

Machine Learning in Engineering: Panacea or Deep Trouble ?

Kostas Plataniotis

ECE Department

www.dsp.utoronto.ca

Concordia University

Montreal, QC,

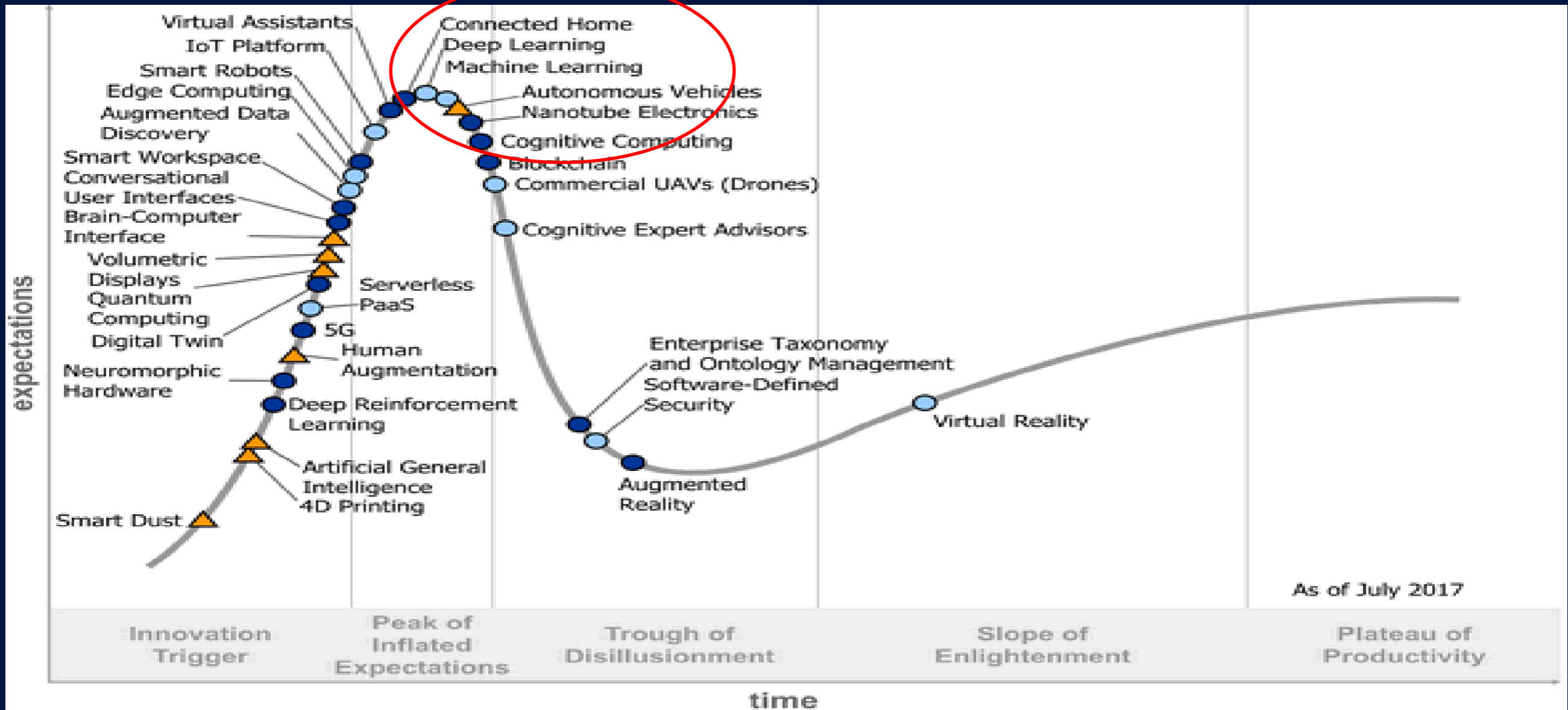
Thursday, August 9, 2018



What this presentation is all about ?

A personal account of (some) key issues in the emerging field of machine learning
(relevant to our engineering practice)

The “hype cycle” (2017-Gartner) (in emerging technologies)



As of July 2017

Plateau will be reached:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

© 2017 Gartner, Inc.

“Priority Matrix” in data science and machine learning (2017-Gartner)

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational		Augmented Data Discovery Deep Learning Event Stream Processing Machine Learning	Algorithm Marketplaces Citizen Data Science Cognitive Computing Conversational Analytics	Artificial General Intelligence Human-in-the-Loop Crowdsourcing
high	Ensemble Learning Model Management Video/Image Analytics	AutoML Guided Analytics Predictive Analytics Self-Service Data Preparation	Graph Analytics IoT Edge Analytics Optimization Prescriptive Analytics Speech Analytics	
moderate		Notebooks Spark Text Analytics	Advanced Anomaly Detection Data Lakes Embedded Analytics Python Simulation	
low				

As of August 2017

© 2017 Gartner, Inc.

“Priority Matrix” in emerging technologies (2017-Gartner)

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational		Augmented Data Discovery Cognitive Expert Advisors Deep Learning Edge Computing IoT Platform Machine Learning Software-Defined Security	Blockchain Cognitive Computing Conversational User Interfaces Deep Reinforcement Learning Digital Twin Nanotube Electronics Smart Workspace Virtual Assistants	4D Printing Artificial General Intelligence Autonomous Vehicles Brain-Computer Interface Human Augmentation Smart Dust
high		Commercial UAVs (Drones)	5G Augmented Reality Connected Home Neuromorphic Hardware Smart Robots	Quantum Computing
moderate		Serverless PaaS Virtual Reality	Enterprise Taxonomy and Ontology Management	Volumetric Displays
low				

As of July 2017

© 2017 Gartner, Inc.



Outline

- **A definition (or two)**
- Altum Visum on deep learning networks
- Machine Learning: Myths & Realities
- Machine Learning as a process
- Explainable Artificial Intelligence
- Epilogue



It's all Greek to me

How we learn / know something:

- **Techné** (skill) - Knowing by doing. A carpenter learns to build by building, a potter by making pots.
- **Epistemé** (science) - Knowing by demonstration. Scientific facts are capable of being repeatedly demonstrated.
- **Nous** (intuition) - Knowing without the demonstration of invariable facts.

Nicomachean Ethics - Aristotle



It's still Greek to me

The pertinent questions :

what are we learning and why?

The Aristotelian answer:

The goal of **episteme** is to know truth from falsehood. The goal of **phronesis (nous)** is to know good from bad, and the goal of **techné** is to know how to express and appreciate beauty.

The Aristotelian view:

Each of these kinds of knowledge is a uniquely human capacity, thus the aim of learning is to help human beings become more fully human.

Nicomachean Ethics - Aristotle



(Lay) Definitions – I

Learning: The activity or process of gaining knowledge or skill by studying, practicing, being taught, or experiencing something. (Merriam Webster Dictionary).

Machine: a mechanically, electrically, or electronically operated device for performing a task. Archaic : a constructed thing whether material or immaterial. (Merriam Webster Dictionary).

(Lay) Definitions - II

- **Artificial Intelligence (AI)**: the broader concept of machines being able to carry out tasks in a way that we would consider “smart”.¹
- **Machine Learning (ML)**: a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves.¹

¹ Bernard Marr, What Is The Difference Between Artificial Intelligence And Machine Learning?, Forbes Magazine, accessed online, December 6, 2016.



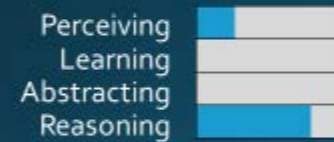
Artificial Intelligence Waves

Three waves of AI



Handcrafted Knowledge
Statistical Learning
Contextual Adaptation

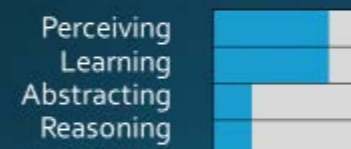
The first wave of AI



Enables reasoning over narrowly defined problems

No learning capability and poor handling of uncertainty

The second wave of AI



Nuanced classification and prediction capabilities

No contextual capability and minimal reasoning ability



Artificial Intelligence Waves

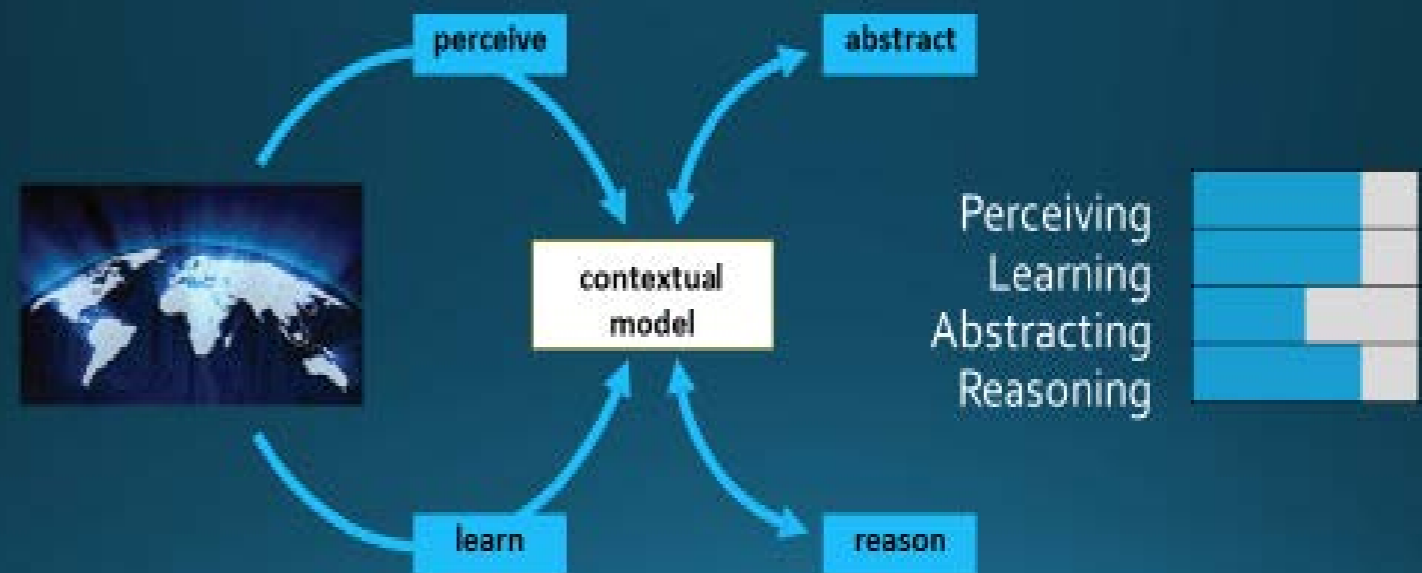
The (future) third wave of AI



Contextual adaptation

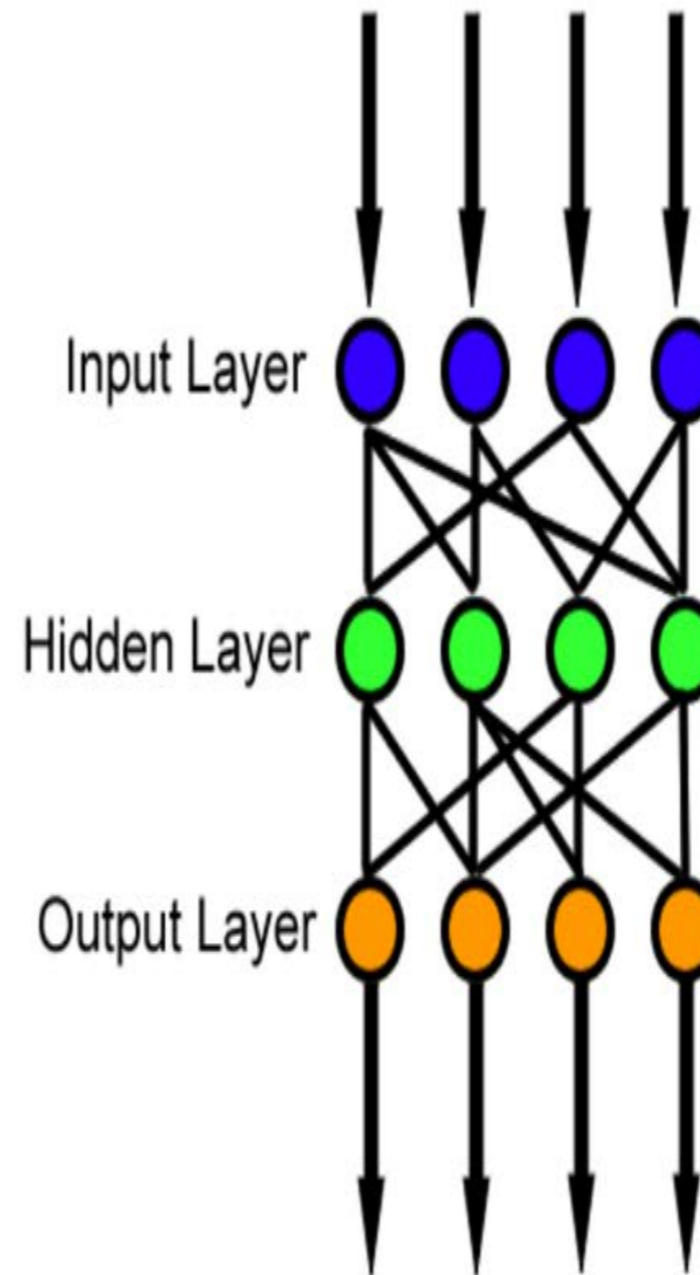
Systems construct contextual explanatory models for classes of real world phenomena

