

Intelligence Artificielle



Réalisé par :
Imen BEN CHaabane

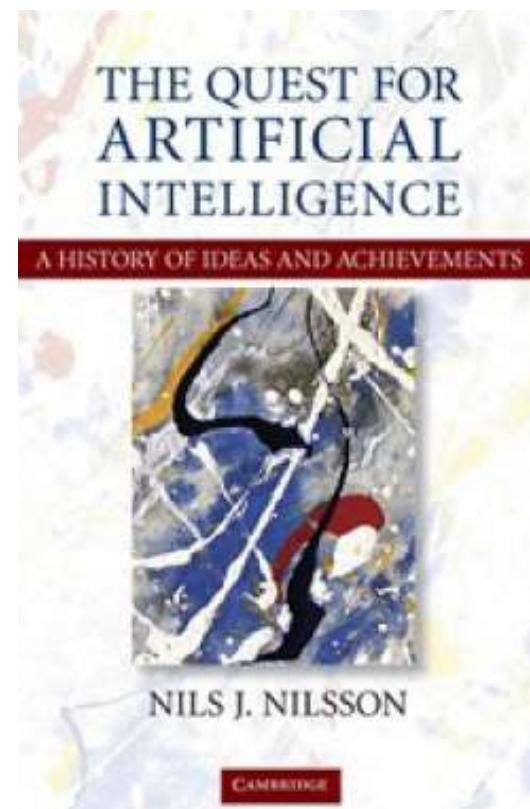
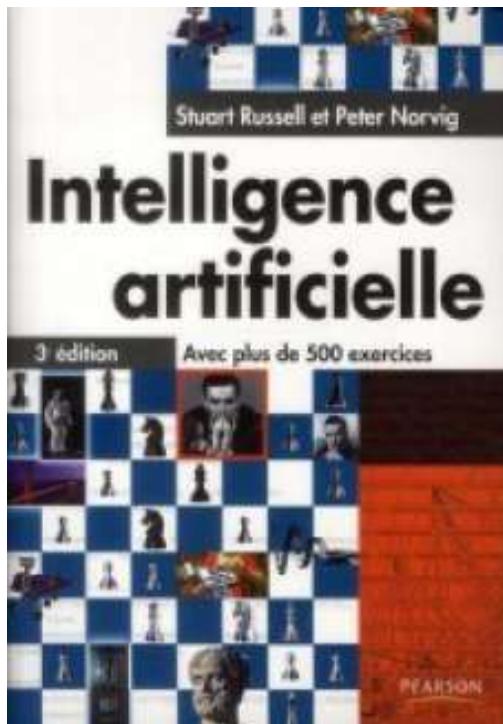


Agenda

1. Historique
2. Définition de l'IA
3. Applications
4. cadre juridique
5. Métiers
6. Risque et futur de l'IA

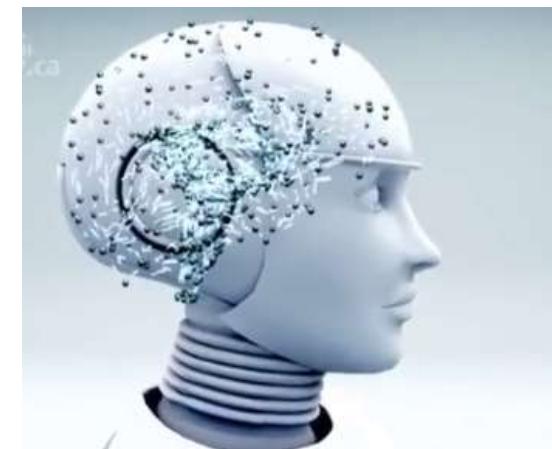


Livres de références



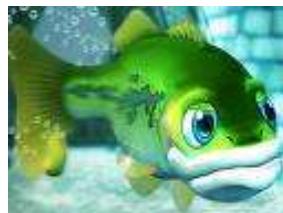
Dictionnaires

- Qu'est-ce que l'intelligence ?
- Qu'est-ce que l'artificiel ?



Question....

- Qu'est-ce que signifie être intelligent pour vous?



Le quotient intellectuel ou QI

Les tests qui sont utilisés pour mesurer l'intelligence des gens



[Tests](#)

[Memoir1](#)

[Memoir2](#)

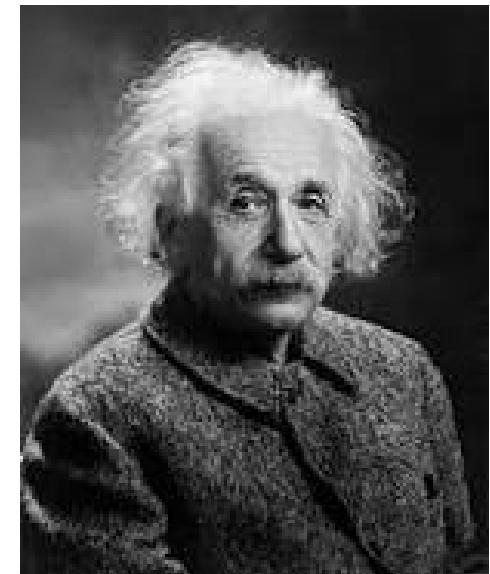
<http://faculty.washington.edu/chudler/experi.html>

Qu'est ce qu'être intelligent ?

- **Apprendre**
 - élaborer un système de connaissances et pouvoir intégrer de nouvelles connaissances
- **Raisonner, déduire, anticiper**
 - à partir du système de connaissances et des données de l'expérience pouvoir produire de nouvelles connaissances
- **Posséder une histoire**
- **Posséder une conscience**
- **Posséder des sentiments**

Intelligence ?

- Capacité d'adaptation
- Capacité de changement de conduite dans l'environnement actuel
- Capacité d'assimiler des connaissances et de les acquérir
- Capacité de comprendre les relations
- Capacité d'évaluation et jugement
- Capacité de penser

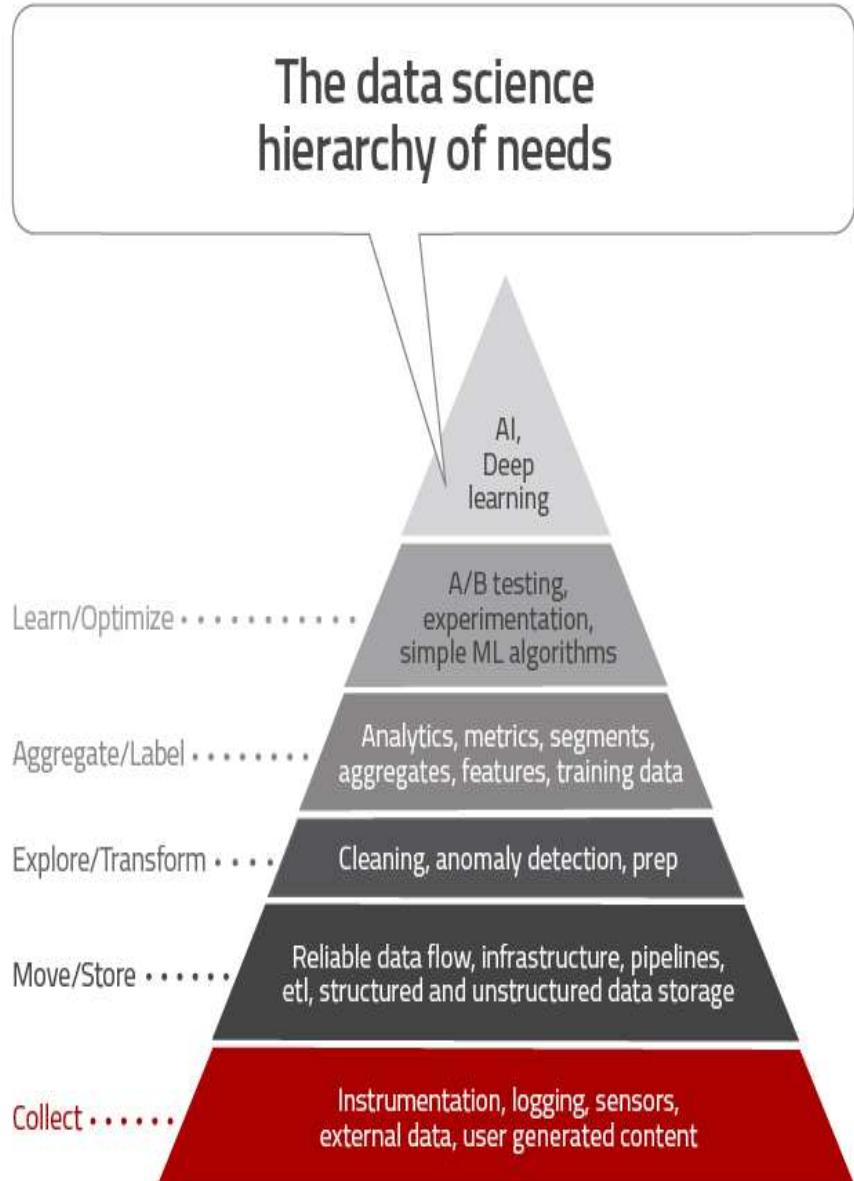


Intelligence ?

- La définition du terme « intelligence » change.
- L'intelligence est liée à l'homme dans ses facultés de compréhension, et d'apprentissage, et observable grâce au comportement (adaptabilité).
- Renvoi à des questions fondamentales : qu 'est-ce que la compréhension? Qu 'est-ce que l 'apprentissage ? Qu 'est-ce que la connaissance ?



Les 5 niveaux de la pyramide cognitive « pyramide de Maslow »



SOURCE: Monica Rogati © August 2017 The Financial Brand

La définition générale

- Le dictionnaire Larousse définit l'intelligence artificielle comme un « **ensemble de théories et de techniques mises en oeuvre en vue de réaliser des machines capables de simuler l'intelligence humaine** ».
- Wikipedia donne une définition similaire décrivant l'intelligence artificielle comme la « **recherche de moyens susceptibles de doter les systèmes informatiques de capacités intellectuelles comparables à celles des êtres humains** ».





John McCarthy



Marvin Minsky

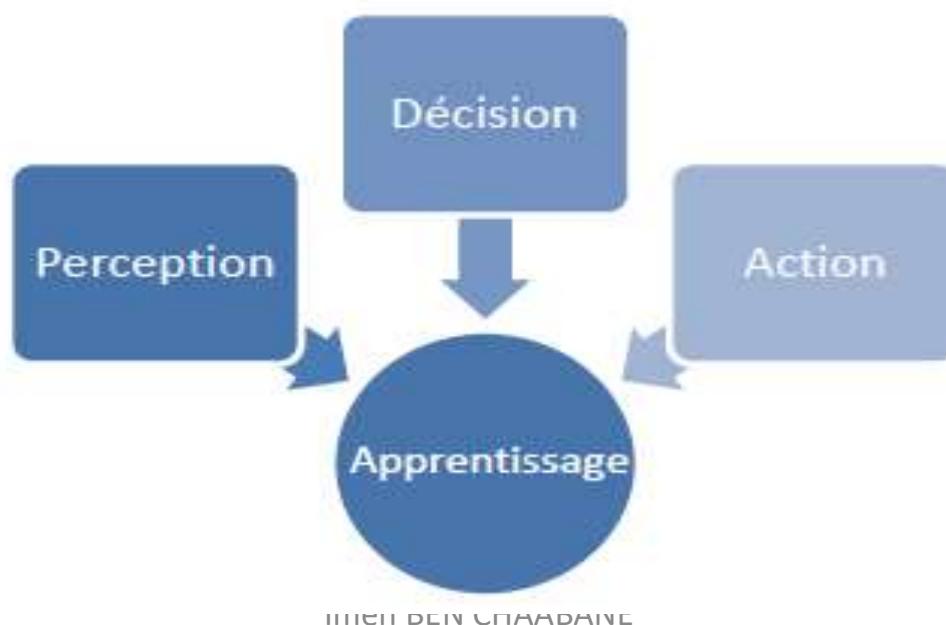
Qq Définition de l'IA

- Apprendre aux ordinateurs à être plus intelligents permettra sans doute d'apprendre à l'homme à être plus intelligent (**P. H. Winston, 1984**)
- L'IA est l'étude des idées qui permettent aux ordinateurs d'être intelligents (**P. H. Winston**)
- L'IA est l'étude des facultés mentales à l'aide de modèles de type calculatoire (**McDermott & Charniak**)
- L'IA a pour but de faire exécuter par l'ordinateur des tâches pour lesquelles l'homme dans un contexte donné est aujourd'hui meilleur que la machine (**Alliot et Schiex 1994**)

La définition technique

Le Centre National de Ressources Textuelles et Lexicales donne une définition technique de l'intelligence artificielle : « **La recherche de moyens susceptibles de doter les systèmes informatiques de capacités intellectuelles comparables à celles des êtres humains** »

L'intelligence artificielle **perçoit** l'environnement, **l'analyse**, et **prend une décision** en conséquence mais surtout **apprend**.

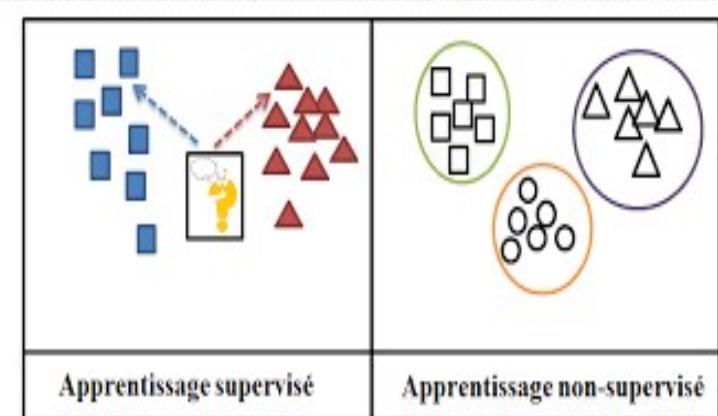


La définition technique

L'apprentissage est donc un point essentiel. Néanmoins, il existe plusieurs types d'apprentissage. Ceux qui apprennent à partir des algorithmes :

- supervisés : le système apprend à fournir la bonne réponse à partir de données lui indiquant des exemples ;
- non supervisés par l'homme : le système apprend seul à partir des données brutes.

Apprentissage Supervisé VS Non-supervisé	
Classification	Clustering
- Nombre de classes connues - Sur entraînement - Utilisé pour classifier des données futures	- Nombre de classes inconnues - Pas de connaissance préalable - Utilisé pour comprendre et explorer les données



La définition technique

La notion d'intelligence artificielle n'est pas unitaire. Les experts font, en effet, une distinction entre deux formes d'intelligence artificielle :

- *l'intelligence artificielle « faible »* : elle vise simplement à imiter certaines fonctions de l'intelligence pour répondre à des missions spécifiques. Il s'agit des programmes les plus utilisés. La machine ne fait que donner une impression d'intelligence ; → **approche pragmatiste**
- *l'intelligence artificielle « forte »* : vise, quant à elle, à faire naître une sorte de conscience. Elle se rapproche du raisonnement humain en modélisant notamment les interactions neuronales et en développant la notion d'apprentissage. → **approche cognitive**



Histoire de l'IA



Préhistoire de l'IA

- ▶ Philosophie (de ~-350 Αριστοτέλης, à -)
 - Logique, méthodes de raisonnement
 - L'esprit vu comme un système physique ou pas (dualisme, matérialisme, ...)
 - L'apprentissage et les sources de connaissances
- ▶ Mathématiques (de 825 الخوارزمي , à -)
 - Logique formelle, preuve
 - Algorithme, décidabilité, complexité
 - Probabilité
- ▶ Économie (de 1776 Adam Smith, à -)
 - Utilité, théorie de la décision, Rech. Op., ...

Préhistoire de l'IA

- ▶ Neurosciences (de 1861 *Broca* à -)
 - Fonctionnement du cerveau
- ▶ Psychologie (de 1879 *Wundt*, à -)
 - Vision, stimulus-réponse, ...
- ▶ Informatique (de 1940 *Stibitz*, à -)
 - Efficacité des ordinateurs
- ▶ Théorie du contrôle et cybernétique (de 1948 *Wiener*, à -)
- ▶ Linguistique (de 1957 *Chomsky*, à -)
 - Représentation des connaissances
 - Grammaire



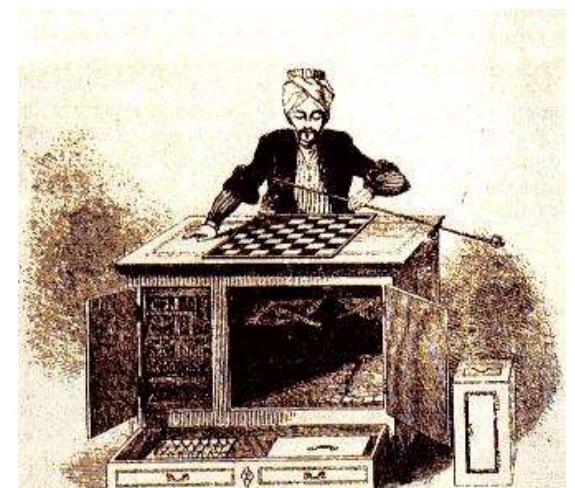
Le Canard Digérateur
Vaucanson, 1739

Automates de Vaucanson

- Jacques Vaucanson 1709 – 1782
 - rival de Prométhée
 - 1738 le joueur de flûte traversière
 - 1739, joueur de tambourin et de flageolet, Canard digérateur
 - 1746, métier à tisser automatique
- Kempelen 1779
 - supercherie du joueur d'échec



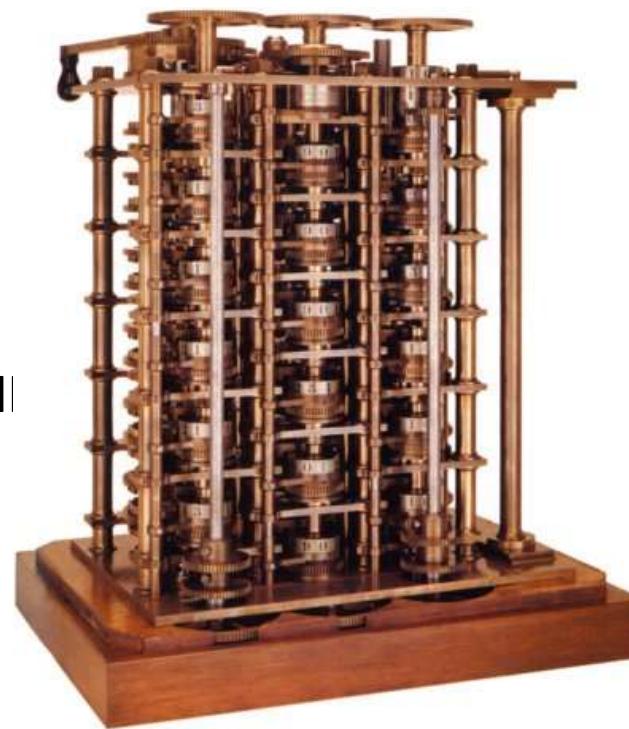
Du calcul à l'automate



Mécanisation du calcul

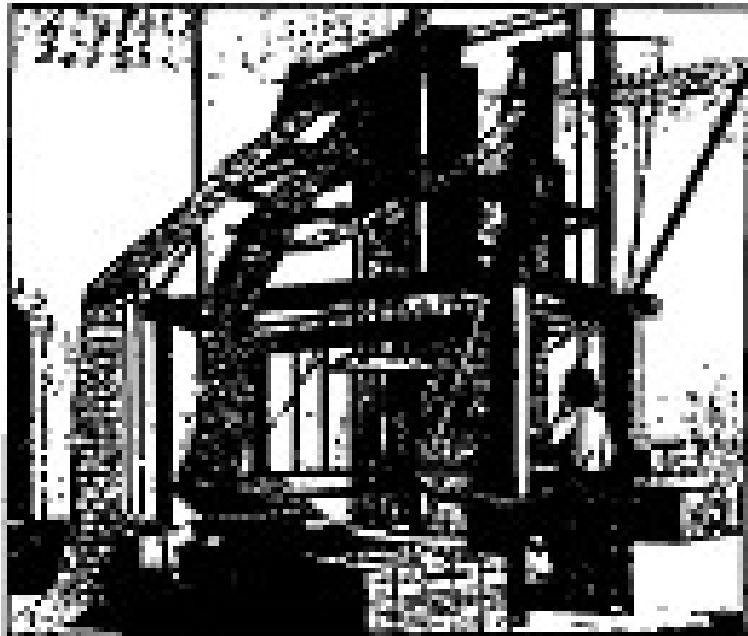
- Automatisation

- 1623 Shickard
- 1642 Pascal
- 1670 Leibnitz
- 1728 Falcon
- Automates de Vancauson
- 1805 Jacquard
- Charles Babbage
 - 1822 Machine différentiel
 - 1830 Machine analytique



Machines Programmables

Métier à tisser
(Jacquard 1805)



Machine Analytique
(Babbage & A. Ada Lovelace 1837)

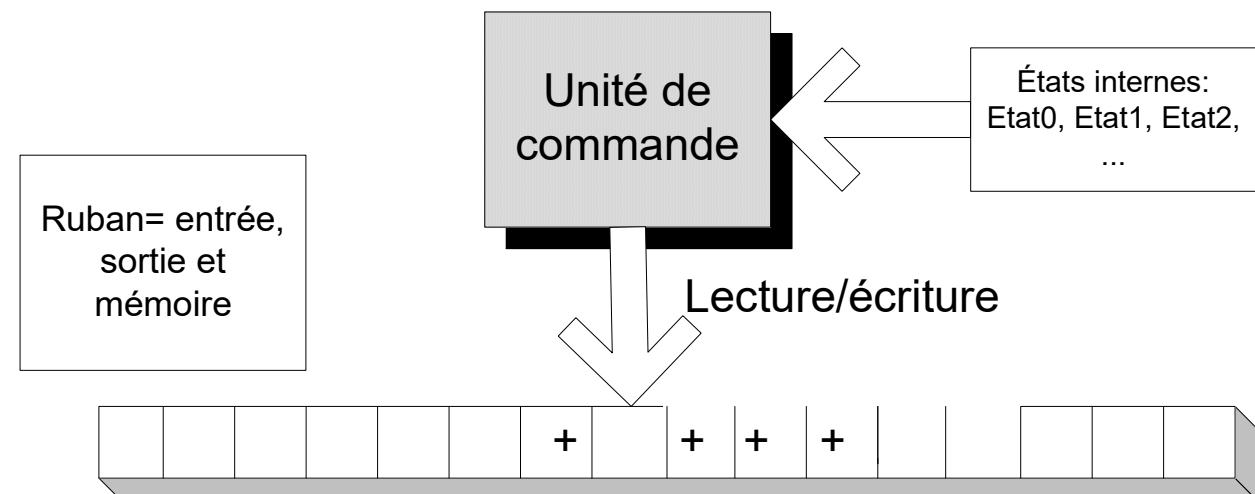
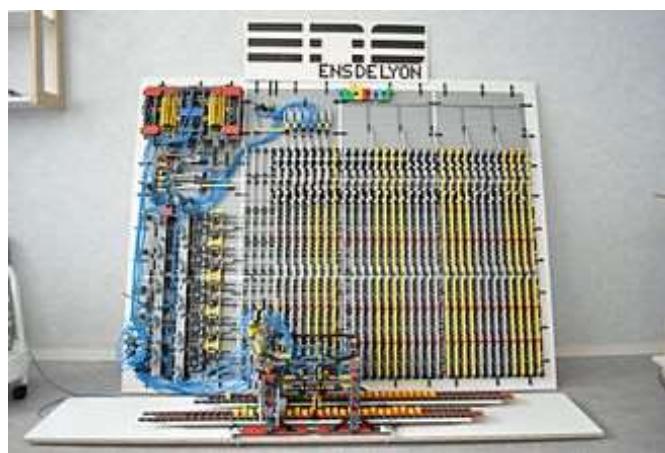


Mécanisation du calcul

Le calcul passe par différentes étapes technologiques

- Mécanique (engrenages)
- Electrique (diode)
- Electro-mécanique (relais)
- Electronique (Transistor)

La machine universelle (Turing 1936)



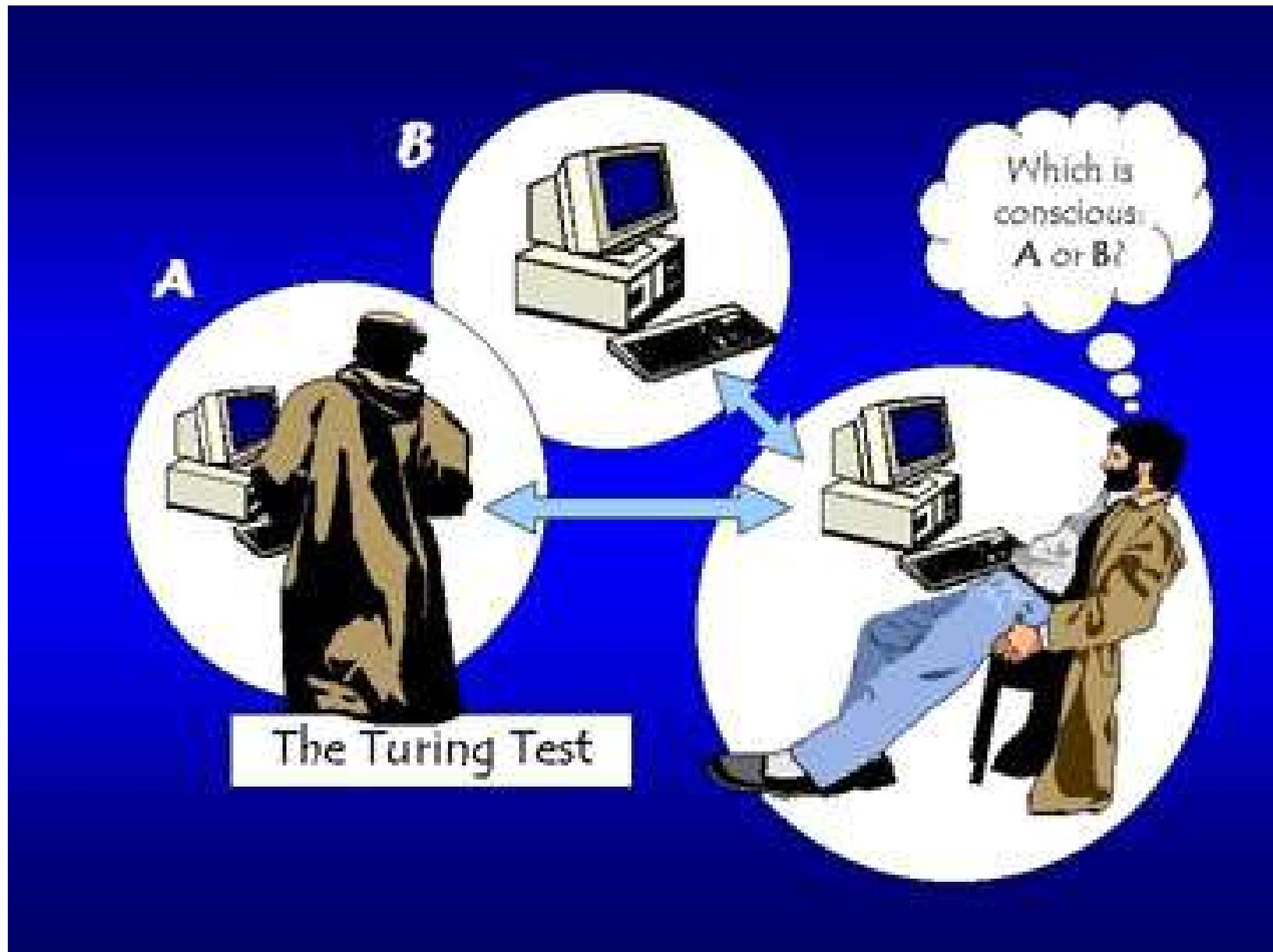
Etat de la machine	Contenu de la cellule	Ecrit sur le ruban	Déplacement ruban	Etat suivant
Etat0	vide		D	Etat0
Etat0	+		D	Etat1

Le Programme

The Turing Test (1950)



The Turing Test (1950)



Naissance de l'IA

- Débuts pendant la 2^{nde} guerre mondiale
 - décryptage → traduction
 - Mise au point d'un traducteur automatique en 5 ans
 - Comment représenter les connaissances ?
 - Comment les extraire d'un individu ?
- 1956 John McCarthy, Dartmouth College
- Objectifs ambitieux
 - Traduction automatique
 - Jouer aux échecs et battre les grands maîtres



Dartmouth College



Dartmouth 1956

- Choix du nom 1956, conférence de Dartmouth
- « L'intelligence artificielle est la science qui consiste à faire faire à des machines ce que l'homme fait moyennant une certaine intelligence » M. Minsky
- Problème de récursivité dans la définition

Histoire de l'IA

- **Les années lumières (euphorie et grands espoirs) 1956-1966**

- **Logic Theorist** (Newell, Shaw et Simon, 1956)
démonstration de théorèmes de la logique des propositions
 - Reconnaissance de caractères, La “souris cybernétique”,
le **perceptron** (Rosenblatt,58), Dames anglaises (Samuel,59)]
 - **General Problem Solver** (1969): résolveur de problèmes général
 - Projet de traduction automatique (1966: rapport **ALPAC**)
 - Weizenbaum, J., (1966) **ELIZA** - A computer program for the study of
natural language communication between man and machine.
Communications of the ACM, 9.1:36-45.

