Applied Machine Learning

Introduction

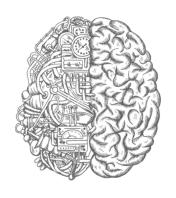
Isabeau Prémont-Schwarz



Outline

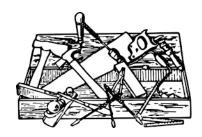
- a short history of machine learning
- understanding the scope of machine learning
 - relation to other areas
- understanding types of machine learning

What is Machine Learning?



ML is the set of "algorithms and statistical models that computer systems use to perform a specific task without using explicit instructions"

ML is the "study of computer algorithms that improve automatically through experience"



while there are some unifying principles, machine learning may still look like a toolbox with different tools suitable for different tasks

Placing Machine Learning

- **Artificial Intelligence**: it's a broader domain (includes search, planning, multiagent systems, robotics, etc.)
- **Statistics**: historically precedes ML. ML is more focused on algorithmic, practical and powerful models (e.g., neural networks) and is built around Al
- Vision & Natural Language Processing: use many ML algorithms and ideas
- Optimization: extensively used in ML
- Data mining: scalability, and performance comes before having theoretical foundations, more space for using heuristics, exploratory analysis, and unsupervised algorithms
- **Data science**: an umbrella term for the above mostly used in industry when the output is knowledge/information to be used for decision making

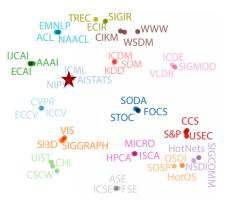


Figure from Dong et al.



- 1950: Turing test
- 1956: checker player that learned as it played (Arthur Samuel)
- 1958: first artificial neural networks called Perceptron (Frank Rosenblatt),
- 1963: support vector machines (Vapnick & Chervonenkis)
- 1969: Minskey and Pappert show the limitations of single-layer neural networks
- 1970-80s: rule-based and symbolic AI dominates (two AI winters)
- 1980's: Bayesian networks (Judea Pearl)
- 1986: Backpropagation rediscovered (Rumelhart, Hinton & Williams)
- 1980-1990s: expert systems are being replaced with general-purpose computers



- 2012: AlexNet wins Imagenet by a large margin
- 2012 now: a new Al spring around deep learning ...
- what is next?



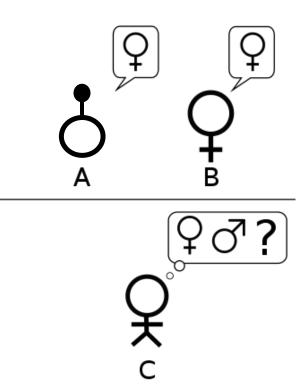


Turing test

In his paper on "Computing Machinery and Intelligence by Alan Turing (**1950**)", Turing tried to replace the abstract question of "can machine thinks?" with something more tangible, the Turing test designed based on a party game.



"What will happen when a machine takes the part of A in this [Imitation] game? Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman? These questions replace our original, "Can machines think?"



Player C, through a series of written questions, attempts to determine which of the other two players is a man, and which of the two is the woman. Player A, the man, tries to trick player C into making the wrong decision, while player B tries to help player C.

Artificial Intelligence

John McCarthy coined the term Artificial Intelligence (AI) and organized the first AI conference in 1956 to bring together researchers to design thinking machines, read more about it here





The Logic Theorist program, "the first artificial intelligence program", designed by Allen Newell, Herbert A. Simon and Cliff Shaw was presented in this conference. It was able to do automated reasoning, i.e. proving mathematical theorems from scratch by exploring a search tree, with the hypothesis as the root and branches as logical deductions, plus ad hoc rules, heuristics, to trim some branches and avoid exponential grow

[brute force or exhaustive search looks at all the possible options, to find the solution: a simple but expensive approach]

Machine Learning

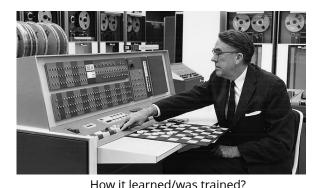
In 1959 Arthur Samuel popularized the term Machine Learning through his seminal paper on "Some Studies in Machine Learning Using the Game of Checkers"

" a computer can learn to play a better game of checkers than its programmer given only rule of the game, a sense of direction, and a redundant and incomplete list of parameters that have something to do with the game but whose values are unknown and unspecified. Programming computers to learn from experience should eventually eliminate the need for much of this detailed programming efforts.