The third wave of AI



(Lay) Definitions - III

Deep Learning (a.k.a. deep neural nets): “Deep learning is a particular kind of machine learning that achieves great power and flexibility by learning to represent the world as nested hierarchy of concepts, with each concept defined in relation to simpler concepts, and more abstract representations computed in terms of less abstract ones.”



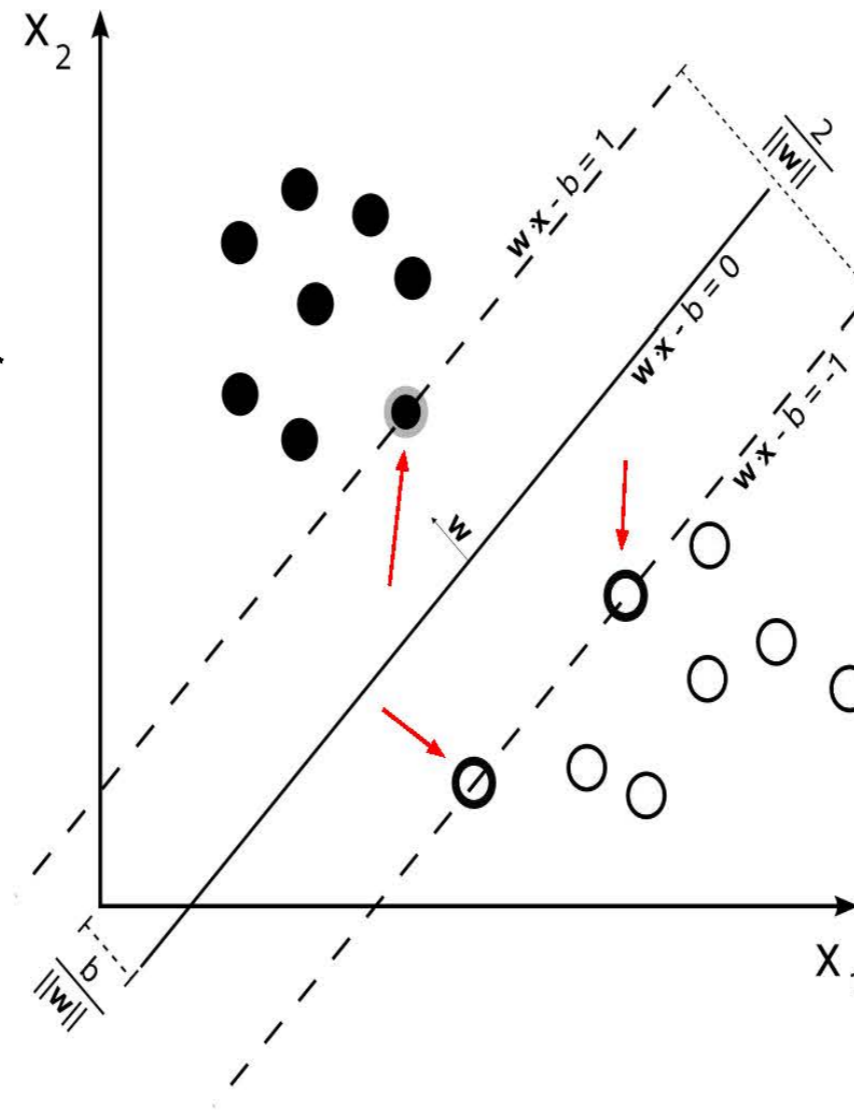
Outline

- A definition (or two)
- **Altum Visum on deep learning networks**
- Machine Learning: Myths & Realities
- Machine Learning as a process
- Explainable Artificial Intelligence
- Epilogue



The two sides of the debate on DNN

DL will solve all of our problems!



DL is all hype!

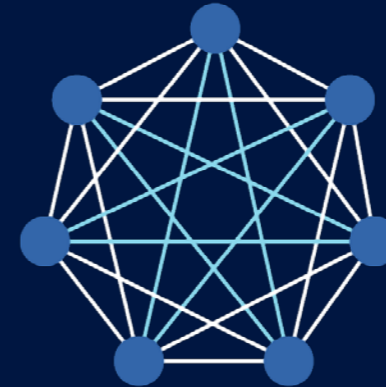
Image credit: Diego Almeida (Enlitic), 2016



Deep Neural Networks – Where we are



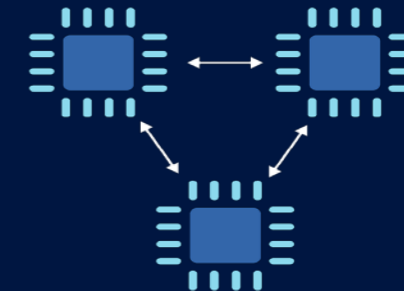
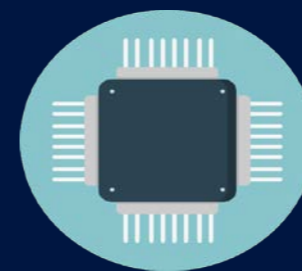
Large data



Large and complex models



Frameworks & Libraries

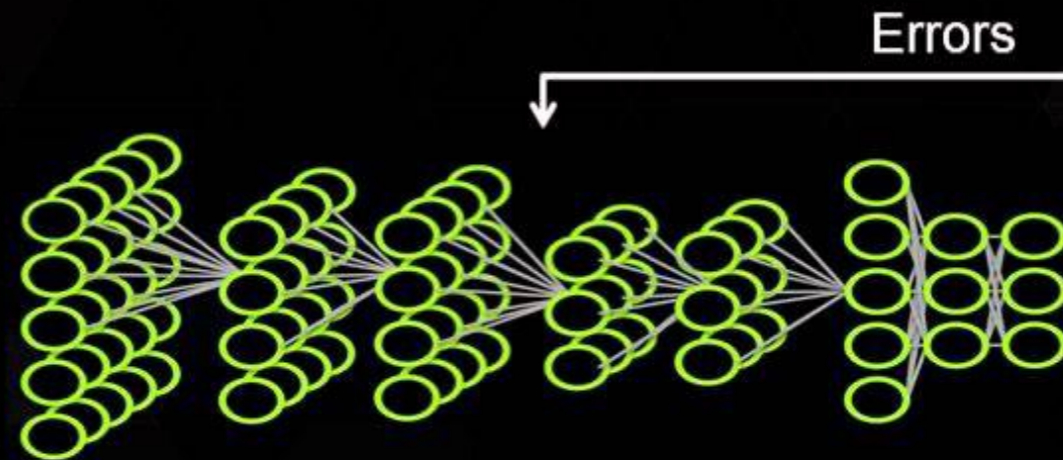


Training Hardware

Modern Deep Neural Networks (DNN)

DEEP LEARNING APPROACH

Train:



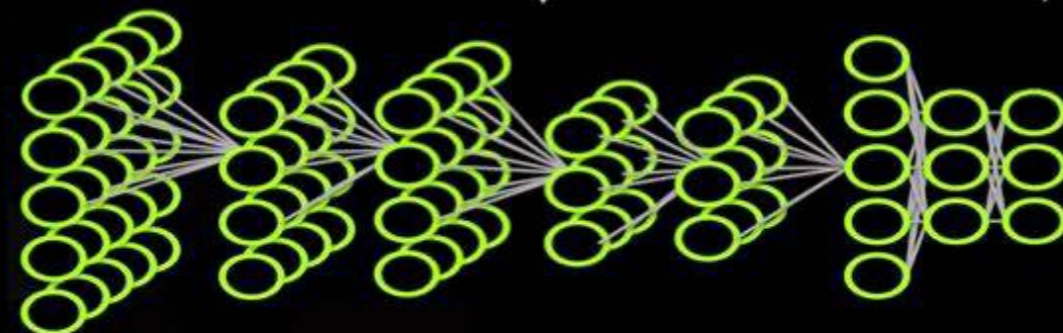
Errors



Dog
Cat
Raccoon



Deploy:



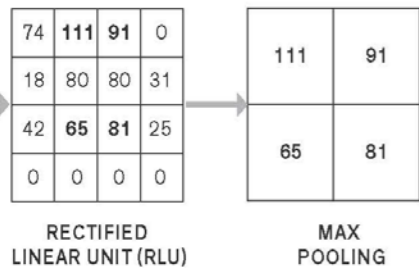
Dog ✓

DNN - Algorithmic Innovation

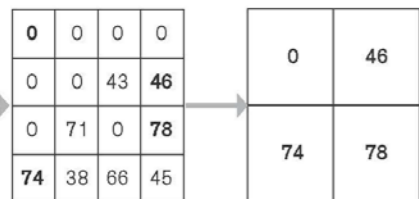
D. The resulting products for the first chunk are summed up, and the total is put down in one cell of a grid. Then the filter moves over one pixel to the right and looks at the next 3-by-3 chunk.

