Part 5:

Introduction into artificial intelligence, machine learning and data science

Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination

Introduction to AI, ML, and DS

Part 1: What is AI? From various perspectives

Part 2: AI techniques

Part 3: AI technologies

Part 1: Introduction

What is AI? from various perspectives…

Review and introduction

(we'll get back to different topics later)

Today's Reading:
Luger 1.1.1 – 1.1.3, 1.2 – 1.4
RN sec. 1

Pause watching …

Answer the question: What is AI? in your opinion

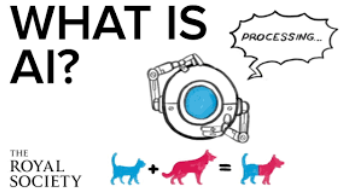
Other questions:

What are AI major features, characteristics?

What makes AI different?

watch video

https://www.youtube.com/watch?v=nASDYRkbQIY



Agenda: What is AI ? from various perspectives

1) Holywood
2) World
3) History
4) Academic
5) Practical (but still rather academic)
6) Competition
7) Business
8) Industry

6

What is AI from Holywood perspective

watch video ies.

- The Top 19 Artificial Intelligence Movies

See
https://www.youtube.com/watch?v=C23Z3ANGk-U

Pause watching …

Answer the question: What is your favorite AI movie?

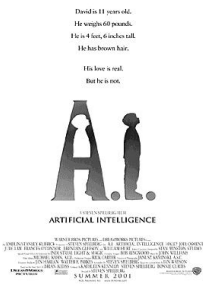
Possible answer: I do not watch movies, I code all my time…

What is AI?

- Director:

Steven Spielberg
Stars: Jude Law, Haley Joel Osment, Frances O'Connor

Plot: In the wake of an environmental disaster, a new kind of self-aware computer is created



What is AI from the World perspective?

A view of the world: Three segments –

Segment 1 – Totally known segment.

- All knowledge in this segment is known→ Methods exist for all problems →
- Solutions are method oriented. Underlying patterns can be ignored.
- Example - Find the square root of a number.

Pause watching …

Answer the question: How much AI is there?

Source: B. Arunkumar, Combatore IT

What is AI from the World perspective

A view of the world: Three segments –

Segment 3 - Totally Unknown

- Hardly anything of topics in this area is known. → Human beings are themselves unable to do much here.
- Example - Life on other planets

Pause watching …

Answer the question: How much AI is there?

Source: B. Arunkumar, Combatore IT

What is AI from the World perspective

A view of the world: Three segments –

Segment 2 – Partially Known.

- Quite a lot is known about topics in this segment, but not everything. => Incomplete, Ambiguous patterns.
- Example – Diagnosing diseases.

Pause watching …

- **Answer the question:**

Where does AI belong?

Source: B. Arunkumar, Combatore IT

Major difference between AI and conventional programming techniques

Understanding
Intelligent systems understand like humans do.

Reasoning
They reason. They understand underlying ideas and concepts. They form hypothesis. They infer and extract concepts.

Learning
They never stop learning getting more valuable with time. Advancing with each new piece of information, interaction, and outcome. They develop "expertise".

Traditional Programming

Machine Learning

ANY questions, comments??

Please, Pause watching …

Look again at the previous slide

Answer the question: Am I ready to change my thinking?

This answer is very important not only for your success in this class but for your professional development

• Definition

•Artificial intelligence (AI) is intelligence exhibited by machines. In computer science, the field of AI research defines itself as the study of "intelligent agents"

•Artificial intelligence is technology that appears to emulate human performance typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people.

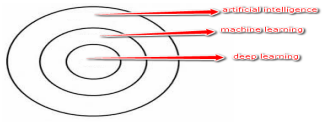
Gartner

•The capability of a functional unit to perform functions that are generally associated with human intelligence such as reasoning and learning. (ISO/IEC 2382-28:1995)

ISO IEC

26-27 September 2017

• Definition



Here is an image that attempts to visualize the distinction between Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL)
Watch: https://www.youtube.com/watch?v=481hvfIVBaw

https://www.youtube.com/watch?v=q7bKMHdxtPU

26-27 September 2017

What is AI from the historical perspective?

- Although the term of AI has been widely used for quite a long time with steadily increasing amount of research and applications, there is no anonymously accepted definition. AI can mean many things to different people and various techniques are considered as belonging to AI.
- The term coined in 1956 by J. McCarthy at MIT
- Two branches: engineering discipline dealing with the creation of intelligent machines and empirical science concerned with the computational modelling of human intelligence
- The goal of AI is developing methods, which allow producing thinking machines that can solve problems
- Which problems?
  - ill-defined and ill-structured
  - complicated taxonomy or classifying
  - Combinatorial optimization

What is AI again? From the historical perspectives

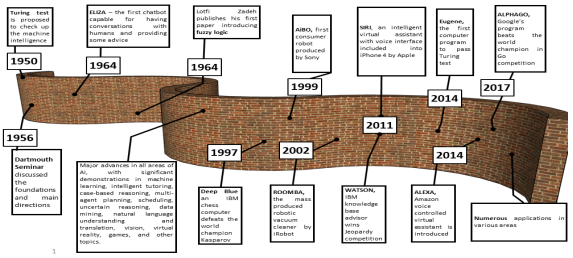
- The great variety of AI techniques have been developed and applied over the history for solving the problems mentioned above.
- Some of these methodologies are "conventional" or "old" methods (1950s):

- search algorithms,
- Probabilistic reasoning,
- natural language processing,
- belief networks, etc.

- Others are "new" (1960s) – soft computing and computational intelligence

What is AI again? From the historical perspectives

Brief history of AI achievements



AI History (old)

- **Philosophy Foundations (400 B.C. – present)**
  - **Mind: dualism (Descartes), materialism (Leibniz), empiricism (Bacon, Locke)**
  - **Thought: syllogism (Aristotle), induction (Hume), logical positivism (Russell)**
  - **Rational agentry (Mill)**
- **Mathematical Foundations (c. 800 – present)**
  - **Early: algorithms (al-Khowarazmi, 9th century Arab mathematician), Boolean logic**
  - **Computability (20th century – present)**
    - **Cantor diagonalization, Gödel's incompleteness theorem**
    - **Formal computuational models: Hilbert's Entscheidungsproblem, Turing**
    - **Intractability and NP-completeness**

AI History (not too old)

- **Computer Engineering (1940 – present)**
- **Linguistics (1957 – present)**
- **Stages of AI**

Gestation (1943 – c. 1956), infancy (c. 1952 – 1969)

Disillusioned early (c. 1966 – 1974), later childhood (1969 – 1979)

"Early" (1980 – 1988), "middle" adolescence (c. 1985 – present)

The history of artificial intelligence (birth)

The birth of artificial intelligence (1943 – 1956)

The first work recognised in the field of AI was presented by **Warren McCulloch** and **Walter Pitts** in 1943. They proposed a model of an artificial neural network and demonstrated that simple network structures could learn.