Game as a vehicle for studying ML

many important concepts: self-play, temporal difference learning, function approximation

[you can read the paper here]



min-max search with alpha-beta pruning, learning to estimate the value of a state

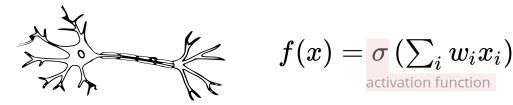
In 1954, four different IBM 704 machines working from midnight to 7 AM playing checkers with themselves and assimilating statistics that they used for the running scheme

[read about Samuel here]

Neural Networks

The Perceptron - A Perceiving and Recognizing Automaton by Frank Rosenblatt (1957), [you can read the pape, here]

The first device to think as the human brain, **learns by doing** based on McCullach-Pitts mathematical model of neurons (1943)



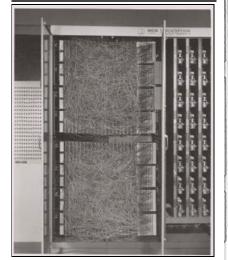
which was in turn based on **Hebbian learning**

We will discuss Perceptron later in the course

[read more about Perceptron here, and on Rosenblatt's here]



Mark I Perceptron machine (1958) **Custom built hardware**



Psychologist Shows Embry

NEW NAVY DEVICE LEARNS BY DOING

Books Today

[read the article from nytimes on July 8, 1958]

How do humans think?



Earliest works in the 1930s and 1940s by Donald Hebb, a psychologist at McGill, Studying behaviour in terms of brain function and connections between neuron assemblies

If an referring to the general type of studies based on Donald Hebb's work at McGIII. The argument goes something like this. The brain of man, like that of the animals, is made up of many cells of a certain type called neurons. These cells... react on an all-or-none basis ('fire'; ...) and transmit a pulse to other neurons through synaptic connections. Each neuron is connected to many others, and a number of input signals are, in general, required before a neuron will 'fire'. ...Learning seems to consist of alterations in the strength and even perhaps in the number of these synaptic interconnections. Now it is possible to devise a variety of mechanical, chemical, and electrical devices which simulate the behavior of individual neurons in a crude sort of way, and we can interconnect these devices in some random fashion to simulate the synaptic interconnections that exist within the brain, and, finally, we can arrange for the automatic strengthening or weakening of these interconnections using a training routine.



Early Real World Applications

ADALINE (Adaptive Linear Neuron) and MADALINE (Many ADALINEs) are similar to Perceptron and were proposed by Bernard Widrow et al., 1958 and 1960 [you can read the paper here]

Had many real-world applications including adaptive echo canceler for telephones, automatic equalizations for modems, speech and pattern recognition, weather forecasting etc. [read more about it, here]

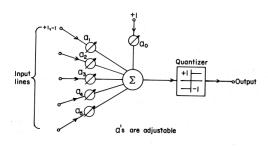


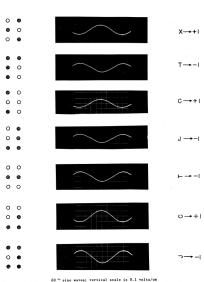
FIG. 1.-- AN ADJUSTABLE NEURON.

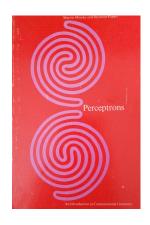
Trained using LMS algorithm: adjusting the weights based on the approximate gradient predecessor to backpropagation

Letter Recognition



FIG. 2.--ADALIS





- 1950: Turing test
- 1956: checker player that learned as it played (Arthur Samuel)
- 1958: first artificial neural networks called Perceptron (Frank Rosenblatt),
- 1963: support vector machines (Vapnick & Chervonenkis)
 - we will discuss SVM's idea later in the course
- 1969: Minskey and Pappert show the limitations of single-layer neural networks
 - for example, it cannot learn a simple XOR function
 - the limitation does not extend to a multilayer perceptron (which was known back then)
 - one of the factors in so-called Al winter
- **1970-80s**: rule-based and symbolic AI dominates
 - in contrast to connectionist AI as in neural networks
 - expert systems find applications in industry
 - these are rule-based systems with their specialized hardware

