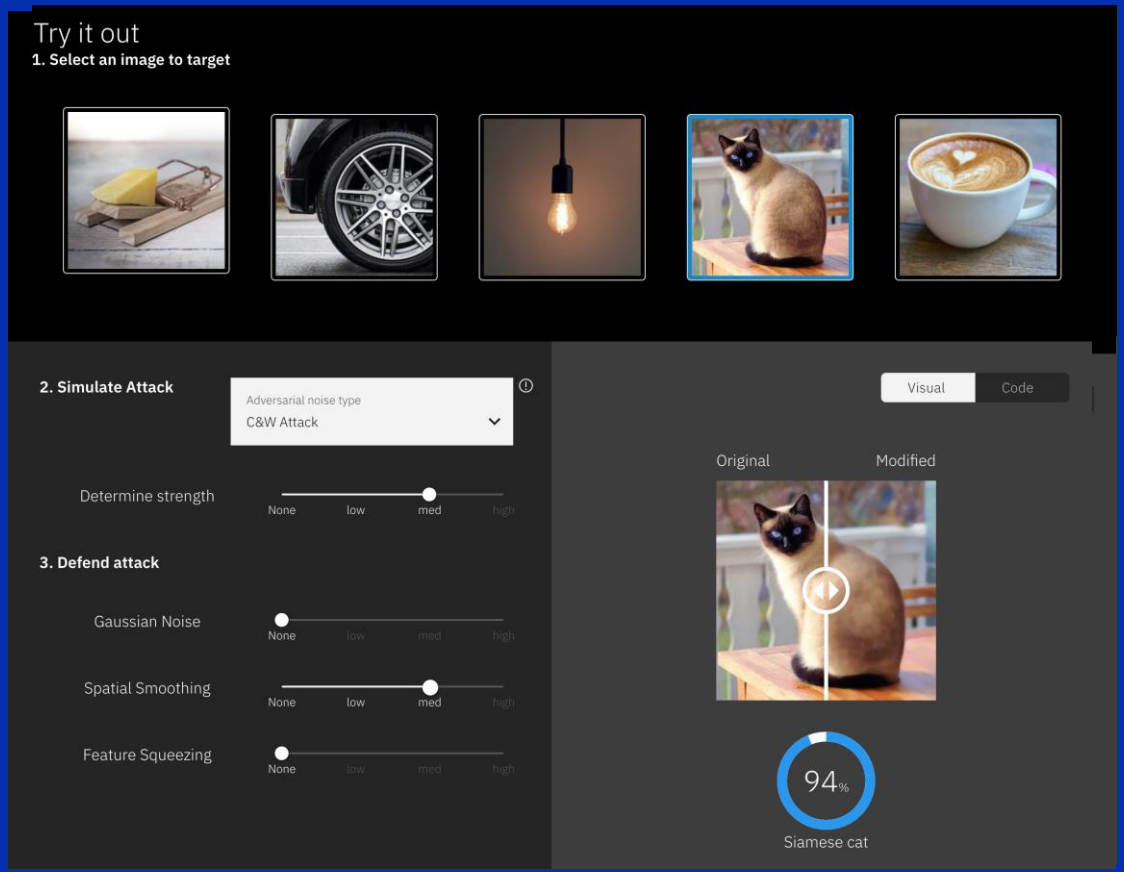
- Library for **adversarial machine learning**
- Baseline implementation of attacks and defenses for classifiers
- Dedicated to images

- MIT license
- Supported frameworks:

TensorFlow PYTORCH Keras mxnet



ART Demo: https://art-demo.mybluemix.net/



AI Fairness 360

Are computer-generated results free of bias?

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Prediction Fails Differently for Black Defendants

	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

Overall, Northpointe's assessment tool correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labeled a higher risk but not actually re-offend. It makes the opposite mistake among whites: They are much more likely than blacks to be labeled lower risk but go on to commit other crimes. (Source: ProPublica analysis of data from Broward County, Fla.)