0	0	0
0	-6	-6
0	-20	18

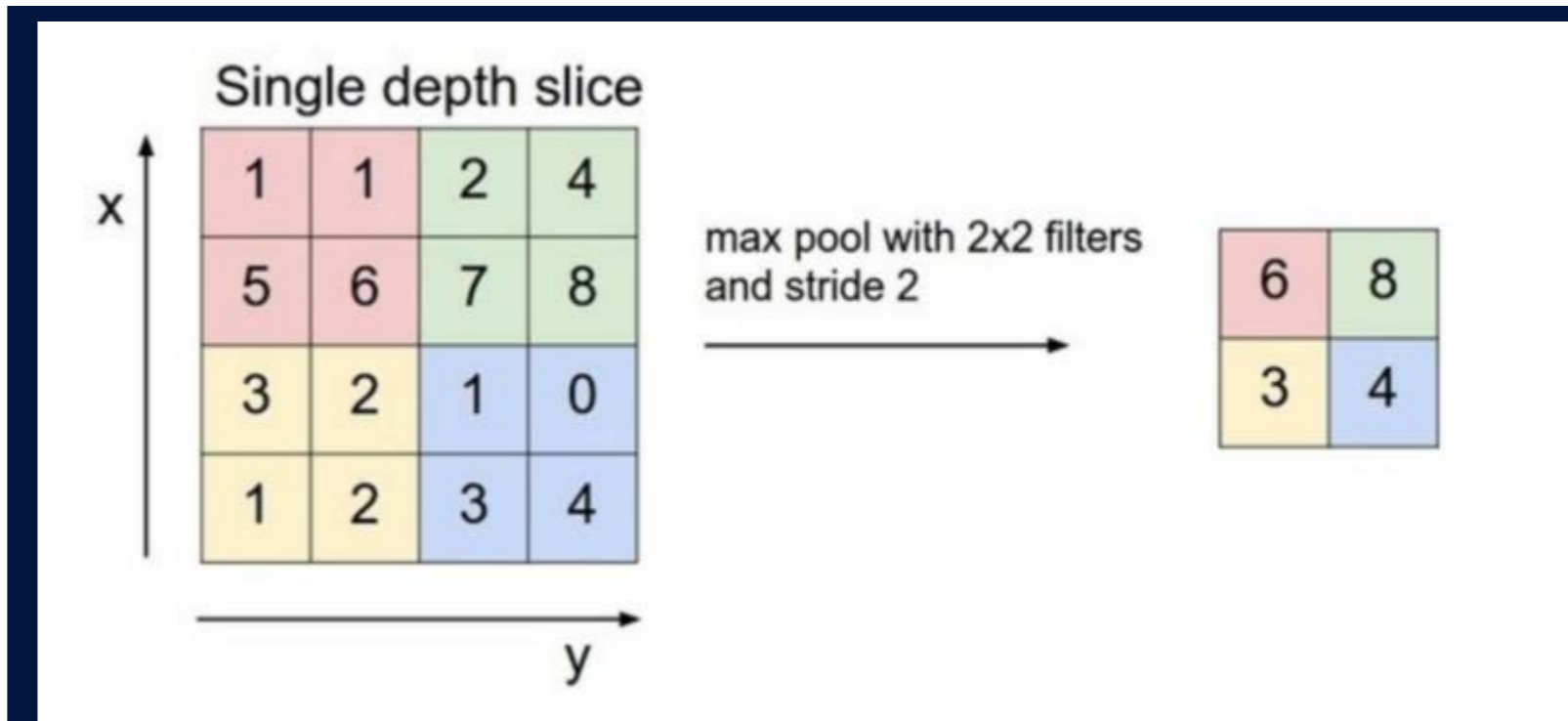
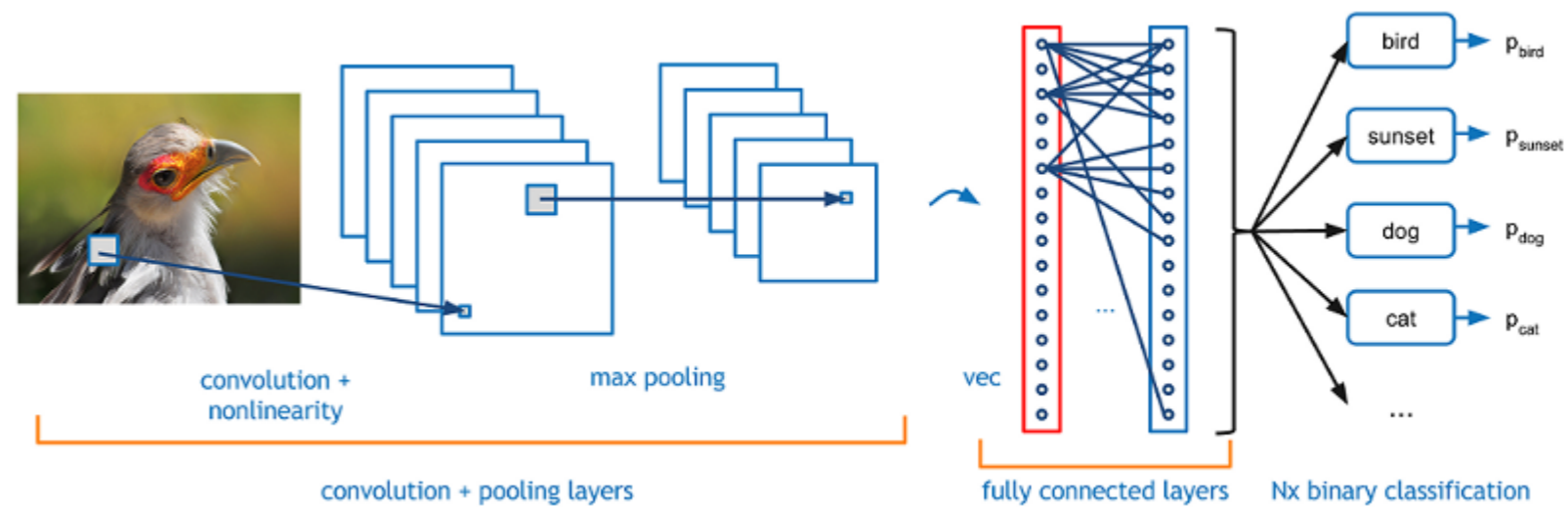
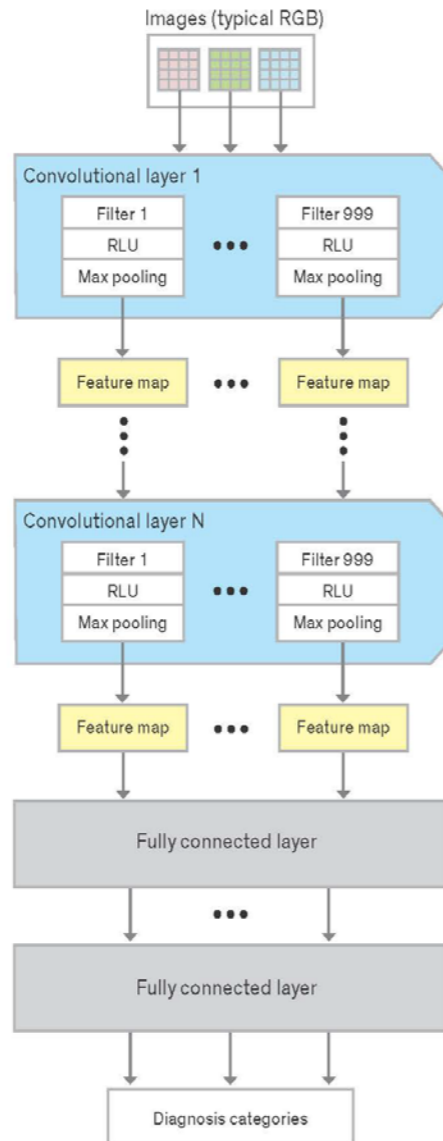
Total: **-14**



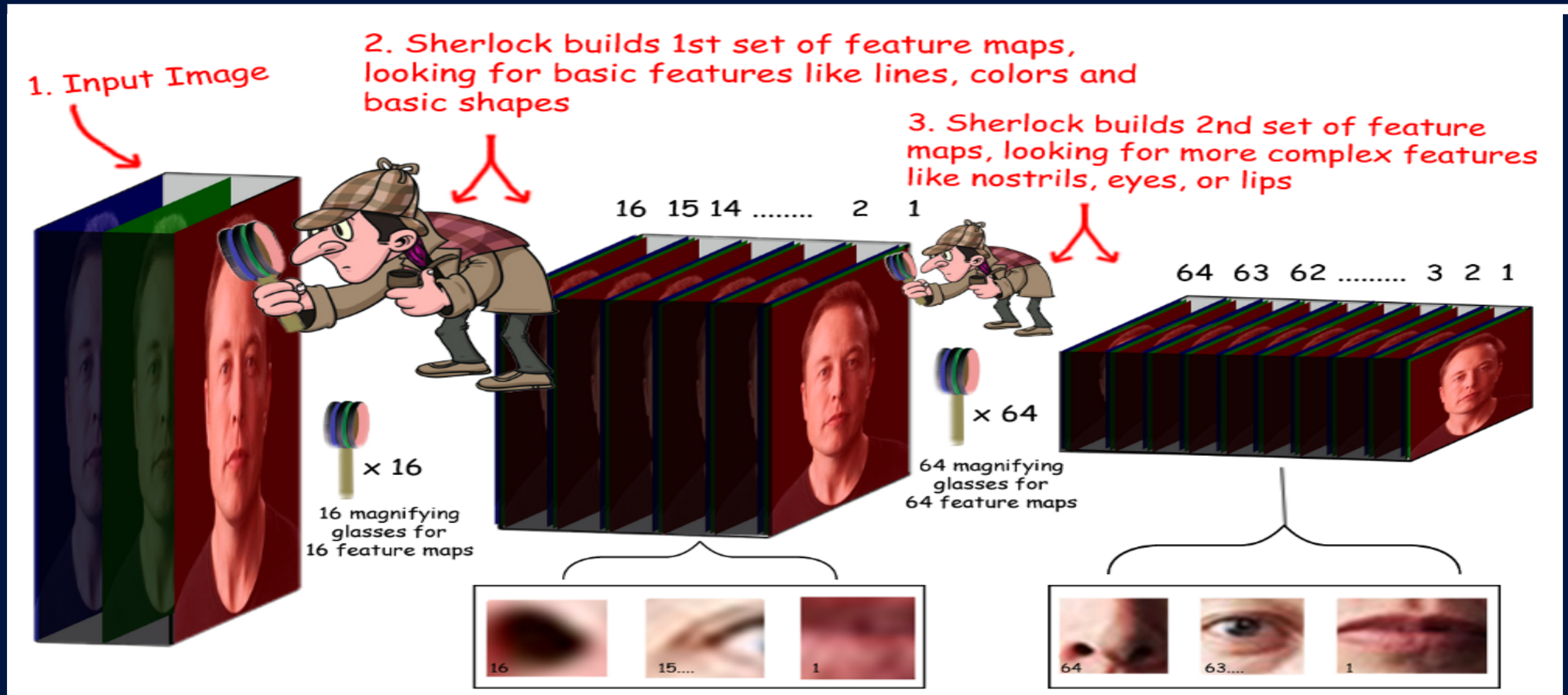
F. Two more simple steps finish this filter's work. In the rectified linear unit (step RLU), the negative numbers in the grid are replaced with zeros. In the max pooling step, the highest value in each 2-by-2 chunk of grid is selected. The end result is a simple set of numbers called a feature map.



H. For each digital image, a CNN uses many layers of convolutional filters. Finally, the last convolutional layer outputs all of its feature maps to a "fully connected" layer, which examines the maps in their entirety. The CNN uses several fully connected layers to make a final determination about the image's content.