- 1950: Turing test
- 1956: checker player that learned as it played (Arthur Samuel)
- 1958: first artificial neural networks called Perceptron (Frank Rosenblatt),
- 1963: support vector machines (Vapnick & Chervonenkis)
- 1969: Minskey and Pappert show the limitations of single-layer neural networks
- 1970-80s: rule-based and symbolic AI dominates
- 1980s: Bayesian networks (Judea Pearl)
 - combine graph structure with probabilistic (and causal) reasoning
 - related to both symbolic and connectionist approach
- 1986: Backpropagation rediscovered (Rumelhart, Hinton & Williams)
 - an efficient method for learning the weights in neural networks using gradient descent
 - it was rediscovered many times since the 1960s
 - we discuss it later in the course
- 1980-1990s: expert systems are being replaced with general-purpose computers





- **1950**: Turing test
- 1956: checker player that learned as it played (Arthur Samuel)
- 1958: first artificial neural networks **Perceptron**, and **ADELINE** (1959)
- 1963: support vector machines (Vapnik & Chervonenkis)
- 1969: Minskey and Pappert show the limitations of single-layer Perceptron
- 1970-1980: ruled based and symbolic AI dominates
- **1980s**: Bayesian networks (Judea Pearl)
- 1986: Backpropagation rediscovered (Rumelhart, Hinton & Williams)
- **1980-1990s**: expert systems are being replaced with general-purpose computers



- 1997: Deep Blue beats the world chess champion
- **2012**: AlexNet wins Imagenet by a large margin
- 2012 now a new Al spring around deep learning ...
 - super-human performance in many tasks
 - **e.g.** AlphaGo defeats Go Master (2017)
- **Future:** what is next?
 - in the short term, Al will impact domain sciences



Basic Terminology

input features predictors independent variable covariate

ML algorithm —)
(hypothesis)

output
targets
labels
predictions
dependent variable
response variable

example

<tumorsize, texture, perimeter> = <18.2, 27.6, 117.5>



cancer = No

Basic Terminology

(labelled) datasets: consist of many training examples or instances

<tumorsize, perimeter="" texture,=""> , <cancer, change="" size=""></cancer,></tumorsize,>						
<18.2,	27.6,	117.5> , < No , +2 >	$x^{(1)}$			
<17.9,	10.3,	122.8> , < No , -4 >	$x^{(2)}$ one instance			
<20.2,	14.3,	111.2> , < Yes , +3 >	$x^{(3)}$			
		• •	• •			
<15.5,	15.2,	135.5> , < No , 0 >	$x^{(N)}$			

Basic Terminology

Ground-Truth, **True** labels

we split the dataset into **train** and **test** sets

Train dataset: <tumorsize, texture, perimeter> , <cancer, size change> used to build the model <18.2. 27.6. 117.5> , < No , +2 > 122.8> , < No , -4 > <17.9, 10.3, 111.2> , < Yes , +3 > <20.2. 14.3. 135.5> , < No , 0 > <15.5, 15.2, Test dataset: <tumorsize, texture, perimeter> <cancer, size change> used to evaluate the model <12.4, 15.7. 120.1> < No, +5 ><15.2. 17.2. 113.3> < Yes , +1 > <19.3, 15.9. 125.4> < No, +2 >< No, -3 ><17.5, 11.9. 122.7>

algorithm shouldn't have access to test set when being trained

<cancer, size change>
< Yes , +4 >
< Yes , +1 >
< No , +1 >
< Yes , -2 >

algorithm shouldn't see the true labels when being evaluated (making predictions on test set), these true labels are only used to compare against the algorithm's results to measure performance

Output labels, algorithm results

- 1. Supervised learning
- 2. Unsupervised & self-supervised learning
- 3. Semi-supervised learning
- 4. Reinforcement learning ...

1. Supervised learning: we have labeled data

most of this course

- classification
- regression

 ${\mathcal D}$: training set

x: D-dimensional vector

 $oldsymbol{y}$: a categorical or nominal variable

N : number of training instances

n: index of training instance ($n \in \{1...N\}$)

 $\mathcal{D} = \{(x^{(n)}, y^{(n)})\}_{n=1}^N$

pairs of input vector and corresponding target or label

	<tumorsize, perimeter="" texture,=""> , <cancer></cancer></tumorsize,>						
$x^{(1)}$	<18.2,	27.6,	117.5> ,	< No >	$y^{(1)}$		
$x^{(2)}$	<17.9,	10.3,	122.8> ,	< No >	$y^{(2)}$		
$x^{(3)}$	<20.2,	14.3,	111.2> ,	< Yes >	$y^{(3)}$		
÷			:		:		
$x^{(N)}$	<15.5,	15.2,	135.5> ,	< No >	$y^{(N)}$		