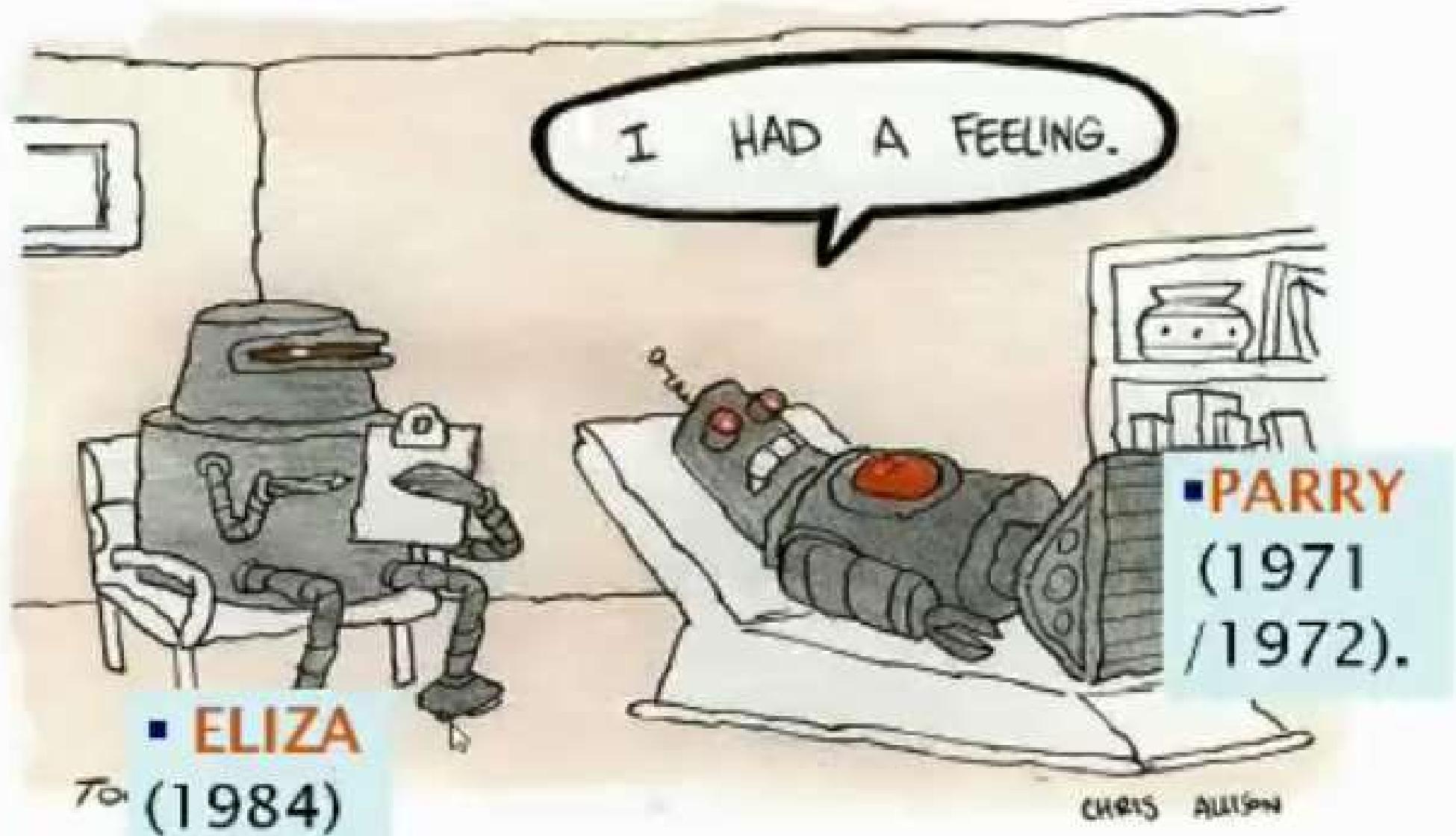


ELIZA

L'EFFET ELIZA

Active Windows

Accédez aux paramètres pour activer Windows

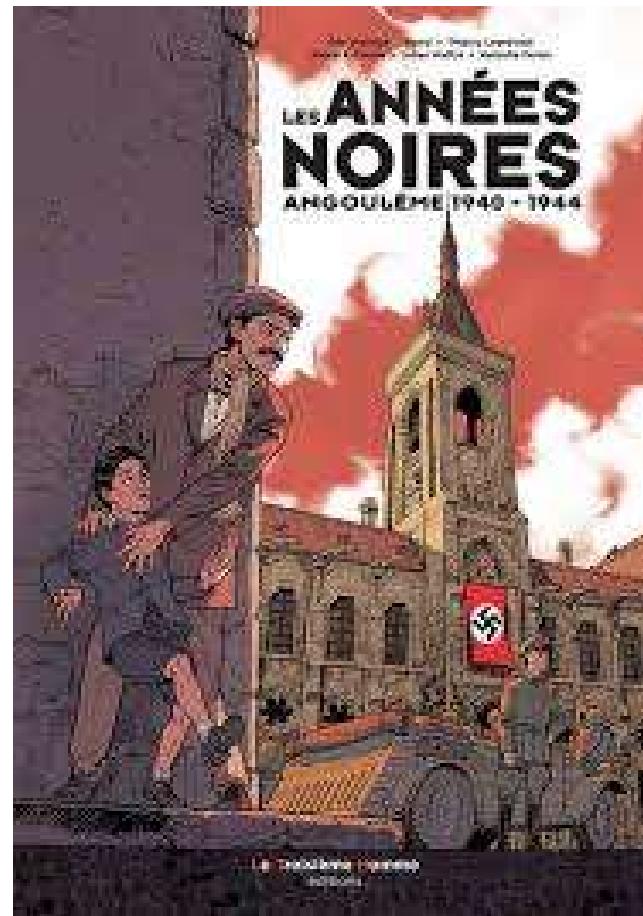


Exemples typiques de problèmes (années 50-60)

- Le fermier, le loup, la chèvre et le choux
- Les recipients : comment obtenir 1 litre d'eau, avec deux récipients de capacité 2 litres et 5 litres (ce dernier étant rempli au départ)
- Intégration symbolique de $\sin(x) \cdot \cos(x)$

Histoire de l'IA

• Les années noires 1966-1969



Années 1970 : la saga star wars R3T2/C3PO



Années 1980



The Society of Mind, Marvin Minsky, 1985

Extrait de *La société de l'esprit*, p. 123, 1988, édition française

IA =
Informatique
Avancée

CRITIQUE: Mais alors, n'en êtes-vous pas réduit à dire que l'évolution elle-même doit être intelligente, puisqu'elle a résolu ces problèmes du vol et de la construction de récifs coralliens ou de nids?

Non, parce que lorsque les gens utilisent le mot « intelligence », ils sous-entendent les idées de rapidité et d'efficacité. Et le rythme de l'évolution est si lent que nous ne la percevons pas comme intelligente, même si elle produit, en fin de compte, des merveilles que nous ne sommes pas encore capables de réaliser. Il n'est de toute façon pas recommandé de traiter un mot aussi ancien et aussi vague qu'« intelligence » comme s'il devait définir quelque chose de bien précis. Plutôt que d'essayer de dire ce qu'un tel mot « signifie », il vaut mieux se contenter d'essayer d'expliquer comment nous l'utilisons.

Notre esprit contient des processus nous permettant de résoudre des problèmes que nous considérons comme difficiles. « Intelligence » est le nom que nous donnons à tous ceux de ces processus que nous ne comprenons pas encore.

Cette « définition » déplaît à certains parce que son sens est voué à changer sans cesse au fur et à mesure que nous nous instruirons en matière de psychologie. Pour moi, c'est bien ainsi qu'il doit en être, parce que le concept d'intelligence est comme un tour de passe-passe, ou comme le concept des « régions inexplorées de l'Afrique » : il disparaît dès que nous perçons son mystère.



Les Systèmes Experts

Systems Expert (SE)

Un des premiers programmes développés en IA
1960s et 1970

“... an intelligent computer system that uses knowledge and inference procedures to solve problems that are difficult enough to require significant human expertise for their solution.”
(Feigenbaum)

programmes qui imitèrent les décisions
d'une experte humaine

Les systèmes experts

Catégories	Types de problèmes
Interprétation	Décrire des situations à partir de données sensorielles.
Prédiction	Prédire des conséquences de situations données.
Diagnostic	Identifier des problèmes de fonctionnement à partir d'observations.
Conception	Configurer des objets à partir de contraintes descriptives.
Planification	Déterminer des plans d'action.
Surveillance et contrôle	Comparer des observations à des défaillances possibles et remédier à ces défaillances.
Réparation	Prescrire des remèdes à des mauvais fonctionnements. Exécuter des plans en fonction de remèdes prescrits.
Formation	Identifier les failles dans les connaissances et proposer des stratégies pédagogiques pour y remédier.

Activ

Exemples de systèmes experts

Systèmes d'interprétation de données. Des systèmes permettant de classifier de nouvelles observations par référence à des observations préstockées.

systèmes de diagnostic en médecine ("de quelle maladie s'agit-il?"),

système d'interprétation géologique ("les mesures seismologiques permettent-elles de croire à l'existence de dépôts minéraux importants?"),

systèmes d'évaluation psychologique ("s'agit-il d'un cas suicidaire?"), etc.

Systèmes de prédiction. Des systèmes effectuant une interprétation prédictive à partir d'observations préstockées.

systèmes de prédiction météorologique ("Il pleut aujourd'hui en France.

Va-t-il pleuvoir en Suisse demain?"),

prédictions géopolitiques ("Les conflits de guerre sont particulièrement fréquents en situation de crise économique. Quelles combinaisons précises de facteurs économiques, sociologiques et politiques prédisent un déclenchement d'hostilités?"),

Activ

Exemples de systèmes experts

Systèmes de planification. Des systèmes capables de planifier des actions humaines ou robotiques dans un univers complexe caractérisé par des contraintes ou règles connues.

Système de réservation de vols aériens, planification des altitudes de vol selon les vents connus et les corridors disponibles,

planification des actions d'assemblage d'un robot industriel, planification des interventions requis pour la construction d'un bâtiment, etc.

Systèmes de conception. Des systèmes de configuration ou de découverte selon un cahier des charges précises.

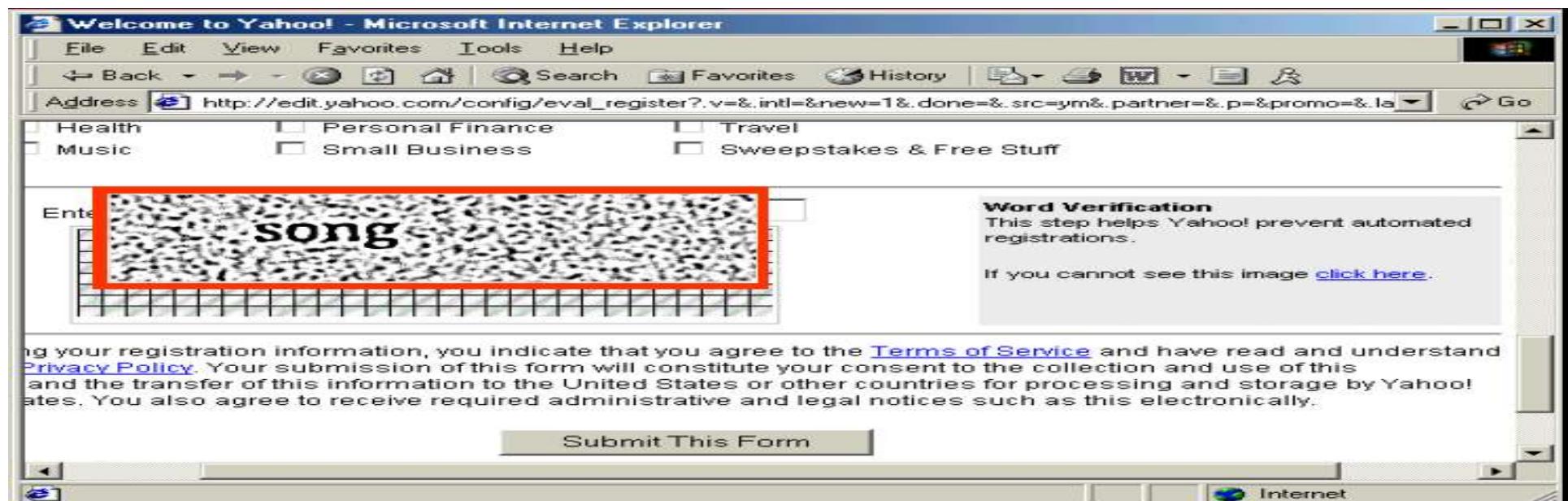
Développement et simplification de circuits intégrés, aménagement d'une cuisine optimale dans un espace donné, clonage de gènes, création d'un nouveau composé chimique, etc.

Année 1990-2000



Les années 2000

- Le système Capatcha, développé à Carnegie Mellon University, s'occupe de différencier les humains des machines.
- Capatcha génère des tests que seuls les humains peuvent passer afin de combattre les spams et les actions malicieuses de certaines machines.



Les années 2000

Wakamaru, robot développé par Mitsubishi Heavy Industries et doté de la parole, est principalement conçu pour veiller sur les personnes âgées. Destiné à s'insérer dans la vie familiale de tout un chacun, il aura pour mission de prévenir l'hôpital ou les services de santé en cas de besoin.

Wakamaru

Wakamaru est un robot domestique commercialisé par la firme [Mitsubishi Heavy Industry](#).

Caractéristiques [modifier]

- Couleur : jaune
- Hauteur : 1 mètre
- Poids : 30 kg
- Se déplace sur des roues
- Reconnaît environ 10 personnes différentes
- Vocabulaire : 10.000 mots
- Prix de vente : 12.000 euros environ
- Designer : Toshi Yukikita

Description [modifier]

Ce robot peut se connecter à internet par liaison Wi-Fi, et dispose d'une voix synthétique. Il est équipé d'un téléphone portable intégré, ce qui lui permet par exemple d'appeler les secours si son maître (une personne âgée par exemple) a un problème.

Il vit en accord avec le programme journalier que son propriétaire lui fournit via Internet.

Wakamaru possède une reconnaissance vocale et une reconnaissance faciale du/des propriétaire(s), de la famille. Il vous regarde en face lorsqu'il parle et incorpore des mouvements du corps pendant la discussion. Wakamaru ne répond pas seulement aux ordres des acteurs, comme le font habituellement les robots conventionnels, mais il sait prendre l'initiative de parler à la famille, en utilisant les informations qu'il a obtenues par observation en restant en contact avec la famille ou bien via son organisateur. Ainsi il n'oubliera pas de dire au chat d'aller manger sa gamelle ou bien encore de fêter son anniversaire à votre belle-maman...



Les années 2000

- Le 13 janvier 2004, une firme québécoise rapporte dans le Medical Post la mise en marché d'un système portatif d'alerte cardiaque appelé **Vital Positionning System (VPS)**
- Incluant un téléphone cellulaire, un ordinateur de poche et un GPS, ce système peut détecter l'approche d'une attaque cardiaque 8 minutes avant que les premières symptômes ne soient humainement perceptibles.
- Il appelle alors automatiquement l'hôpital le plus proche et précise l'emplacement du futur patient



Historique de l'intelligence artificielle

- 2009
 - Le MIT a lancé un projet visant à repenser la recherche en intelligence artificielle
- 2011
 - Watson, le superordinateur d'IBM, remporte deux des trois manches du jeu télévisé Jeopardy! La performance a consisté pour cette IA à répondre à des questions de culture générale
- 2013
 - Human Brain Project
 - Google ouvre un laboratoire de recherches dans les locaux de la NASA
- 2014
 - Deep Knowledge Ventures nomme à son conseil d'administration VITAL, un algorithme capable d'élaborer ses décisions en analysant les bilans comptables des entreprises potentiellement intéressantes, les test cliniques, la propriété intellectuelle et les précédents investissements
 - Eugene Goostman, programme informatique conçu en Russie, est parvenu, lors d'une compétition organisée par l'université britannique de Reading, à tromper plusieurs personnes dans le cadre d'un test de Turing
- 2015
 - Facebook Artificial Intelligence Research (FAIR)
 - Google rend sa technologie d'IA TensorFlow accessible à tous
 - Développement d'une crainte que l'intelligence artificielle dépasse à terme les performances de l'intelligence humaine
- 2016
 - Amelia d'IPSoft, un agent virtuel
 - AlphaGo bat trois fois consécutives le champion du monde du jeu de go, Lee Se-Dol, en cinq manches

A nighttime photograph of the Massachusetts Institute of Technology. The image shows the iconic Great Dome, which is brightly lit from within, casting a glow upwards. Below the dome, a plaque displays the year "MCMXVI". In front of the dome is a large, white, classical-style building with a portico supported by several columns. The words "MASSACHUSETTS INSTITUTE OF TECHNOLOGY" are engraved in a band above the entrance. The building's windows are illuminated from within, creating a warm glow. The sky is dark, and trees are visible on either side of the building.

Massachusetts Institute of Technology

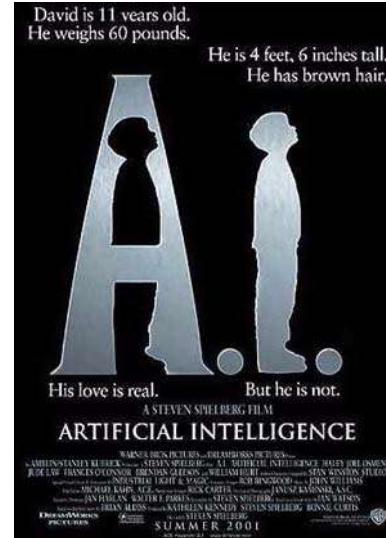
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

L'IA aujourd'hui



Exemples d'IA (irréalistes ?)

- Exemples (Science-Fiction)
 - TRON
 - La Guerre des Etoiles (Z6PO)
 - IA (Spielberg)
 - I, Robot
 - K 2000
 - Galactica (Cylons)
 - 2001 L'Odyssée de l'espace
 - Matrix
 - Terminator
 - ...



LES GRANDS ACTEURS DE L'INTELLIGENCE ARTIFICIELLE

Google, Apple, Facebook et Amazon ne pouvaient pas ne pas s'investir fortement dans l'intelligence artificielle alors qu'ils possèdent des données en énorme quantité.





- Google, très impliqué dans l'intelligence artificielle, procède habituellement par rachat.
- En 2014, Google a acheté la société anglaise DeepMind, qui avait développé des réseaux de neurones pour jouer aux jeux vidéo. Mais l'objectif avoué de **DeepMind** est actuellement de « comprendre ce qu'est l'intelligence ». DeepMind est célèbre pour son programme AlphaGo, qui a battu le champion du monde de go.
- En octobre 2017, le programme a franchi une étape supplémentaire : en jouant contre lui-même, non seulement son apprentissage a été plus court, mais surtout il est devenu plus fort que la version précédente . Nous avons ici un premier exemple d'apprentissage non supervisé, facilité par le fait que le contexte, à savoir les règles du jeu de go, est parfaitement mathématisable.
- Google a aussi son propre moteur de recommandation nommé **Google Home**, un haut-parleur et un assistant vocal disponible en trois versions différentes.



Traduction

Désact

Anglais Français Arabe Déetecter la langue ▾



Français Anglais Arabe ▾

Traduire

je suis ton père



je suis ton père

I am your father

15/5000

Saisissez du texte ou l'adresse d'un site Web, ou importez un document à traduire.

Google Traduction pour les entreprises : [Google Kit du traducteur](#) [Gadget Traduction](#) [Outil d'aide à l'export](#)

Trump versus Macron dans une requête Google

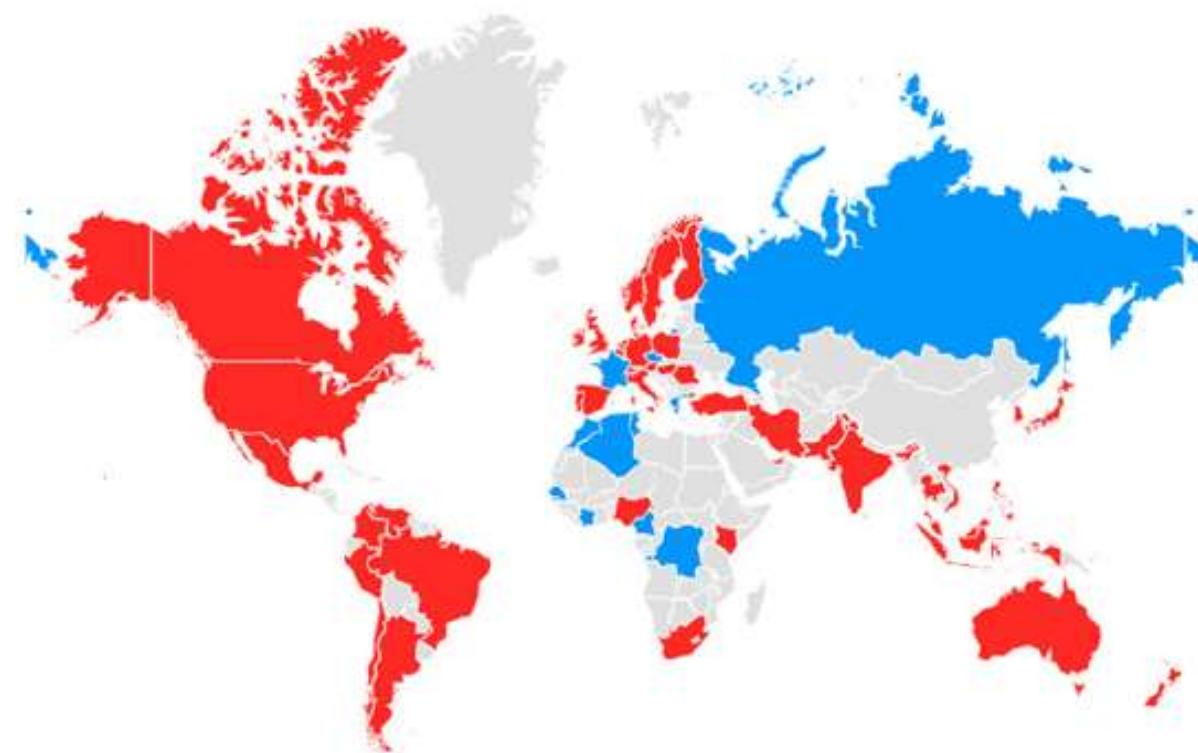
À titre d'exemple, nous pouvons ainsi comparer l'évolution de l'intérêt pour la recherche « Macron » versus « Trump » entre novembre 2016 et novembre 2017



Source : Google trends : <https://trends.google.com/trends/explore?q=Macron,Trump>.

On voit que les recherches « Macron » ont dépassé les recherches « Trump » début mai 2017.

Requêtes Trump contre Macron selon les pays



Source : <https://trends.google.fr/trends/>.



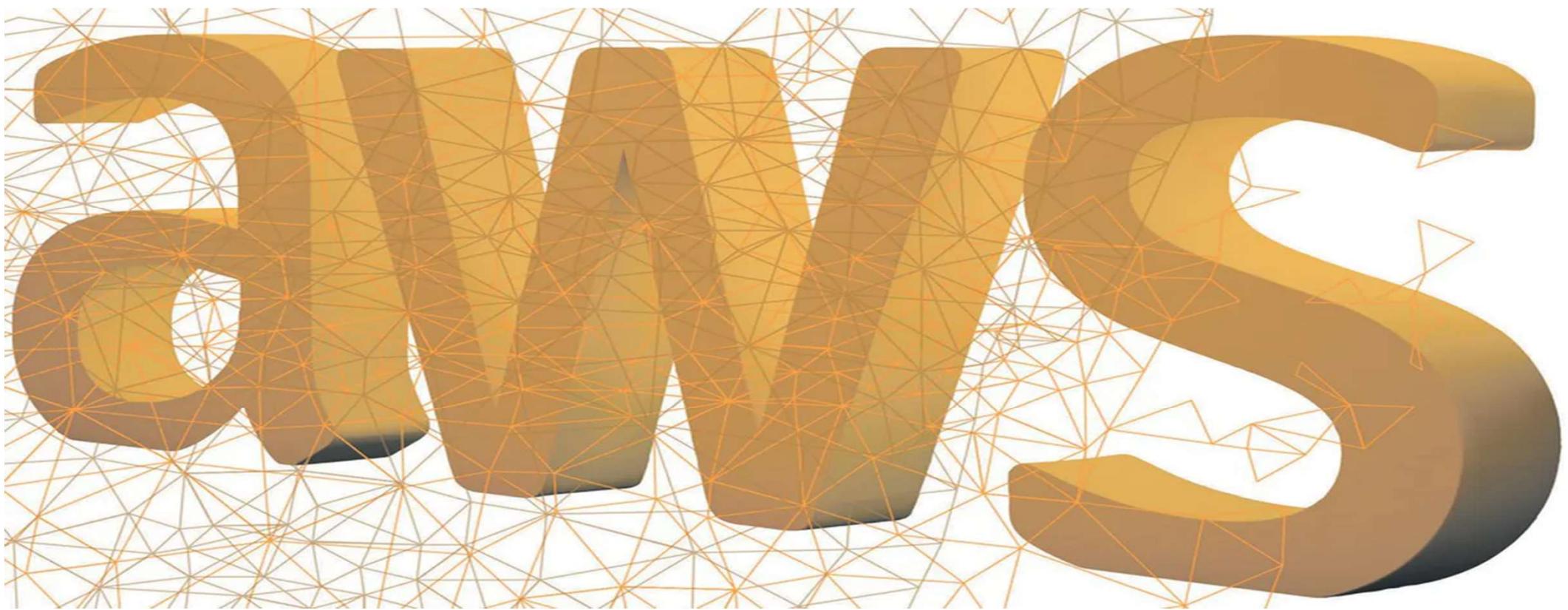
Google I/O est une conférence annuelle de deux jours, organisée par [Google](#) au [Moscone Center](#) de [San Francisco](#), en [Californie](#). Le "I" et le "O" signifient respectivement "Input" et "Output" ou "Innovation in the Open"



1. **Android P** : il introduit des réglages de batterie et de luminosité adaptatifs + une nouvelle fonction appelée Shush mettra un téléphone en mode Ne pas déranger lorsqu'il est placé face cachée sur un bureau
2. **Une nouvelle fonctionnalité Gmail appelée «smart compose»** : La méthode est une saisie semi-automatique pour les emails
3. **L'Assistant Google peut effectuer vos appels téléphoniques** : sa voix d'intelligence artificielle pouvait appeler un coiffeur ou un restaurant et prendre rendez-vous. L'assistant se réfère au calendrier de la personne pour trouver un créneau horaire approprié, puis informe l'utilisateur lorsqu'un rendez-vous est prévu.
4. **Le créateur de Google News** : indique qu'il rend le service plus personnalisé en fournissant des «briefings»
5. **Google a également montré une version augmentée de Google Maps** : qui charge automatiquement streetview lorsqu'une application appareil photo est ouverte. L'entreprise a appelé cela un système de positionnement visuel qui reconnaît les bâtiments et les points de repère qui se trouvent devant elle.