McCulloch, the second "founding father" of AI after Alan Turing, had created the corner stone of neural computing and artificial neural networks (ANN).

The third founder of AI was **John von Neumann**, the brilliant Hungarian-born mathematician. In 1930, he joined the Princeton University, lecturing in mathematical physics. He was an adviser for the Electronic Numerical Integrator and Calculator project at the University of Pennsylvania and helped to design the **Electronic Discrete Variable Calculator**.

He was influenced by McCulloch and Pitts's neural network model. When **Marvin Minsky** and **Dean Edmonds**, two graduate students in the Princeton mathematics department, built the first neural network computer in 1951, von Neumann encouraged and supported them.

- Another of the first generation researchers was **Claude Shannon**. He graduated from MIT and joined Bell Telephone Laboratories in 1941. Shannon shared Alan Turing's ideas on the possibility of machine intelligence. In 1950, he published a paper on chess-playing machines, which pointed out that a typical chess game involved about 10^{120} possible moves (Shannon, 1950). Even if the new von Neumann-type computer could examine one move per microsecond, it would take 3×10^{106} years to make its first move. Thus Shannon demonstrated the need to use heuristics in the search for the solution.

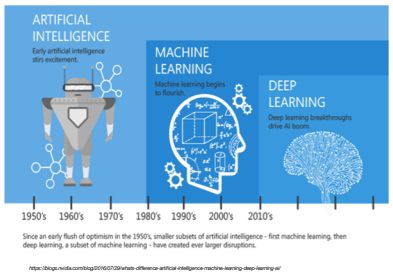
- In 1956, **John McCarthy**, **Marvin Minsky** and **Claude Shannon** organised a summer workshop at Dartmouth College. They brought together researchers interested in the study of machine intelligence, artificial neural nets and automata theory. Although there were just ten researchers, this workshop gave birth to a new science called ***artificial intelligence***.

The rise of artificial intelligence, or the era of great expectations (1956 – late 1960s)

- The early works on neural computing and artificial neural networks started by McCulloch and Pitts was continued. Learning methods were improved and **Frank Rosenblatt** proved the ***perceptron convergence theorem***, demonstrating that his learning algorithm could adjust the connection strengths of a perceptron.

- One of the most ambitious projects of the era of great expectations was the **General Problem Solver (GPS)**. **Allen Newell** and **Herbert Simon** from the Carnegie Mellon University developed a general-purpose program to simulate human-solving methods.
- Newell and Simon postulated that a problem to be solved could be defined in terms of ***states***. They used the mean-end analysis to determine a difference between the current and desirable or *goal state* of the problem, and to choose and apply *operators* to reach the goal state. The set of operators determined the solution plan.

- However, GPS failed to solve complex problems. The program was based on formal logic and could generate an infinite number of possible operators. The amount of computer time and memory that GPS required to solve real-world problems led to the project being abandoned.
- In the sixties, AI researchers attempted to simulate the thinking process by inventing *general methods* for solving *broad classes of problems*. They used the general-purpose search mechanism to find a solution to the problem. Such approaches, now referred to as ***weak methods***, applied weak information about the problem domain.



What is AI again? From the historical perspectives

Modern AI:

- More rigorous, scientific, formal/mathematical
- Fewer grandiose promises
- Divided into many subareas invested in particular aspects
- More directly connected to "neighboring" disciplines
  - Theoretical computer science, statistics, economics, operations research, biology, psychology/neuroscience, …
  - Often leads to question "Is this really AI"?
- Some senior AI researchers are calling for re-integration of all these topics, return to more grandiose goals of AI
  - Somewhat risky proposition for graduate students and junior faculty…

A Brief History of Artificial Intelligence

- Time: 2:50
- Watch: https://www.youtube.com/watch?v=056v4OxKwlI

Answer the questions:

What will be the major AI development of the next decade?

32

What is AI again? From the academic perspectives

- **Intelligent systems**

  Four Categories of Systemic Definitions
  - **1. Think like humans**
  - **2. Act like humans**
  - **3. Think *rationally***
  - **4. Act *rationally***

What is AI again? Systematic approach

- **Thinking Like Humans**
  - ***Machines with minds*** **(Haugeland, 1985)**
  - **Automation of "decision making, problem solving, learning…" (Bellman, 1978)**
- **Acting Like Humans**
  - ***Functions*** **that *require intelligence when performed by people* (Kurzweil, 1990)**
  - **Making computers do things *people currently do better* (Rich and Knight, 1991)**
- **Thinking Rationally**
  - **Computational models of mental faculties (Charniak and McDermott, 1985)**
  - **Computations that make it possible to *perceive, reason*, and *act* (Winston, 1992)**
- **Acting Rationally**
  - **Explaining, emulating intelligent behavior via computation (Schalkoff, 1990)**
  - **Branch of CS concerned with automation of intelligent behavior (Luger and Stubblefield, 1993)**

What is AI?
Thinking and Acting Like Humans

- **Concerns: Human Performance (Figure 1.1 R&N, Left-Hand Side)**
  - **Top: thought processes and reasoning (learning and inference)**
  - **Bottom: behavior (interacting with environment)**
- **Machines With Minds**
  - **Cognitive modelling**
    - **Early historical examples: problem solvers (see R&N Section 1.1)**
    - **Application (and one driving force) of cognitive science**
  - **Deeper questions**
    - **What is intelligence?**
    - **What is consciousness?**
- **Acting Humanly: The Turing Test Approach**
  - **Capabilities required**
    - **Natural language processing**
    - **Knowledge representation**
    - **Automated reasoning**
    - **Machine learning**
  - **Turing Test: can a machine appear indistinguishable from a human to an experimenter?**

What is AI again? From the practical (but still academic) perspectives

One of the most significant papers on machine intelligence, ***"Computing Machinery and Intelligence"***, was written by the British mathematician ***Alan Turing*** over fifty years ago . However, it still stands up well under the test of time, and the Turing's approach remains universal.

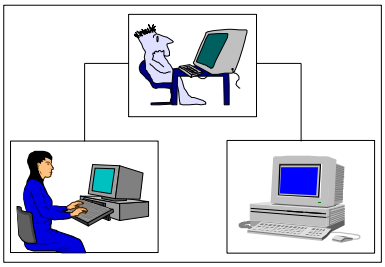
See the presentation about Turing test and ideas at https://www.youtube.com/watch?v=njmAUhUwKys

- Turing did not provide definitions of machines and thinking, he just avoided semantic arguments by inventing a game, the ***Turing Imitation Game***.
- The imitation game originally included two phases. In the first phase, the interrogator, a man and a woman are each placed in separate rooms. The interrogator's objective is to work out who is the man and who is the woman by questioning them. The man should attempt to deceive the interrogator that *he* is the woman, while the woman has to convince the interrogator that *she* is the woman.