1. Supervised learning: we have labeled data

most of this course

- classification
- regression

$$\mathcal{D} = \{(x^{(n)}, y^{(n)})\}_{n=1}^N$$

$$x^{(n)}=(x_1^{(n)},x_2^{(n)})$$

shows samples with desired output to the algorithm to learn from it

1. Supervised learning: we have labeled data

Classification: categorical/discrete output

<tumorsize, texture, perimeter>, <cancer><18.2,</td>27.6,117.5>, < No ><17.9,</td>10.3,122.8>, < No ><20.2,</td>14.3,111.2>, < Yes ><15.5,</td>15.2,135.5>, < No >

Regression: continuous output

<tumorsize< th=""><th>e, texture, p</th><th>erimeter> , ·</th><th><size change=""></size></th></tumorsize<>	e, texture, p	erimeter> , ·	<size change=""></size>
<18.2,	27.6,	117.5> ,	< +2 >
<17.9,	10.3,	122.8> ,	< -4 >
<20.2,	14.3,	111.2> ,	< +3 >
<15.5,	15.2,	135.5> ,	< 0 >

target

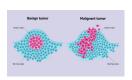
target

1. Supervised learning: we have labeled data

Classification: categorical/discrete output

binary classification

classifying benign (noncancerous) vs malignant (cancerous) tutors



<tumorsize< th=""><th>perimeter> ,</th><th><cancer></cancer></th></tumorsize<>	perimeter> ,	<cancer></cancer>	
<18.2,	27.6,	117.5> ,	< No >
<17.9,	10.3,	122.8> ,	< No >
<20.2,	14.3,	111.2> ,	< Yes >
<15.5,	15.2,	135.5> ,	< No >

multiclass classification

classifying Iris flowers

N = 150 instances of flowers

D=4 features {the length and the width of the sepals and petals}

C=3 classes {setosa, versicolor, virginica}: 50 samples of each

		,		0 ,	· · · · · · · · · · · · · · · · · · ·
index	$_{ m sl}$	sw	pl	pw	label
0	5.1	3.5	1.4	0.2	Setosa
1	4.9	3.0	1.4	0.2	Setosa
50	7.0	3.2	4.7	1.4	Versicolor
149	5.9	3.0	5.1	1.8	Virginica



1. Supervised learning: we have labeled data

classifying Iris flowers

N = 150 instances of flowers

D=4 features {the length and the width of the sepals and petals}

C=3 classes {setosa, versicolor, virginica} : 50 samples of each

index	$_{ m sl}$	$\mathbf{s}\mathbf{w}$	$_{ m pl}$	$\mathbf{p}\mathbf{w}$	label
0	5.1	3.5	1.4	0.2	Setosa
1	4.9	3.0	1.4	0.2	Setosa
50	7.0	3.2	4.7	1.4	Versicolor
149	5.9	3.0	5.1	1.8	Virginica

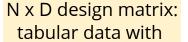
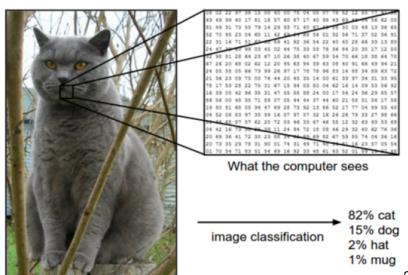








Image classification



MIT Technology Review

Topics+

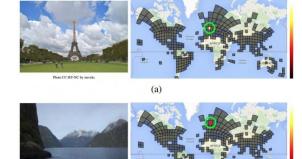
The Download

Intelligent Machines

Google Unveils Neural Network with "Superhuman" Ability to Determine the Location of Almost Any Image

Guessing the location of a randomly chosen Street View image is hard, even for well-traveled humans. But Google's latest artificial-intelligence machine manages it with relative ease.

by Emerging Technology from the arXiv February 24, 2016



trained on a database of geolocated images from the Web

[read about it here]

DeepL schools other online translators with clever machine learning



trained using billions of high-quality translation segments from reliable sources such as the European Parliament, Unesco patents, and literary works, bilingual sentences collected by Linguee's web crawler on the Internet

Machine Translation: data consists of input-output sentence pairs (x,y), similarly we may consider **text-to-speech**, with text and voice as input and target (x,y), or **speech recognition** where input and output above are swapped.

[read about it here, try it out here]

Supervised methods are powered by large datasets often crawled from the web or curated with crowdsourcing

What is COCO?