- ❑ Amazon utilise de l'intelligence artificielle dans son moteur de recommandation, nommé **Echo**,
- ❑ et dans ses assistants basés sur son système de **reconnaissance vocale, Alexa**, disponible en sept versions différentes.
- ❑ *Via son offre de services dans le cloud, Amazon propose également des services fondés sur l'intelligence artificielle, comme la reconnaissance de la parole ou des robots de discussion, les fameux **chatbot***



ALEXA
L'ASSISTANT VIRTUEL D'AMAZON



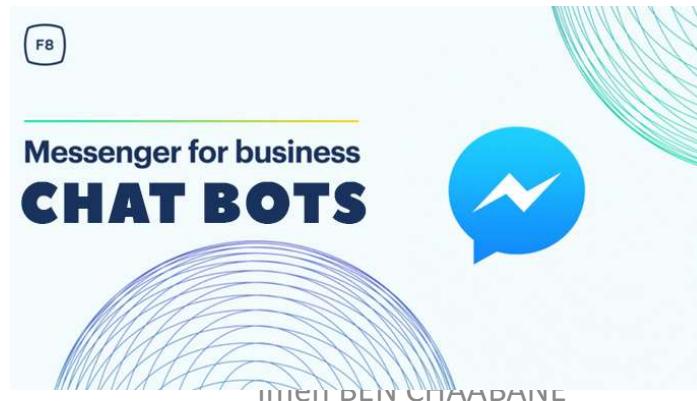
Systèmes de recommandation

Amazon

- L'un des premiers adoptants des systèmes de recommandation
- Grand impact sur les ventes
 - Prix de Netflix
- Grand prix de \$ 1,000,000 pour l'algorithme qui bat Netflix algorithme

facebook

- Facebook est un énorme utilisateur d'intelligence artificielle. Il choisit les messages qu'il affiche en utilisant un moteur de type moteur de recommandation.
- Récemment, Facebook a mis en place un moteur d'intelligence artificielle pour détecter les tendances suicidaires .
- Comme le dit Joaquin Candela, directeur du département d'intelligence artificielle appliquée, « Facebook n'existerait pas sans intelligence artificielle ».

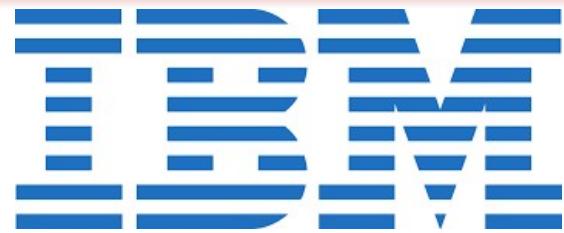




Hey Siri



- ❑ Apple investit énormément dans l'intelligence artificielle et propose même un blog où sont expliquées ses recherches.
- ❑ Siri en est l'expression la plus évidente : ce système de reconnaissance de la parole très performant utilise des réseaux de neurones de dernière génération qui permettent de comprendre des commandes même dans des environnements très bruyants, comme dans la rue.
- ❑ Apple va également bientôt lancer son propre moteur de recommandation, nommé **HomePod**, un haut-parleur connecté avec Apple Music.



IBM a créé Watson, un système d'intelligence artificielle pour jouer, à ses débuts, au jeu *Jeopardy*, l'équivalent américain de l'émission française *Questions pour un champion*. Watson a analysé 200 millions de pages 27 pour finalement battre les anciens champions et ainsi gagner le premier prix. Maintenant, Watson est proposé par IBM dans d'autres domaines, comme la médecine ou le droit. IBM présente aussi un blog sur le sujet de l'intelligence artificielle.



Participation à *Jeopardy!*



Applications actuelles et futures



Google DeepMind, Microsoft et IBM sont rejoints par Facebook et Amazon pour former un partenariat sur l'intelligence artificielle au profit des populations et de la société.

→répondre aux défis mondiaux importantsle changement climatique, la nourriture, l'inégalité, la santé et l'éducation.



Les domaines de l'IA



UNE AMBITION POUR VALORISER L'INTELLIGENCE ARTIFICIELLE DANS LES ENTREPRISES

- ❑ L'intelligence artificielle n'est pas une filière à part entière mais apparaît de manière transversale dans plusieurs domaines.
- ❑ Elle est spécialement présente en robotique mais ne se limite pas à ce secteur.

En 1988, le chercheur en informatique **indien Raj Reddy** définissait ainsi les grands challenges de l'intelligence artificielle : le téléphone qui traduit (en cours de développement), le champion de jeu d'échecs (réalisé), la résolution de théorèmes mathématiques (certains théorèmes le sont déjà), les voitures autonomes (réalisé), les systèmes auto-organisants (en cours) et les systèmes autorépliquants (en cours)



Les Grands domaines de l'IA

- Reconnaissance et synthèse de la **parole** (ex: réservation d'hôtel, 11artificial)
- Reconnaissance et synthèse **d'images** (ex. recherche d'info)
- Reconnaissance de **l'écriture** (ex: recon. cheques, codes postaux)
- **Langage naturel** (ex: interfaces, text mining, Web Mining)
- **Planification** (ex: Partage resource satellite DigitalWpress 's service PCAI April2000)
- **Aide à la décision**
(ex: SE temps réels et autonome: contrôle de trajectoire du satellite Voyager)
- **Aide à la programmation** (ex: agents d'interface)
- **Apprentissage / Adatptatif**
(ex: construction de systèmes experts, classification automatique de galaxie, contrôleur de robots ...)
- **Jeux**
(e.g. Echecs(DeeperBlue à 2600), Checkers (Champion), Othello (Champion), BackGammon(champion GO (bon amateur)).
- **Médecine:**

Aide à la décision (SE), prédiction de patients à risques, analyse automatique d 'images médicales

Les robots, avatars et *chatbots*

Définition de robot par ses caractéristiques. Le terme robot est difficile à définir. Tout peut potentiellement être un robot. Toutefois, il convient d'avoir quatre caractéristiques pour en être un :

- une polyvalence ;
- un apprentissage ;
- une autonomie ;
- une interactivité.

Cela permet d'encadrer la notion d'intelligence artificielle chez le robot, et de mieux la comprendre.

Le robot est une machine qui perçoit, décide et prend une action.

C'est une boucle perpétuelle. Ce qui reste encore difficile à maîtriser, ce sont les parties « perception » et « action » du robot.

Il y a par ailleurs, trois sortes de robot, celui qui :

- n'a aucune partie perception, il est donc sourd et aveugle ;
- est en interaction, doté de bras mais n'en fait pas grand-chose ;
- est une machine intermédiaire, telle que le robot aspirateur.



Les robots, avatars et *chatbots*

Avatars. L'intelligence artificielle sans coque, sans enveloppe corporelle, constitue des avatars.

Les avatars n'existent que dans le monde virtuel. Néanmoins, les plateformes d'intelligence artificielle posent des problématiques similaires à celles des robots.



Les robots, avatars et *chatbots*



Les dernières avancées en matière de robotique nous permettent d'assister au début de la robotique émotionnelle liée à l'intelligence artificielle. La robotique émotionnelle repose sur le mimétisme des sentiments humains et une grande capacité d'analyse. Notons **que 80% de la communication chez l'être humain est non verbale** ; ce qui ne va pas sans poser de nombreux défis dans la robotique pour analyser cette gestuelle et la traduire en langage informatique.



La particularité du robot par rapport à d'autres types d'intelligence artificielle est son lien physique avec l'environnement *via des capteurs*. *Il y a de l'intelligence artificielle dans la décision mais aussi* dans la perception et l'action. Le robot est amené à prendre de l'information dans le monde réel contrairement au logiciel qui prend des informations déjà numérisées, les données. Il a fallu 20 ans de recherches pour réussir le bouclage perception, décision, action.

Les robots, avatars et *chatbots*



- La voiture autonome sera en 2020 sur toutes les routes et est à la pointe dans la robotique.
- Elle illustre le fait que la perception, l'action et la décision sont les critères et la définition de l'intelligence artificielle dans le monde 4.0.



Les robots, avatars et *chatbots*

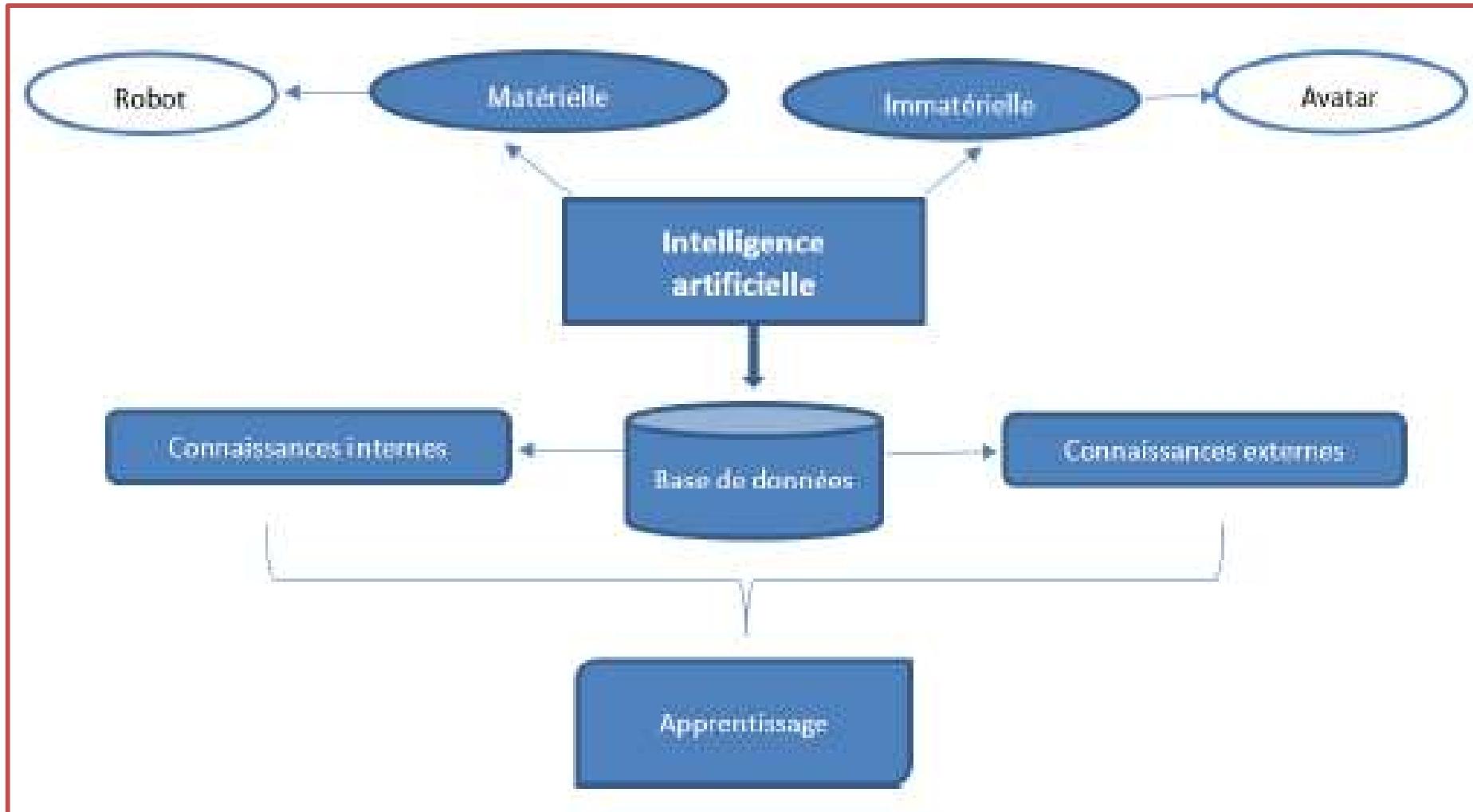
- *Les chatbots ou agents conversationnels sont des robots logiciels dotés d'intelligence* artificielle pouvant dialoguer avec un être humain en langage naturel ou à l'écrit par *chat*.
- Ce sont des systèmes capables de **percevoir, décider, agir et apprendre**, dotés d'une indépendance, qui bousculent la logique marketing relationnelle mais aussi représentent à eux-seuls un *e-helpdesk* qui désengorge les centres d'assistance en donnant notamment des conseils et des informations.
- Ces agents virtuels peuvent exécuter des processus assez complexes et permettent de profiter de leur élasticité pour augmenter la qualité des services et des besoins au sein d'une entreprise.



Imen BEN CHAABANE



Les robots, avatars et *chatbots*



Robotique

- Selon Bill Gates :
 - « .. les défis auxquels est confrontée l'industrie robotique sont très semblables à ceux que nous avons relevés en informatique il y a trois décennies »,

Pour la Science,
Juin 2007



LEGO Mindstorm NXT

La robotique peut être vue comme une interconnexion intelligente de la perception, de l'action ainsi que du fonctionnement des robots

Robotique

- Chaînes de production :
 - automobile,
 - Informatique
 - Industrie en général
- Concours de robots pour résoudre un problème donné
- **ASIMO (Honda)** [site](#)
 - Reproduction du comportement humain (déplacement, mouvements)



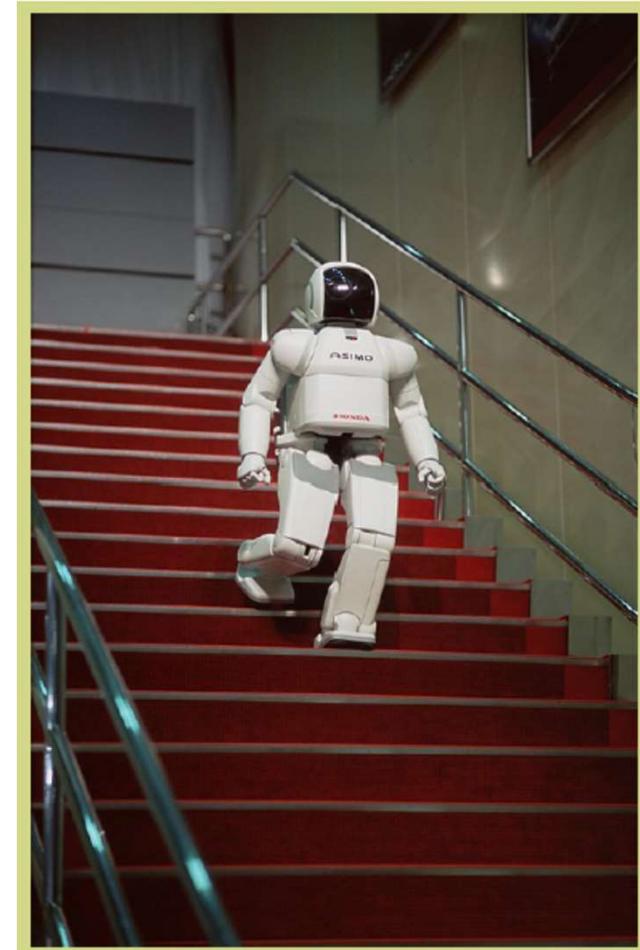
Compétences physiques

Conduire une voiture

- 2007 DARPA Grand Challenge
- le "Urban Challenge"
- 2 millions de dollars a été lauréat
- Tartan Racing
- trace de 96 km
- obéir à toutes les réglementations du trafic
- de négocier avec d'autres véhicules et les obstacles
- intégration dans le trafic

Marcher

- ASIMO
- Honda Motor Company
 - coûte moins de 1 million de dollars pour fabriquer







Activer Windows
Accédez aux paramètres pour activer V

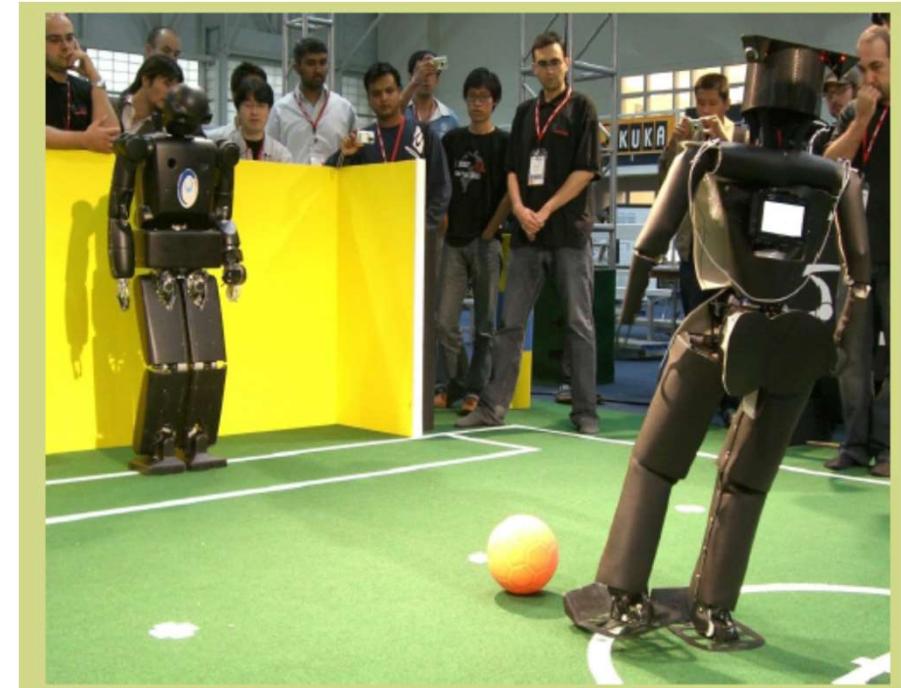


Football

RoboCup 2007

Mission: 2050, de développer une équipe entièrement autonome de robots humanoïdes qui peuvent gagner contre l'homme le champion du monde

www.robocup.org



Conduire une moto

- 2005 DARPA Grand Challenge
- 130 mile désert cours
- Ghostrider Robotic Moto
- Blue Team: UC Berkeley et Texas A & M

Faire du Vélo



MURATA BOY is a bicycle-riding robot.

We will introduce you to MURATA BOY's capabilities,
and the "Murata Technologies" that made MURATA BOY possible.

Natation

robot poisson
exposé à Londres
Aquarium



Autres jeux de l'IA



Les robots insectes bientôt au service des humains au Japon : Actualités > Actualités : Aujourd'hui le Japon Mozilla Firefox

Échec Édition Affichage Historique Marque-pages Outils 2

Les plus visités Débuter avec Firefox À la une

<http://www.aujourdhuijapon.com/actualites-japon-les-robots-insectes-bientot-au-service-des-humains-au-japon-66/>

Aujourd'hui le Japon

Rechercher... Valider Newsletter Votre email OK

ACTUALITÉS ECONOMIE CULTURE TOURISME VIVRE LE JAPON

Blogs Forum Japon Liens Boutique Météo

ANNONCES GOOGLE Tokyo Villes du Japon Japon Actuel Guide Japon

Economie Politique Technologie Chine Environnement Santé Crime Diplomatie Automobile Sport Armée Défense Peche Corée du Nord Culture

ACTUALITÉS > ACTUALITÉS : News et informations sur le Japon

Les robots insectes bientôt au service des humains au Japon

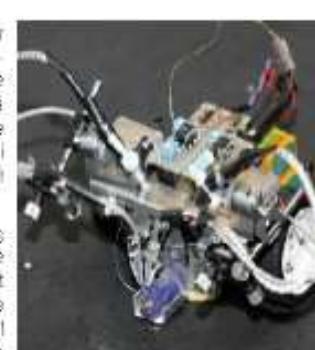
le 16/03/2009 à 12h01 par Hiwa Suzuki (AFP)

Poster un commentaire (1 avis) T T D

S'aidant d'études menées sur les insectes, des chercheurs japonais créent des robots-insectes, capables de déceler la présence de drogue, des mines anti-personnelles, des gaz toxiques, ou des survivants enterrés sous les décombres.

La police lâche une volée de robots-papillons pour aller renifler une planque de drogue. Des robots abeilles s'intègrent sous les décombres d'un séisme pour rechercher des survivants. On pourrait croire à un scénario de science-fiction, mais il s'agit de projets bien réels de chercheurs japonais qui espèrent copier les comportements des insectes afin de les programmer à des tâches spécifiques.

Rochel Karzaili, professeur au Centre de recherches sur la science et la technologie de l'Université de Tokyo, a étudié les cerveaux des insectes pendant trois décennies et est devenu un pionnier dans le domaine des insecte-machines hybrides. Son but initial et ultime est de comprendre le cerveau humain afin de pouvoir rétablir artificiellement les îlots où



La tête d'un vol à soleil a été installée

Toshiba présente sa télévision 3D

Le premier robot "oiseau-mouche" inventé au Japon

Les produits écolos, un marché porteur au Japon

pour l'environnement, les industriels japonais pensent à la maison durable

Au Japon, les robots industriels remplaceront-ils les humains ?

Dépêches...

Bases américaines: Hillary Clinton s'implante le 13/03/2010 à 10h43

Un pickpocket dérobe des milliers d'euros sur un vol Tokyo-Paris le 12/03/2010 à 11h51

Terminé Active

Robots domestiques : dans les coulisses des labos japonais

10 septembre 2010



Installez vous tranquillement et passez les cinq prochaines minutes en compagnie de cette gentille présentatrice de la télévision nipponne qui nous emmène dans un tour des laboratoires de l'entreprise Toshiba et de l'université de Tokyo.

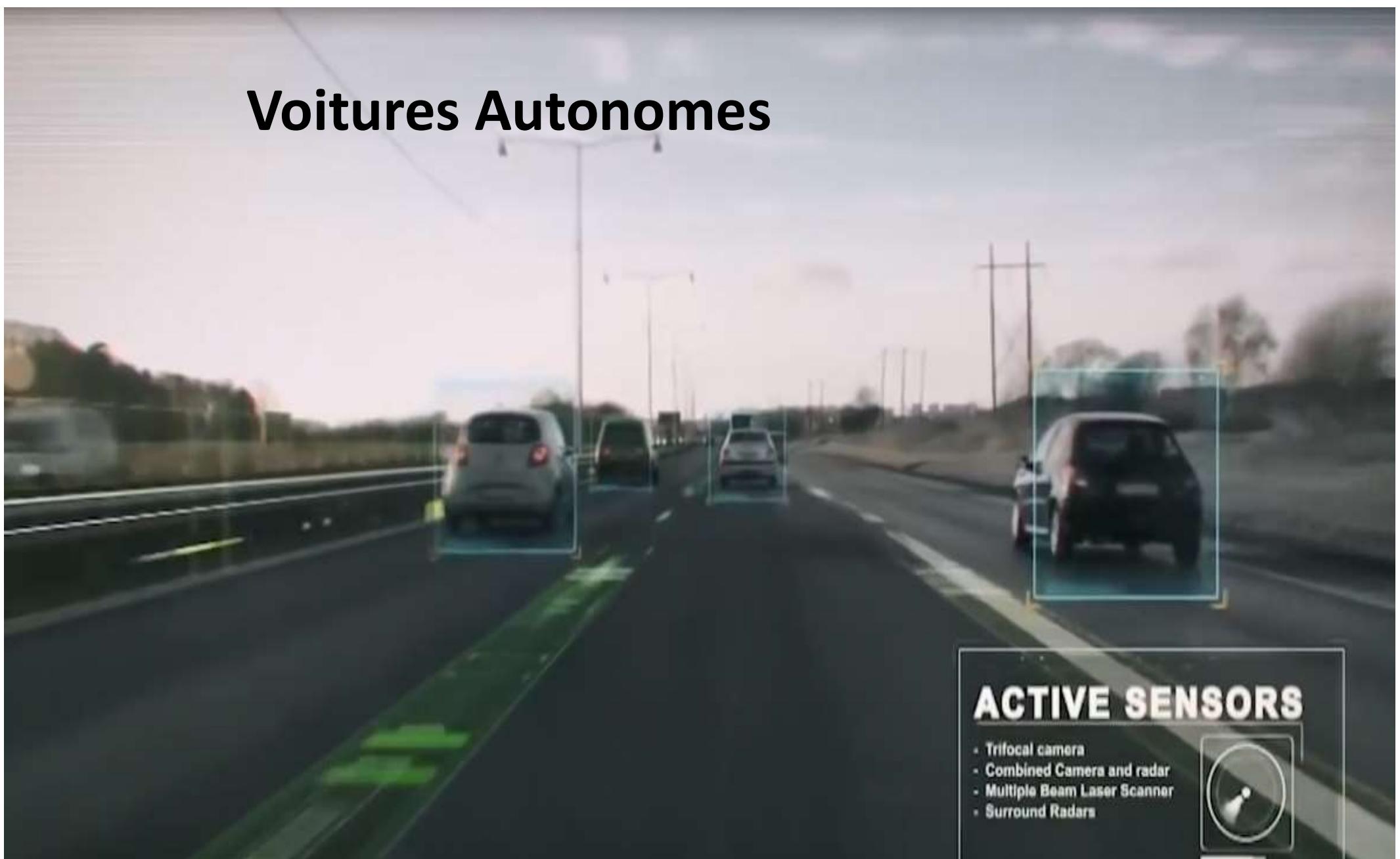




Pas besoin de comprendre le japonais pour reconnaître Apricopo cet hybride Robot de compagnie / Robot Multimedia qui remplace par des commandes vocales les différentes télécommandes de votre maison. Et comment ? Et bien c'est simple, à chaque fois qu'il détecte un signal infrarouge envoyé par l'un de nos appareils électroniques (TV, lecteur DVD etc...) il nous demande ce que l'on fait et retient nos explications qu'il associera à une future commande vocale. Nous pouvons voir par exemple dans cette vidéo l'apprentissage d'Apricopo à éteindre la télévision. Attendu déjà depuis quelques années, peut-on espérer qu'il deviendra un jour aussi populaire que le célèbre Roomba ?



Voitures Autonomes





Aviation

hélicoptère autonome:
MQ-8B Fire Scout





Système experts



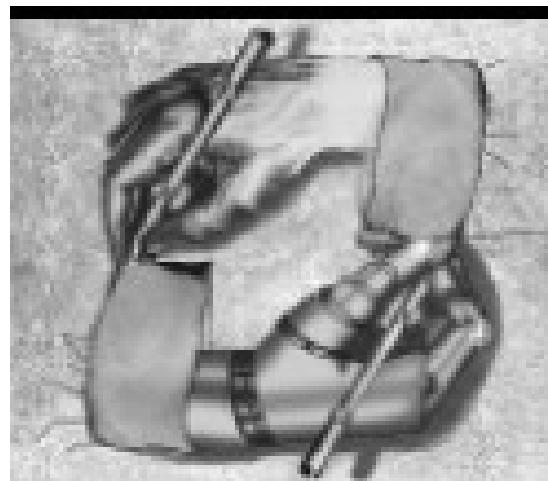
Activer

Histoire des Jeux

Les premières préoccupations des chercheurs en intelligence artificielle – créer des programmes jouant aux: échecs, GO, Dames, Bridge, etc.