Convolutional NN (DNN) in popular blogs - I

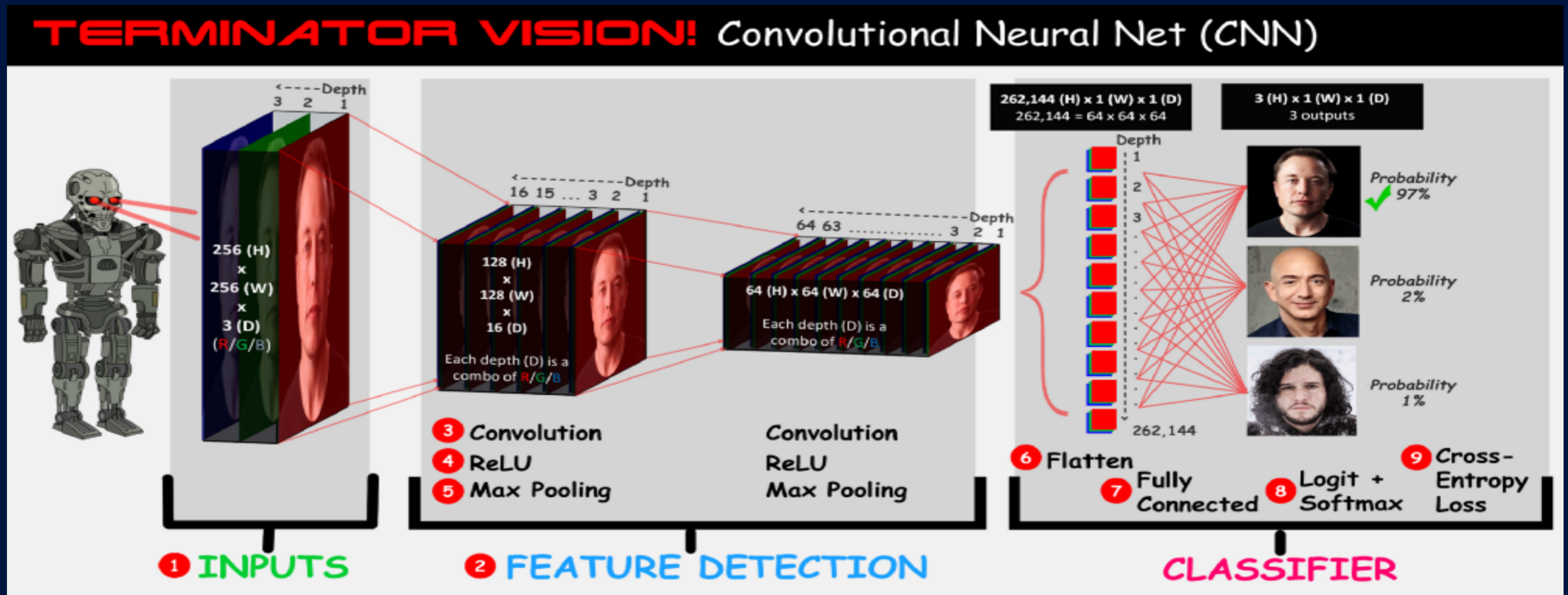


Sherlock Holmes
the "Feature Detective"

www.ExcelwithML.com

Image Credit: Dave Smith;
<https://towardsdatascience.com/cutting-edge-face-recognition-is-complicated-these-spreadsheets-make-it-easier-e7864dbf0e1a>
Accessed; August 7, 2018

Convolutional NN (DNN) in popular blogs - II
















You will learn:

- 1 Inputs - How computers see
- 2 Feature Detection - Think like Sherlock Holmes
- 3 Convolution Math - Sherlock Holmes' detective kit
- 4 ReLU - Non-linear pattern recognition
- 5 Max Pooling - Keeping the most important clues
- 6 Flatten - Lining up all the clues
- 7 Fully Connected - Connecting the dots in the case
- 8 Logit + Softmax - Cracking the case
- 9 Cross-Entropy Loss - Sherlock's "rightness/wrongness"

Image Credit: Dave Smith;
<https://towardsdatascience.com/cutting-edge-face-recognition-is-complicated-these-spreadsheets-make-it-easier-e7864dbf0e1a>
 Accessed; August 7, 2018

A mostly complete chart of Neural Networks

©2016 Fjodor van Veen - asimovinstitute.org

-  Backfed Input Cell
-  Input Cell
-  Noisy Input Cell
-  Hidden Cell
-  Probabilistic Hidden Cell
-  Spiking Hidden Cell
-  Output Cell
-  Match Input Output Cell
-  Recurrent Cell
-  Memory Cell
-  Different Memory Cell
-  Kernel
-  Convolution or Pool

Perceptron (P)



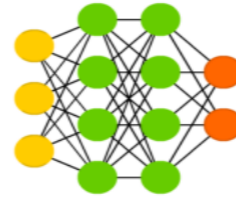
Feed Forward (FF)



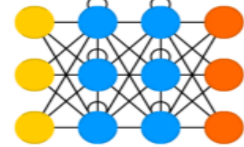
Radial Basis Network (RBF)



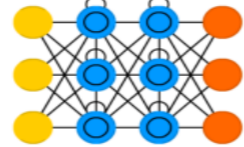
Deep Feed Forward (DFF)



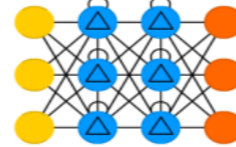
Recurrent Neural Network (RNN)



Long / Short Term Memory (LSTM)



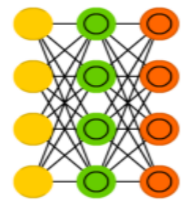
Gated Recurrent Unit (GRU)



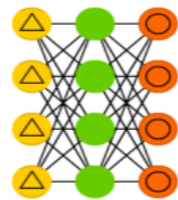
Auto Encoder (AE)



Variational AE (VAE)



Denosing AE (DAE)



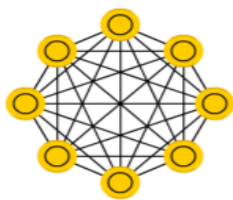
Sparse AE (SAE)



Markov Chain (MC)



Hopfield Network (HN)



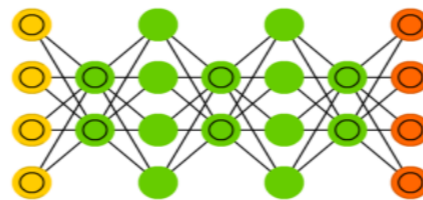
Boltzmann Machine (BM)



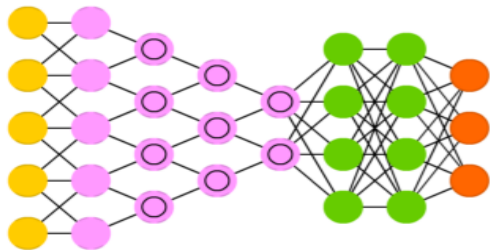
Restricted BM (RBM)



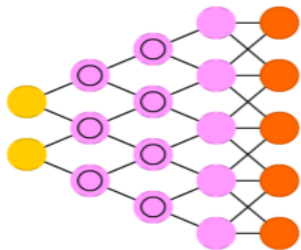
Deep Belief Network (DBN)



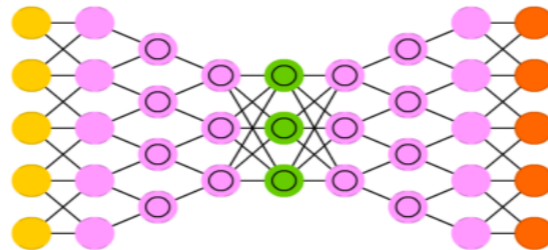
Deep Convolutional Network (DCN)



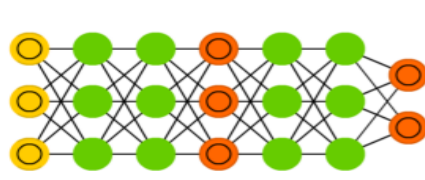
Deconvolutional Network (DN)



Deep Convolutional Inverse Graphics Network (DCIGN)



Generative Adversarial Network (GAN)



Liquid State Machine (LSM)



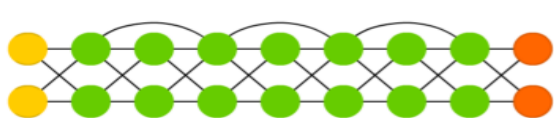
Extreme Learning Machine (ELM)



Echo State Network (ESN)



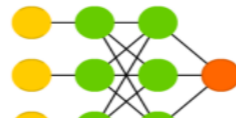
Deep Residual Network (DRN)



Kohonen Network (KN)



Support Vector Machine (SVM)



Neural Turing Machine (NTM)



Taxonomy

Source:

<http://www.asimovinstitute.org/neural-network-zoo/>



Training Hardware

Deep Learning Hardware (2016)

GPUs: Nvidia is dominating

One of the first GPU neural nets was on a NVIDIA GTX 280 up to 9 layers neural network. (2010 Ciresan and Schmidhuber)

- Nvidia chips tend to outperform AMD
- More importantly, all the major frameworks use CUDA as first-class citizen. Poor support for AMD's OpenCL



Libraries – A ‘revolution’ in the making ?

Python For Data Science Cheat Sheet

SciPy - Linear Algebra

Learn More Python for Data Science [interactively](http://www.datacamp.com) at www.datacamp.com



Linear Algebra

You'll use the `linalg` and `sparse` modules. Note that `scipy.linalg` contains and expands on `numpy.linalg`.

```
>>> from scipy import linalg, sparse
```

Creating Matrices

```
>>> A = np.matrix(np.random.random((2,2)))
>>> B = np.asmatrix(b)
>>> C = np.mat(np.random.random((10,5)))
>>> D = np.mat([[3,4], [5,6]])
```

Basic Matrix Routines

Inverse >>> A.I >>> linalg.inv(A)	Inverse Inverse
Transposition >>> A.T >>> A.H	Transpose matrix Conjugate transposition
Trace >>> np.trace(A)	Trace
Norm >>> linalg.norm(A) >>> linalg.norm(A,1) >>> linalg.norm(A,np.inf)	Frobenius norm L1 norm (max column sum) L inf norm (max row sum)
Rank >>> np.linalg.matrix_rank(C)	Matrix rank
Determinant >>> linalg.det(A)	Determinant
Solving linear problems >>> linalg.solve(A,b) >>> E = np.mat(a).T >>> linalg.lstsq(F,E)	Solver for dense matrices Solver for dense matrices Least-squares solution to linear matrix equation
Generalized inverse >>> linalg.pinv(C) >>> linalg.pinv2(C)	Compute the pseudo-inverse of a matrix (least-squares solver) Compute the pseudo-inverse of a matrix (SVD)

Creating Sparse Matrices

```
>>> F = np.eye(3, k=1)
>>> G = np.mat(np.identity(2))
>>> C[C > 0.5] = 0
>>> H = sparse.csr_matrix(C)
>>> I = sparse.csc_matrix(D)
>>> J = sparse.dok_matrix(A)
>>> E.todense()
>>> sparse.lnspmatrix_csc(A)
```

Sparse Matrix Routines

Inverse >>> sparse.linalg.inv(I)	Inverse
Norm >>> sparse.linalg.norm(I)	Norm
Solving linear problems >>> sparse.linalg.spsolve(H, I)	Solver for sparse matrices

Sparse Matrix Functions

```
>>> sparse.linalg.expm(I)
```

Sparse matrix exponential

Also see NumPy

Matrix Functions

Addition >>> np.add(A, D)	Addition
Subtraction >>> np.subtract(A, D)	Subtraction
Division >>> np.divide(A, D)	Division
Multiplication >>> A @ D	Multiplication operator (Python 3)
>>> np.multiply(D, A)	Multiplication
>>> np.dot(A, D)	Dot product
>>> np.vdot(A, D)	Vector dot product
>>> np.inner(A, D)	Inner product
>>> np.outer(A, D)	Outer product
>>> np.tensordot(A, D)	Tensor dot product
>>> np.kron(A, D)	Kronecker product
Exponential Functions >>> linalg.expm(A) >>> linalg.expm2(A) >>> linalg.expm3(D)	Matrix exponential Matrix exponential (Taylor Series) Matrix exponential (eigenvalue decomposition)
Logarithm Function >>> linalg.logm(A)	Matrix logarithm
Trigonometric Functions >>> linalg.sinm(D) >>> linalg.cosm(D) >>> linalg.tanm(A)	Matrix sine Matrix cosine Matrix tangent
Hyperbolic Trigonometric Functions >>> linalg.sinhm(D) >>> linalg.coshm(D) >>> linalg.tanhm(A)	Hyperbolic matrix sine Hyperbolic matrix cosine Hyperbolic matrix tangent
Matrix Sign Function >>> np.signm(A)	Matrix sign function
Matrix Square Root >>> linalg.sqrtm(A)	Matrix square root
Arbitrary Functions >>> linalg.funm(A, lambda x: x*x)	Evaluate matrix function

Decompositions

Eigenvalues and Eigenvectors >>> la, v = linalg.eig(A) >>> l1, l2 = la >>> v[:,0] >>> v[:,1] >>> linalg.eigvals(A)	Solve ordinary or generalized eigenvalue problem for square matrix Unpack eigenvalues First eigenvector Second eigenvector Unpack eigenvalues
Singular Value Decomposition >>> U, s, Vh = linalg.svd(B) >>> M, N = B.shape >>> Sig = linalg.diagsvd(s, M, N)	Singular Value Decomposition (SVD) Construct sigma matrix in SVD
LU Decomposition >>> P, L, U = linalg.lu(C)	LU Decomposition