Turing Imitation Game: Phase 2

- In the second phase of the game, the man is replaced by a computer programmed to deceive the interrogator as the man did. It would even be programmed to make mistakes and provide fuzzy answers in the way a human would. If the computer can fool the interrogator as often as the man did, we may say this computer has passed the intelligent behaviour test.

Turing Imitation Game: Phase 2



The Turing test has two remarkable qualities that make it really universal.

- By maintaining communication between the human and the machine via terminals, the test gives us an objective standard view on intelligence.
- The test itself is quite independent from the details of the experiment. It can be conducted as a two-phase game, or even as a single-phase game when the interrogator needs to choose between the human and the machine from the beginning of the test.

- Turing believed that by the end of the 20th century it would be possible to program a digital computer to play the imitation game. Turing test has been passed in June 2014 by a computer program called Eugene Goostman, which simulates a 13-year-old Ukrainian boy. Turing test provides a basis for the verification and validation of knowledge-based systems.
- **A program thought intelligent in some narrow area of expertise is evaluated by comparing its performance with the performance of a human expert.**
- To build an intelligent computer system, we have to capture, organise and use human expert knowledge in some narrow area of expertise.

watch video

- See the presentation about Turing test and ideas https://video.rit.edu/hapi/v1/contents/06e26b70-0696-470c-86a5-14a5c7f99a84/preview
- See the presentation about virtual assistants of the present and future https://video.rit.edu/hapi/v1/contents/a9aa95c7-3c4a-40ae-af9a-a59f1a7de15d/preview

What is AI again?
From perspectives of competing with humans

Watson defeats Jeopardy champions (2011)

DeepMind achieves human-level performance on many Atari games (2015)

AlphaGo defeats Go champion (2016)

CMU's Libratus defeats top human poker players (2017)

https://www.youtube.com/watch?v=P18EdAKuC1U
https://www.youtube.com/watch?v=8dMFIpEGNLQ
https://www.youtube.com/watch?v=CRiH8yCskAE

Source: Vincent Conitzer, Duke Uni

What is AI again?
From the business perspectives

- Microsoft, Amid Dwindling Interest, Talks Up Computing as a Career March 1, 2004 By STEVE LOHR
Mr. Gates scoffed at the notion, advanced by some, that the computer industry was a mature business of waning opportunity. In one question-and-answer session, a student asked if there could ever be another technology company as successful as Microsoft.
"If you invent a breakthrough in artificial intelligence, so machines can learn," Mr. Gates responded, "that is worth 10 Microsofts."
source:
http://www.nytimes.com/2004/03/01/technology/01bill.html?ex=1079243652&ei=1&en=c1b404b245663675

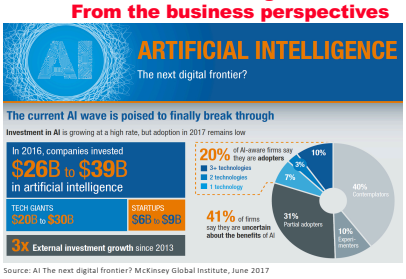
Mark Cuban: The world's first trillionaire will be an artificial intelligence entrepreneur — CNBC, March 13, 2017

- "I am telling you, the world's first trillionaires are going to come from somebody who masters AI and all its derivatives and applies it in ways we never thought of," says the star investor of ABC's "Shark Tank,"
- Ever faster computer processors and exponentially larger data sets are creating opportunity to apply artificial intelligence to new industries like insurance, says Cuban .
- We will "see more technological advances over the next ten years than we have over the last thirty. It's just going to blow everything away," says Cuban , who himself started out as the child of a blue-collar family from Pittsburgh.

Mark Cuban: The world's first trillionaire will be an artificial intelligence entrepreneur — CNBC, March 13, 2017

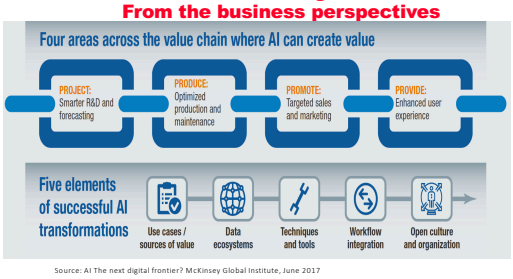
- He and Todd Wagner launched the internet start-up Broadcast.com and sold it to Yahoo for $5.7 billion in 1999.
- Google recently started using AI and has added $9 billion to its revenues as a result, Cuban has been told by sources within the Internet search giant.
- "Whatever you are studying right now if you are not getting up to speed on deep learning, neural networks, etc., you lose," says Cuban. "We are going through the process where software will automate software, automation will automate automation."
- **Watch** https://www.youtube.com/watch?v=Hs2d6U_XDsw

What is AI again?
From the business perspectives



Source: AI The next digital frontier? McKinsey Global Institute, June 2017

What is AI again?
From the business perspectives



Source: AI The next digital frontier? McKinsey Global Institute, June 2017

What is AI again? From the practical (now real) industry perspectives

See AI at Google at https://ai.google

Microsoft at https://www.microsoft.com/en-us/ai?activetab=pivot1%3aprimaryr5

Facebook at https://ai.facebook.com

Amazon at https://blog.aboutamazon.com/amazon-ai and https://www.forbes.com/sites/blakemorgan/2018/07/16/how-amazon-has-re-organized-around-artificial-intelligence-and-machine-learning/#709e41cd7361

Visit for Ideas

What is AI again? From the practical (now real) industry perspectives

IBM - https://www.research.ibm.com/artificial-intelligence/

Intel - https://www.intel.ai/#gs.ihwdhz

NVDIA - https://www.nvidia.com/en-us/deep-learning-ai/

Visit for Ideas

What is AI?

watch video

What is Artificial Intelligence (or Machine Learning)?
https://www.youtube.com/watch?v=mJeNghZXtMo

How artificial intelligence will change your world, for better or worse
https://www.youtube.com/watch?v=XvzNuw5VjBU

Part 2: AI techniques

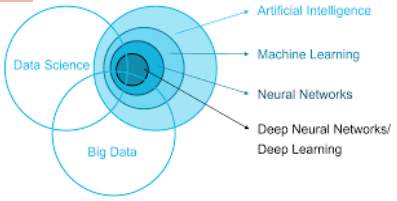
Pause watching …

Answer the question: Name as many AI techniques as you can now

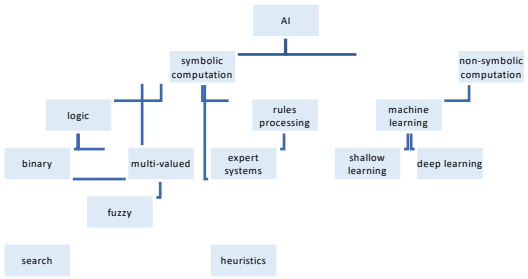
watch video https://www.youtube.com/watch?v=uhVLySyLWd4

Exploring AI: AI techniques

What is their relationship?