Le père des idées est Claude Shannon (1949)

Doodle



Les échecs

- Probablement le problème le plus étudié en IA
 - Etudes psychologiques des GMI (De Groot)
 - Positions pensées (non calculées)
 - Recherche sélective
 - Profondeur faible (quelques coups)
 - Fonction d'évaluation floue (protéger une tour, un fou)





Deep Blue

Activer Windows

Accédez aux paramètres pour activer Windo



Garry Kasparov

Activer Windows
Accédez aux fonctionnalités pour activer Wind

C:/USERS/KASPAROV/QUOTES/1989/

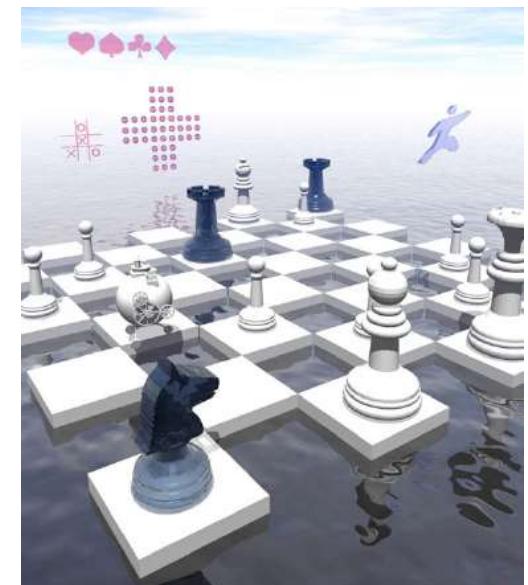
➤ L'ORDINATEUR NE SERA
JAMAIS PLUS FORT QUE L'HOMME

Les échecs

Deep Blue a gagné contre Garry Kasparov en 1997

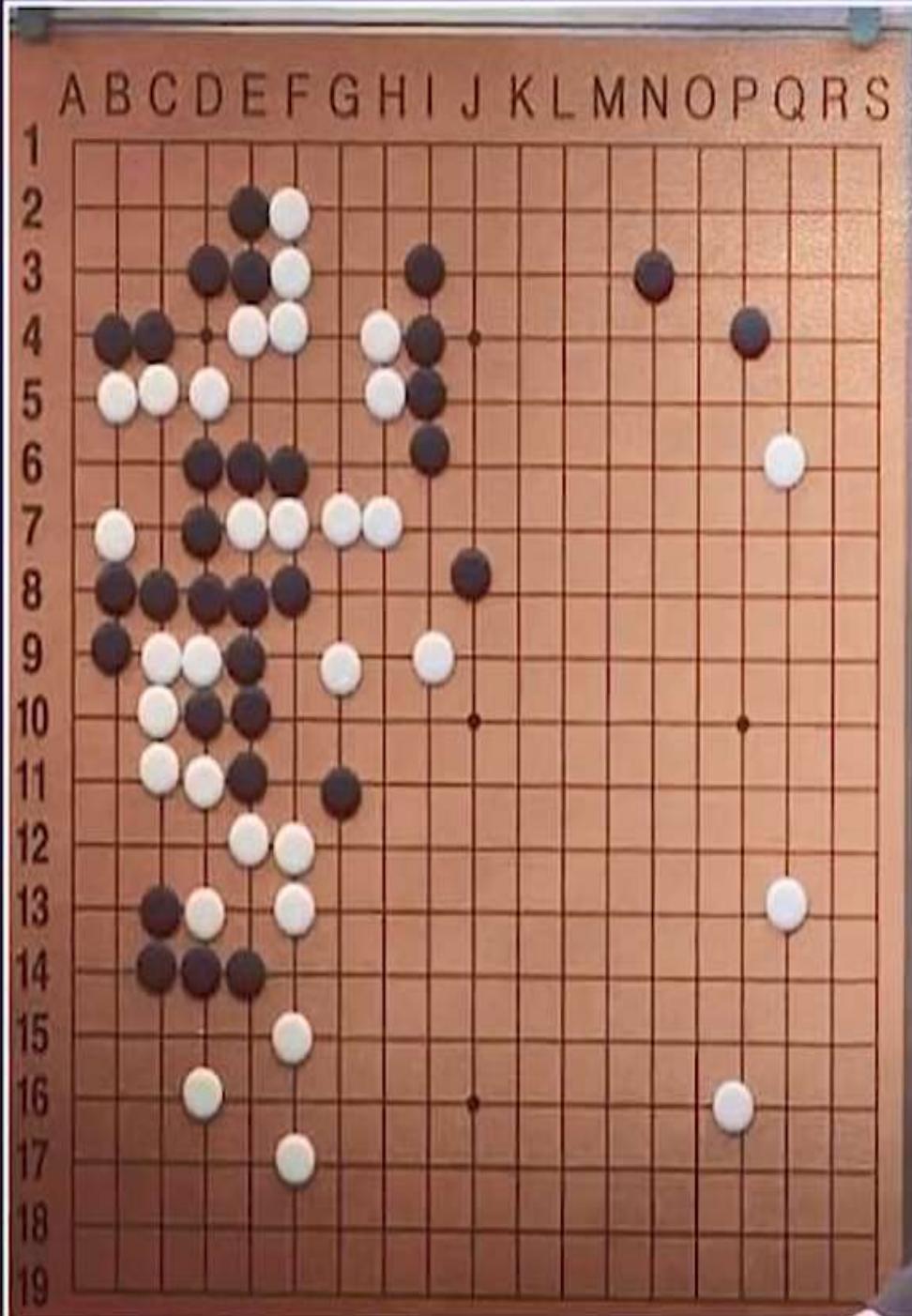
- 6 jeux : 2 victoires, 1 perte, 3 tirages
- La force brute approche
- IBM Deep Blue a pris sa retraite immédiatement après le match

Votre tour a joue!!!



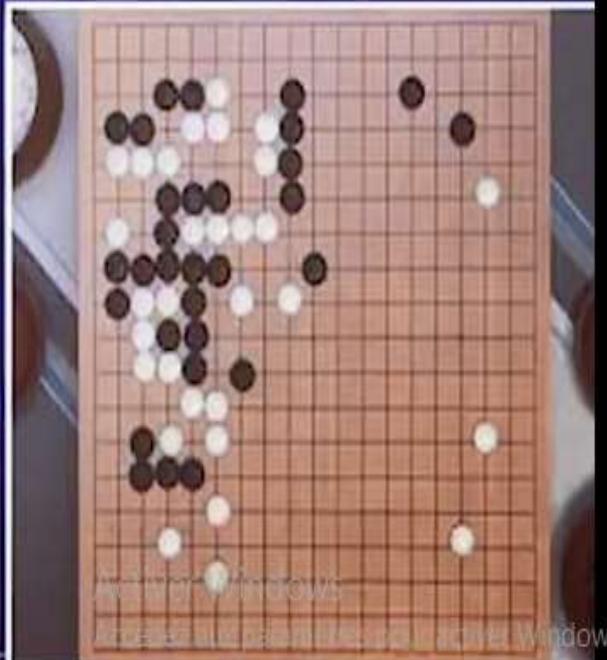


NE SE DÉCONCENTRENT PAS
N'ONT PAS DE PRESSION
ONT LA MÊME HUMEUR



ALPHAGO
01:27:15

LEE SEDOL
00:45:18



Dames

meilleur programme [Chinook](#)

- Mis au point par l'équipe de l'Université de l'Alberta
- Dirigée par Jonathan Schaeffer
- Jeu complet d'arbre de recherche
- À partir de Juillet 2007, Chinook ne peut pas perdre à Checkers



Ping-Pong

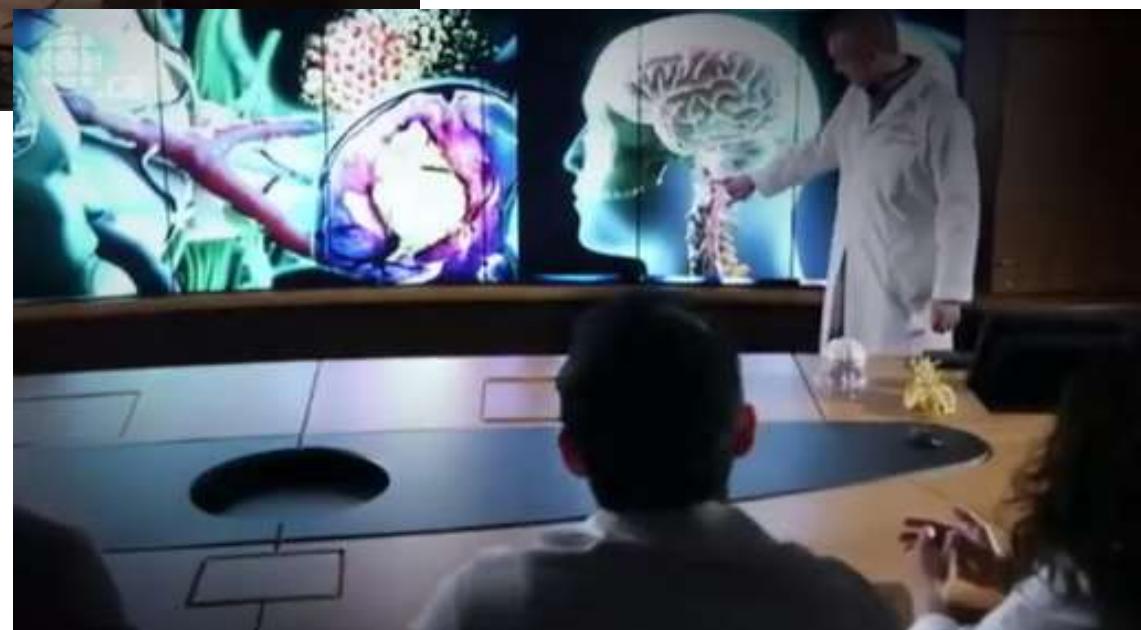
- TOPIO robot
- TOSY Robotics, Vietnam



Médecine (thérapie, surveillance d'appareils, diagnostic)

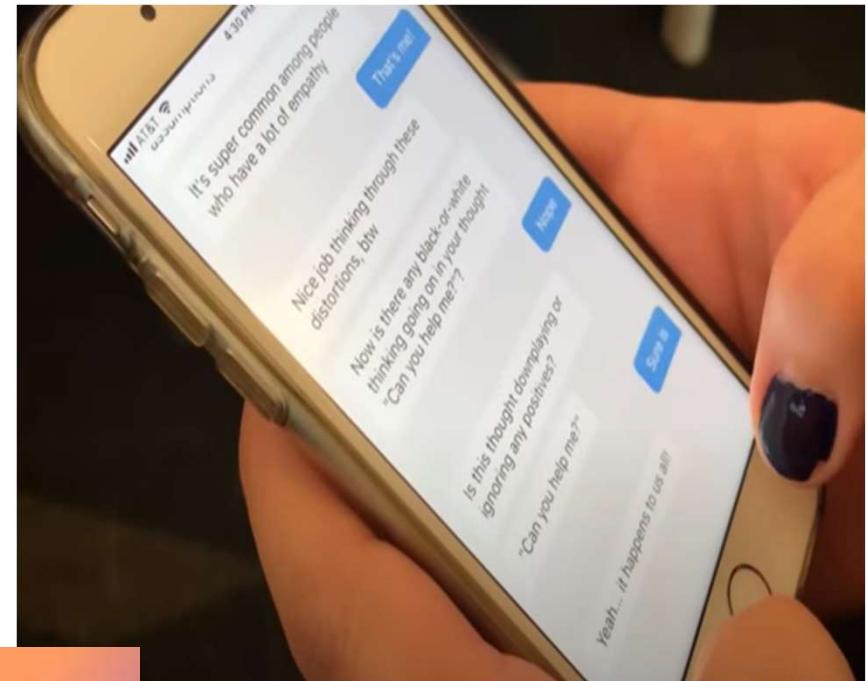
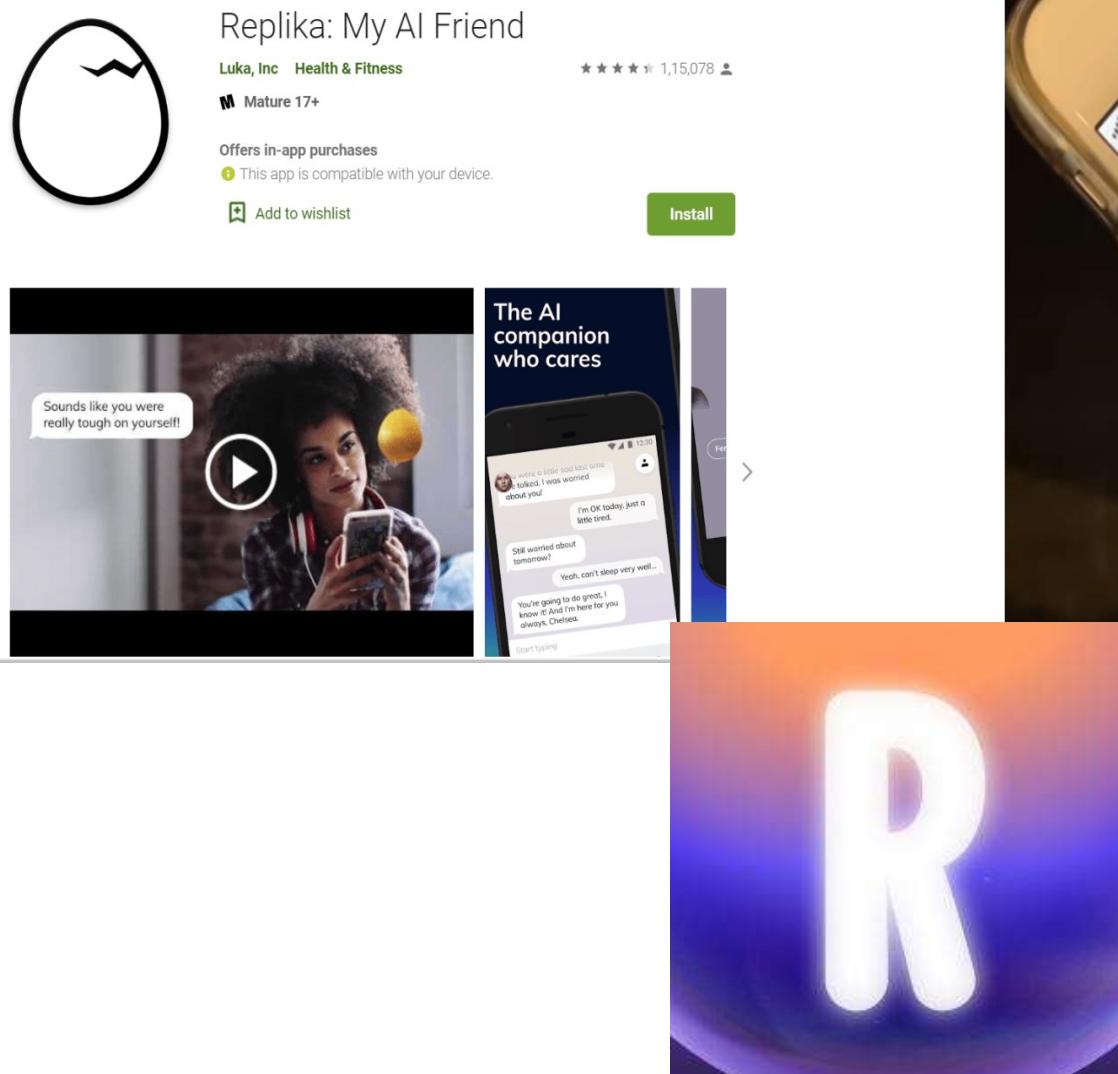


Médecine (classification)



Réduire les problème psychologique

- AI chat robots help alleviate mental health problems such as autism by combining psychological knowledge.



Réalité virtuelle

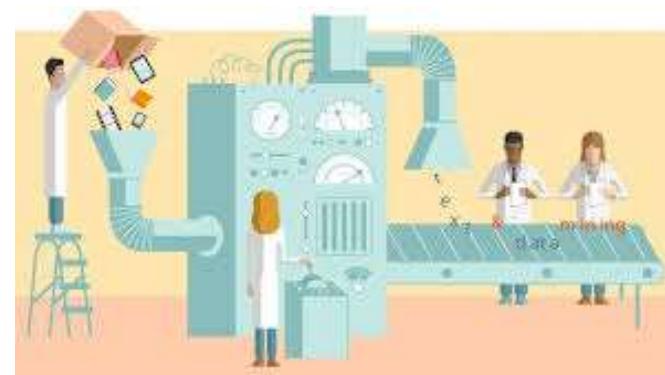
- Ce domaine propose de nouvelles formes d'interaction entre l'homme et la machine. L'arrivée d'ordinateurs plus puissants, dotés d'impressionnantes capacités graphiques en trois dimensions, couplés à des périphériques de visualisation et d'interactions (casques, gant, etc.) permet de fournir les informations sensorielles nécessaires pour convaincre des utilisateurs qu'ils sont en immersion.
- Certains l'utilisent depuis longtemps pour guérir certaines phobies comme celle de l'ascenseur ou celles des araignées.



Indexation multimédia

Les ressources multimédia que l'on retrouve sont à la fois nombreuses et volumineuses et parfois non pertinente.

L'IA propose des outils comme la fouille des données de bases de données → Data mining afin d'extraire des connaissances synthétiques ou d'y découvrir des info cachés ou faire du diagnostics des situations



L'Art

Musique

- David Cope
- Expériences en musique Intelligence (EMI)
- prend des échantillons de travaux par un compositeur en entrée
- analyser le style d'entrée
- générer de nouveaux travaux dans le même style

Sculpture

L'Art

Peinture

- [AARON](#)
- kurzweilcyberart.com
- mis au point par Harold Cohen
- les peintures sur papier avec une pinceau





L'intelligence artificielle dans l'éducation



Langage

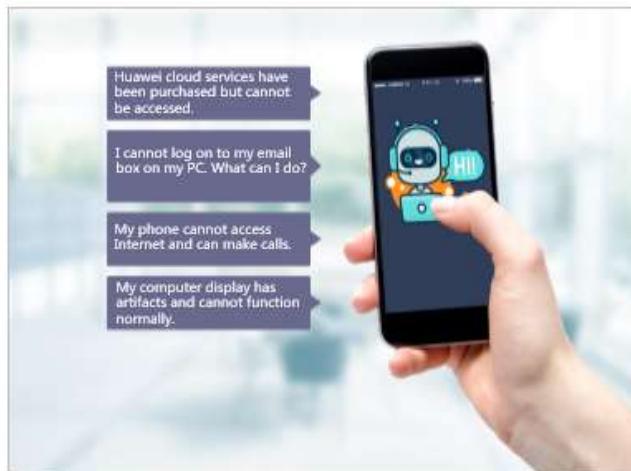
- Traduction automatique
(google.com,
<http://babelfish.yahoo.com/>)
- Reconnaissance de la voix
- Reconnaissance de caractères
(*peu avoir facile des livres en version électroniques*)



Voice Processing Application

- The main topics of voice processing research include voice recognition, voice synthesis, voice wakeup, voiceprint recognition, and audio-based incident detection. Among them, the most mature technology is voice recognition. As for near field recognition in a quite indoor environment, the recognition accuracy can reach 96%.
- Application scenarios:

Question Answering Bot (QABot)

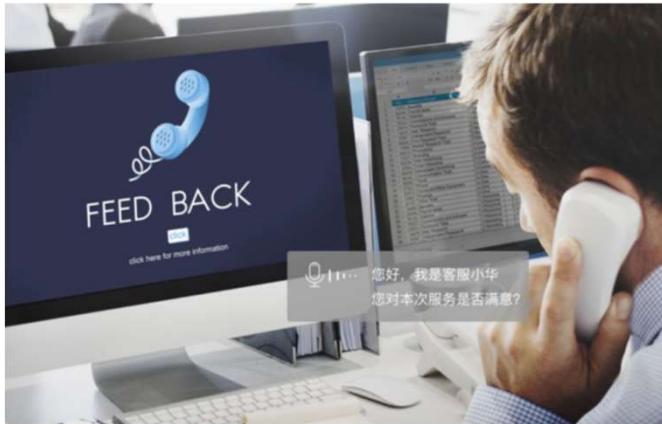


Voice navigation



Voice Processing Application Scenario (2)

Return Visit



Real-time conference records

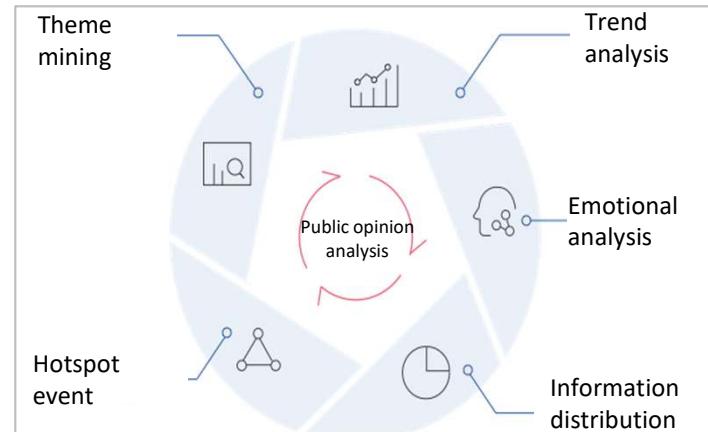


- Other applications:
 - Spoken language evaluation
 - Diagnostic robot
 - Voiceprint recognition
 - Smart sound box
 - ...

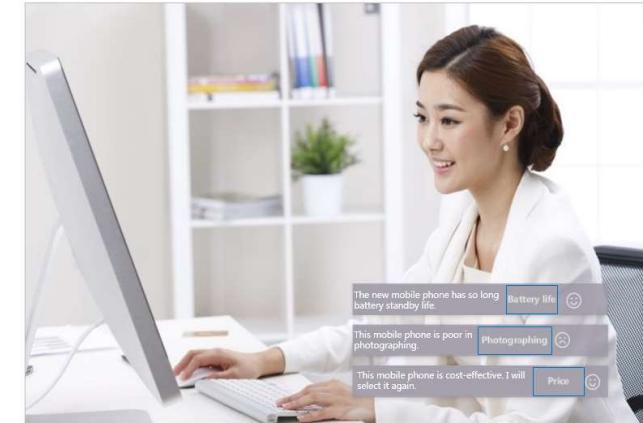
NLP Application Scenario (1)

- The main topics of NLP research include machine translation, text mining, and sentiment analysis. NLP imposes high requirements on technologies but confronts low technology maturity. Due to high complexity of semantics, it is hard to reach the human understanding level using parallel computing based on big data and parallel computing only.
- In future, NLP will achieve more growth: understanding of shallow semantics → automatic extraction of features and understanding of deep semantics; single-purpose intelligence (ML) → hybrid intelligence (ML, DL, and RL)
- Application scenarios:

Public opinion analysis

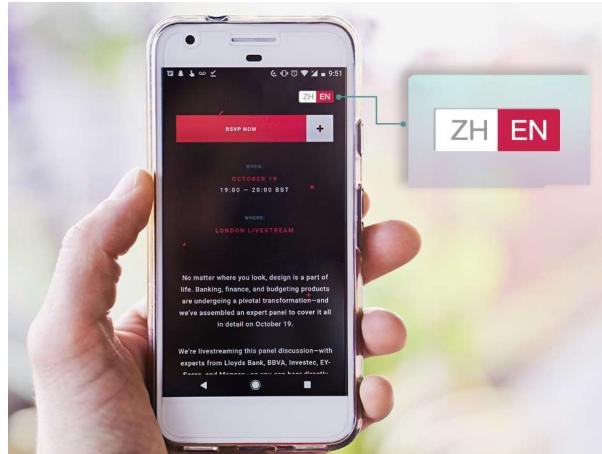


Evaluation analysis



NLP Application Scenario (2)

Machine translation



Text classification



- Other applications:
 - Knowledge graph
 - Intelligent copywriting
 - Video subtitle
 - ...

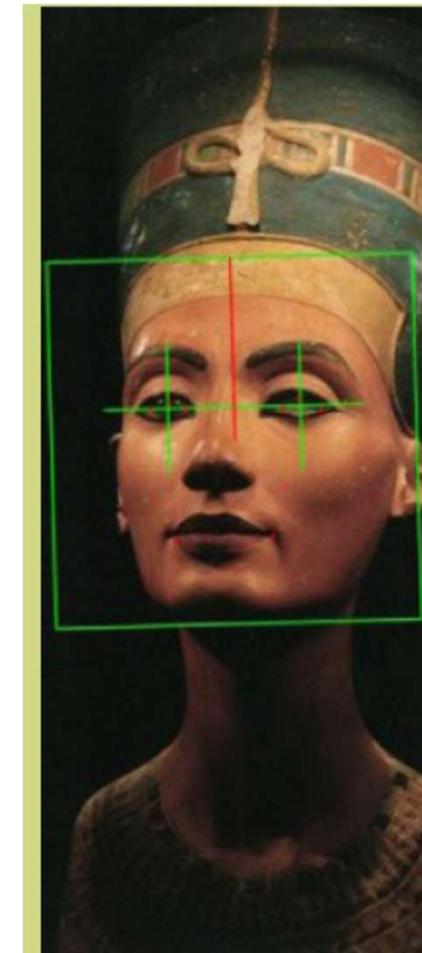
La Reconnaissance de Formes / Sons

- **Image :**
 - Imagerie médicale
 - Environnement (déforestation, inondations)
 - Espionnage militaire
 - Sécurité (reconnaissance du visage)
- **Son**
 - Ecriture
 - Domotique
 - Sécurité (reconnaissance de la voix)
- Biométrie
- Lecture optique de documents
- synthèse d'image

Les progrès en reconnaissance d'images vidéo permettant à la police de repérer une cible dans une foule

Vision

- détection de visage
 - Déetecter les traits du visage
 - Ignore les bâtiments, les plantes, les animaux
 - la reconnaissance du visage
 - Arrêter les criminels
 - Prévenir la fraude
 - Vérifier l'identité pour l'accès à un bâtiment ou d'un ordinateur

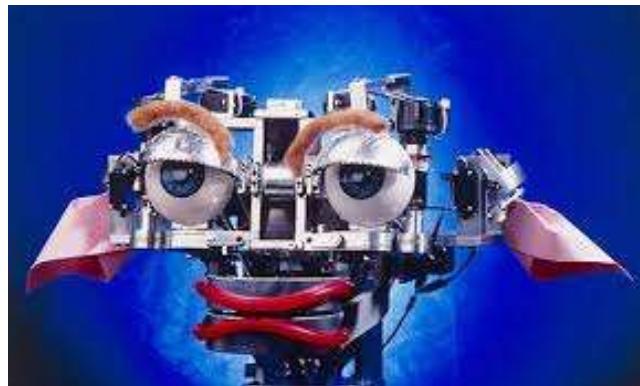


Recherche en IA

Intelligence Sociale

- agents qui prévoient les actions des autres agents en comprenant les motivations, états émotionnelles
- agents qui sont capables de démontrer des émotions

KISMET – robot avec des compétences sociales





Anger



Surprise



Fear



Happy



Calm



Interest



Tired



Disgust



Sad

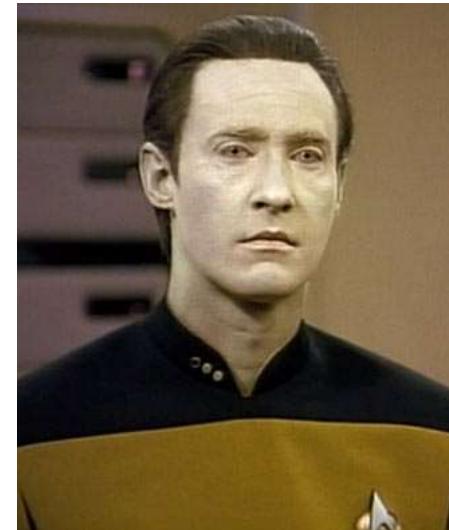
Recherche en IA

Intelligence Générale

systèmes qui combinent tous les autres pour dépasser les compétences des humaines

Mr Data

Androïde – robot qui ressemble à une homme



Le commerce et l'industrie

En 2006, 30% de tous les métiers de stock ont été automatisés par des programmes

- Qui devrait atteindre 50% en 2010
- Des logiciels de trading automatique moniteurs de mesure des nouvelles positives et les opinions négatives sur les stocks
- La vitesse de la négociation est de plus en plus
- Microsecondes peuvent déterminer si le commerce est rentable



Detection de spam

- la détection automatique des courriels pourriel
- en utilisant l'apprentissage machine technique pour le texte classification
- doivent constamment s'adapter aux nouvelles techniques de pollupostage
- conférence annuelle de Pourriel le pourriel automatisé de détection, a commencé 2003



Recherche en IA

Déduction, Raisonnement, Résolution de problèmes

simulation des raisonnements que font les humains quand: jouons des jeux, résoudre des problèmes

Représentation de la connaissance

ontologies – donne structures e.g oiseau

Organisation – avoir un but et développer une stratégie pour le réaliser

Recherche en IA

Apprentissage [YooName](#)

Traitement du langage naturel

- Vérification automatique d'orthographe et de grammaire
- Service téléphonique automatique (Emily Bell)
- Recherche automatique de textes sur un sujet donne et création automatique de résumés de textes
- Outils de traduction automatique

Recherche en IA

Motion et manipulation - Robotiques

Perception

reconnaissance de la voix

reconnaissance du visage

reconnaissance des objets

Office Automation

- AI is automating management, but the different nature and format of data makes it a challenging task. While each industry and application has its own unique challenges, different industries are gradually adopting machine learning-based workflow solutions.