COCO is a large-scale object detection, segmentation, and captioning dataset. COCO has several features:

- **✓** Object segmentation
- Recognition in context
- **✓** Superpixel stuff segmentation
- 330K images (>200K labeled)
- ✓ 1.5 million object instances
- ◆ 80 object categories
- 91 stuff categories
- 5 captions per image
- **★** 250,000 people with keypoints



Fig. 6: Samples of annotated images in the MS COCO dataset.

Object Recognition

image: https://bitmovin.com/object-detection/

input: image

output: a set of bounding box

coordinates

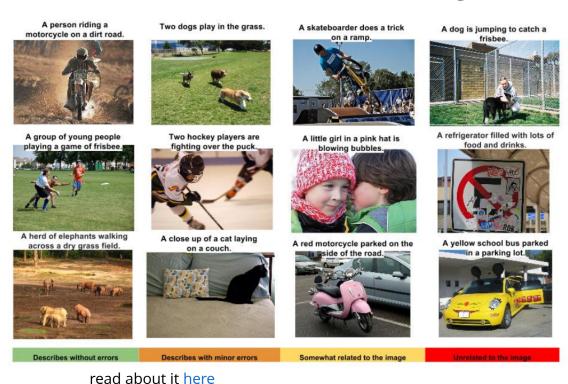


Image Captioning

input: image output: text



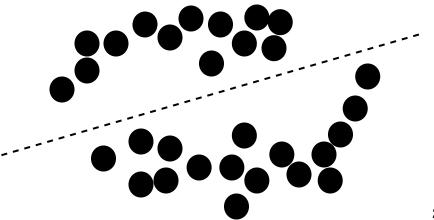
DALL·E: Creating Images from Text

2. Unsupervised Learning: only unlabeled data

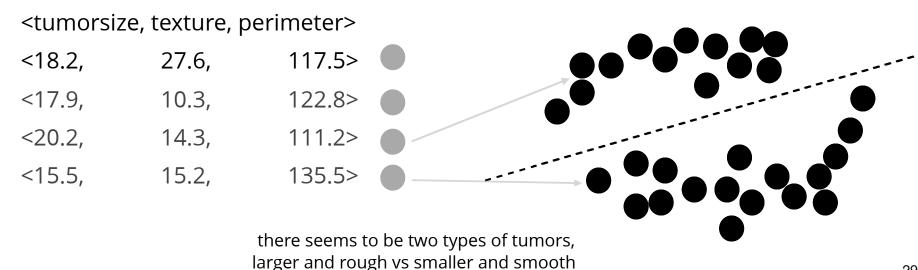
- clustering
- dimensionality reduction
- density estimation / generative modeling
- anomaly detection
- discovering latent factors and structures

The algorithm doesn't see the desired outputs, mines the patterns in the input data

- helps explore and understand the data
- closer to data mining
- we have much more unlabeled data
- more open challenges



Clustering: similar to classification but labels/classes should be inferred and are not given to the algorithm



Clustering: similar to classification but labels/classes should be inferred and are not given to the algorithm

clustering Iris flowers

N = 150 instances of flowers

D=4 features {the length and the width of the sepals and petals}

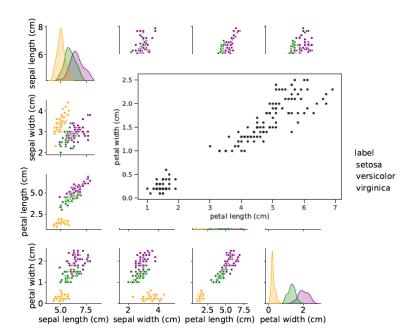
C=3 classes {setosa, versicolor, virginica} : 50 samples of each

inde	x	sl	sw	pl	pw	label
	0	5.1	3.5	1.4	0.2	Setosa
	1	4.9	3.0	1.4	0.2	Setosa
5	0	7.0	3.2	4.7	1.4	Versicolor
14	9	5.9	3.0	5.1	1.8	Virginica



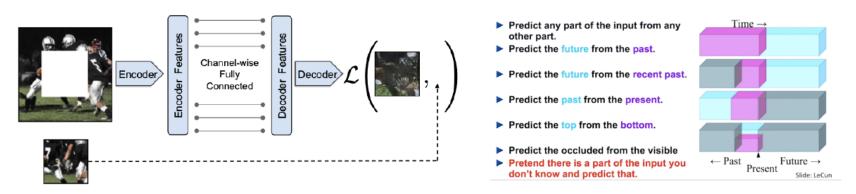






Self supervised learning: create proxy supervised tasks from unlabeled data, e.g. predict a color image from a grayscale image or mask out words in a sentence and then try to predict them given the surrounding context

Goal: learn useful features from the data, that can then be used in standard, downstream supervised tasks [see a list of relevant papers here]



Let's make [MASK] chicken! [SEP] It [MASK] great with orange sauce.