Sparse Matrix Decompositions

```
>>> la, v = sparse.linalg.eigs(F, 1)
>>> sparse.linalg.svds(H, 2)
```

Eigenvalues and eigenvectors
SVD

Asking For Help

```
>>> help(scipy.linalg.diagsvd)
>>> np.info(np.matrix)
```

DataCamp

Learn Python for Data Science [interactively](http://www.datacamp.com)

Frameworks & Libraries – I

TensorFlow

Created by Google

TensorFlow is written with a Python API over a C/C++ engine

TensorFlow generates a computational graph (e.g. a series of matrix operations) and performs automatic differentiation



Pros:

- Uses Python + Numpy
- Lots of interest from the community
- Highly parallel, and designed to use various backends (software, gpu, asic)
- Apache License

Cons:

- Slower than other frameworks^[1]
- More features, more abstractions than torch
- Not many pretrained models yet

<https://arxiv.org/pdf/1511.06435v3.pdf>



Some fundamentals

Data-Knowledge spectrum

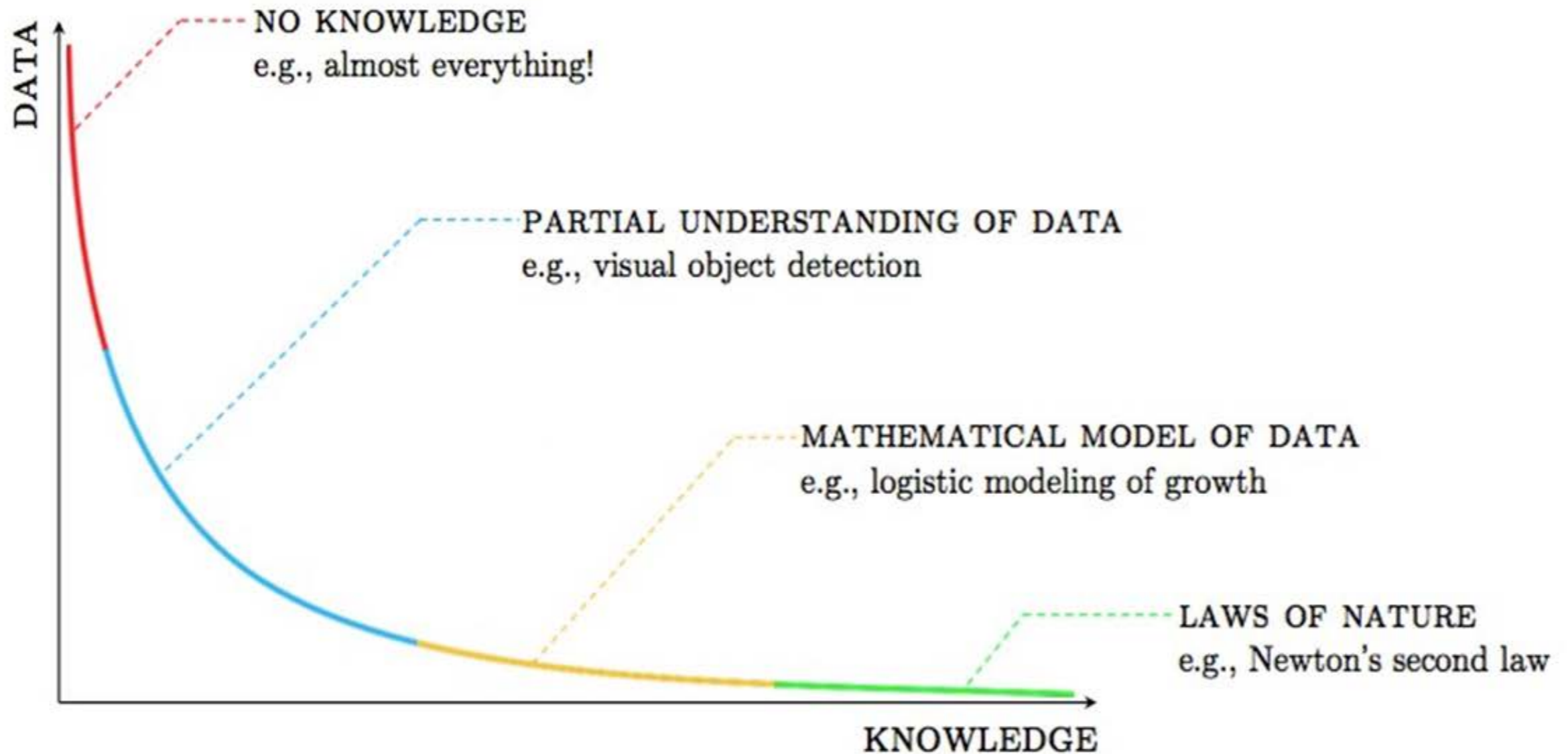


Image taken from Machine Learning Refined, by Watt - Borhani - Katsaggelos



The Edward S. Rogers Sr. Department
of Electrical & Computer Engineering
UNIVERSITY OF TORONTO

FACULTY
OF APPLIED
SCIENCE &
ENGINEERING

The "Data Sets" (laboratory style)

Image credit: Xuedong Huang

ImageNet: Microsoft 2015 ResNet

Microsoft Store Products Support

Next The Official Microsoft Blog The Fire Hose Microsoft On the Issues Transform

Microsoft researchers win ImageNet computer vision challenge

Jian Sun, a principal research manager at Microsoft Research, led the image understanding project. Photo: Craig Tuschhoff/Microsoft

Posted December 10, 2015 By Allison Linn

Microsoft researchers on Thursday announced a major advance in technology designed to identify the objects in a photograph or video, showcasing a system whose accuracy meets and sometimes exceeds human-level performance.

Microsoft's new approach to recognizing images also took first place in several major categories of image recognition challenges Thursday, beating out many other competitors from academic, corporate and research institutions in the ImageNet and Microsoft

The *ImageNet* Large Scale Visual Recognition Challenge (ILSVRC) evaluates algorithms for object detection and image classification at large scale

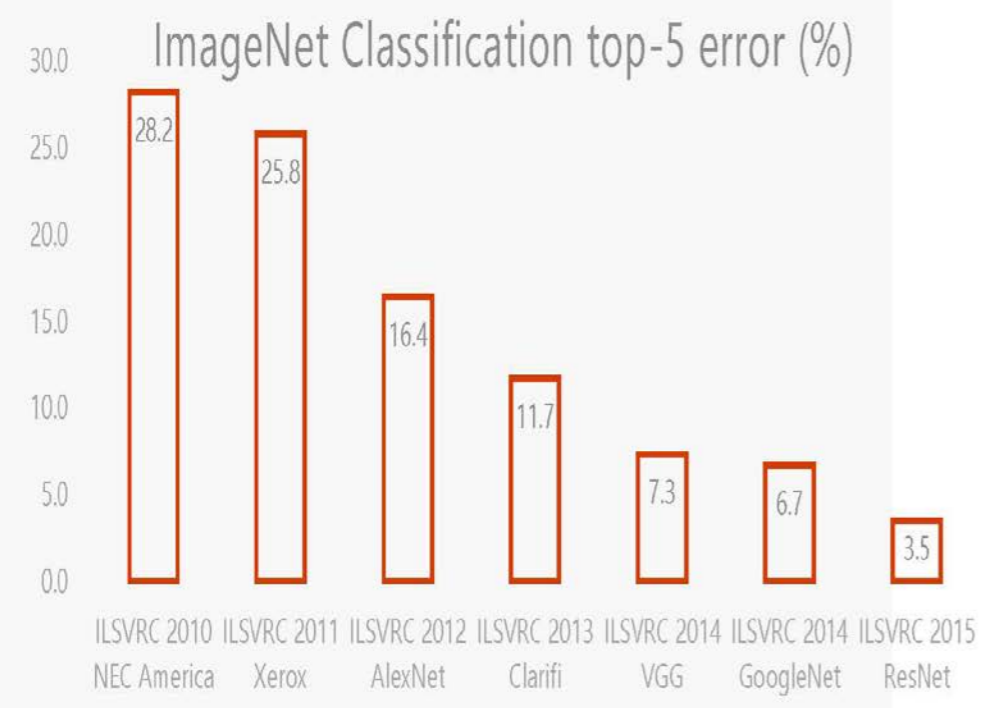


Image Credit : Ferenc Huszar



Deep Learning → Real World Problems

What matters: Real-world label distributions; Understanding black box models; Pre-training.

Medical vision: if you want to build a system which detects lymph nodes in the human body in Computed Tomography (CT) images, you need annotated images where the lymph node is labeled. This is a rather time consuming task, as the images are in 3D and it is required to recognize very small structures. Assuming that a radiologist earns 100\$/h and can carefully annotate 4 images per hour, this implies that you incur costs of 25\$ per image or 250k\$ for 10000 labeled images. Considering that you require several physicians to label the same image to ensure close to 100% diagnosis correctness, acquiring a dataset for the given medical task would easily exceed those 250k\$." ¹

Credit scoring: if you want to build a system that makes credit decisions, you need to know who is likely to default so you can train a machine learning system to recognize them beforehand. Unfortunately, you only know for sure if somebody defaults when it happens. Thus, a naive strategy would be to give loans of say 10k\$ to everyone. However, this means that every person that defaults will cost you 10k\$. This puts a very expensive price tag on each labeled data point." ¹

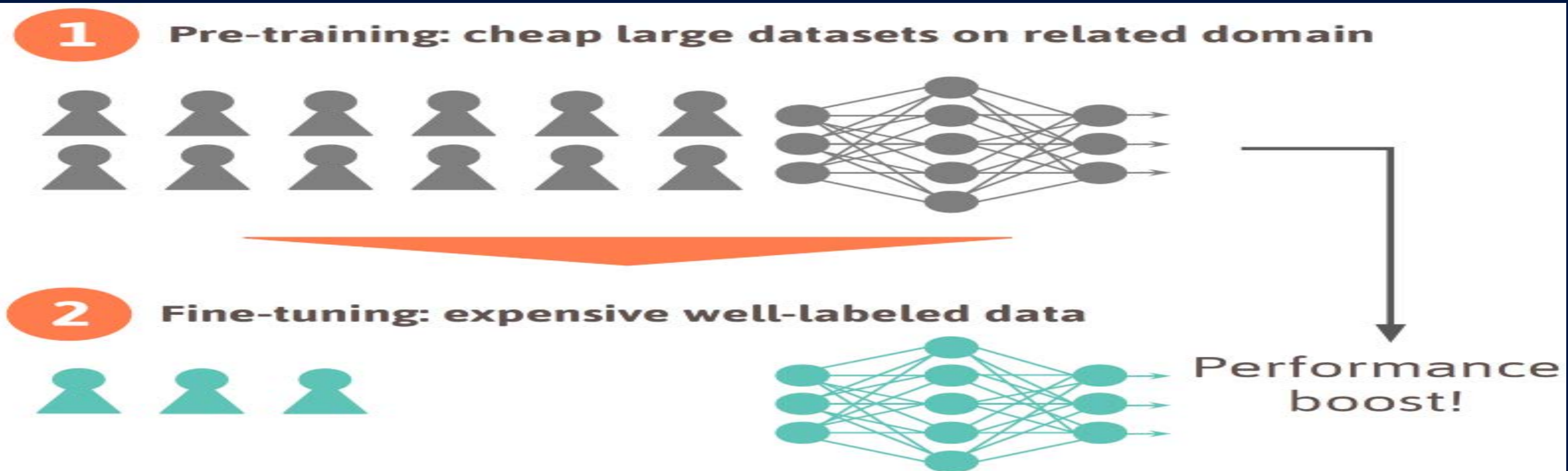
¹ Credit: Rasmus Rothe, MERANDIX



Deep Learning → Real World Problems

What matters: Real-world label distributions; Understanding black box models; Pre-training.