AI techniques – an Overview



AI techniques – an Overview

Artificial intelligence techniques can be divided into two types:

1. Symbolic Computation has two branches

1. Heuristic search – Adjoining, Segment 1 of the World view.
   Heuristic – A guide, an approximation, a thumb rule. Basically helps in pruning the search tree.
2. Knowledge-based systems – In the world view, between heuristic search and sub-symbolic computation.
   Knowledge – Data is an understood, recognized format, Information is Useful data and Knowledge is Generalized Information. => Concepts, Patterns.

2. **Non- symbolic computation**

AI techniques overview – an Overview

Knowledge Based Systems:

Core Areas of Knowledge Based systems

1. Knowledge Base Representation
2. Inference Engine
3. User interface
4. Knowledge acquisition module

AI techniques– an Overview

Representation techniques are primarily:

1. Production rules – sets of if-then rules, similar to production rules used to specify a grammar.
   Example: If the car does not start check the battery, by pressing the horn.
2. Semantic Networks – Set of Nodes and Links between them. The links represent Relationships between the nodes
   Example: Nodes – Man, Hands, Legs, Walk

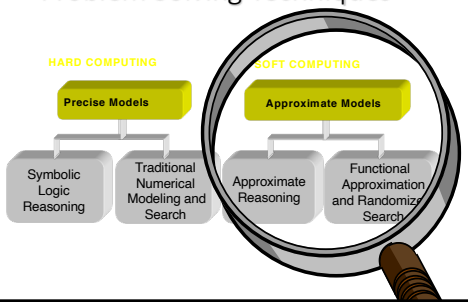
Relationships – Has (between Man and hands and between Man and Legs) and Can (between Man and Walk).

A type of Semantic networks is Frames (Slot-filler notation). These encode default (commonly occurring) values (filler) for the attributes in a relation (slot).

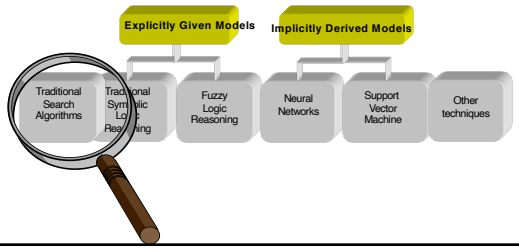
Soft Computing

- Soft Computing (SC): the symbiotic use of many emerging problem-solving disciplines.
- According to Prof. Zadeh:
  "...in contrast to traditional hard computing, soft computing exploits the tolerance for imprecision, uncertainty, and partial truth to achieve tractability, robustness, low solution-cost, and better rapport with reality"
- Soft Computing Main Components:
  -Approximate Reasoning:
  » Probabilistic Reasoning, Fuzzy Logic
  -Search & Optimization:
  » Neural Networks, Evolutionary Algorithms

Problem Solving Techniques



Knowledge classification: models



Pause watching …

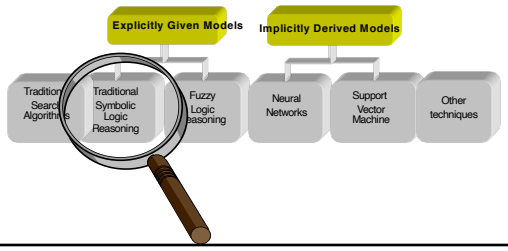
Answer the questions:

1. **What search algorithms do you remember?**
2. **Which ones could be employed in AI?**
3. **Which ones are ACTUALLY AI?**

watch video — Search algorithms types

@ https://www.youtube.com/watch?v=AneIXxdu_g4

Knowledge classification: models



Rules as a knowledge representation technique

- The term *rule* in AI, which is the most commonly used type of knowledge representation, can be defined as an IF-THEN structure that relates given information or facts in the IF part to some action in the THEN part. A rule provides some description of how to solve a problem. Rules are relatively easy to create and understand.
- Any rule consists of two parts: the IF part, called the *antecedent* (*premise* or *condition*) and the THEN part called the *consequent* (*conclusion* or *action*).

Rules systems generic examples

IF antecedent
THEN consequent

A rule can have multiple antecedents joined by the keywords **AND** (**conjunction**), **OR** (**disjunction**) or a combination of both.

IF antecedent 1
AND antecedent 2
⋮
AND antecedent *n*
THEN consequent

IF antecedent 1
OR antecedent 2
⋮
OR antecedent *n*
THEN consequent

67

Rules systems specific examples

IF packet origin address is xxx
THEN attack AAA

- A rule can have multiple antecedents joined by the keywords **AND** (**conjunction**), **OR** (**disjunction**) or a combination of both.

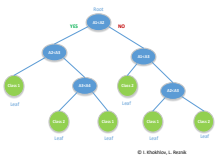
IF packet destination address is AAA2
AND port number is CCC1 **OR** CCC2
⋮ ⋮
AND OR antecedent *n*
THEN consequent
THEN consequent

68

Decision Trees

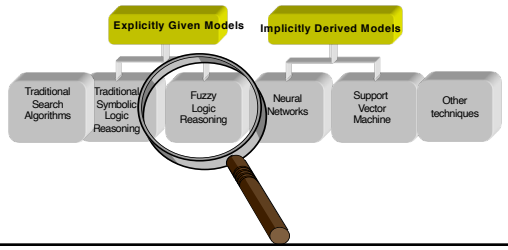
J48 Decision Tree:

1. Based on the training set we identify the attribute that discriminates the various instances most clearly or the highest possible gain
2. If we can get 100% classification – end
3. For other cases, we look for another attribute that gives us the highest information gain
4. Continue



69

Knowledge classification: models



Fuzzy Logic Genealogy

Origins: MVL for treatment of imprecision and vagueness

- **1930s**: Post, Kleene, and Lukasiewicz attempted to represent *undetermined*, *unknown,* and other possible intermediate truth-values.
- **1937**: Max Black suggested the use of a *consistency profile* to represent vague (ambiguous) concepts
- **1965**: Lotfi Zadeh proposed a complete theory of fuzzy sets (and its isomorphic fuzzy logic), to represent and manipulate ill-defined concepts

71

Fuzzy Logic : Linguistic Variables

•Fuzzy logic gives us a language (with syntax and local semantics), in which we can translate our qualitative domain knowledge.