Autres applications

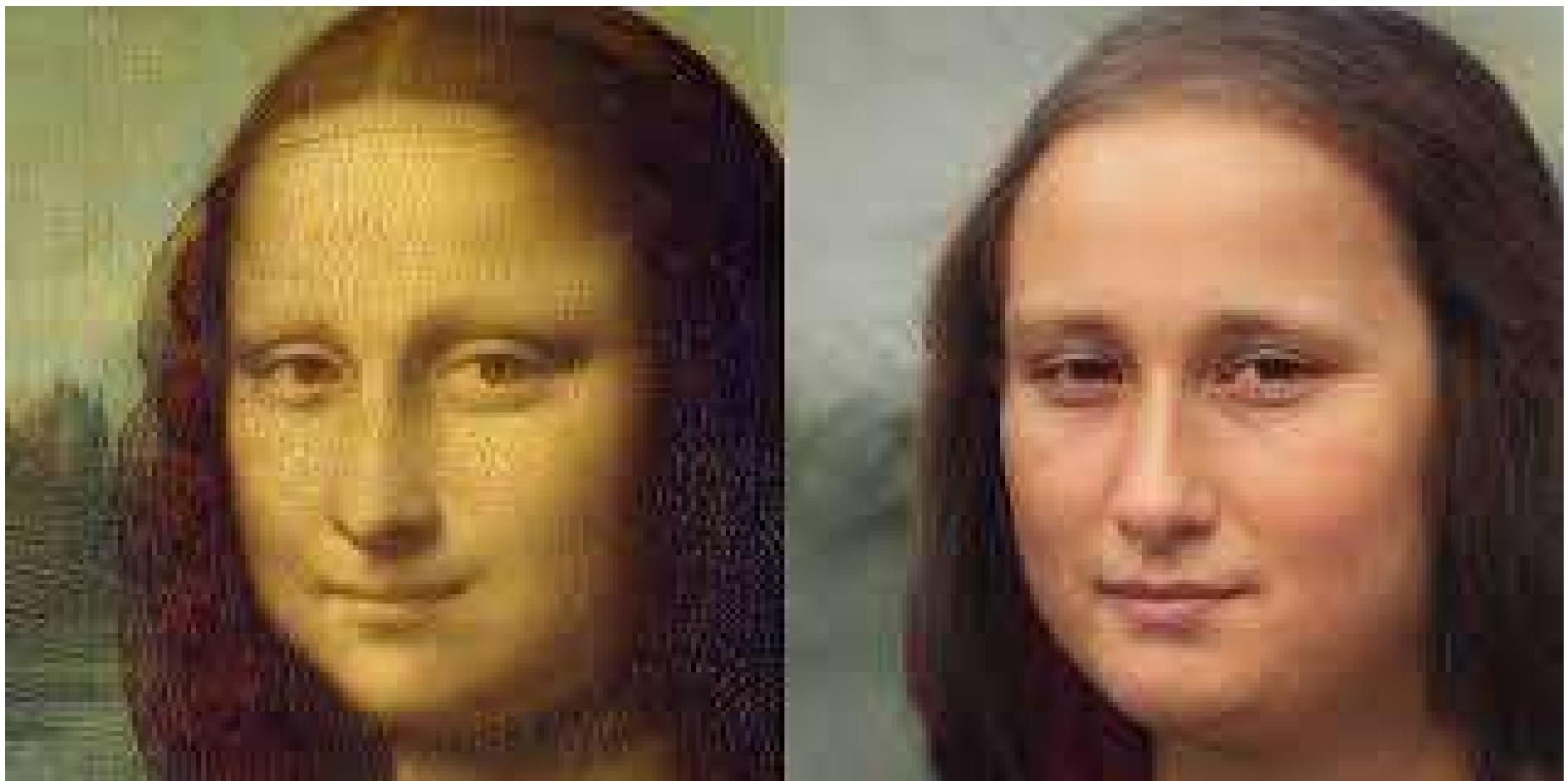
- ❑ Planification des tâches (prédiction financières,...)
- ❑ Architecture (conception assistée par ordinateur,...)
- ❑ Détection des pannes
- ❑ Classification naturelles (biologie, minérologie,...)
- ❑ Education (systèmes tutoriels intelligents, e-learning)
- ❑ Prospection géologique (gisements miniers)
- ❑ Centrales nucléaires, feux de forêts (systèmes à temps réel)
- ❑ Simulateurs de vols (Bombardier, CAE,...)

Réseaux antagonistes génératifs



Generative Adversarial Network (GAN)





L'état des lieux de l'intelligence artificielle dans les grandes entreprises

- ❑ l'intelligence artificielle, ainsi que les plateformes digitales associées à la multitude, l'Internet of Everything et la Blockchain, restructurent et réorientent profondément les flux et les relations qui s'établissent entre acteurs.
- ❑ Il faut aller aujourd'hui au-delà de l'idée de transformation (qui exprime fort bien les changements d'états), au-delà de l'idée de transition (qui exprime fort bien le changement dans la continuité et la préservation des ressources), au-delà de l'idée de révolution (qui exprime fort bien les ruptures qui interviennent dans notre environnement). Il faut désormais penser l'entreprise au travers de **l'idée de métamorphose**, la seule idée à présenter, comme le rappelle Edgar Morin, « le même niveau de radicalité que l'idée de révolution tout en contenant l'idée de conservation » des ressources.
- ❑ Pour faciliter l'adaptation de l'entreprise et de ses collaborateurs aux profondes mutations de notre environnement, il nous faut aujourd'hui, à la fois penser en rupture et agir en continuité ».

L'état des lieux de l'intelligence artificielle dans les grandes entreprises

- Certaines entreprises ont eu l'idée d'une cellule « Innovation et prospective » afin de mener une analyse et une réflexion de l'impact de l'intelligence artificielle dans l'entreprise.
- Cela a pour objectif de franchir le pas sans pour autant délaisser les salariés qui sont au centre du sujet.



L'IMPACT DE L'INTELLIGENCE ARTIFICIELLE POUR LES ENTREPRISES

Aujourd'hui l'intelligence artificielle génère déjà de nombreux bénéfices pour les entreprises, notamment en :

- Répondant aux enjeux du *Big data* ; l'intelligence artificielle repose en effet pour une grande partie sur la fouille et l'analyse de masse de données à partir desquelles elle pourra apprendre ;
- Augmentant l'expertise humaine d'aide à la décision, assistant d'aide en ligne : une société à Hong Kong, *Deep knowledge venture (DKV)*, spécialisée dans les investissements en capital risque, possède par exemple une intelligence artificielle à son conseil d'administration, nommée Vital (*Validating Investment Tool for Advancing Life sciences*) qui fait des recommandations en matière d'investissement et possède également un droit de vote ;
- Optimisant les services et produits : amélioration de la connaissance client, de la prise de décision, mais aussi des processus opérationnels ;
- Renforçant la sécurité des systèmes : en matière de cybersécurité, l'intelligence artificielle devient un élément structurant des infrastructures IT, afin de sécuriser les réseaux. Michael Hack, *Senior Vice-President EMEA Operations, Ipswich*, affirme en effet que « la reconnaissance automatique est désormais bien établie pour la détection des fraudes, et des développements sont en cours pour créer des algorithmes qui identifieront les menaces que les cerveaux humains et les mécanismes de sécurité traditionnels échouent à reconnaître. »
- Aidant à faire des découvertes : certaines entreprises dans le domaine de la santé utilisent par exemple Watson pour analyser toutes les publications scientifiques ayant trait à un domaine particulier de recherche, ce qui leur permet de chercher de nouvelles propriétés, de nouvelles molécules.

LE CADRE JURIDIQUE

- Il n'existe pas aujourd'hui de cadre juridique propre à l'intelligence artificielle.
- Aucune disposition française ou européenne spécifique à l'intelligence artificielle n'existe ou ne prend en considération les spécificités des algorithmes, de ses capacités décisionnelles, d'apprentissage et d'autonomie, ni même de sa coopération avec l'être humain.



Il est cependant nécessaire de mettre en avant les aspects juridiques majeurs liés au développement considérable tant du point de vue quantitatif que qualitatif de l'intelligence artificielle.

LE CADRE JURIDIQUE

La problématique juridique générale s'articule autour des axes suivants :

- **quelle protection pour l'intelligence artificielle ?**

Les problématiques juridiques majeures plus spécifiques auxquelles est confrontée aujourd’hui l’intelligence artificielle sont tout d’abord la protection des concepts innovants développés par les chercheurs en intelligence artificielle, notamment sur le plan de la propriété intellectuelle, la protection des données à caractère personnel, mais également des problématiques liées à la mise en oeuvre de la responsabilité de l’intelligence artificielle en cas de dommage

- **quelle responsabilité en cas de dommage causé par une intelligence artificielle ?**

L’entreprise qui développe l’intelligence artificielle devra tenir une attention pour toute particulière pour la protection de son innovation. Toutes les entreprises en transition intelligente devront analyser les contrats les liant avec le fabricant d’intelligence artificielle.



LE REFERENTIEL LEGAL DE L'INTELLIGENCE ARTIFICIELLE



- A ce jour, l'intelligence artificielle apparaît uniquement dans deux définitions légales et normatives.
- La norme **ISO 2382-28** définit l'intelligence artificielle comme la « capacité d'une unité fonctionnelle à exécuter des fonctions généralement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage ».



Le terme « autonomie » est défini par la **norme ISO 8373:2012** comme la « capacité d'exécuter des tâches prévues à partir de l'état courant et des détections, sans intervention humaine ».



LE CADRE JURIDIQUE



L'action à venir de la **Commission européenne concerne l'adaptation de la législation à la robotique et à l'intelligence artificielle** et serait fondée sur l'article 114 du traité sur le fonctionnement de l'Union européenne pour légiférer et l'article 5§3 du Traité sur l'Union européenne instaure, quant à lui, le principe de subsidiarité, permettant à l'Union européenne d'intervenir dans les cas où « les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres ».

LA PROTECTION DE L'INTELLIGENCE ARTIFICIELLE PAR LA PROPRIETE INTELLECTUELLE

La protection des différents composants de la machine, qu'il s'agisse d'un robot ou de tout type d'autre machine, doit se distinguer de la protection de l'intelligence artificielle en tant que telle, qui donne à la machine une « **autonomie** », ou une « **conscience** » pour reprendre l'expression de certains chercheurs.



La protection de l'innovation par le droit d'auteur

Droit d'auteur. Le concept innovant comportant de l'intelligence artificielle doit être protégé en tant

que tel par le droit d'auteur sous réserve de réunir trois conditions cumulatives :

- une forme d'expression ;
- qui soit susceptible d'être qualifiée d'oeuvre de l'esprit ;
- et ayant un caractère original.

L'originalité de l'intelligence artificielle, qui lui donne un aspect unique, ressort nécessairement de l'**algorithme** qui en est le fondement, et qui doit faire l'objet d'une protection.



La protection des algorithmes

Les algorithmes, entendus comme des méthodes ou des principes mathématiques, ne sont pas protégés « en tant que tels » par le droit d'auteur. Toutefois, la mise en forme de ces algorithmes par des documents ou encore le logiciel incorporant l'algorithme pourrait être protégé par le droit d'auteur, à condition de comporter un certain degré d'originalité.

US Copyright. L'US Copyright Act organise la protection par le droit d'auteur des œuvres de l'esprit et précise la procédure de dépôt auprès du Copyright Office de ces œuvres.

Les logiciels sont protégeables par le droit d'auteur américain sous réserve de leur originalité et d'être formalisés.



La protection par le brevet

Le brevet protège les innovations techniques sous réserve de remplir les critères de nouveauté, d'inventivité et d'application industrielle

Dans un document rédigé par l'Office européen des brevets intitulé « Des brevets pour les logiciels ? », l'OEB affirme que « un brevet peut être délivré pour une invention mise en oeuvre par ordinateur qui résout un problème technique de manière non évidente ».



LA PROTECTION DU SAVOIR-FAIRE



- Les algorithmes et donc l'intelligence artificielle sont susceptibles de constituer un savoir faire protégeable s'ils font partie d'un ensemble d'informations pratiques non brevetées, résultant de l'expérience, du savoir-faire et testées.
- En revanche, le savoir-faire ne donne pas lieu à un droit privatif (droit de propriété intellectuelle ou autre droit de propriété).
- Son détournement peut cependant donner lieu à des actions civiles en concurrence déloyale ou parasitaire, voire à des actions pénales.



LA PROTECTION DES OEUVRES DE L'AGENT INTELLIGENT

Il convient de procéder à la distinction suivante :

- la protection des œuvres assistées concerne les œuvres créées par assistance robotique ;
- la protection des œuvres autonomes : concerne celles entièrement réalisées par le robot.

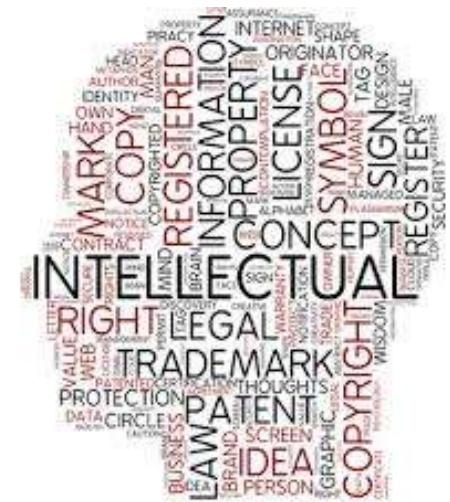
La question de la propriété des œuvres créées par des agents intelligents doit se poser, et plusieurs hypothèses pourront être envisagées quant à la personne titulaire des droits de propriété intellectuelle attachés à de telles œuvres :

- le fabriquant ;
- le propriétaire ;
- l'employeur, dans les cas où des agents intelligents remplaceraient des salariés pour certaines tâches.



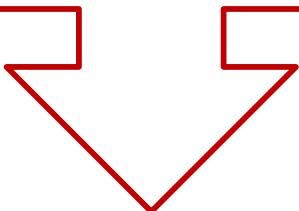
LA PROTECTION DES OEUVRES DE L'AGENT INTELLIGENT

Il n'existe encore **aucune** protection spécifique à ce sujet. Si cela arrivait, il faudrait alors consacrer une personnalité juridique à part entière au bénéfice des agents intelligents afin qu'ils puissent jouir de droits de propriété intellectuelle sur leurs créations ou cocréations.



LES DONNEES A CARACTERE PERSONNEL ET VIE PRIVEE

Les données sont considérées comme nouvelle matière première de l'entreprise, et sont aujourd'hui au centre de l'activité des entreprises et indispensables pour l'intelligence artificielle.



Le recours à des algorithmes prédictifs et aux données d'apprentissage de l'intelligence artificielle doit être encadré conformément aux dispositions applicables en matière de protection des données à caractère personnel

Les cinq principes de la loi IL à respecter pour chaque traitement de données à caractère personnel



LA RESPONSABILITE

La détermination du responsable d'un dommage impliquant une intelligence artificielle est une question complexe dans la mesure où il y a une pluralité d'acteurs :

- le concepteur ;
- le programmeur ;
- l'intégrateur ;
- l'utilisateur ;
- voire de l'intelligence artificielle elle-même.

La responsabilité pénale de l'entreprise peut également être engagée dès lors que l'infraction de l'intelligence artificielle a été commise pour le compte de cette personne morale.



La responsabilité pénale

Dans le Droit pénal général, l'infraction est caractérisée par la réunion de trois éléments :

- un élément matériel : la commission d'un fait ou l'abstention d'exécuter une obligation ;
- un élément légal : un fait ou une obligation prévue par la loi ;
- un élément moral : l'intention, c'est à dire la conscience d'enfreindre la loi.

L'auteur de l'infraction est en principe une personne physique.



La responsabilité civile

Par principe, chacun n'est responsable que de son propre fait.

La responsabilité civile délictuelle suppose la réunion de trois conditions :

- une faute ;
- un préjudice ;
- un lien de causalité entre la faute et le préjudice.

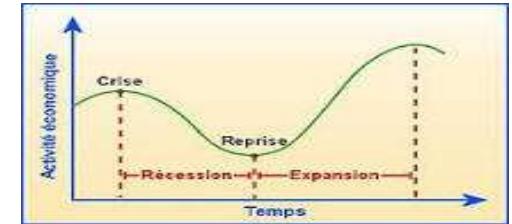


LES ENJEUX ETHIQUES

Les craintes liées au développement de l'intelligence artificielle, plus ou moins fantasmées, sont au cœur du débat.



L'AVENIR DE L'EMPLOI ET L'ACCEPTATION SOCIALE



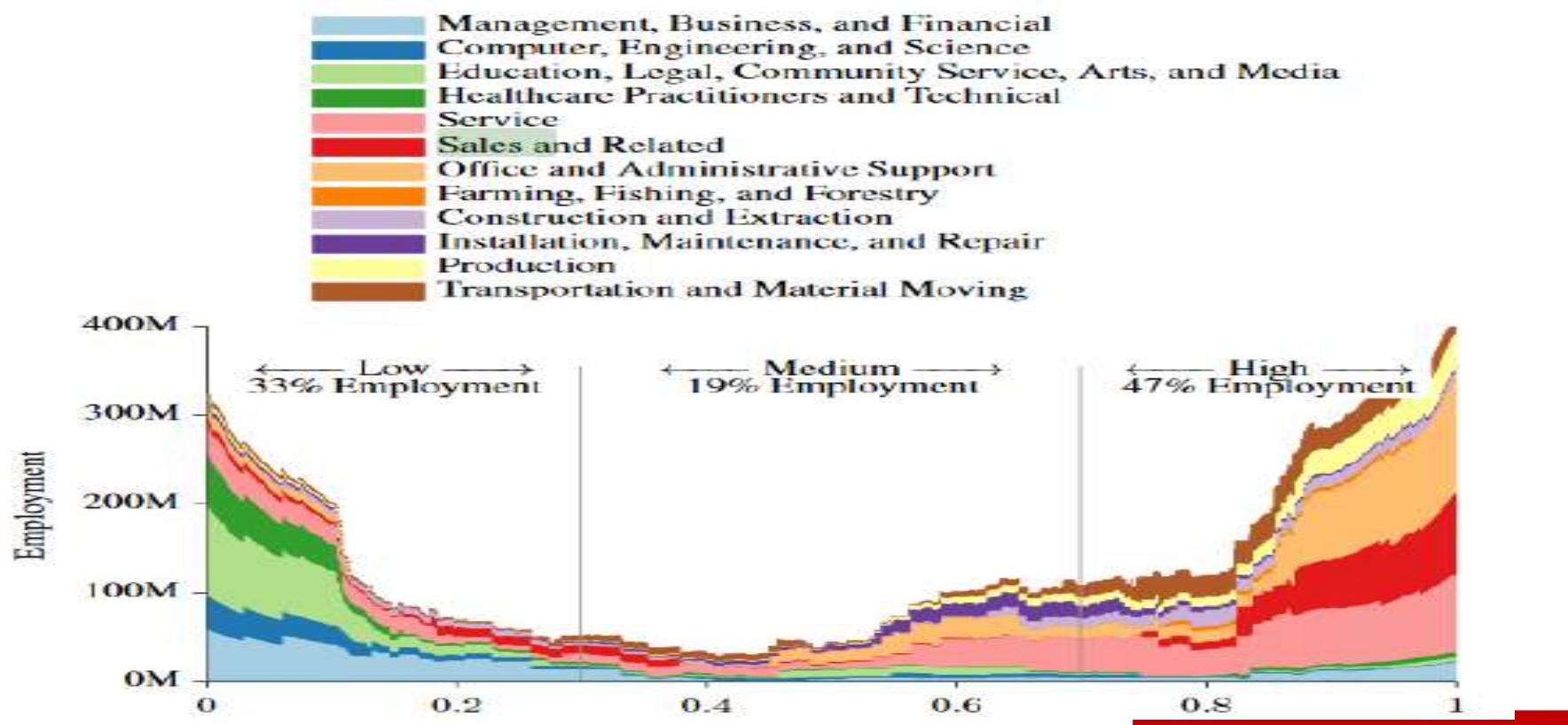
- ❑ Selon la vision schumpétérienne du monde, la balance « destruction-création » maintiendra une certaine stabilité.

- ❑ En effet, de nouveaux métiers pourront se créer dans des domaines connexes.



Une étude anglaise du 17 septembre 2013

- ❑ Les métiers qui ont le moins de risques de se faire remplacer par des automates ou des intelligences artificielles sont les fonctions de management, les métiers de la finance, du numérique, de l'éducation ou de la santé.
- ❑ À l'opposé, les métiers qui seront le plus susceptibles de disparaître concernent surtout les services, la vente, l'administratif, les transports

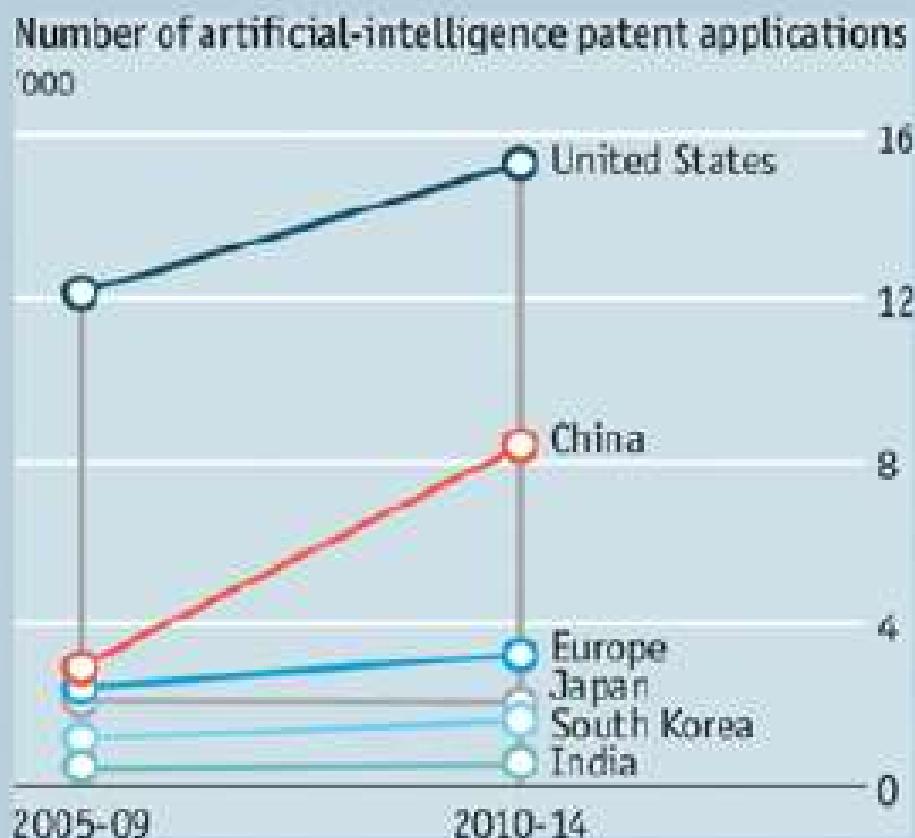


AI Development = Rising Unemployment?

- Looking back, human beings have always been seeking ways to improve efficiency, that is, obtain more with less resources. We used sharp stones to hunt and collect food more efficiently. We used steam engines to reduce the need for horses. Every step in achieving automation will change our life and work. In the era of AI, what jobs will be replaced by AI?
- The answer is repetitive jobs that involve little creativity and social interaction.

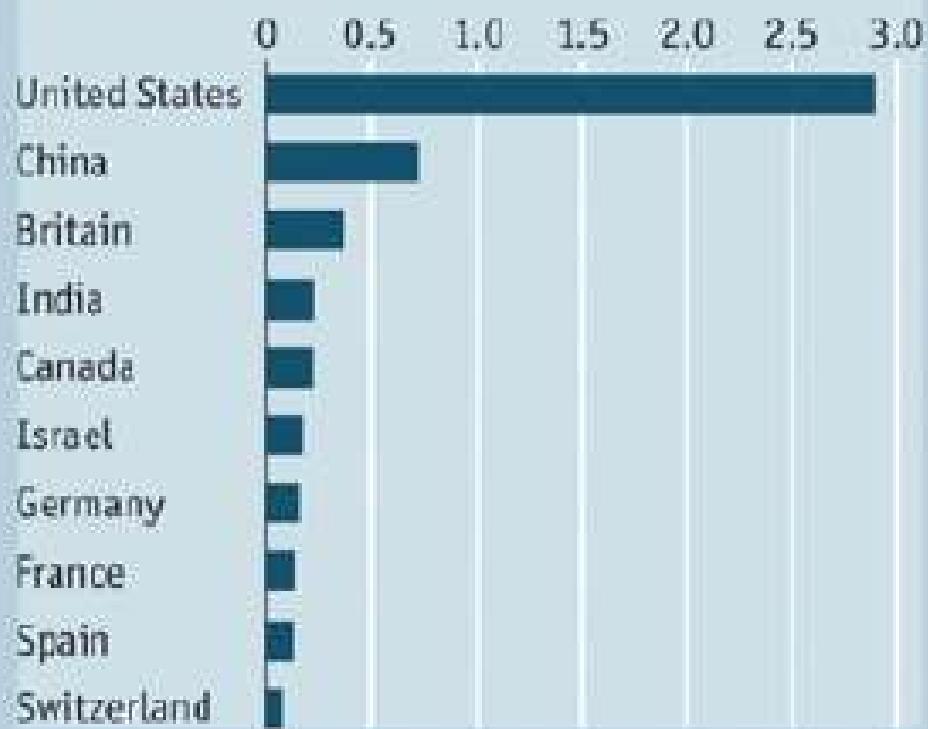
Jobs Most Likely to Be Replaced by AI	Jobs Most Unlikely to Be Replaced by AI
Courier	Writer
Taxi driver	Management personnel
Soldier	Software engineers
Accounting	HR manager
Telesales personnel	Designer
Customer service	Activity planner
...	...