" **Medical Care:** Researchers at the University of Pittsburg in the late 1990s evaluated machine learning algorithms for predicting mortality rates from pneumonia. The algorithms recommended that hospitals send home pneumonia patients who were also asthma sufferers, estimating their risk of death from pneumonia to be lower. It turned out that the dataset fed into the algorithms did not account for the fact that asthma sufferers had been immediately sent to intensive care, and had fared better only due to the additional attention." ¹

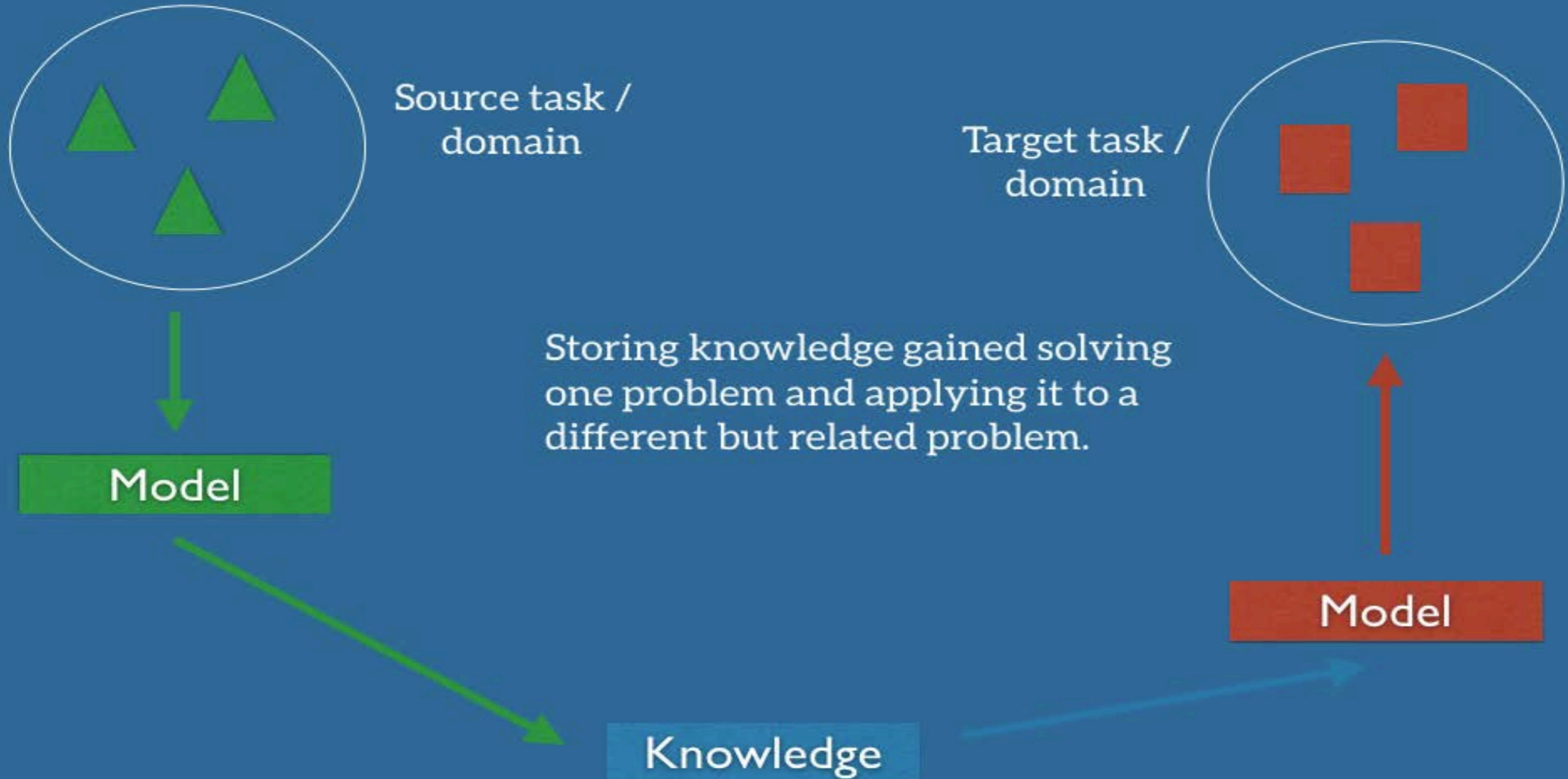


¹ Credit: Anastassia Fendyk, Harvard

Image Credit: Rasmus Rothe, MERANDIX

Deep Learning → Real World Problems

Transfer learning



Neural Nets - The Achilles Heel

- Great empirical achievements (in certain application areas) were obtained with hardly any theoretical understanding of the underlying paradigm.
- The optimization employed in the learning process is highly non-convex and intractable from a theoretical viewpoint.
- Proponents offer very little interpretability of the found solution or understanding of the underlying phenomena.



Neural Nets - Challenges



a young boy is holding a
baseball bat

Statistically impressive, but
individually unreliable

["Deep Visual-Semantic Alignments for
Generating Image Descriptions"](#)
by [Andrej Karpathy](#), [Li Fei-Fei](#) (CVPR
2015).

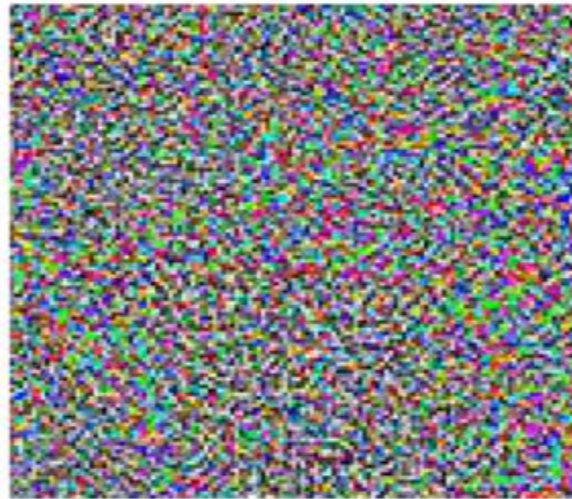
Neural Nets - Challenges



Panda

57.7% confidence

+ E



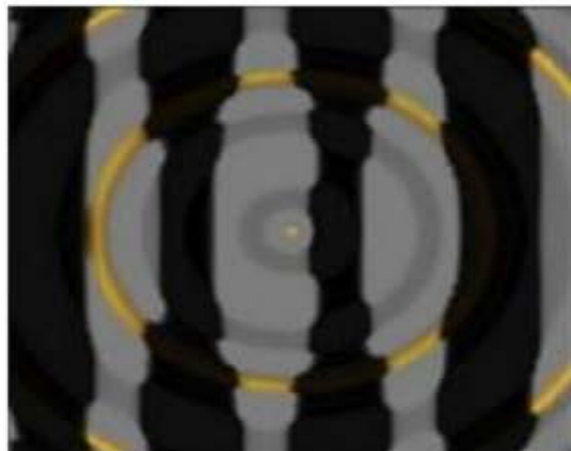
less than 1%
targeted distortion

=



Gibbon

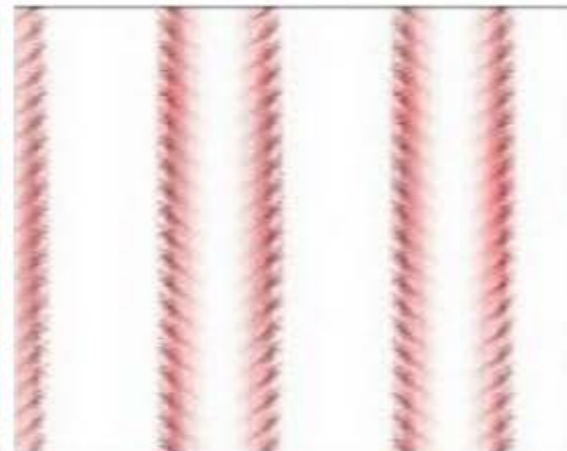
99.3% confidence



King penguin



Starfish



Baseball



Electric guitar

Conclusion: Inherent flaws can be exploited



Neural Nets - Challenges



Internet trolls cause the AI bot, Tay, to act offensively

Skewed training data creates maladaptation

Outline

- A definition (or two)
- Altum Visum on deep learning networks
- **Machine Learning: Myths & Realities**
- Machine Learning as a process
- Explainable Artificial Intelligence
- Epilogue



Myth

Machine Learning = Deep Neural Networks

Quiz question: When the term “A.I. Winter” was invented and why ?



Reality

Machine Learning Algorithms Cheat Sheet

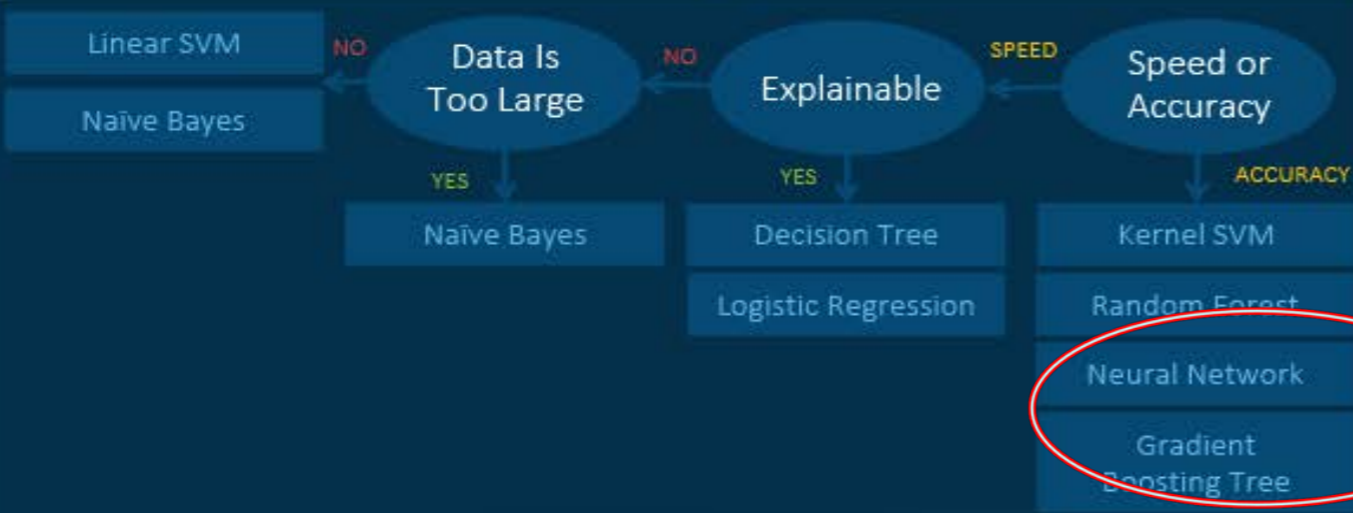
Unsupervised Learning: Clustering



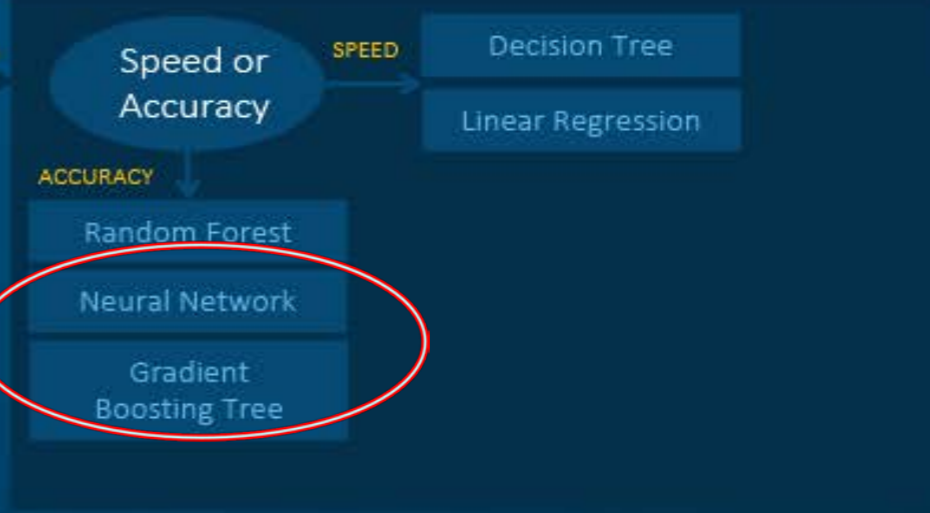
Unsupervised Learning: Dimension Reduction