- Linguistic variables model dynamic systems
- These variables take linguistic values that are characterized by:
  - a label - a sentence generated from the syntax
  - a meaning - a membership function determined by a local semantic procedure

72

Fuzzy Logic : Reasoning Methods

- The meaning of a linguistic variable may be interpreted as an elastic constraint on its value.
- These constraints are propagated by fuzzy inference operations, based on the generalized *processing engine*
- A FL Controller (FLC) applies this reasoning system to a Knowledge Base (KB) containing the problem domain heuristics.
- The inference is the result of interpolating among the outputs of all relevant rules.
- The outcome is a membership distribution on the output space, which is defuzzified to produce a crisp output.

73

watch video

What is fuzzy logic?

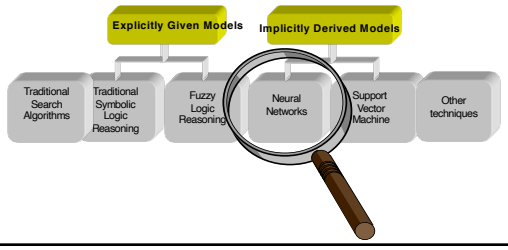
- Watch:

https://www.youtube.com/watch?v=rIn_kZbYaWc
https://www.youtube.com/watch?v=M4KJHddlyqE
https://www.youtube.com/watch?v=P8wY6mi1vV8

Answer the questions:

What are the main differences between binary and fuzzy logic?

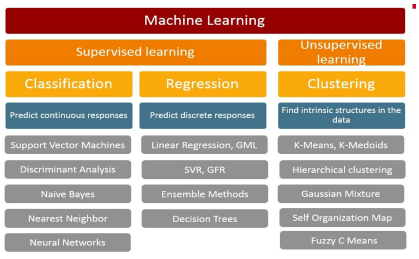
Knowledge classification: models



Pause watching …

Answer the questions:

1. **What do you know about machine learning?**
2. **What differentiates ML from other AI?**
3. **Which ML techniques do you remember?**



Source: steemit.com

watch video

Machine learning basics

@
https://www.youtube.com/watch?v=ukzFI9rgwfU

AI techniques– an Overview

Sub Symbolic Computation (Neurocomputing):

Adjoins Segment 3 of the world view.

Deals with signal level computation.

Required because a number of problems do not have explicit knowledge associated with them. Example – recognizing people or recognizing handwriting.

This area deals with patterns that are more complex than the ones dealt with by symbolic computation.

AI techniques– an Overview

Core areas of Sub-symbolic computation are:

1. Architecture
2. Learning mechanism

In sub-symbolic computation all the knowledge is learnt by the system.

Neuro-computing attempts to mimic the structure of the human intelligence system, with its neurons and synapses.

Neuron – receives input from many other neurons. Each input is magnified by a multiplication factor. (This multiplication factor represents the degree of interest, effect that the particular input has on the neuron.)

All the multiplied values are summed up and compared to a 'threshold value'. If the threshold value is less then the neuron fires an output.

AI techniques– an Overview

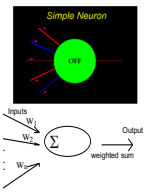
Knowledge is acquired by learning the correct multiplication values.

Learning is done in one of three ways:

1. Supervised learning - Here the desired output for a given input is known. A simple method is Back Propagation. Here the real output is compared with the desired output. Differences are propagated backwards, to make changes to the multiplication factors.
2. Unsupervised learning – Here the desired output is not given to the system. The system uses Clustering to club similar input together. Example – Kohonen
3. Reinforcement learning

81

Artificial neural networks

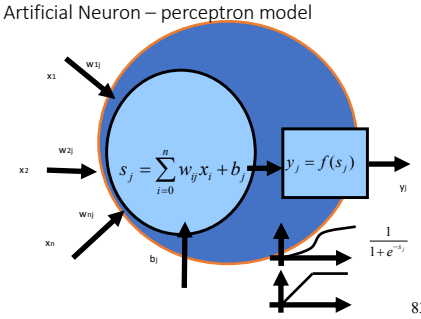


The artificial neuron is a mathematical construct that emulates the more salient function of biological neurons, namely this signal integration and threshold firing behavior.

Just as in the biological case, such neurons are bound together by various connection weights that determine how the outputs from one neuron are to be algebraically weighted before arriving at receiving neurons.

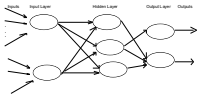
The intelligence within these collective structures of artificial neurons (i.e., ANNs) is stored within these connection weights.

Artificial neuron – perceptron model



83

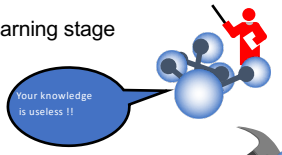
Artificial Neural Networks (ANN)



- All of the information stored within an artificial neural network (i.e., its virtual computer programs) takes the form of connection strengths between neurons.
- These are values by which the signals from one artificial neuron to another are multiplied before being summed up within the receiving neuron. Important to note is that these weights are not 'hand wired' into these networks by computer nerds.
- Special computer programs mathematically change the net until it consistently yields the correct outputs for any given set of inputs.

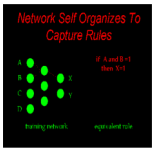
Neural Networks
in supervised learning

1. Learning stage



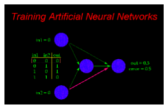
2. Test stage
(working stage)

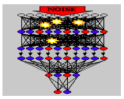
Artificial Neural Networks (ANN)



- How ANNs Capture Rules - Artificial Neural Networks have taken a rap for being 'black boxes'. That is, they give the right results, but don't explain why they do so. In reality, they internally develop connection traces that embody the rules behind the conceptual space they are training on. Here we see a network learning three implicit rules hidden within a database of numbers.

Artificial Neural Networks (ANN)





- ANN training procedures:
- successively apply all known inputs to the net (here the Exclusive Or data) propagating signals in the forward direction,
- observe network output,
- backwardly propagate corrections to the respective connections in the net.
- continue this process until the net yields the correct output for all known test cases.
- at this point conclude that we have a neural network model of some conceptual space.
- the most important aspect of this process is that the network discovers on its own what the underlying rules actually are.

Neural Network In 5 Minutes | What Is A Neural Network? | How Neural Networks Work | Simplilearn

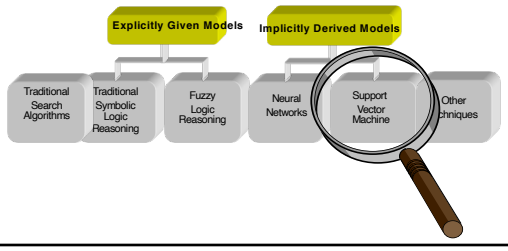
Time: 5:44

https://www.youtube.com/watch?v=bfmFfD2RIcg

Answer the questions:

Why is ANN so popular in various applications? Please, deliberate.