Race of the machines

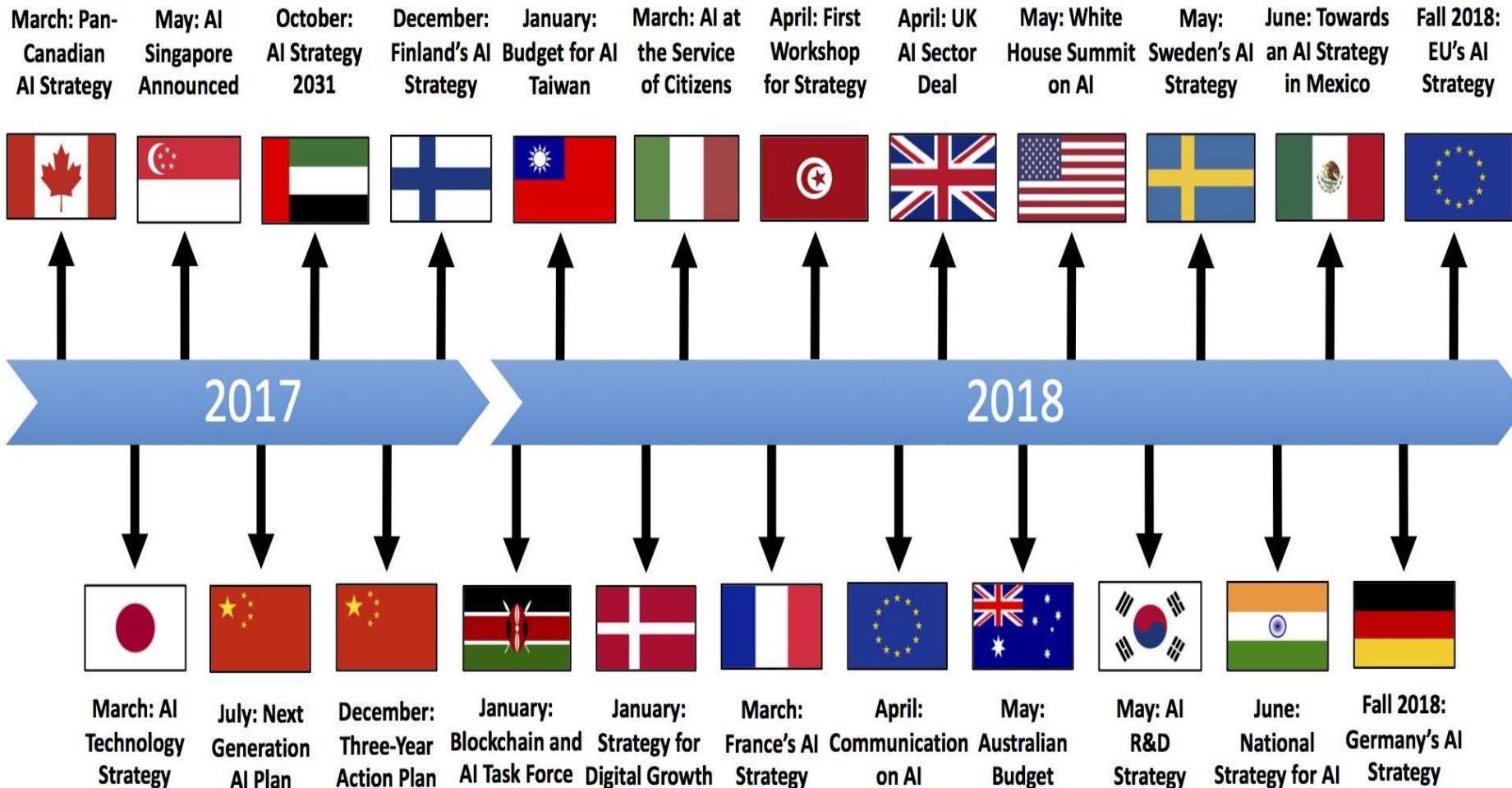


Sources: Press reports; Wuzhen Institute

Number of artificial-intelligence companies
Selected countries, 2016, '000



Artificial Intelligence Strategies



2018-07-13 | Politics + AI | Tim Dutton

Lancement de la stratégie nationale de l'IA





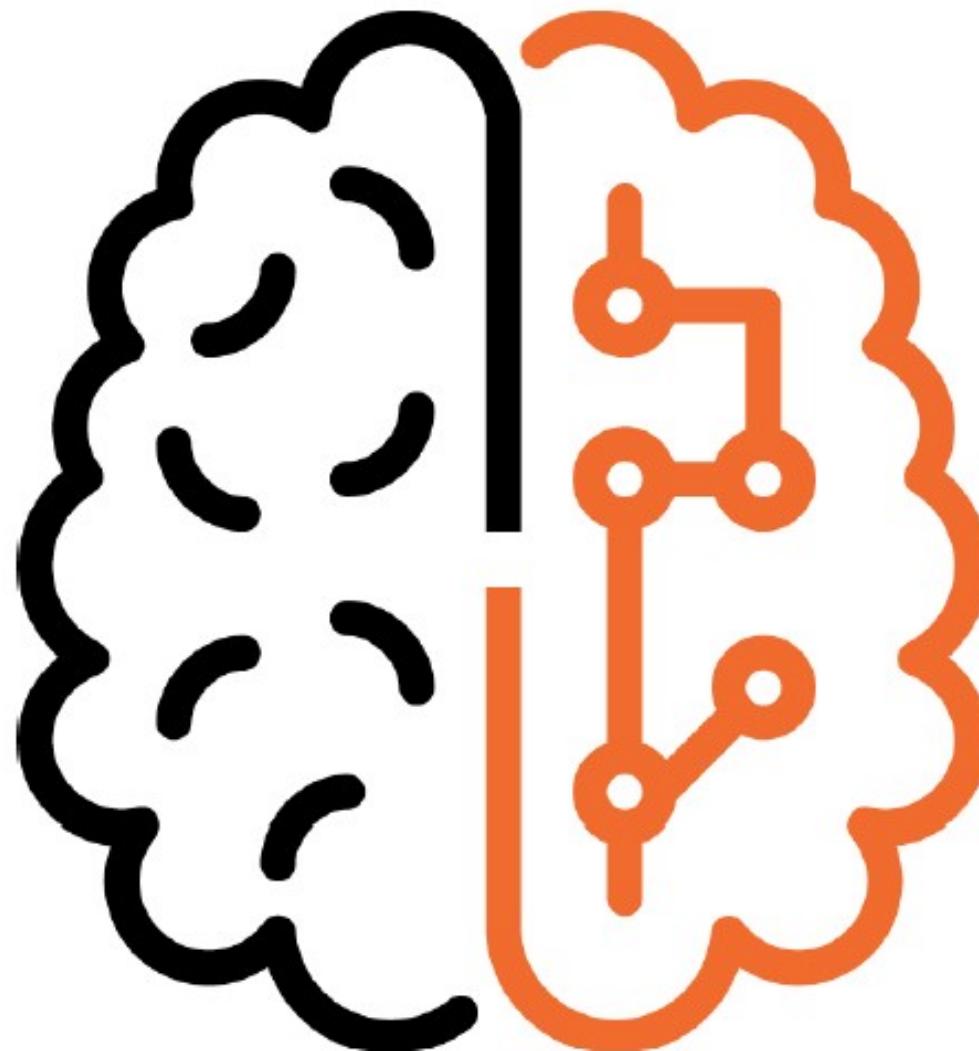
Merci pour Votre Attention

Imen BEN CHaabane

Imen.benchaabane@isetcom.tn



Machine Learning

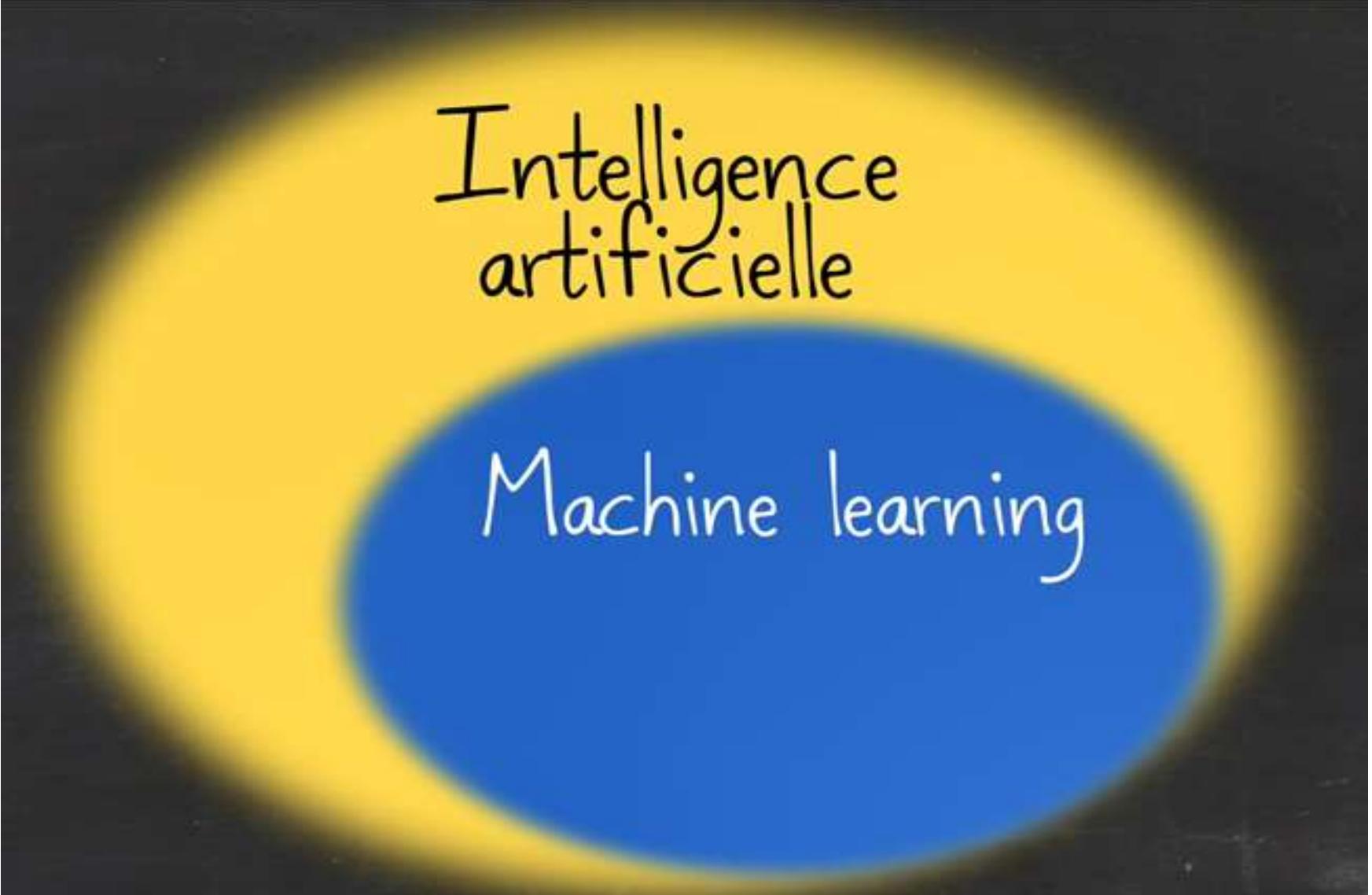


L'EXPRESSION DE L'INTELLIGENCE ARTIFICIELLE

La matérialisation

L'intelligence artificielle a intégré depuis plusieurs décennies de nombreuses applications et divers processus.

→ Aujourd'hui, certaines technologies d'intelligence artificielle permettent de mieux répondre aux exigences du *Big data*. C'est le cas du *Machine Learning* notamment.



Intelligence
artificielle

Machine learning

Le Machine Learning

- ❑ Le Machine Learning regroupe des algorithmes qui apprennent à partir d'exemples, de données.
- ❑ Le Machine Learning essaie de prédire des valeurs à partir de jeux de données qui lui servent d'exemples.
- ❑ La qualité du Machine Learning dépend de la qualité des données. Une rupture risque donc de se créer entre les entreprises qui ont les données (de qualité) et celles qui ne les ont pas.
- ❑ Cela permet une analyse prédictive afin de détecter notamment les risques, les usages et les besoins.
- ❑ Google utilise notamment le Machine Learning avec Youtube afin de classer toutes les vidéos.
- ❑ L'objectif est d'obtenir une prédiction dotée d'une grande puissance.



L'apprentissage supervisé

- Le ***Supervised Learning*** consiste à fournir des exemples au système en lui indiquant la bonne réponse, et il apprend à fournir la bonne réponse dans de nouveaux cas. Il s'agit par exemple de la :
 - o classification : des milliers de vidéos de sport sont données au système en lui indiquant de quel sport il s'agit, et il est ensuite capable d'identifier le sport dans de nouvelles vidéos ;
 - o régression ou prédiction de valeur : de nombreux exemples de maisons sont donnés au système en précisant toutes les caractéristiques et le prix de vente, et il est ensuite capable de prédire le prix de vente d'une nouvelle maison, étant données ses caractéristiques ;
 - o prédiction de risque : de nombreuses caractéristiques de patients sont fournies au système en indiquant s'ils ont souffert ou non d'une maladie et le système prédit ensuite le risque qu'un nouveau patient développe cette maladie, en fonction de ses caractéristiques.

L'apprentissage non-supervisé

L'Unsupervised Learning consiste à fournir de nombreux exemples au système, mais cette fois sans lui donner de « bonne réponse ».

o le partitionnement ou clustering : le système apprend tout seul à détecter des groupes

de clients similaires en vue d'un marketing particulier pour chacun ;

o la détection d'anomalie ou de nouveauté : le système apprend tout seul à identifier des cas qui sortent de l'ordinaire, pour la détection de fraude à la carte bancaire ou la détection de défauts de production dans l'industrie ;

o la réduction de dimensions : le système apprend tout seul à identifier les dimensions les plus importantes dans un jeu de données afin, par exemple, de les représenter visuellement d'une façon qui permette à un humain de mieux comprendre les données, ou simplement afin de les compresser ;

o les règles d'association : le système apprend tout seul à détecter des corrélations fortes. Par exemple, les clients qui achètent un produit achète souvent un autre avec, donc il faut placer ces deux produits à proximité dans un supermarché.

L'apprentissage semi-supervisé.

Le *Semi-supervised Learning* consiste à fournir de nombreux

- Google Photos détecte automatiquement les personnes sur les photos et crée tout seul un dossier pour chaque personne.
- Il donne ensuite à l'utilisateur la possibilité de préciser qui sont ces personnes et de corriger quelques erreurs.
- Le système utilise ces informations pour s'améliorer.



L'apprentissage par renforcement ou le *Reinforcement Learning*

Le système est libre d'évoluer dans son environnement qui peut être physique dans le cas d'un robot, mais peut également être un environnement virtuel. Ce système reçoit des récompenses ou des punitions selon ce qu'il fait et il tente de s'améliorer pour avoir le plus de récompenses possibles. C'est l'exemple :

o d'un robot qui apprend à marcher tout seul. On lui donne une récompense quand il approche de son objectif, et on lui donne une punition lorsqu'il tombe ou perd du temps. A partir de cette supervision réduite, il est capable d'apprendre tout seul à contrôler ses moteurs pour se déplacer efficacement ;

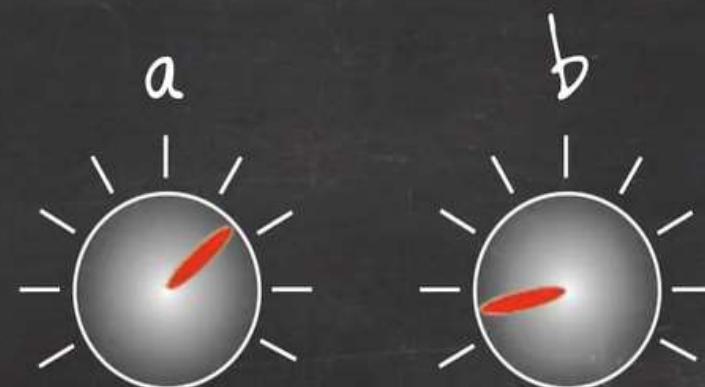
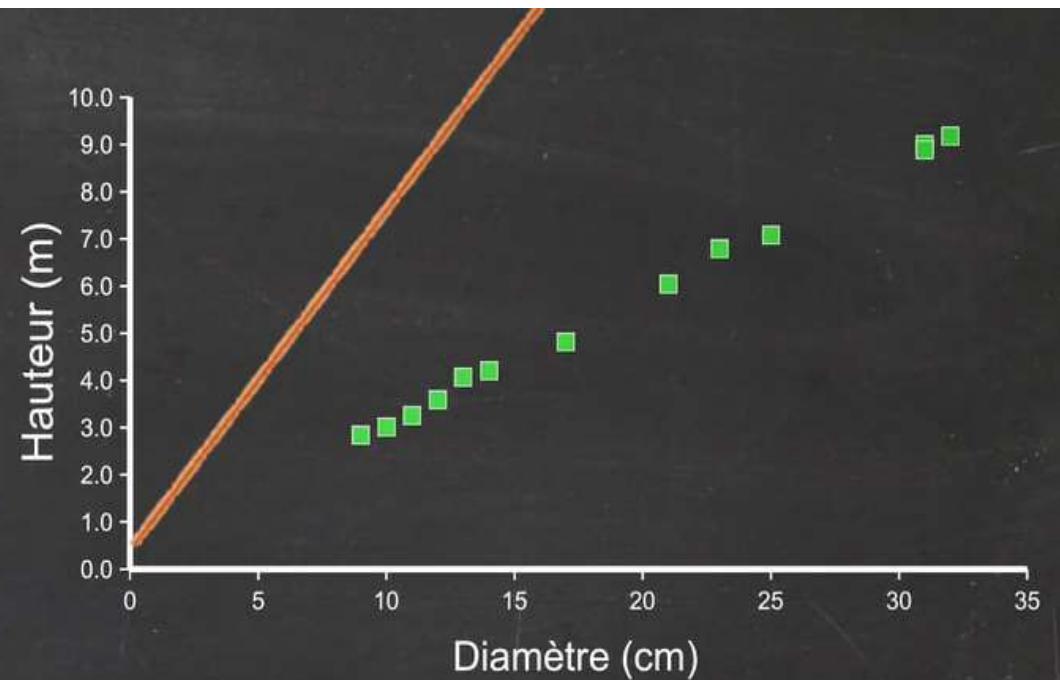
o d'un « *bot* » dans un jeu vidéo qui joue contre le joueur et apprend de ses erreurs pour s'améliorer.

Machine Learning

- ❑ Toutes les entreprises peuvent bénéficier d'un Machine Learning utile notamment pour le marketing afin d'estimer la valeur des clients, identifier les segments d'utilisateurs et mettre en place des targeting de réduction.
- ❑ Mais il est très utile aussi dans le domaine des ventes en priorisant les prospects via la détermination des probabilités d'achat ou l'espérance des bénéfices (en faisant de la prévision sur les demandes).
- ❑ Le Machine Learning permet aussi de déterminer tout type de risque comme la détection de fraudes, l'estimation des recouvrements. Les ressources humaines pourraient aussi profiter des bénéfices du Machine Learning afin de filtrer les CV, prédire les employés susceptibles de partir, recommander des cours ou formations ou encore détecter des talents.

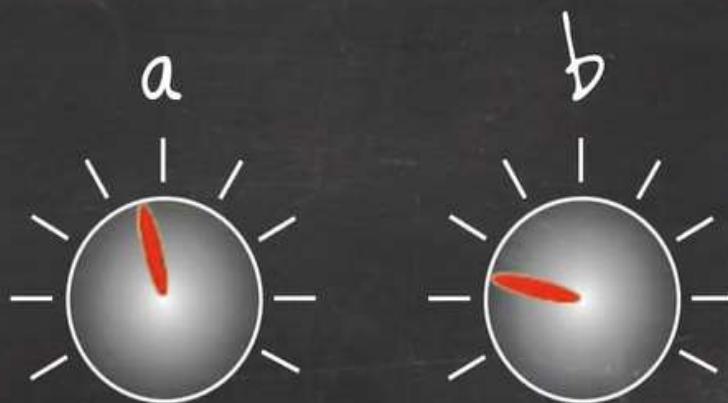
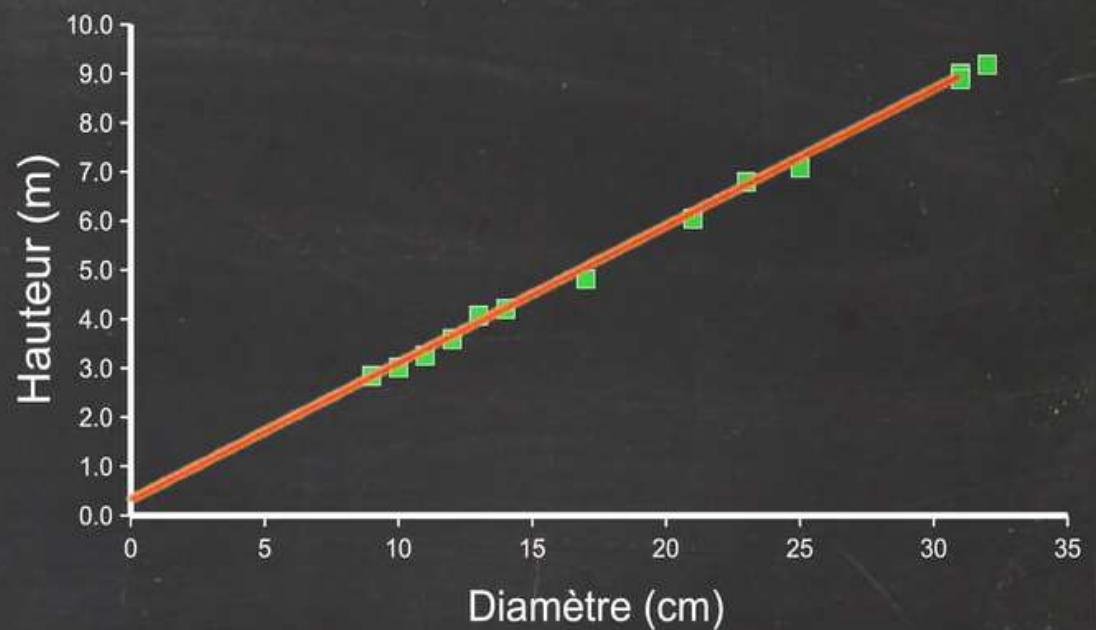
Machine Learning

Diamètre (cm)	Hauteur (m)
10	2.8
17	4.6
14	4.0
9	2.6
21	5.8
25	6.9
31	8.8
12	3.4
23	6.6
32	9.0
31	8.7
11	3.0
13	3.8



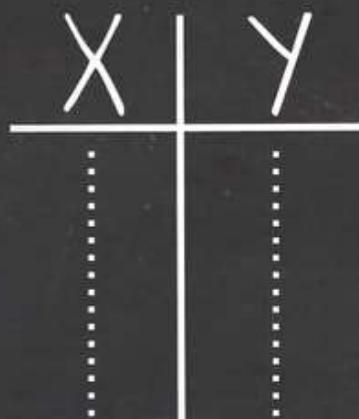
Machine Learning

Diamètre (cm)	Hauteur (m)
10	2.8
17	4.6
14	4.0
9	2.6
21	5.8
25	6.9
31	8.8
12	3.4
23	6.6
32	9.0
31	8.7
11	3.0
13	3.8

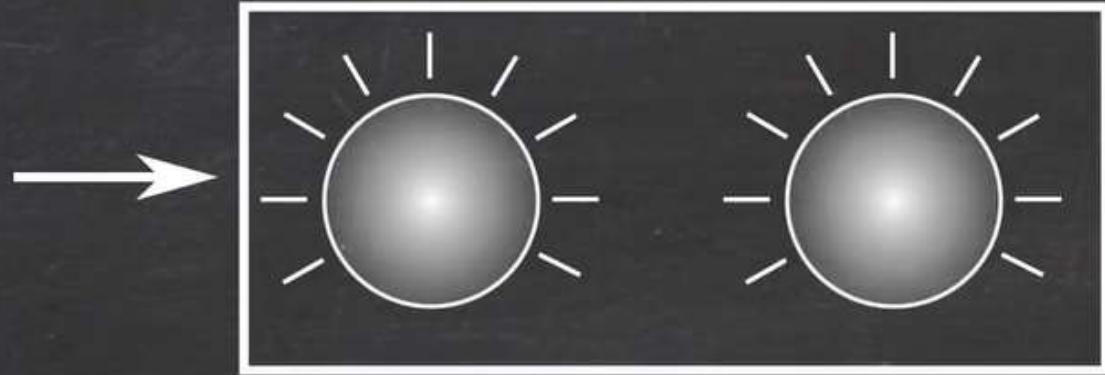


Machine Learning

Machine learning



Entrée
 X



Sortie
 Y

Phase d'apprentissage

This collage illustrates the evolution and variety of Facebook's user interface and features over time. The screenshots are arranged in three rows:

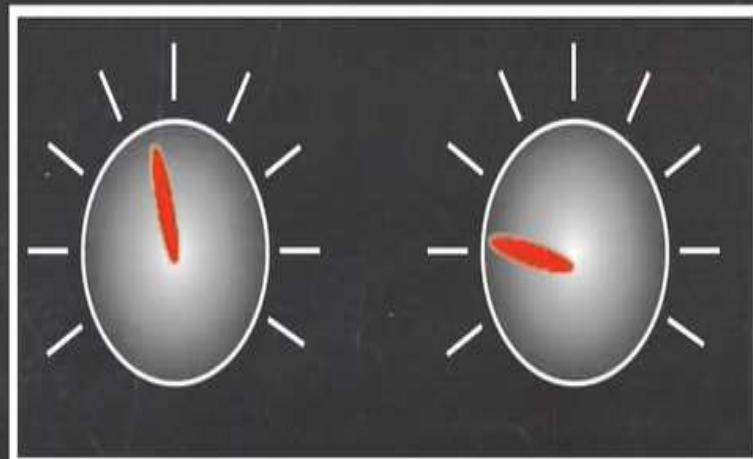
- Top Row:** Shows the 'Facebook for Business' dashboard, a 'B-Side Community' page, a 'Facebook for Education' page, a 'Facebook for Nonprofits' page, a 'Facebook for Events' page, and a 'Facebook for Sports' page.
- Middle Row:** Shows a standard Facebook news feed, a 'Live Feed' feature, a 'Facebook for Nonprofits' page, a 'Facebook for Events' page, and a 'Facebook for Sports' page.
- Bottom Row:** Shows a 'Facebook for Business' dashboard, a 'Facebook for Education' page, a 'Facebook for Nonprofits' page, a 'Facebook for Events' page, and a 'Facebook for Sports' page.

The images demonstrate how Facebook has integrated various business and community-oriented features into its core platform, such as live feeds, event management, and sports tracking, while maintaining its core social networking functions.