AIFairness 360

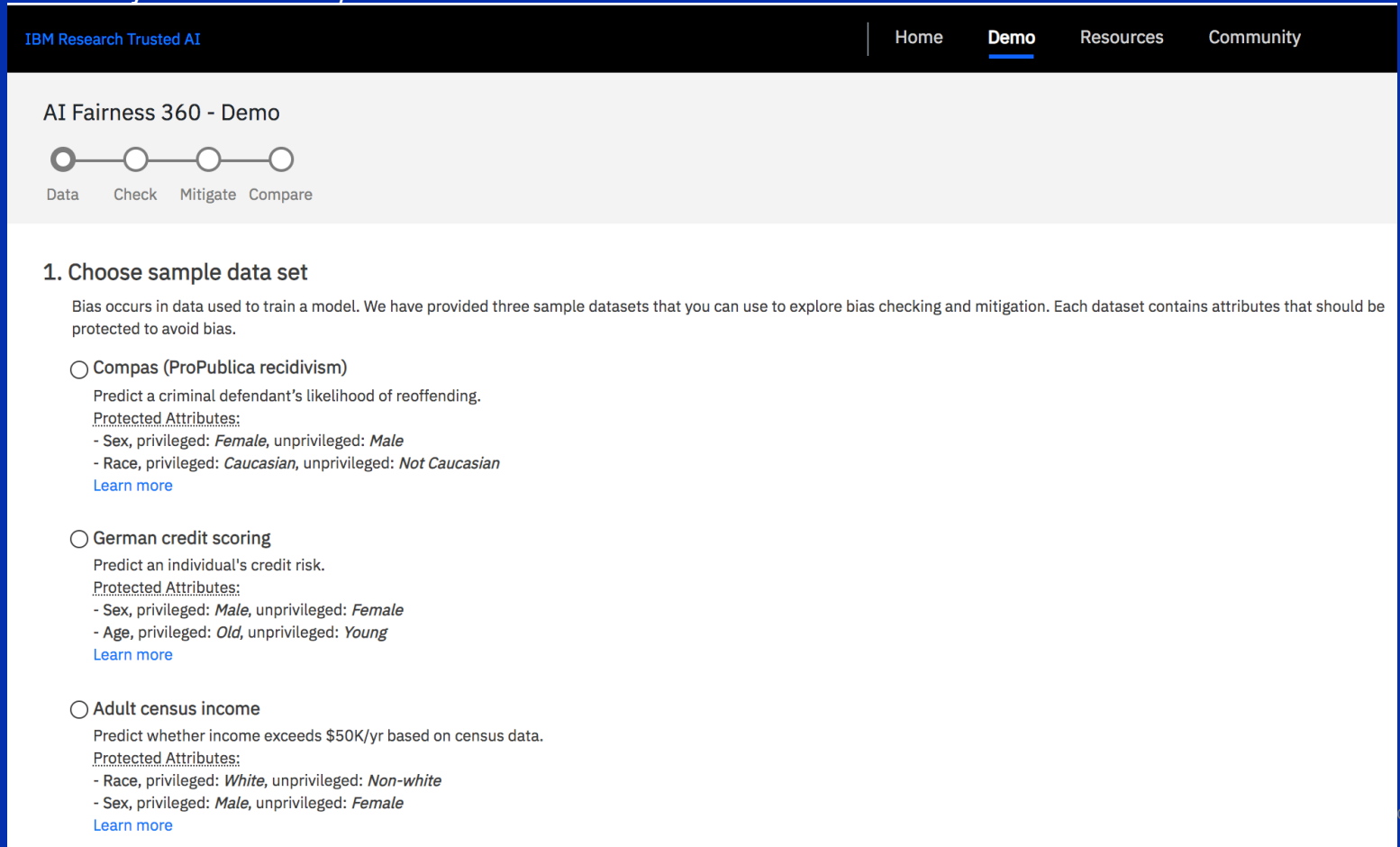
Open source Python library

70+ Fairness metrics and explanations

10 Bias mitigation algorithms

Demo Application: AI Fairness 360 Web Application

http://aif360.mybluemix.net/



2. Check bias metrics

Dataset: Adult census income

Mitigation: none

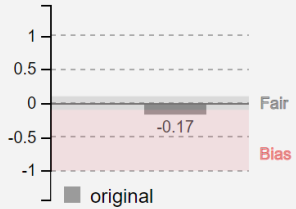
Protected Attribute: Race

Privileged Group: ***White***, Unprivileged Group: ***Non-white***

Accuracy with no mitigation applied is 82%

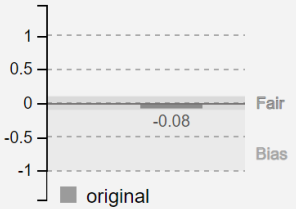
With default thresholds, bias against unprivileged group detected in 2 out of 5 metrics