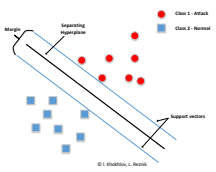
Knowledge classification: models



Support Vector Machine (SVM)

Tries to build a hyperplane (set of hyperplanes) that separates classes in the training dataset.

A good hyperplane has the biggest margin.

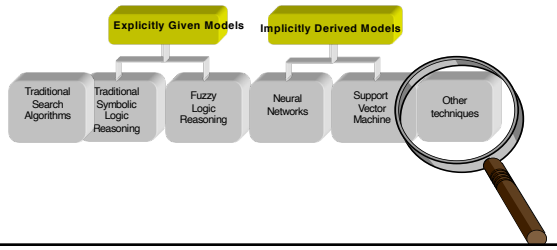


watch video

Support vector machines

@ https://www.youtube.com/watch?v=Y6RRHw9uN9o

Knowledge classification: models

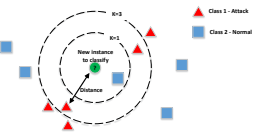


K-nearest neighbor

Algorithm:

- Compute distance to every training example x_i
- Select K closest instances $x_{i1}...x_{iK}$ and their labels $y_{i1}...y_{iK}$
- Output is the majority voting of $y_{i1}...y_{iK}$

$$\hat{y} = MajorityVote(y_{i1} \dots y_{iK})$$



93

Naïve Bayes:

Based on the Bayes rule of conditional probability, consider all the attribute values but independently for each other .

Prediction: $v_{NB} = argmax_j P(v_j) \prod_i P(a_i|v_j)$

- Estimates the probabilities of $P(v_j)$ and $P(a_i|v_j)$ based on their frequencies over the training data
- The learned hypothesis consists of the set of estimates

94

watch video

Naïve Bayes classification

@ https://www.youtube.com/watch?v=CPqOCl0ahss

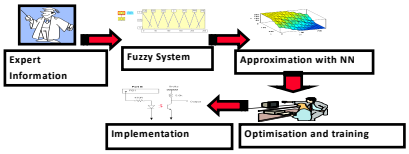
watch video

K-means clustering

@ https://www.youtube.com/watch?v=_aWzGGNrcic

Hybridization: Implementation of FS with NN

- **Advantages:**
- Knowledge acquisition ability of FS
- Learning ability of NN
- Optimisation and adjustment against any criteria (including multi-criteria)
- Simpler and cheaper implementation



Evolutionary Algorithms (EA)

EA are part of the Derivative-Free Optimization and Search Methods:

- **Evolutionary Algorithms**
- **Simulated annealing (SA)**
- **Random search**
- **Downhill simplex search**
- **Tabu search**

EA consists of:

- **Evolution Strategies (ES)**
- **Evolutionary Programming (EP)**
- **Genetic Algorithms (GA)**
  - **Genetic Programming (GP)**

98

Evolutionary Algorithms Characteristics

- Most Evolutionary Algorithms can be described by

$$x[t+1] = s(v(x[t]))$$

  - $x[t]$: the population at time t under representation x
  - v : is the variation operator(s)
  - s : is the selection operator

99

Evolutionary Algorithms: EP

- Evolutionary Programming (EP)
  - Originally proposed for sequence prediction and optimal gaming strategies
  - Currently focused on continuous parameter optimization and training of NNs
  - Could be considered a special case of (μ + μ) -ES without recombination operator
  - Focus on behavior of species (hence no crossover)
  - Proposed by ***Larry Fogel (1963)***

Pause watching …

Try to summarize:

1.What is AI again?

2. Which features does Aihave?

3. What differentiates AI techniques from others?

Part 3: AI technologies

102

Which recent AI advances are exploited in technological development?

- **New Computational Capabilities**
  - **Advances in uncertain reasoning, knowledge representations**
  - **Learning to act: robot planning, control optimization, decision support**
  - **Database mining: converting (technical) records into knowledge**
  - **Self-customizing programs: learning news filters, adaptive monitors**
  - **Applications that are hard to program: automated driving, speech recognition**

Which recent AI advances are exploited in technological development?

- **Better Understanding of Human Cognition**
  - **Cognitive science: theories of knowledge acquisition (e.g., through practice)**
  - **Performance elements: reasoning (inference) and *recommender* systems**
- **Time is Right**
  - **Recent progress in algorithms and theory**
  - **Rapidly growing volume of online data from various sources**
  - **Available computational power**
  - **Growth and interest of AI-based industries (e.g., data mining/KDD, planning)**

What is AI again? From the practical (now real) industry perspectives

See AI

at Google at https://ai.google

Microsoft at https://www.microsoft.com/en-us/ai?activetab=pivot1%3aprimaryr5

Facebook at https://ai.facebook.com

Amazon at https://blog.aboutamazon.com/amazon-ai and https://www.forbes.com/sites/blakemorgan/2018/07/16/how-amazon-has-re-organized-around-artificial-intelligence-and-machine-learning/#709e41c47361

Visit for Technology descriptions

What is AI again? From the practical (now real) industry perspectives

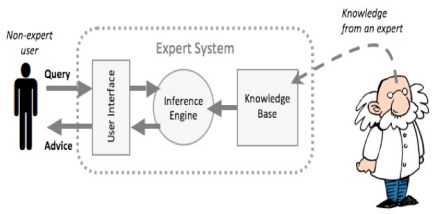
IBM - https://www.research.ibm.com/artificial-intelligence/

Intel - https://www.intel.ai/#gs.ihwdhz

NVDIA - https://www.nvidia.com/en-us/deep-learning-ai/

Visit for Technology descriptions

Expert systems: idea



Source: http://igcseict.info/theory/7_2/expert/index.html

Human Experts	***Expert Systems***	*Conventional Programs*
Use knowledge in the form of rules of thumb or heuristics to solve problems in a narrow domain.	**Process knowledge expressed in the form of rules and use symbolic reasoning to solve problems in a *narrow domain*.**	Process data and use algorithms, a series of well-defined operations, to solve general numerical problems.
In a human brain, knowledge exists in a compiled form.	**Provide a *clear separation of knowledge from its processing*.**	Do not separate knowledge from the control structure to process this knowledge.
Capable of explaining a line of reasoning and providing the details.	**Trace the rules fired during a problem-solving session and *explain how* a particular conclusion was reached and *why* specific data was needed.**	Do not explain how a particular result was obtained and why input data was needed.