Machine Learning

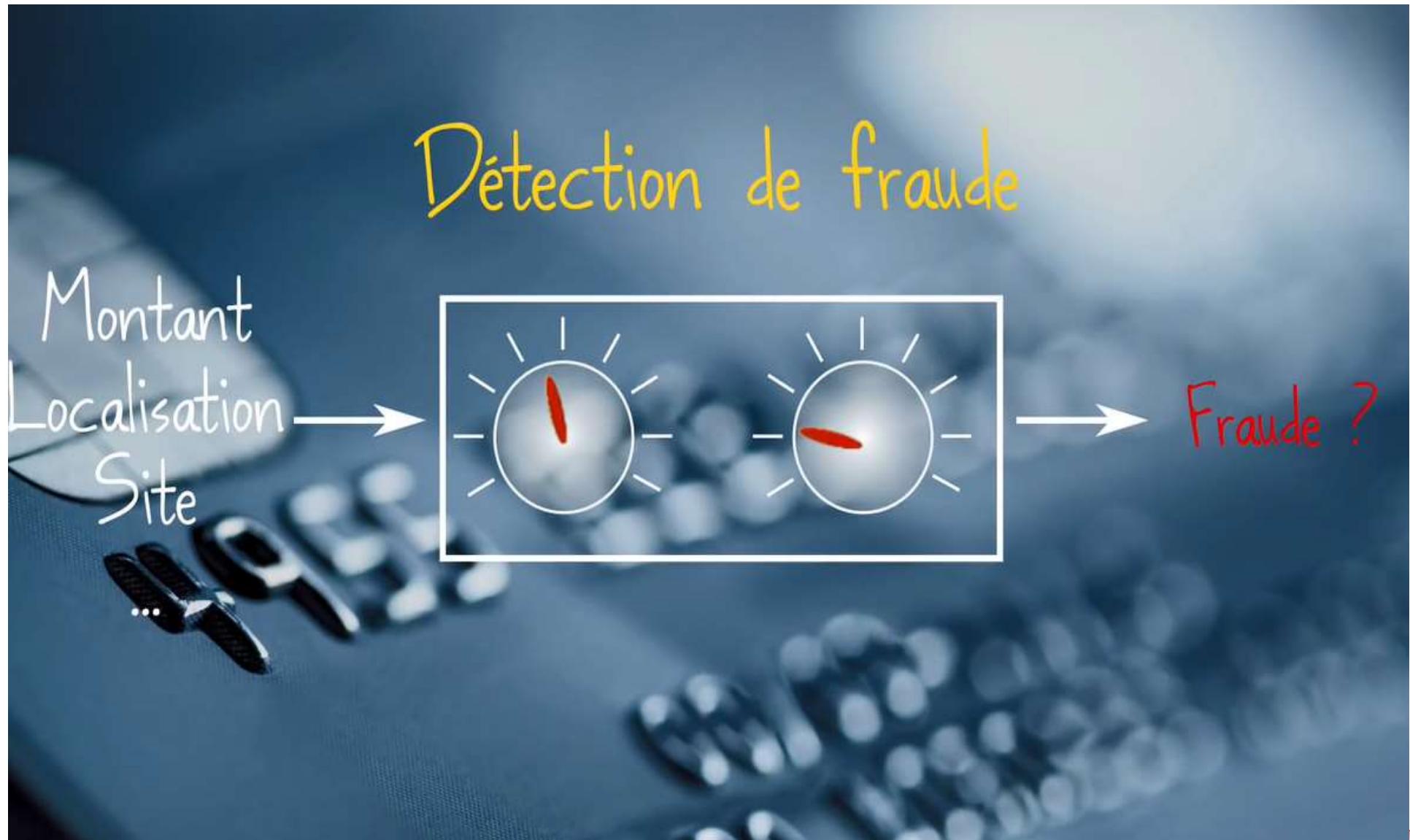
L'algorithme du flux Facebook

Qui a posté ?
Quand ?
Nature
Sujet
Réactions des autres
...



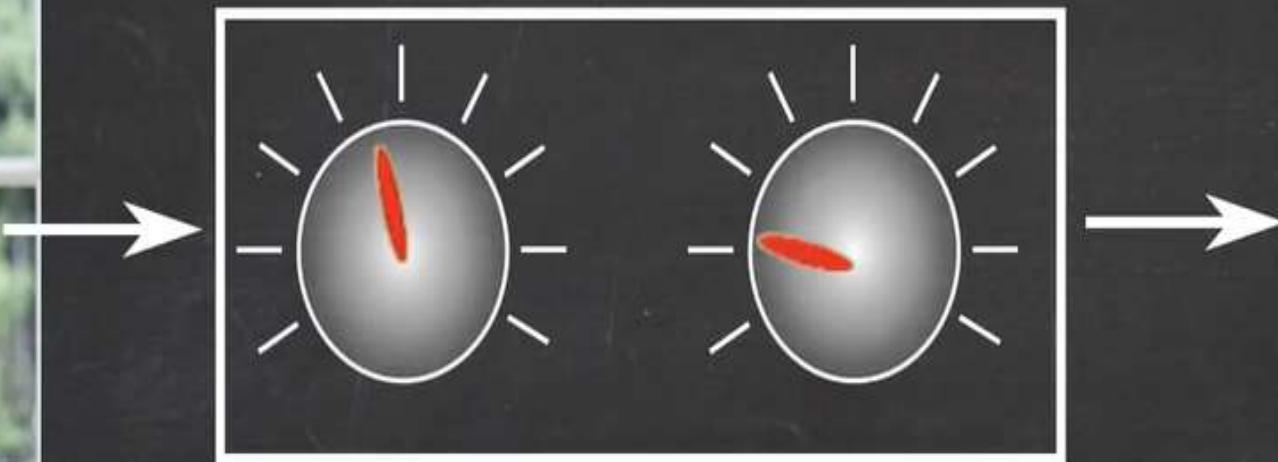
Allez vous
aimer, cliquer,
commenter,
interagir... ?

Machine Learning



Machine Learning

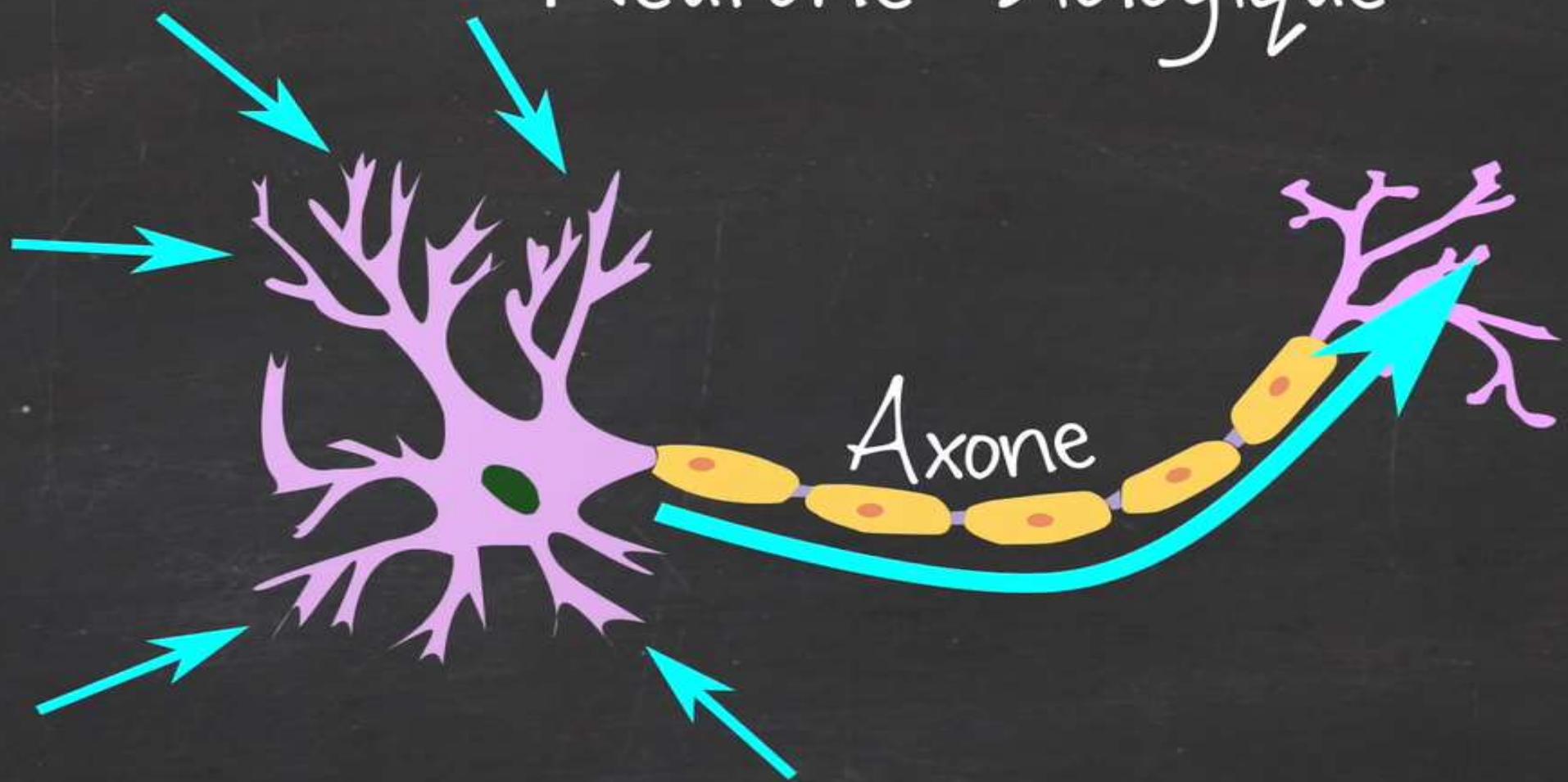
Reconnaissance d'image



Fleur ?
Héron ?
Lampe ?
Robot ?
...

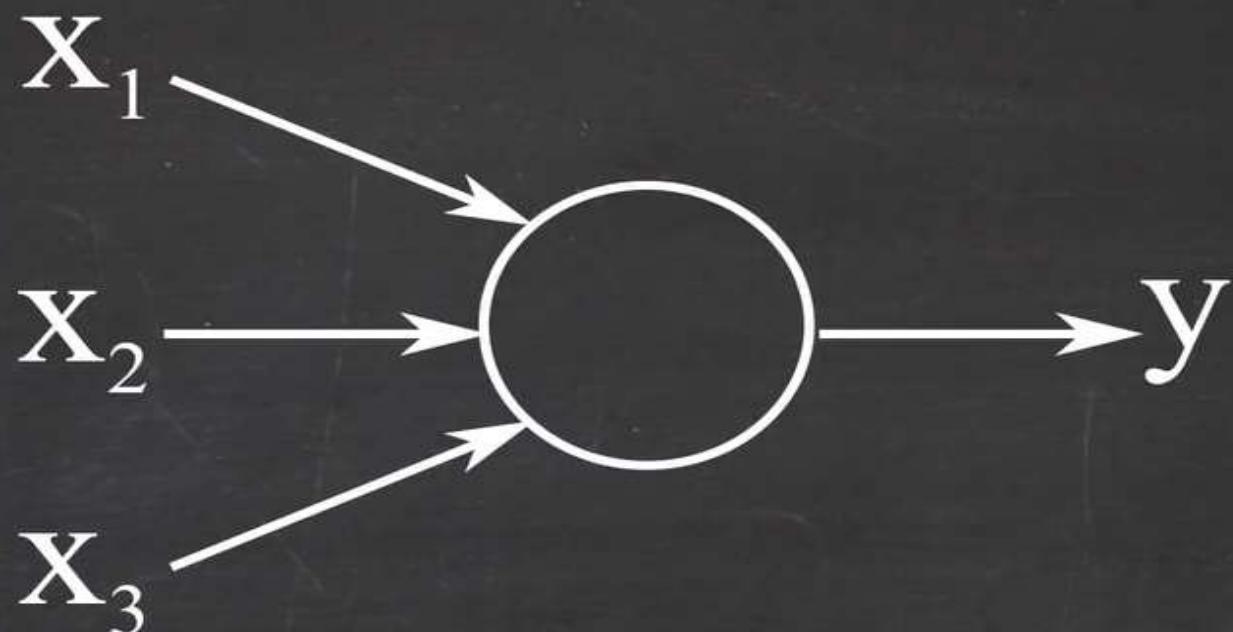
Machine Learning

Neurone biologique



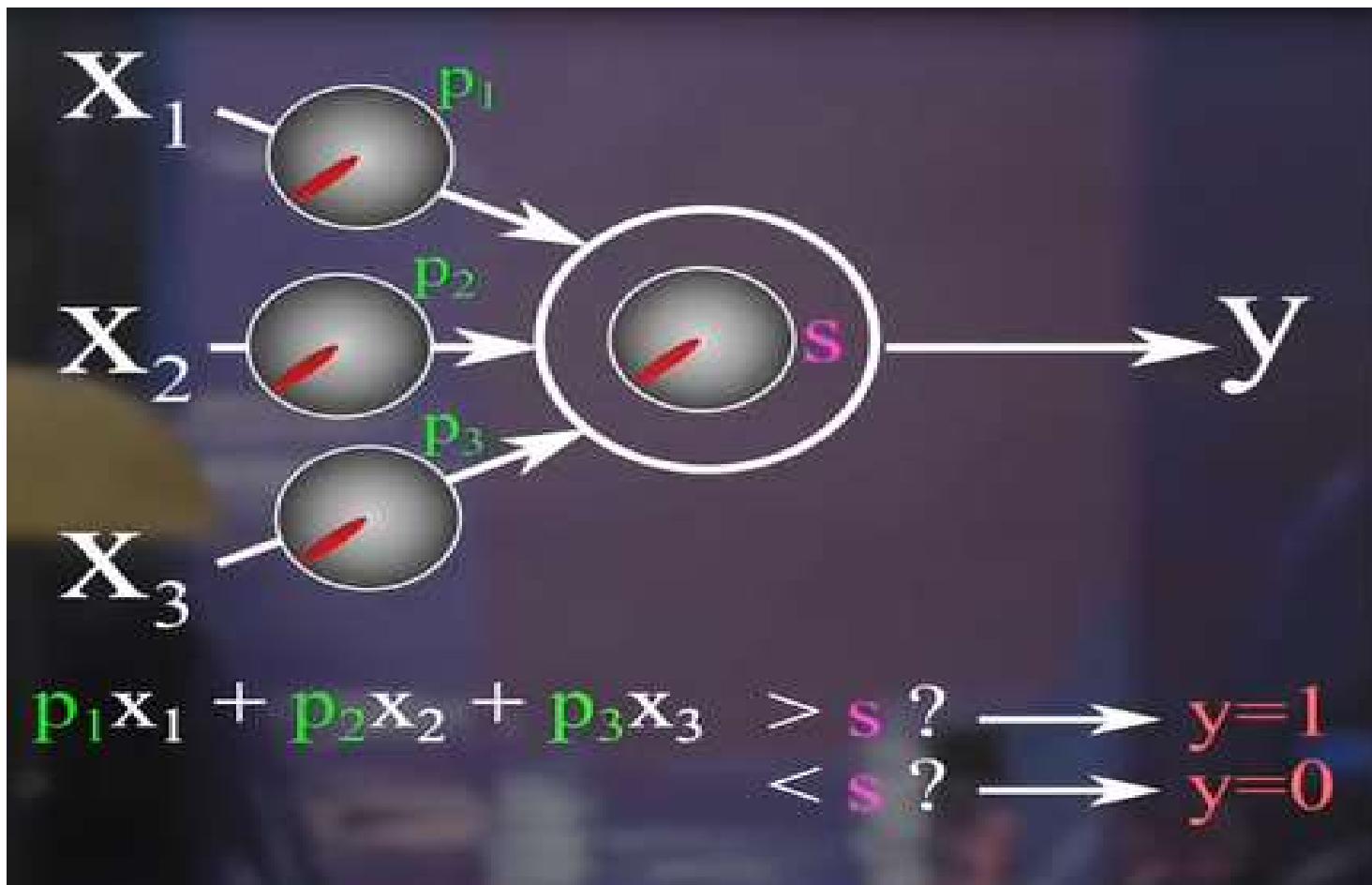
Machine Learning

Neurone artificiel



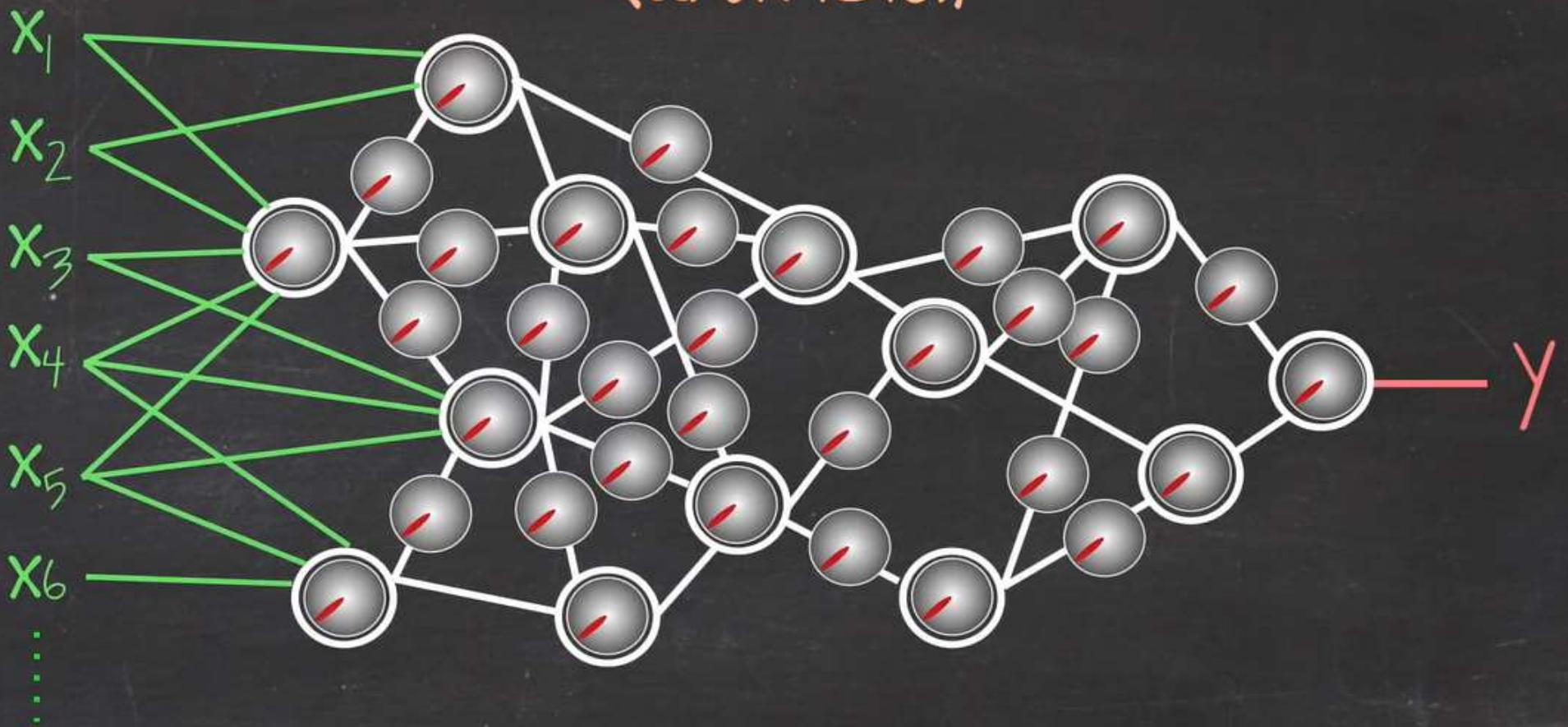
$$p_1x_1 + p_2x_2 + p_3x_3 > s ? \rightarrow y=1$$
$$< s ? \rightarrow y=0$$

Machine Learning

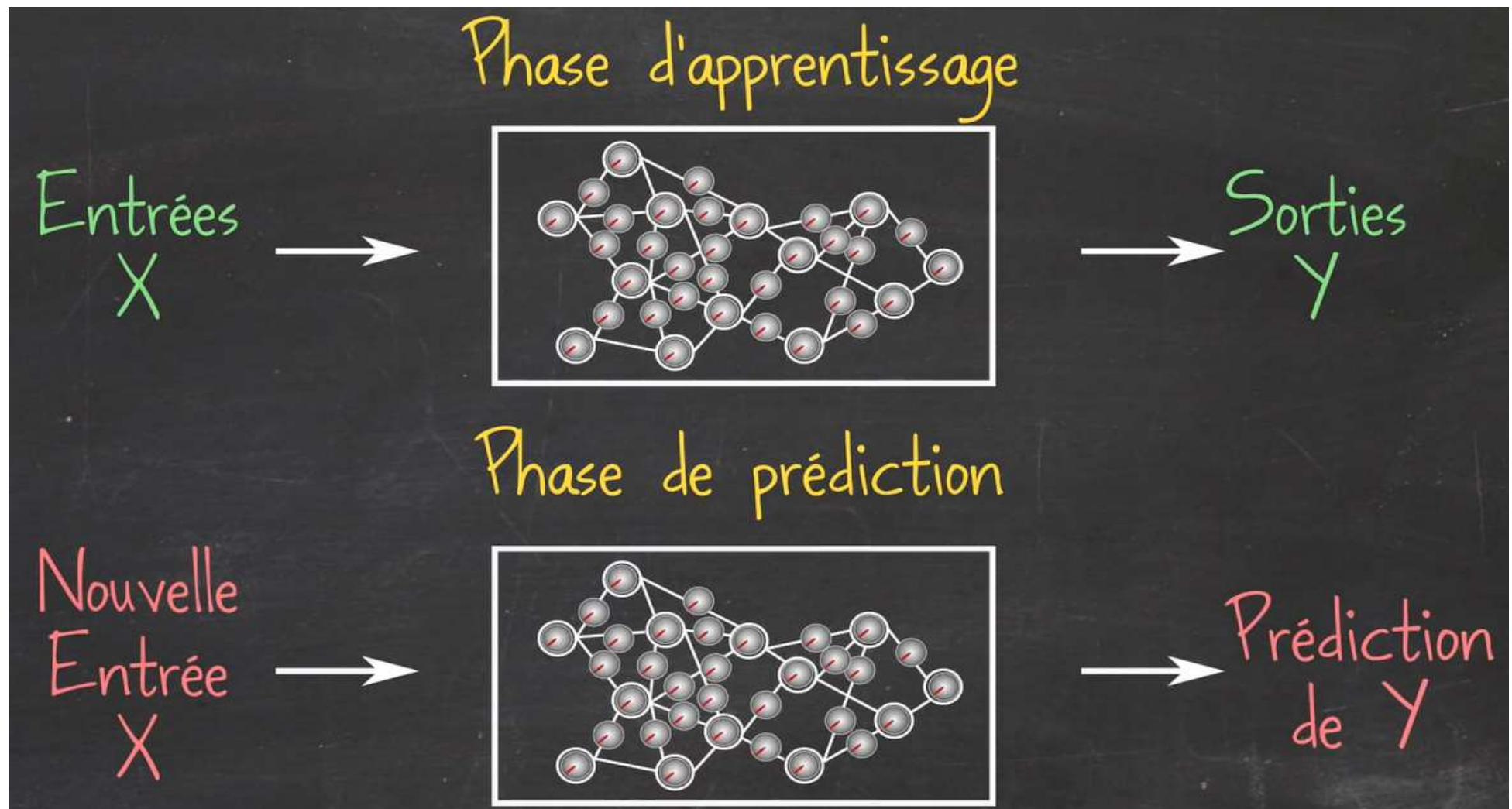


Machine Learning

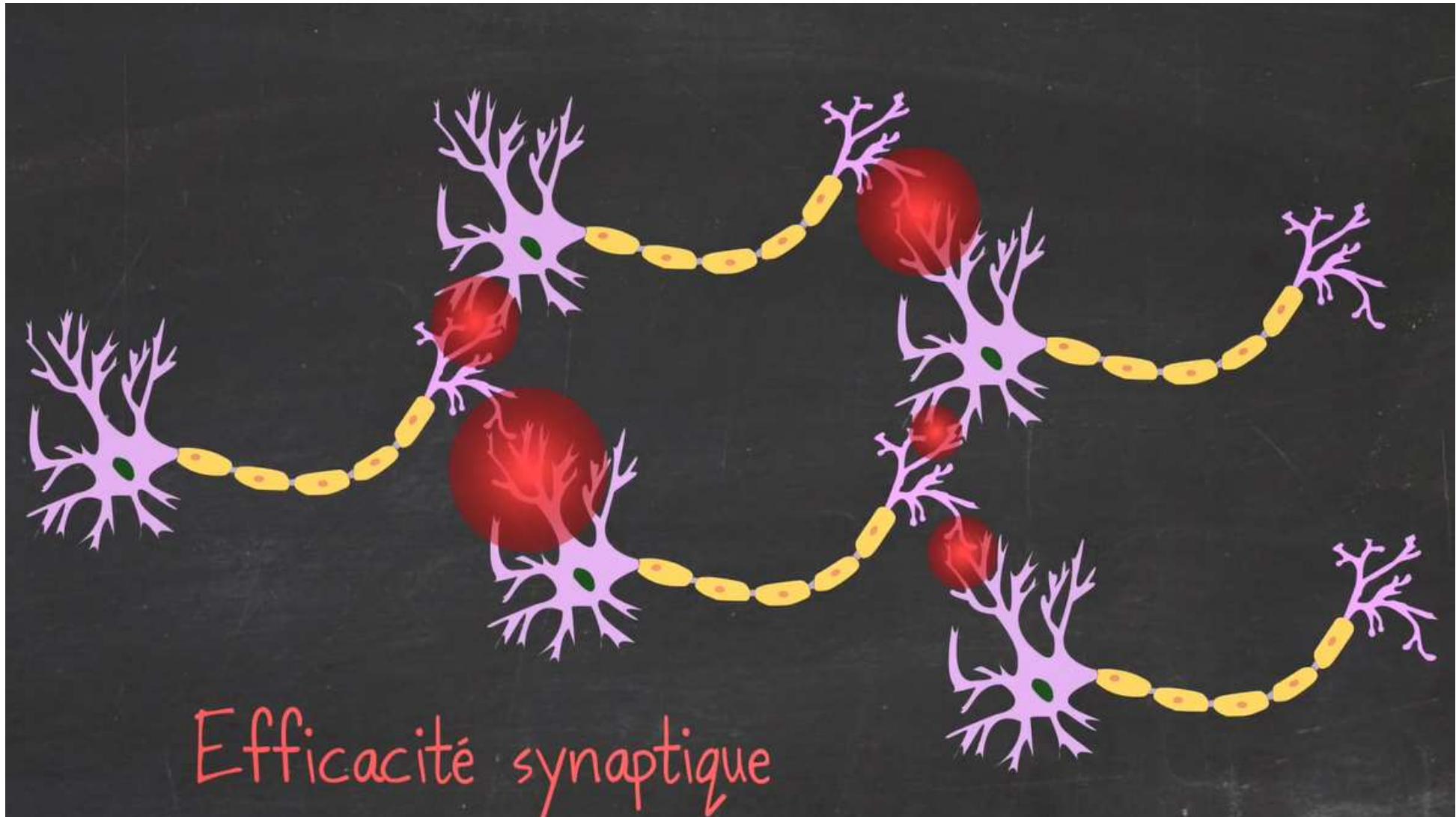
Réseau de neurones
(artificiel)