Statistical Parity Difference

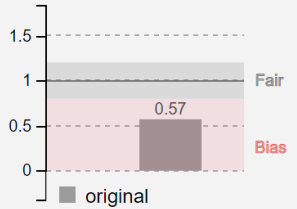


Equal Opportunity Difference

Average Odds Difference

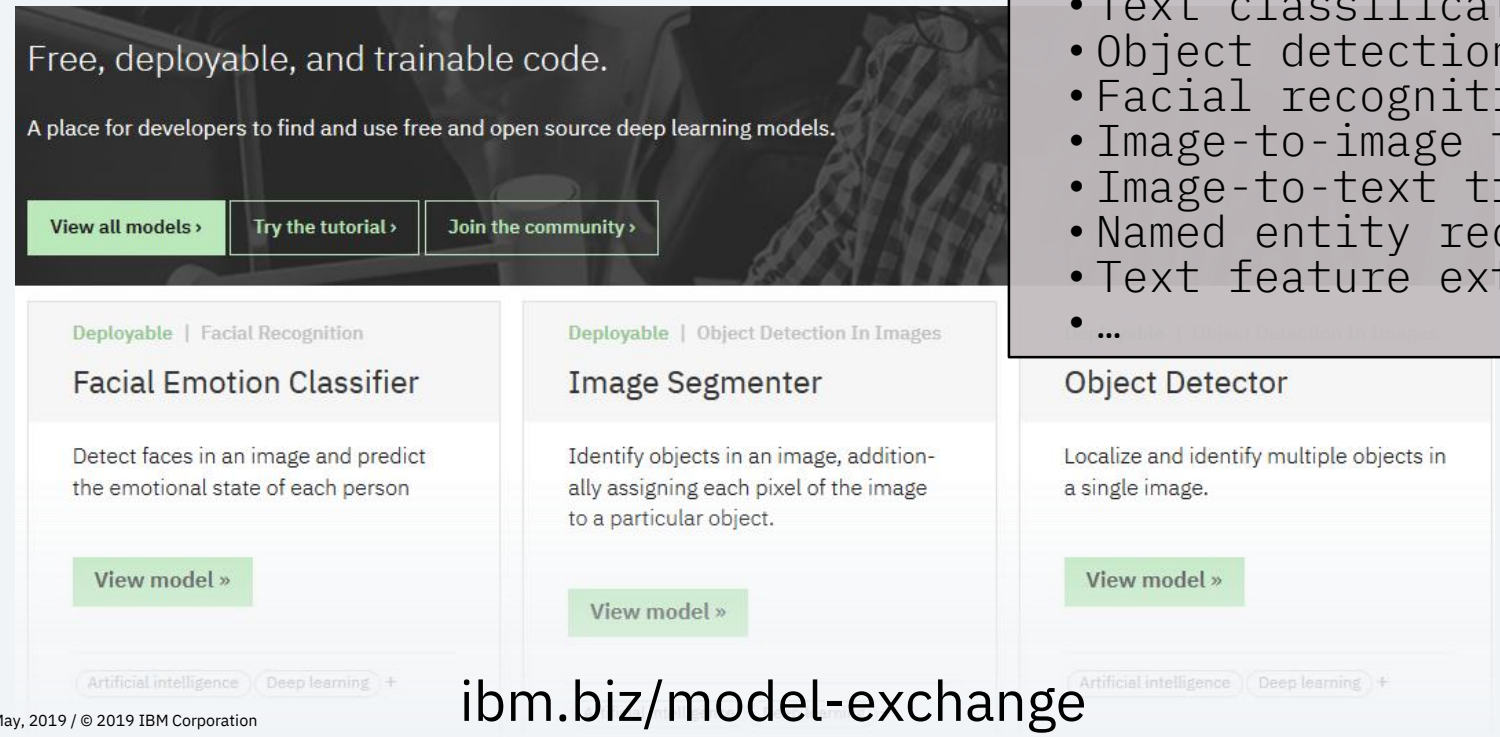


Disparate Impact



MAX: Reduces “time to value” for developers

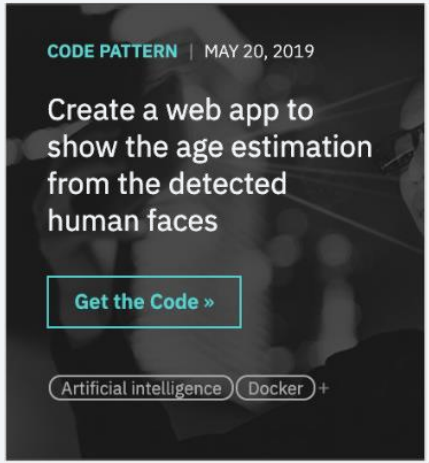
Find model asset → Deploy pre-trained model asset → Use model asset