Comparison of expert systems with conventional systems and human experts (*Continued*)

Human Experts	***Expert Systems***	*Conventional Programs*
Use inexact reasoning and can deal with incomplete, uncertain and fuzzy information.	**Permit *inexact reasoning* and can deal with incomplete, uncertain and fuzzy data.**	Work only on problems where data is complete and exact.
Can make mistakes when information is incomplete or fuzzy.	***Can make mistakes* when data is incomplete or fuzzy.**	Provide no solution at all, or a wrong one, when data is incomplete or fuzzy.
Enhance the quality of problem solving via years of learning and practical training. This process is	**Enhance the quality of problem solving by adding**	Enhance the quality of problem solving by changing the program code, which affects both

State of the Industry

- As stated previously, many expert and fuzzy systems are available.
  - Dozens (if not hundreds) available on every major platform.
- To demonstrate the variability in the available platforms, a survey of a small number of popular, widely used systems was taken.
- Each expert system was rated on four criteria
  - Learning Curve
  - Portability
  - Features
  - Footprint (resource consumption)

State of the Industry

Prolog

- Initial language version developed between 1971-1973
  - Widely used in industry, particularly as a prototyping language for small scale systems
- Language Learning Curve
  - Shallow. A simple, yet powerful language
  - Popular teaching language
- Portability
  - Available on many platforms
  - Subtle variations between platforms
  - Over two dozen "flavors" of the language in use today
- Features
  - A small, but powerful set of features
  - Limited extensibility
- Resource Consumption
  - Very small footprint when compared to other systems.

At a Glance…

State of the Industry

	Learning Curve	Portability	Features	Resource Consumption
Prolog	Shallow	Medium	Medium	Low
CLIPS	Steep	Medium	High	Medium
JESS	Medium	High	High	High
Blaze Advisor	Extremely Steep	Low	Extremely High	Extremely High

Each language has strengths and weaknesses.

- *Prolog* is small, easy to learn, and widely available.
- *CLIPS* is feature rich, but has a steep learning curve, and may be difficult to port.
- *JESS* is feature rich, and highly portable, but is resource intensive.
- *Blaze Advisor* has an incredibly robust set of features, but a dramatic learning curve, limited portability, and consumes a massive amount of resources.

112

Machine Learning Tools

113

Machine Learning Tools

Azure ML

IBM Watson

Azure Machine Learning Studio - is a collaborative, drag-and-drop tool you can use to build, test, and deploy predictive analytics solutions on your data. publishes models as web services that can easily be consumed by custom apps or BI tools such as Excel – see https://studio.azureml.net

IBM Watson Studio provides tools for data scientists, application developers and subject matter experts to collaboratively and easily work with data to build and train models at scale.

114

Machine Learning Tools

What is TensorFlow?

- TensorFlow is an open-source deep learning library developed by Google.
- TensorFlow provides primitives for defining functions on tensors and automatically computing their derivatives.
  - W https://www.youtube.com/watch?v=2FmcHiLCwTU

watch video

115

Tensor

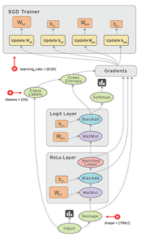
- TensorFlow programs use a tensor data structure to represent all data — only tensors are passed between operations in the computation graph.
- You can think of a **tensor** as an n-dimensional array or list.
- A tensor has a rank, a shape and a static type, so a tensor can be represented as a multidimensional array of numbers.

Rank is the number of dimensions of the tensor (a rank one tensor is a vector)

116

TensorFlow Computation Graph

- "TensorFlow programs are usually structured into a construction phase, that assembles a graph, and an execution phase that uses a session to execute ops in the graph." [TensorFlow docs]
- All computations add nodes to global default graph



117

TensorFlow Advantages

- **Flexibility.** The architecture of TensorFlow is highly modular, which means you can use some parts individually or can use all the parts together.
- **Portability.** It runs on GPUs, CPUs, desktops, servers, and mobile computing platforms.
- **Performance.** TensorFlow allows you to make the most of your available hardware with its advanced support for threads, asynchronous computation, and queues. Just assign compute elements of your TensorFlow graph to different devices and let it manage the copies itself.

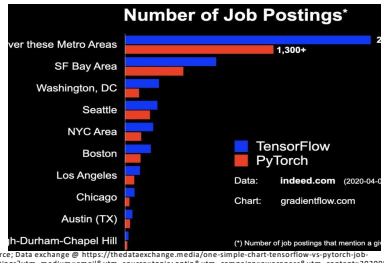
118

PyTorch

- **PyTorch** is an open source machine learning library based on the Torch library, used for applications such as computer vision and natural language processing, primarily developed by Facebook's AI Research lab. It is free and open-source software released under the Modified BSD license.

watch video

https://www.youtube.com/watch?v=nbJ-2G2GXL0



Source: Data exchange @ https://thedataexchange.media/one-simple-chart-tensorflow-vs-pytorch-job-postings?utm_medium=email&utm_source=topic+optin&utm_campaign=awareness&utm_content=20200511+ai+nl&mkt_tok=eyJpIjoiWW1ZeFlGVmlaREV6TGdWbSIsInQiOiJTbjNcLlh5ckRxWEJ2RTBcL2RWbFpTZFTQZN15FpZS1YraZT5mQzbUw5Z3VtcUMzYXYwTGlVZGx2YkNjaVwvYWdMQ2g5dXEySHduQndVNnJXM0RWclhyYjgzVDE2bzRVa01qVmFsTFFodjhPb3JXWTJpV3FrSFZnUzQObVZBSFh1In0%3D

Android Neural Networks API

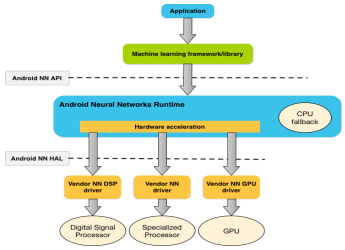
The Android Neural Networks API (**NNAPI**) is an Android C API designed for running computationally intensive operations for machine learning on mobile devices.

- Compatible with TensorFlow Lite, Caffe2, and others.
- Allows using previously trained models (preferred).
  - https://www.youtube.com/watch?v=NzIn_dhDq2U

watch video

121

NNAPI Architecture



122

Main Abstractions

Model: A computation graph of mathematical operations and the constant values learned through a training process.

Compilation: Represents a configuration for compiling an NNAPI model into lower-level code.

Memory: Represents shared memory, memory mapped files, and similar memory buffers. Using a memory buffer lets the NNAPI runtime transfer data to drivers more efficiently.

Execution: Interface for applying an NNAPI model to a set of inputs and to gather the results.

123

NNAPI Pros and Cons

Advantages:

- **Latency**: You don't need to send a request over a network connection and wait for a response.
- **Availability**: The application runs even when outside of network coverage.
- **Speed**: New hardware specific to neural networks processing provide significantly faster computation than with general-use CPU alone.
- **Privacy**: The data does not leave the device.
- **Cost**: No server farm is needed when all the computations are performed on the device.