Supervised Learning: Classification



Supervised Learning: Regression



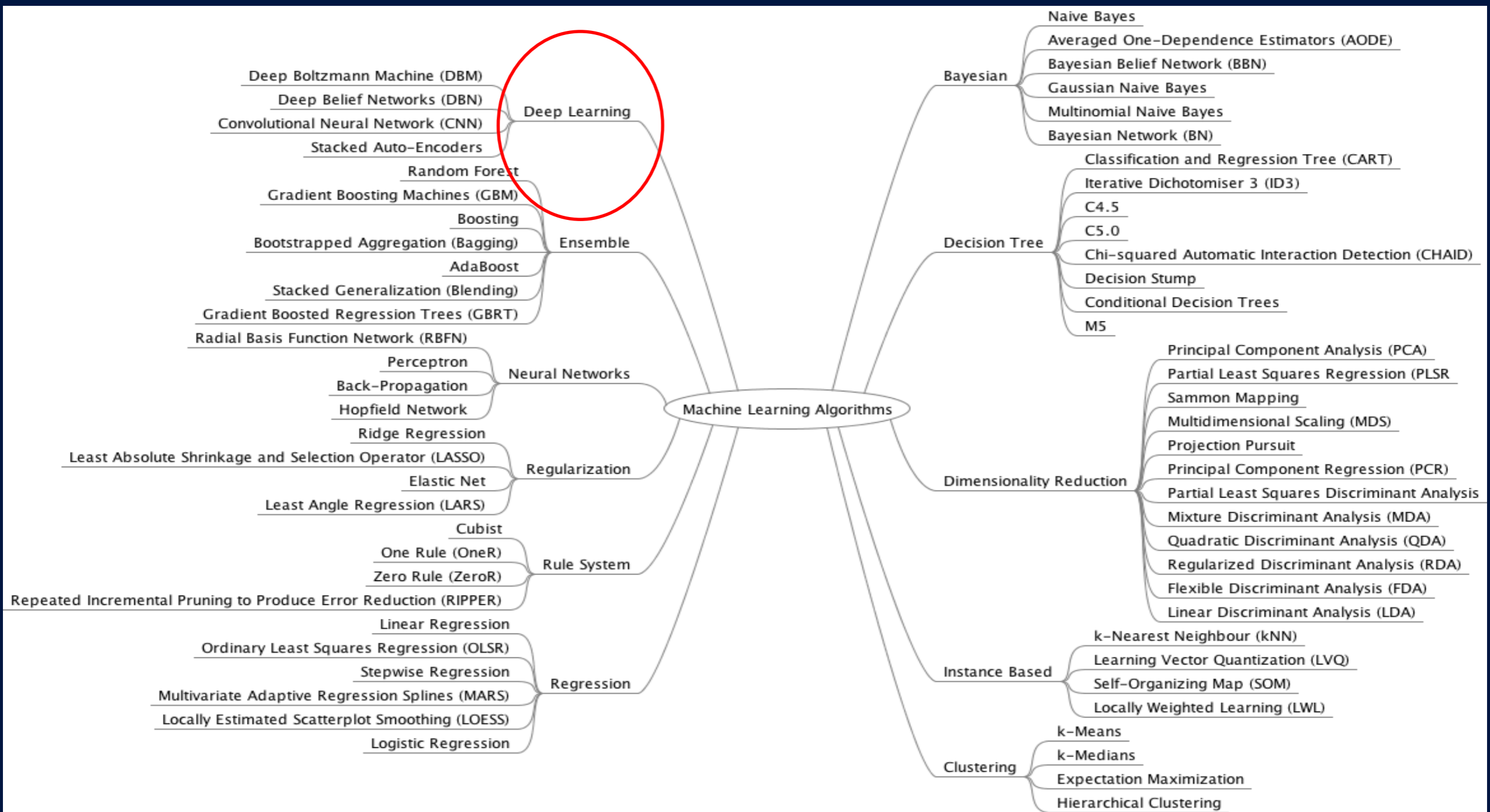
Credit: Hui Li, SAS Analytics, April 2017



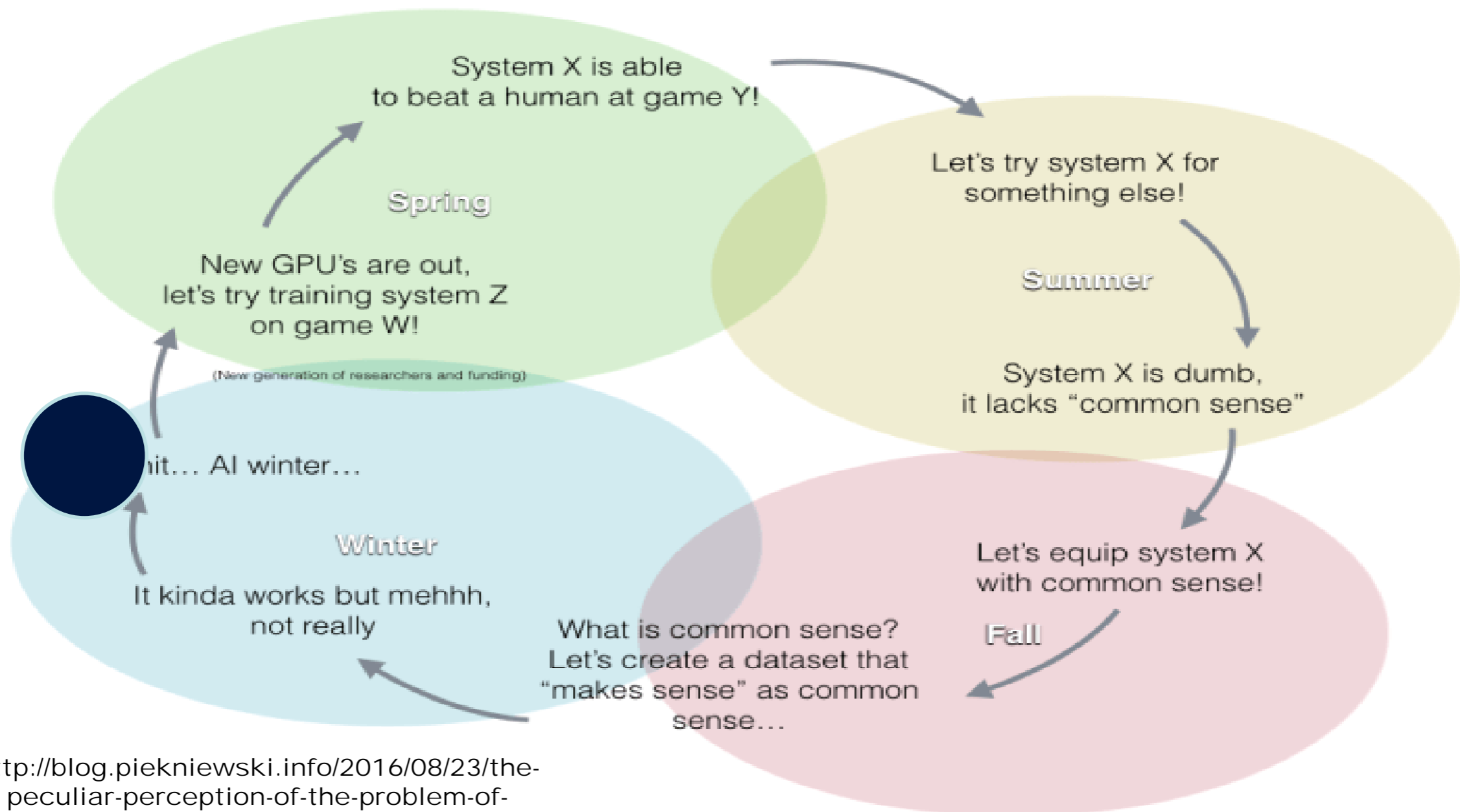
The Edward S. Rogers Sr. Department
of Electrical & Computer Engineering
UNIVERSITY OF TORONTO

FACULTY
OF APPLIED
SCIENCE &
ENGINEERING

Reality



Reality or Myth: The four Seasons



<http://blog.piekniowski.info/2016/08/23/the-peculiar-perception-of-the-problem-of-perception/>

Consider

“If your only tool is a hammer, then all of the problems look like nails”.

Abraham H. Maslow (1962) **via** S. (Pas) Pasupathy (1999).

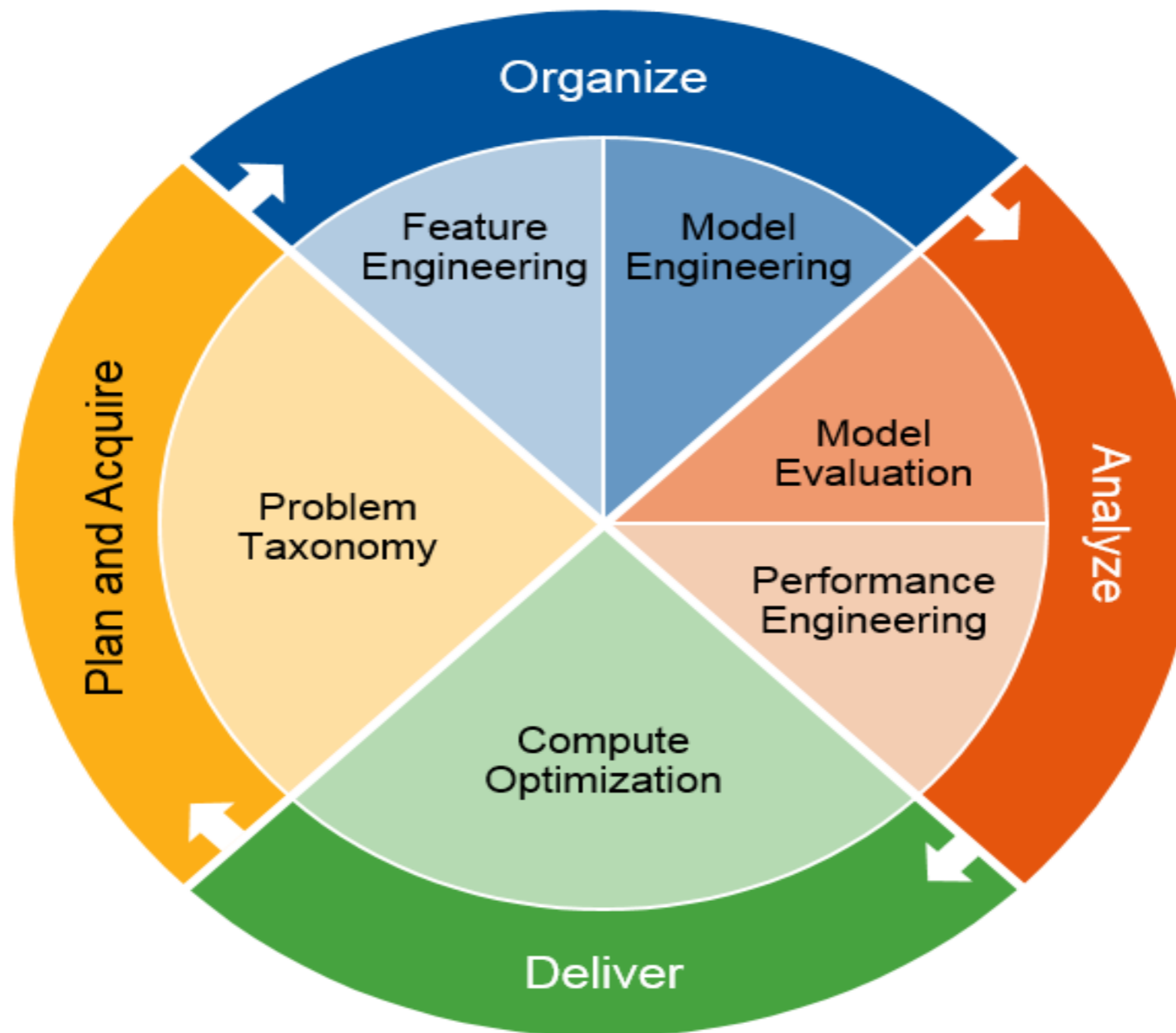


Outline

- A definition (or two)
- Altum Visum on deep learning networks
- Machine Learning: Myths & Realities
- **Machine Learning as a process**
- Explainable Artificial Intelligence
- Epilogue