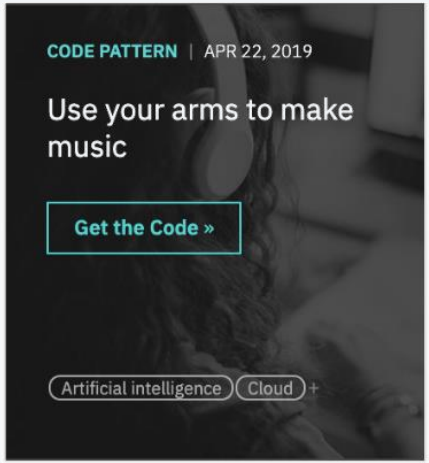


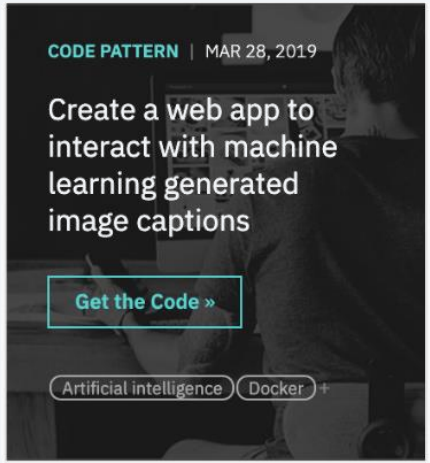
- Audio classification
- Image classification
- Text classification
- Object detection
- Facial recognition
- Image-to-image translation
- Image-to-text translation
- Named entity recognition
- Text feature extraction
- …