124

NNAPI Pros and Cons

Disadvantages:

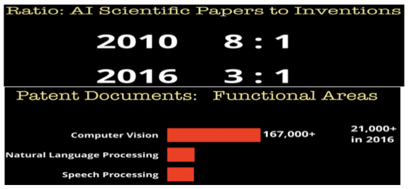
- **System utilization**: Evaluating neural networks involve a lot of computation, which could increase battery power usage.
- **Application size**: Models may take up multiple megabytes of space. NNAPI does not provide functionality for running models in the cloud.
- **NDK**: NNAPI requires Android NDK knowledge

125

Where to next ?

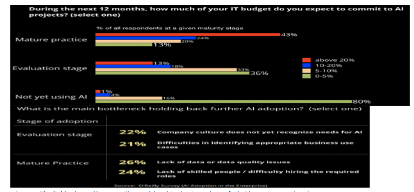
126

“We now are in the implementation phase for AI technologies.”
By Ben Lorica, CTO of Determined AI, June 11, 2019



Source: O’Reily blog https://www.oreilly.com/ideas/ai-adoption-is-being-fueled-by-an-improved-tool
ecosystem?utm_medium=email&utm_source=topic+optin&utm_campaign=awareness&utm_content=20190617+ai+nl&mkt_tok=eyJpIjoiT1dWbU1tRmtNV1E1TkRJdyIsInQiOiJPdzFhTlRnbHBCbFRFRDFpU3FhYUNCbWFCY25kblwvdHJ1ekQ2RDkwMlVDUXkzNHorVlY3c3VQVStsRDZUcEU2QmhrT1hFVno2R2pMdFBpVkFBNWkrd3NXZ2NkRDhZV0tCaE9admpqVTBZTVYrWExQemREVWN4eTN2dVo4bmxZS0YifQ%3D%3D

“We now are in the implementation phase for AI technologies.”
By Ben Lorica, CTO of Determined AI, June 11, 2019



Source: O’Reily blog https://www.oreilly.com/ideas/ai-adoption-is-being-fueled-by-an-improved-tool
ecosystem?utm_medium=email&utm_source=topic+optin&utm_campaign=awareness&utm_content=20190617+ai+nl&mkt_tok=eyJpIjoiT1dWbU1tRmtNV1E1TkRJdyIsInQiOiJPdzFhTlRnbHBCbFRFRDFpU3FhYUNCbWFCY25kblwvdHJ1ekQ2RDkwMlVDUXkzNHorVlY3c3VQVStsRDZUcEU2QmhrT1hFVno2R2pMdFBpVkFBNWkrd3NXZ2NkRDhZV0tCaE9admpqVTBZTVYrWExQemREVWN4eTN2dVo4bmxZS0YifQ%3D%3D

AI based customer care

By 2020, 85% of all customer interactions will be handled without a human agent – source Gartner” https://www.gartner.com/imagesrv/summits/docs/na/customer360/C360_2011_brochure_FINAL.pdf

- Resolving customer service issues before they arise could significantly lower customer churning rate

HOW to achieve?

- Anticipate customer needs by continuously profiling user behaviors (anomaly detection)
- Extract potential complaints published on social networks (sentiment analysis)
- Correlate user complaints with detected network failures (cluster analysis)
- Compare incoming problems to support cases already evaluated (root cause analysis)
- Predict potential problems (time-series analysis)

Source: Gabriele Randelli HPE PointNext, May 2018

AI Recommended Reading

Textbooks:
Intelligent Security Systems: How AI, ML and DS can work for and against computer security by Leon Reznik, IEEE-Wiley, 2022

Artificial Intelligence: A System Approach by M. Tim Jones
Artificial Intelligence: A Modern Approach
by S. Russell and P. Norvig
Artificial Intelligence by R.Luger

Machine Learning by Tom M. Mitchell
Deep Learning (Adaptive Computation and Machine Learning series) by Ian Goodfellow

Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build… by Aurélien Géron

Recommended Reading

Special issues of journals and magazines as well as webinars available:

Singularity report that published in IEEE Spectrum, June 2008 issue, also with webinars available at IEEE website at http://spectrum.ieee.org/singularity

AI Rise of Machines in the special issue of Science Magazine, vol. 349, issue 6245 published on17 July 2015

Recommended Reading

Reports:
AI The next digital frontier? McKinsey Global Institute, June 2017 available at https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx
Market Guide for AIOps Platforms
Published 12 November 2018 - ID G00340492 - 18 min readAvailable at https://www.gartner.com/doc/reprints?id=1-5UWPRFW&ct=181126&st=sb after registration at https://www.bmc.com/forms/tools-and-strategies-for-effective-aiops.html?cid=ps-DSO_NA_Gartner_Market_Guide_for_AIOps_AR_Google_US-BS-05-f-04012019&cc=ps&adch=ggl&adcat=dso&elqcid=8774&sfcid=7011O0000038HFF&gclid=CjwKCAjw583nBRBwEiwA7MKvoCBJOg4dtcmcNTr4IdH959c8xaRgBaGmfvmQMx-V26EceCgkO2ebWRoCHNsQAvD_BwE
The Path to Predictive Analytics and Machine Learning Free O'Reilly eBook available at http://go.memsql.com/oreilly-predictive-analytics/?utm_source=google&utm_medium=cpc&utm_campaign=18_02_02-Ebook-Predictive_Analytics-Search-Google&utm_term=azure%20machine%20learning&campaignid=1053701017&google_device=c&google_mls=ps&_bt=324813453339&_bk=azure%20machine%20learning&_bm=e&_bn=g&_bg=61061881409&gclid=Cj0KCQjwi43oBRDBARIsAExSRQGoWZiIga5MhvcSriYilRcoGSb60625E2Fr5assulUExGrNQ2p-TJ4aAvp-EALw_wcB
Amazon Machine Learning Developer Guide available after registration at https://docs.aws.amazon.com/machine-learning/latest/dg/machinelearning-dg.pdf
Artificial Intelligence in the Real World , Opentext , 2018 available after registration at https://www.opentext.com/campaigns/ai-powered-analytics-magellan
Best Practices for Scaling Deep Learning Training and Inference with TensorFlow* On Intel® Xeon® Processor-Based HPC Infrastructures available at https://www.intel.ai/wp-content/uploads/sites/69/TensorFlow_Best_Practices_Intel_Xeon_AI-HPC_v1.1_Q119.pdf

Disclaimer

- Copyrighted material might have been used here under 'Fair Use' approach, for sake of educational purposes only.
- Thank you for your understanding.

133