Engineering Cycle of Machine Learning

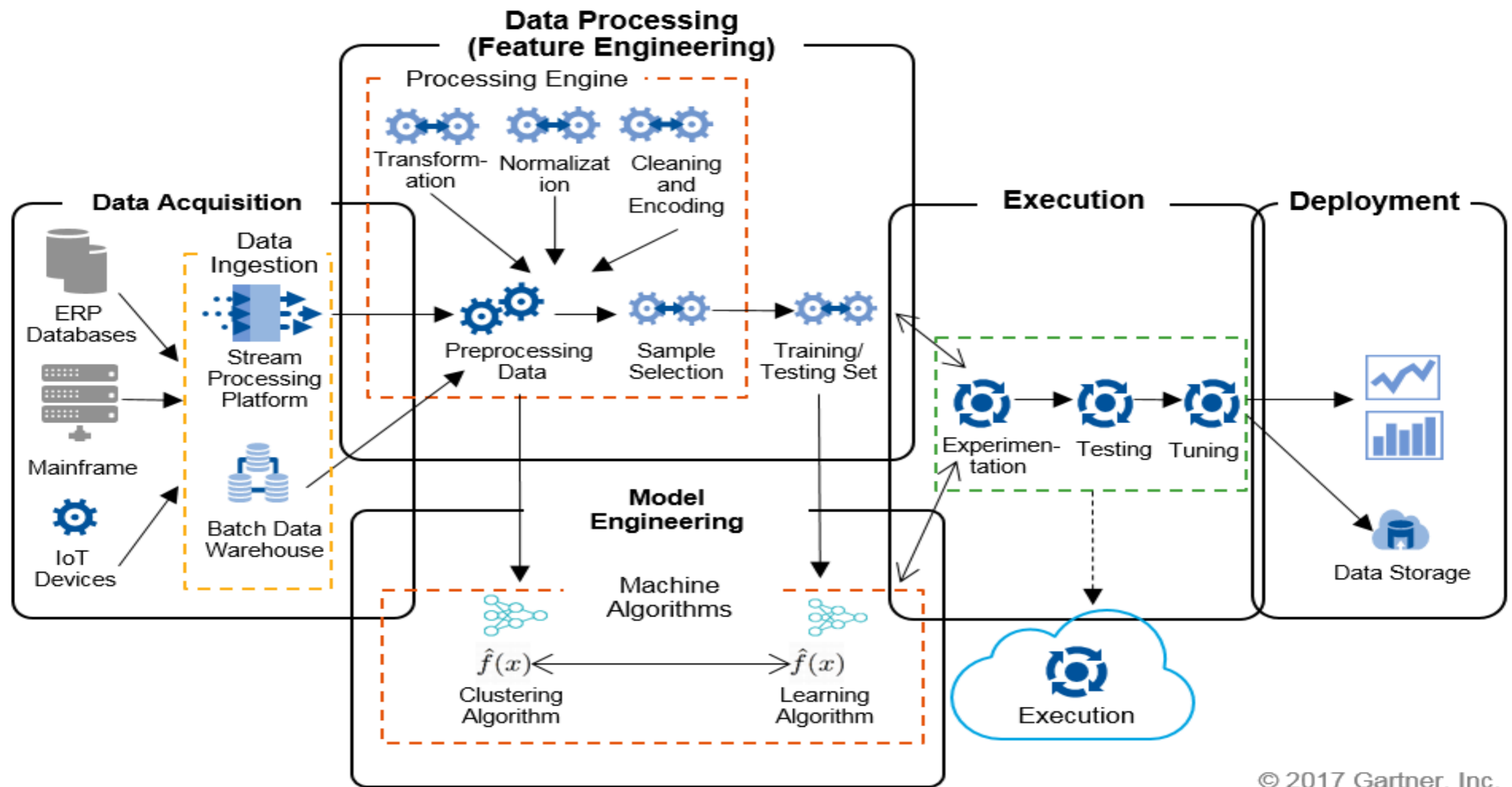


© 2017 Gartner, Inc.

46



Machine Learning: Engineering Architecture



What is the expected impact & where

Machine learning has great impact potential across industries and use case types

Impact potential
Low  High

Problem type	Automotive	Manufacturing	Consumer	Finance	Agriculture	Energy	Health care	Pharma- ceuticals	Public/ social	Media	Telecom	Transport and logistics
Real-time optimization	High	High	High	Low	High	High	Low	Low	High	High	High	Low
Strategic optimization	High	High	High	High	High	High	High	High	High	High	High	Low
Predictive analytics	Low	High	High	High	High	High	High	High	High	High	High	High
Predictive maintenance	High	High	High	High	High	Low	Low	Low	High	Low	High	Low
Radical personalization	High	Low	High	High	High	Low	High	Low	High	Low	High	High
Discover new trends/anomalies	High	High	Low	High	Low	Low	High	High	Low	High	High	Low
Forecasting	High	High	High	High	High	High	High	High	High	Low	High	High
Process unstructured data	High	High	High	Low	High	Low	High	Low	Low	High	Low	High

SOURCE: McKinsey Global Institute analysis



Outline

- A definition (or two)
- Altum Visum on deep learning networks
- Machine Learning: Myths & Realities
- Machine Learning as a process
- **Explainable Artificial Intelligence**
- Epilogue



A definition revised:

“Machine learning (ML): a subset of artificial intelligence (AI) is more than a technique for analyzing data. It's a system that is fueled by data, with the ability to learn and improve by using algorithms that provide new insights without being explicitly programmed to do so.”

Gartner, “Preparing and Architecting for Machine Learning”, Technical Professional Advice, published January 17, 2017.



Explainable Artificial Intelligence

DARPA

Concept: Explainable Artificial Intelligence

Today

Training Data

Machine Learning Process

Learned Function

Decision or Recommendation

Task



User

- Why did you do that?
- Why not something else?
- When do you succeed?
- When do you fail?
- When can I trust you?
- How do I correct an error?

XAI

Training Data

New Machine Learning Process

Explainable Model

Explanation Interface

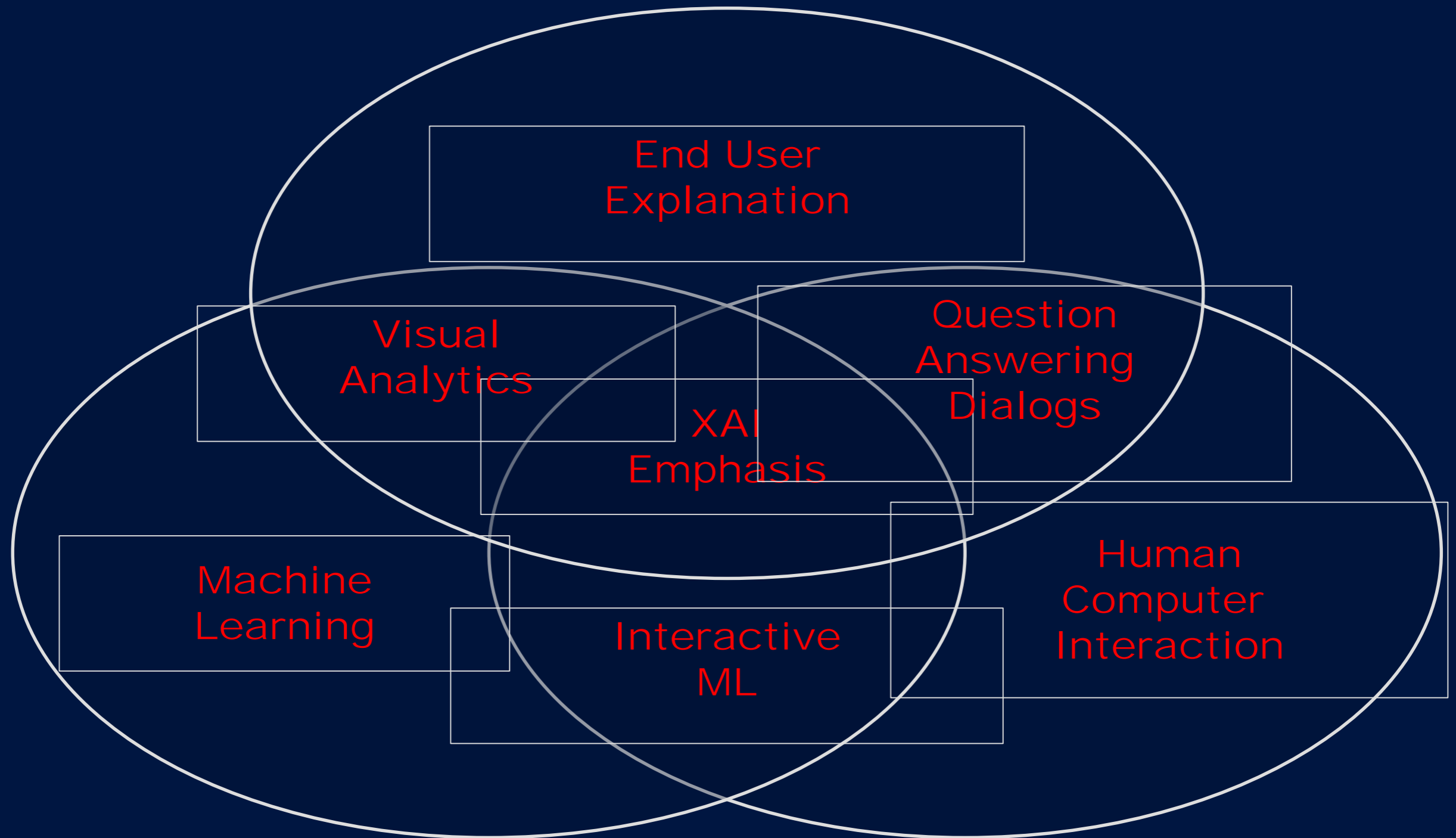
Task



User

- I understand why
- I understand why not
- I know when you succeed
- I know when you fail
- I know when to trust you
- I know why you erred

Explainable Artificial Intelligence (XAI)



Outline

- A definition (or two)
- Altum Visum on deep learning networks
- Machine Learning: Myths & Realities
- Machine Learning as a process
- Explainable Artificial Intelligence
- **Epilogue**



An old (?) paradox

The Moravec's Paradox (1988): “it is comparatively easy to make computers exhibit adult level performance on intelligent tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility” .¹

¹ Hans Moravec, *Mind Children: The Future of Robot and Human Intelligence*, Harvard University Press, 1988, ([ISBN 0674576187](#)).



Big Picture

Is DNN (or ML in general) a “Deus ex Machina Moment” ?



Epilogue

- Machine learning is best-suited for dealing with big, **albeit curated**, data.
- Supervised networks (DNN) can learn semantically relevant representations useful in areas such as (image) classification, content-aware advertising, content filtering, social networks.
- Preparing data for Machine Learning pipelines is challenging.
- Machine Learning implies “learning” – the ability to generalize from experience – not yet there.

Thank you!

kostas@ece.utoronto.ca

www.dsp.utoronto.ca