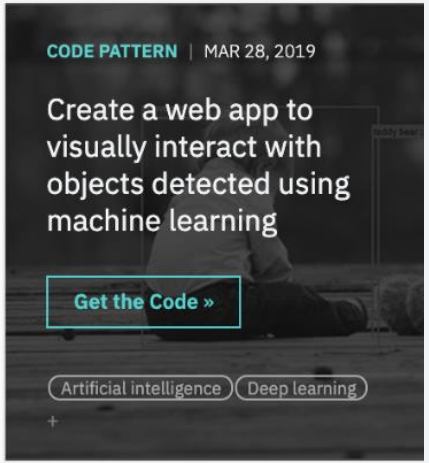
ibm.biz/model-exchange

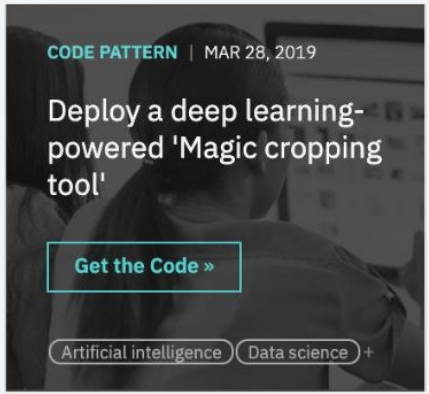
↳ Deep Learning Code Patterns

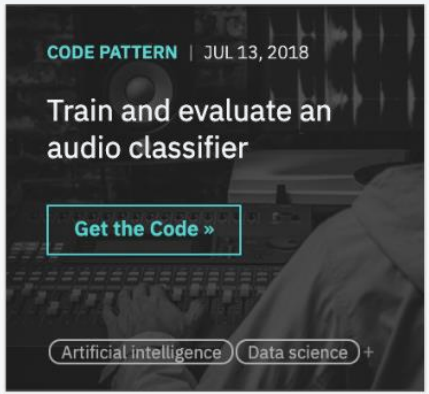








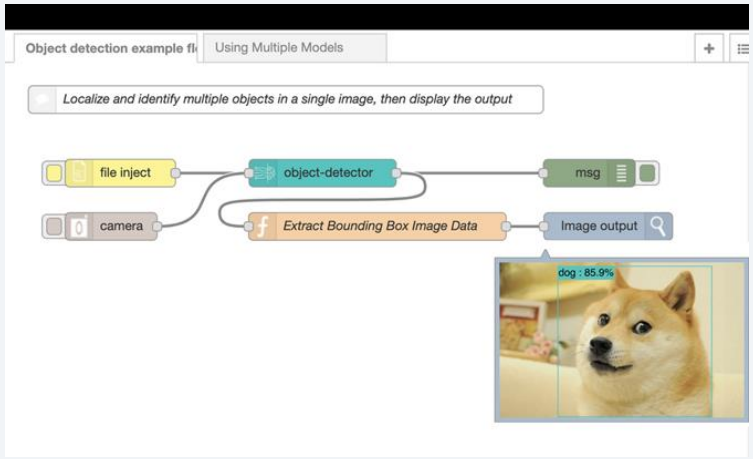


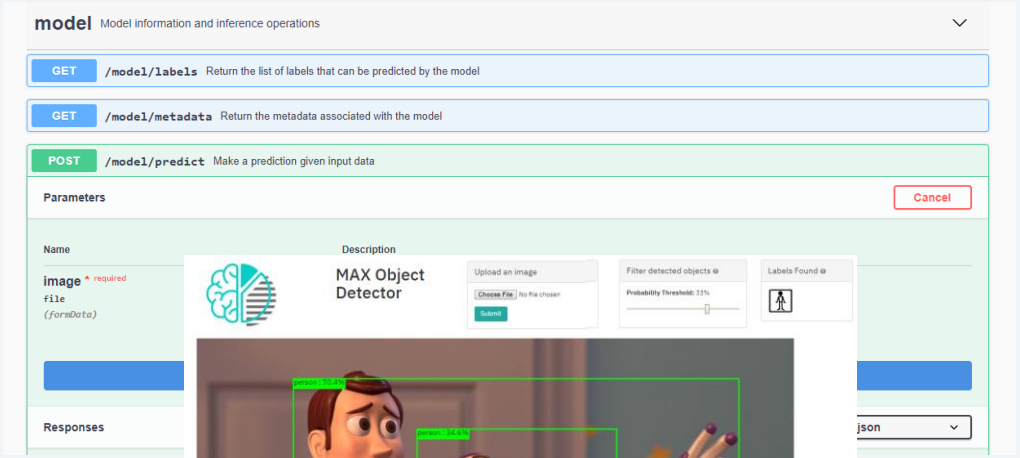


https://developer.ibm.com/patterns/category/model-asset-exchange/

MAX Consumption scenarios

- Model-serving microservice (Docker-based)
- Internet of Things: Node-RED
- JavaScript/Node.js packages



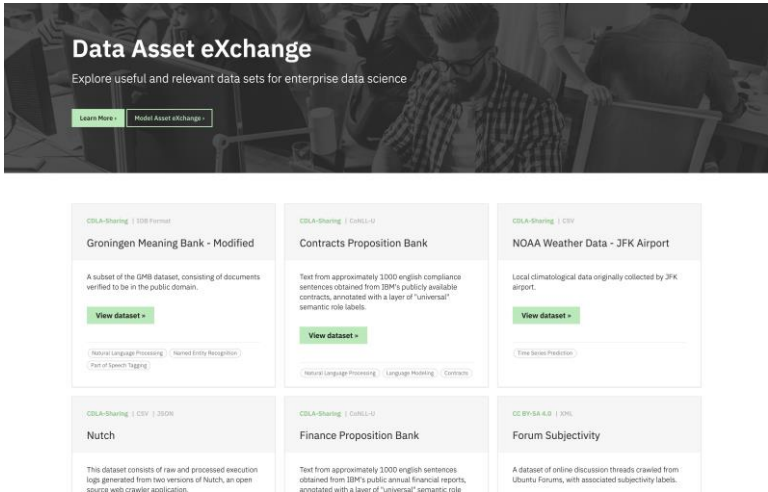


IBM Data Asset eXchange (DAX)

- Curated free and open datasets under open data licenses
- Standardized dataset formats and metadata
- Ready for use in enterprise AI applications
- Complement to the Model Asset eXchange (MAX)

Data Asset eXchange
ibm.biz/data-asset-exchange

Model Asset eXchange
ibm.biz/model-exchange



Conclusions

Deep neural networks are used widely

IBM Watson Studio provides tools for model building, deployment, monitoring, as well as detection and remediation of bias and adversarial attacks

MAX models are ready to use in a variety of applications

Learn more on deep learning

Watson Studio: sign up for IBM Cloud: https://ibm.biz/Bdz4N5

Codait.org Onnx.ai @SvetaLevitan @dpnichols

AIFairness 360: https://github.com/IBM/AIF360

ART: https://github.com/IBM/adversarial-robustness-toolbox

MAX: ibm.biz/model-exchange