Generative Modelling: model the distribution of the data and learns to generate the data instead of directly categorizing/discriminating the instances into different classes.



Generate faces that look like celebrity images

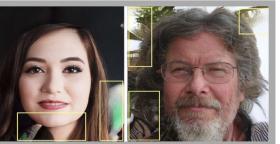
from the paper here

click here to get a random fake person

Ethical Challenges: Misuse

Facebook Removes Accounts With Al-Generated Profile Photos

Researchers said it appears to be the first use of artificial intelligence to support an inauthentic social media campaign.



Profile pictures for Facebook accounts "Mary Keen" and "Jacobs Guillermo," admins on groups associated with The BL highlighted by Graphika. COURTESY OF GRAPHIKA

How a fake persona laid the groundwork for a Hunter Biden conspiracy deluge



A viral dossier about Hunter Biden was written by "Martin Aspen," a fake identity whose profile picture was created by artificial intelligence. TyphoonInvesti1 / via Twitter

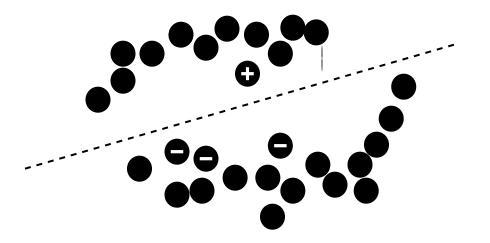
Experts: Spy used Al-generated face to connect with targets



3. **Semisupervised learning:** a few labeled examples

- we can include structured problems such as
 - matrix completion (a few entries are observed)
 - link prediction

The algorithm sees few examples of the desired outputs

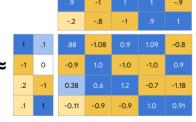


Matrix Completion in Recommendation Systems

Predict what movies you will like based on what you liked sofar and what others users liked who like similar movies to you

Ethical
Challenges:
Privacy of Users
Polarizing Users





[figure from here]

Netflix Awards \$1 Million Prize and Starts a New Contest



Jason Kempin/Getty Images Netflix prize winners, from left: Yehuda Koren, Martin Chabbert, Martin Piotte, Michael Jahrer, Andreas Toscher, Chris Volinsky and Robert Bell.

Update | 1:45 p.m. Adding details announced Monday about the extremely close finish to the contest.

[read about it here]

RYAN SINGEL SECURITY 03.12.10 02:40 PM

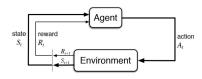
NetFlix Cancels Recommendation Contest After Privacy Lawsuit



Netflix is canceling its second \$1 million Netflix Prize to settle a legal challenge that it breached customer privacy as part of the first contest's race for a better movie-recommendation engin@A

4. Reinforcement Learning:

- weak supervision through the reward signal
- sequential decision making
- biologically motivated



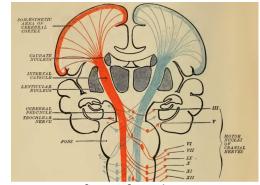


figure from here

also related:

imitation learning: learning from demonstrations

- behavior cloning (is supervised learning!)
- inverse reinforcement learning (learning the reward function)



figure from here

Reinforcement Learning: Examples



Human Level Control Through Deep Reinforcement Learning

Abstract

The theory of reinforcement learning provides a normative account deeply rooted in psychological and neuroscientific perspectives on animal behaviour, of how agents may optimize their control of an environment. To use reinforcement learning successfully in situations approaching real-world complexity, however, agents are confronted with a difficult task: they must derive efficient

Playing Atari like a pro 2015, see here

Google's AlphaGo Defeats Chinese Go Master in Win for A.I.



Ke Jie, the world's top Go player, reacting during his match on Tuesday against AlphaGo, artificial intelligence

Summary

Supervised Learning: we have labeled data

- classification
- regression

Unsupervised Learning: only unlabeled data

- clustering & self-supervised learning
- density estimation / generative modeling

Semisupervised learning: a few labeled examples

Reinforcement Learning: reward signal