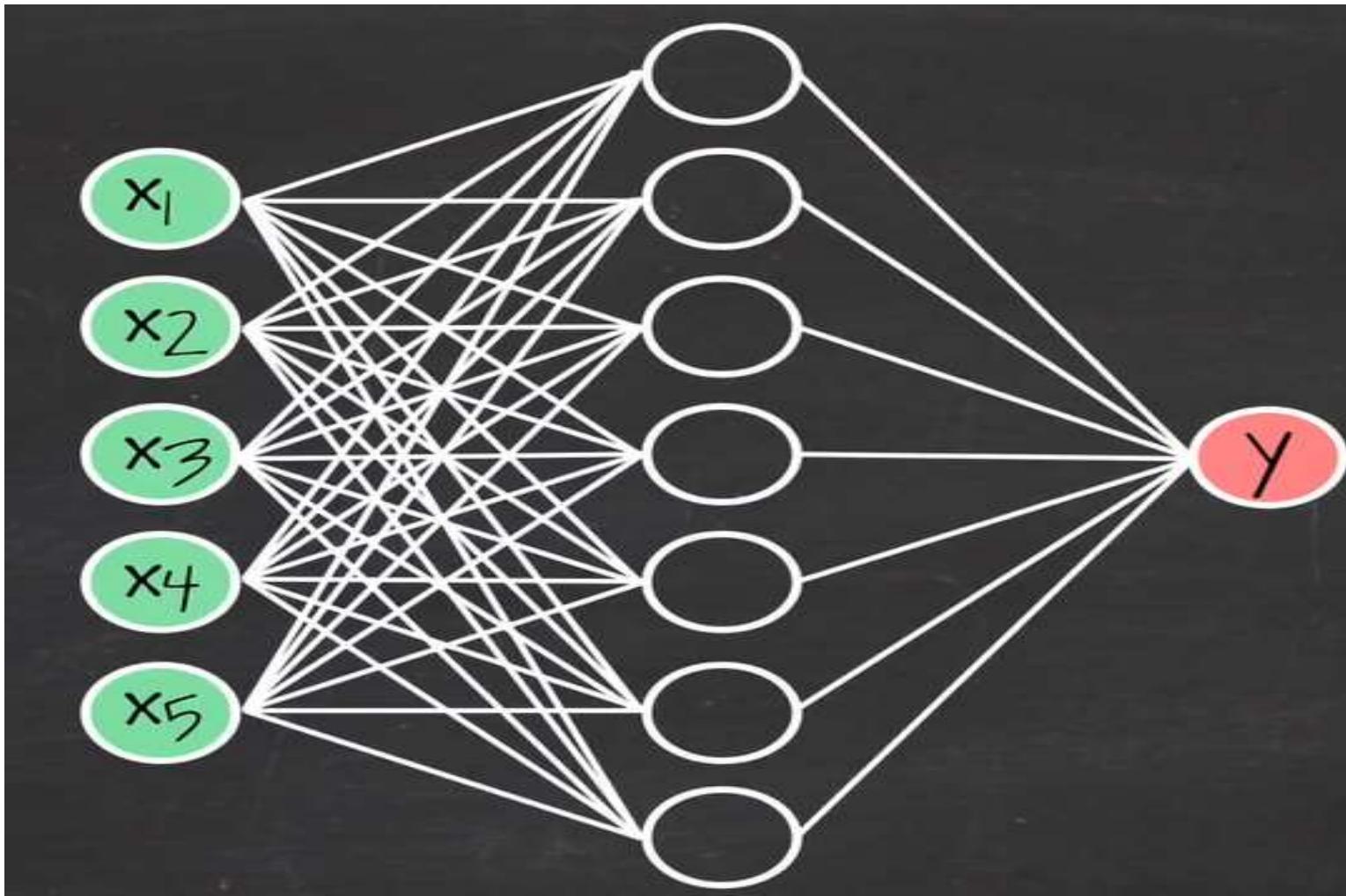
Machine Learning



Machine Learning



Machine Learning



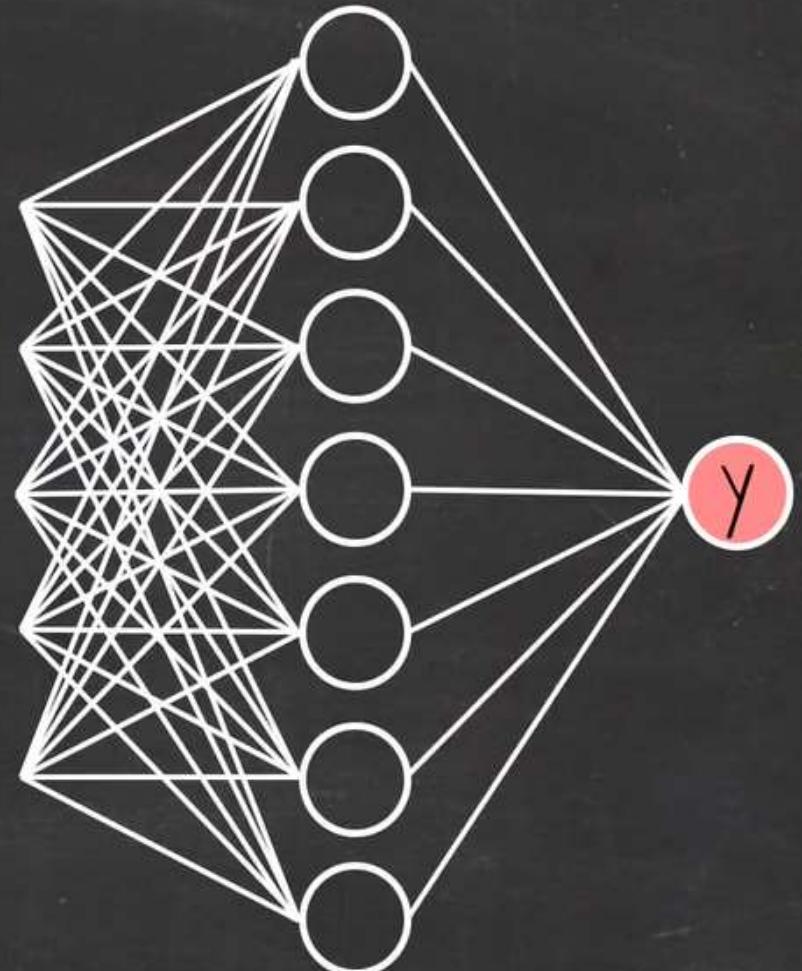
Machine Learning

Image 400x400



160 000 nombres
en entrée

?



Machine Learning

Reconnaissance de véhicule



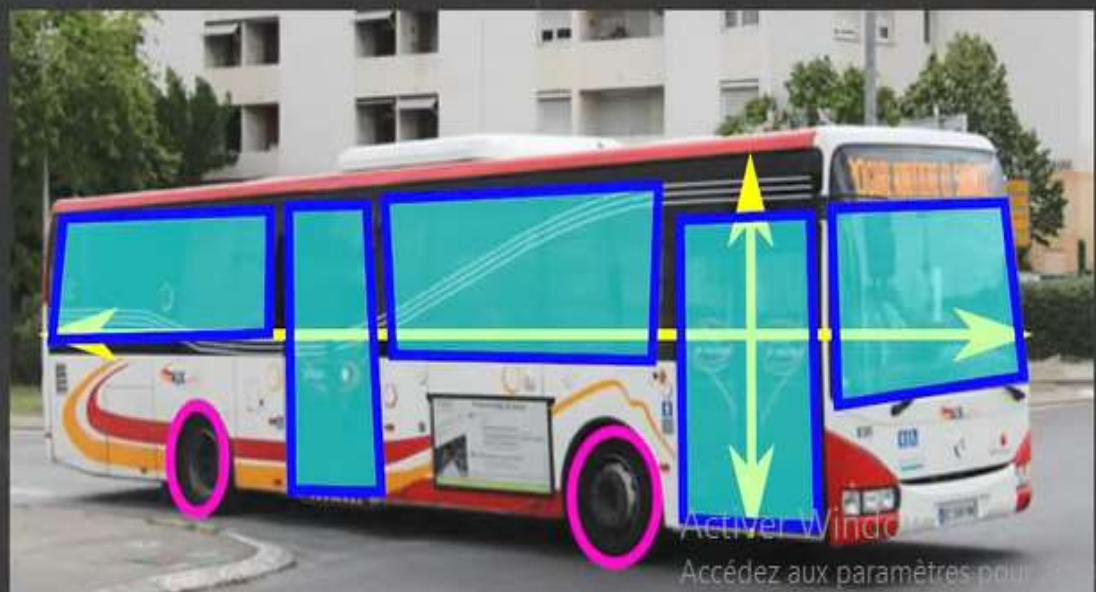
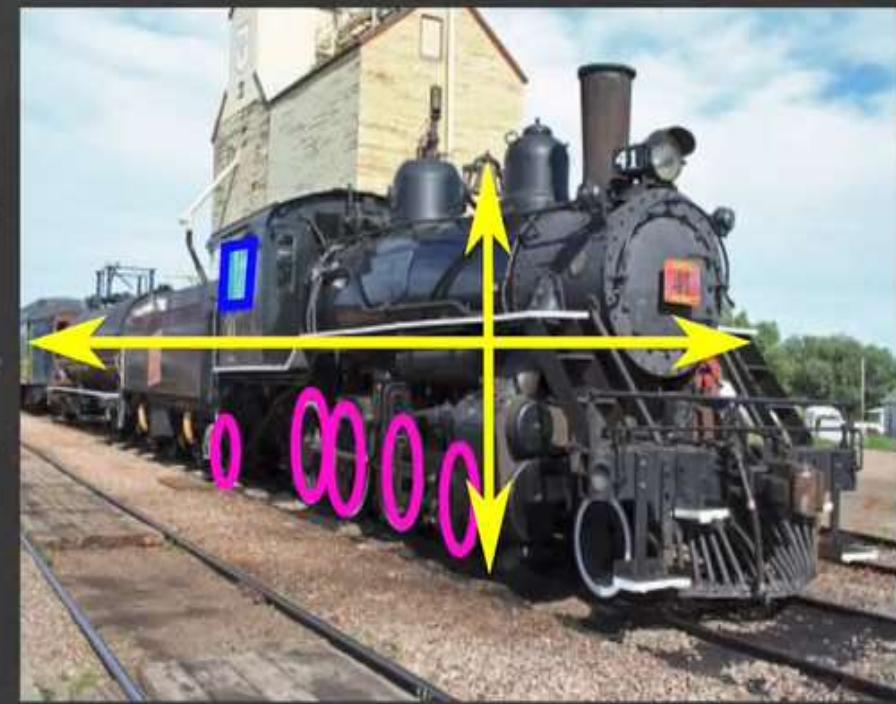
Algorithme



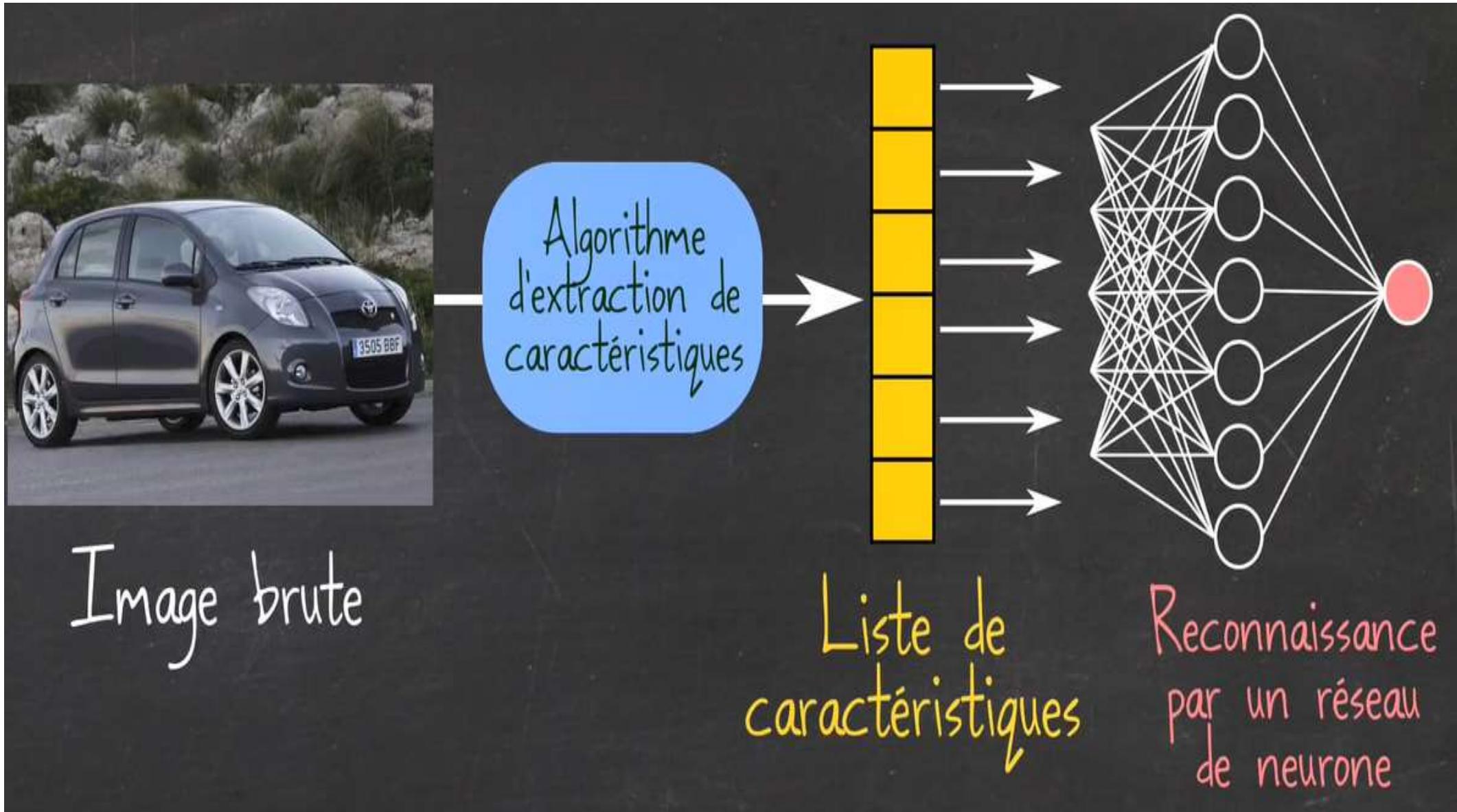
Voiture ?
Bus ?
Train ?
Moto ?
...

Machine Learning





Machine Learning



Machine Learning

Abstraction de l'image



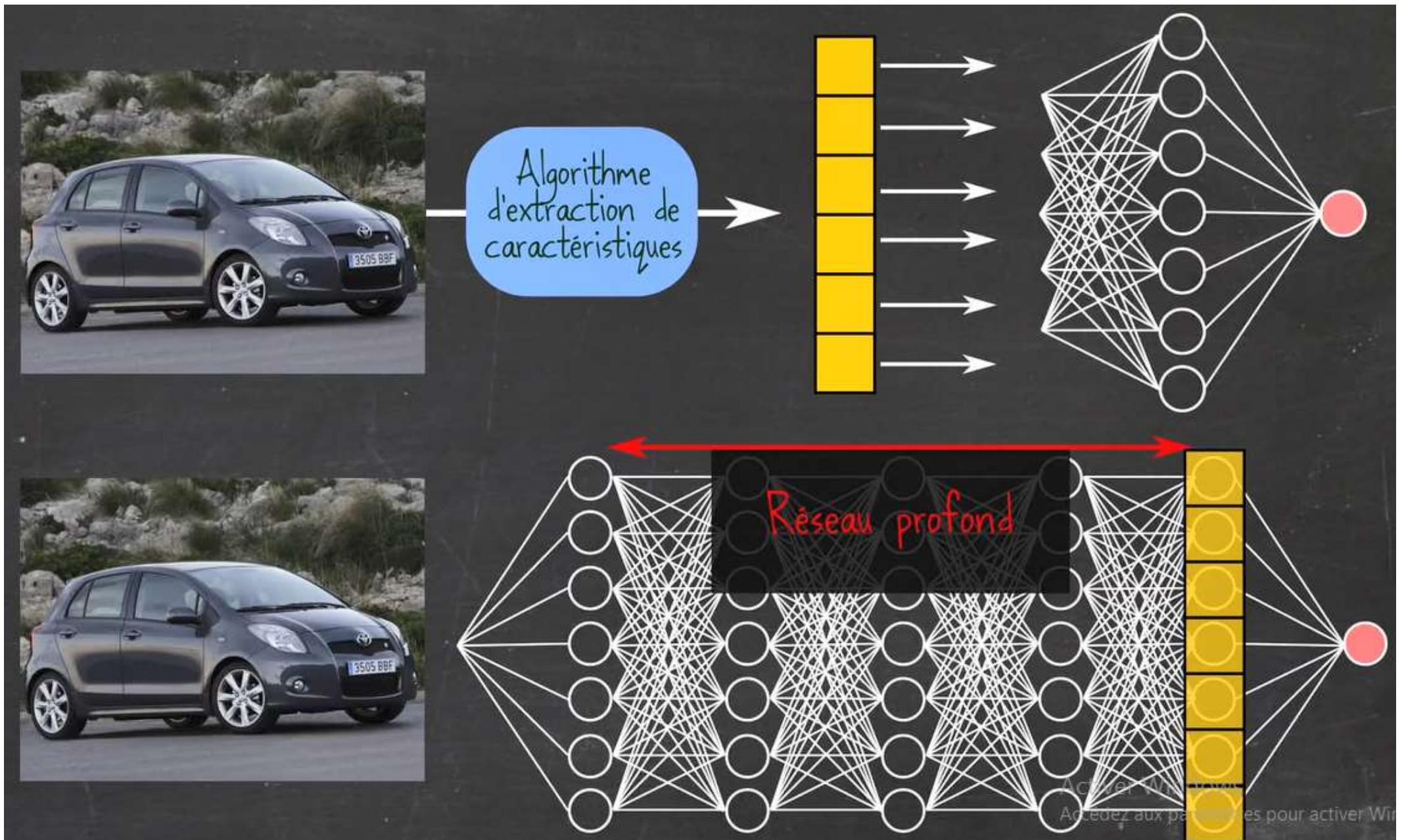
Image brute
(millions de pixels)

Algorithme
d'extraction de
caractéristiques



Liste de
caractéristiques
(quelques dizaines)

Machine Learning

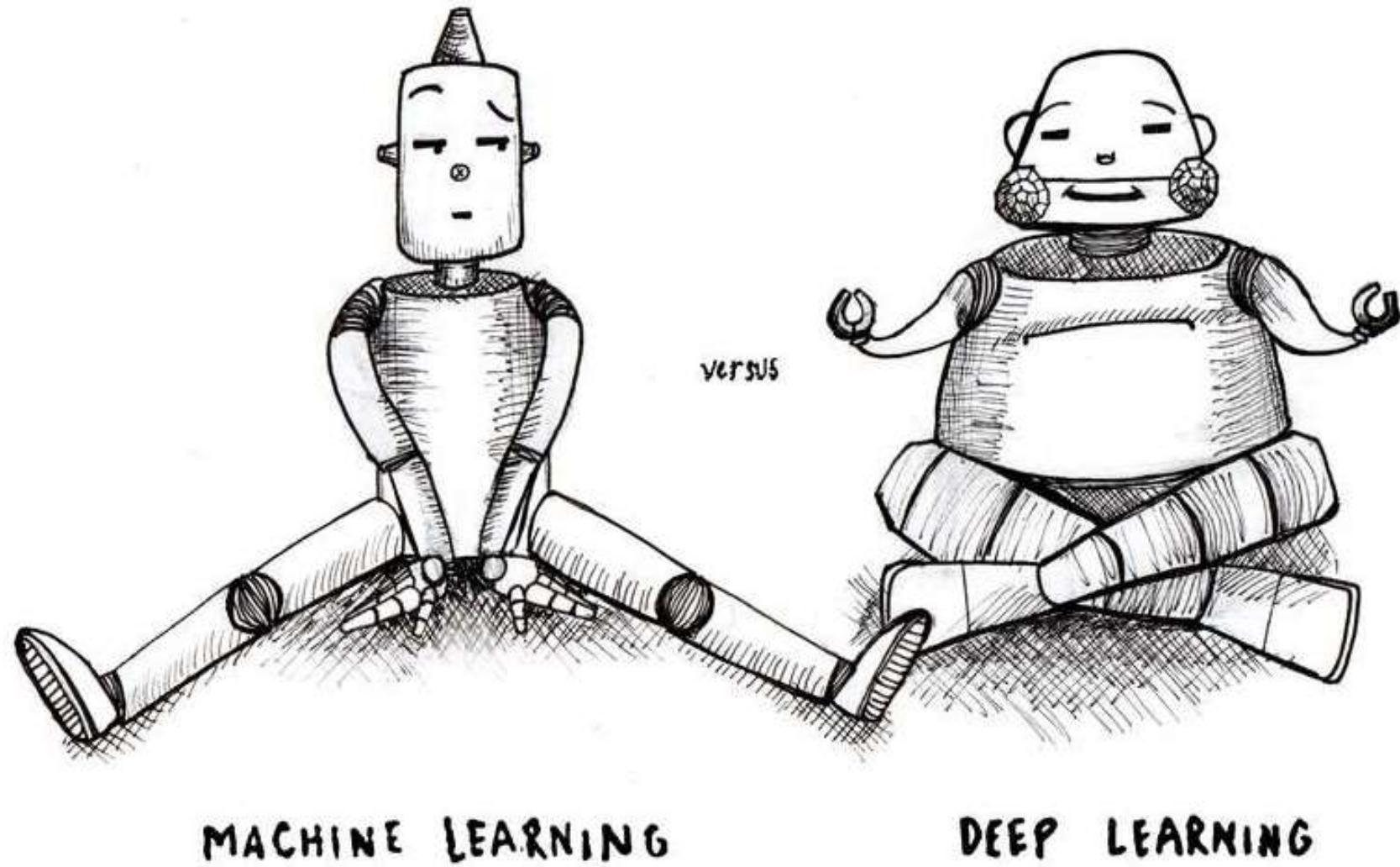


Intelligence
artificielle

Machine learning

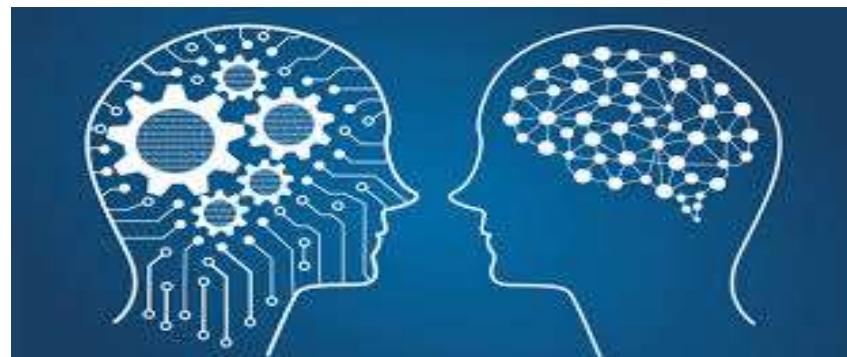
Deep learning

How can developments in deep learning make for a better approach to value investing?



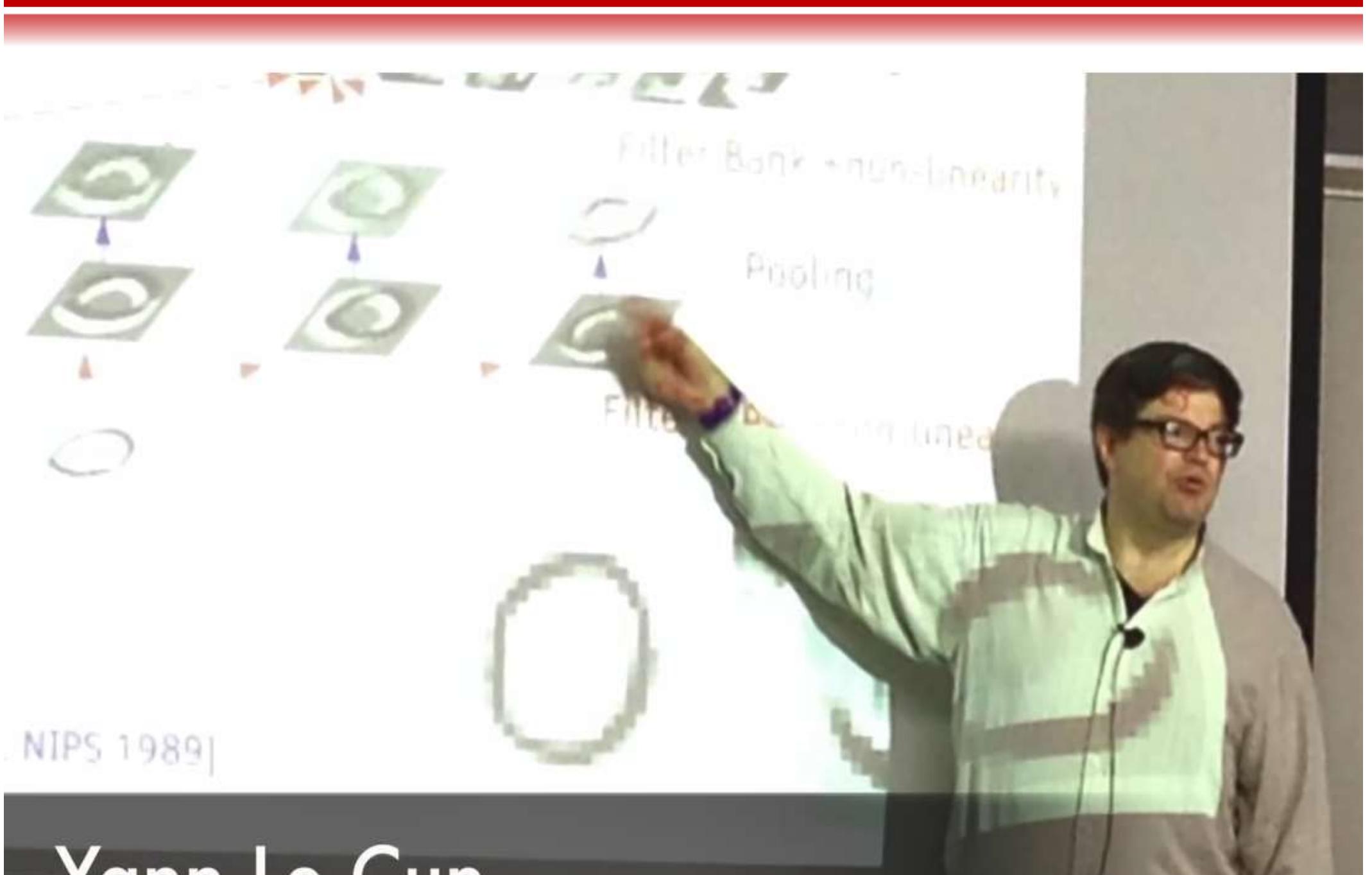
Le Deep Learning

- Le *Deep Learning* qui est considéré comme l'avancée opérationnelle majeure en termes d'intelligence artificielle repose sur la capacité d'une technologie à apprendre à partir de données brutes.
- On le retrouve dans le domaine de la reconnaissance vocale ou faciale et dans le traitement de texte.
- Il s'agit d'un modèle proche du fonctionnement biologique du cerveau humain.



Le Deep Learning

- Le Deep Learning a été développé progressivement depuis les années 1950, avec des périodes de grandes promesses et des périodes de gel. Parmi les grands noms du Deep Learning, il faut citer **Yann LeCun**, chercheur en intelligence artificielle, vision artificielle et robotique, professeur à l'Université de New York et directeur de *Facebook AI Research (FAIR)*, qui a développé des systèmes de reconnaissance de caractères ultra-performants à base de réseaux de neurones.
- Mais aussi, **Geoffrey Hinton**, psychologue spécialisé en cognition et informaticien, chercheur en intelligence artificielle, professeur à l'Université de Toronto et employé chez Google, qui est parvenu à entraîner des réseaux de neurones profonds avec des techniques nouvelles en 2006.



NIPS 1989]

Yann Le Cun

Active Windows
Accédez aux paramètres



Imen BEN CHAABANE

Le Deep Learning

- Un réseau de neurones est un ensemble de neurones artificiels, inspirés des neurones biologiques mais extrêmement simplifiés, qui sont connectés les uns aux autres et s'échangent des signaux très simples, par exemple un nombre de 0 à 1. Il existe de nombreuses façons d'interconnecter ces neurones.
- La plus fréquente est une organisation en couches superposées : tous les neurones d'une couche sont connectés à tous les neurones de la couche suivante. Lorsqu'il y a plus de deux couches, on parle de *Deep Learning*. *Les données à analyser, par exemple une photographie dont il faut détecter si elle contient un chat ou un chien, sont fournies en entrée de la couche basse.*

- ❑ Certains neurones s'activent et envoient des signaux à la couche supérieure, et ainsi de suite jusqu'à la couche la plus haute, parfois constituée d'un seul neurone. Dans l'exemple précédent, si ce neurone s'active c'est un chat, sinon c'est un chien.
- ❑ Entrainer le réseau de neurones consiste à lui donner de nombreux exemples de photographies et à corriger légèrement la force de connexion entre chaque neurone lorsque le système fait une erreur, de façon à réduire cette erreur.



Le Deep Learning est donc très puissant
mais aussi coûteux

Le Deep Learning

Large Scale Visual Recognition Challenge

2010

1.	NEC	28%
2.	XRCE	34%
3.	ISIL	45%
4.	UCI	47%
5.	Hminmax	54%

2011

1.	XRCE	26%
2.	UV A	31%
3.	ISI	36%
4.	NII	50%

2012

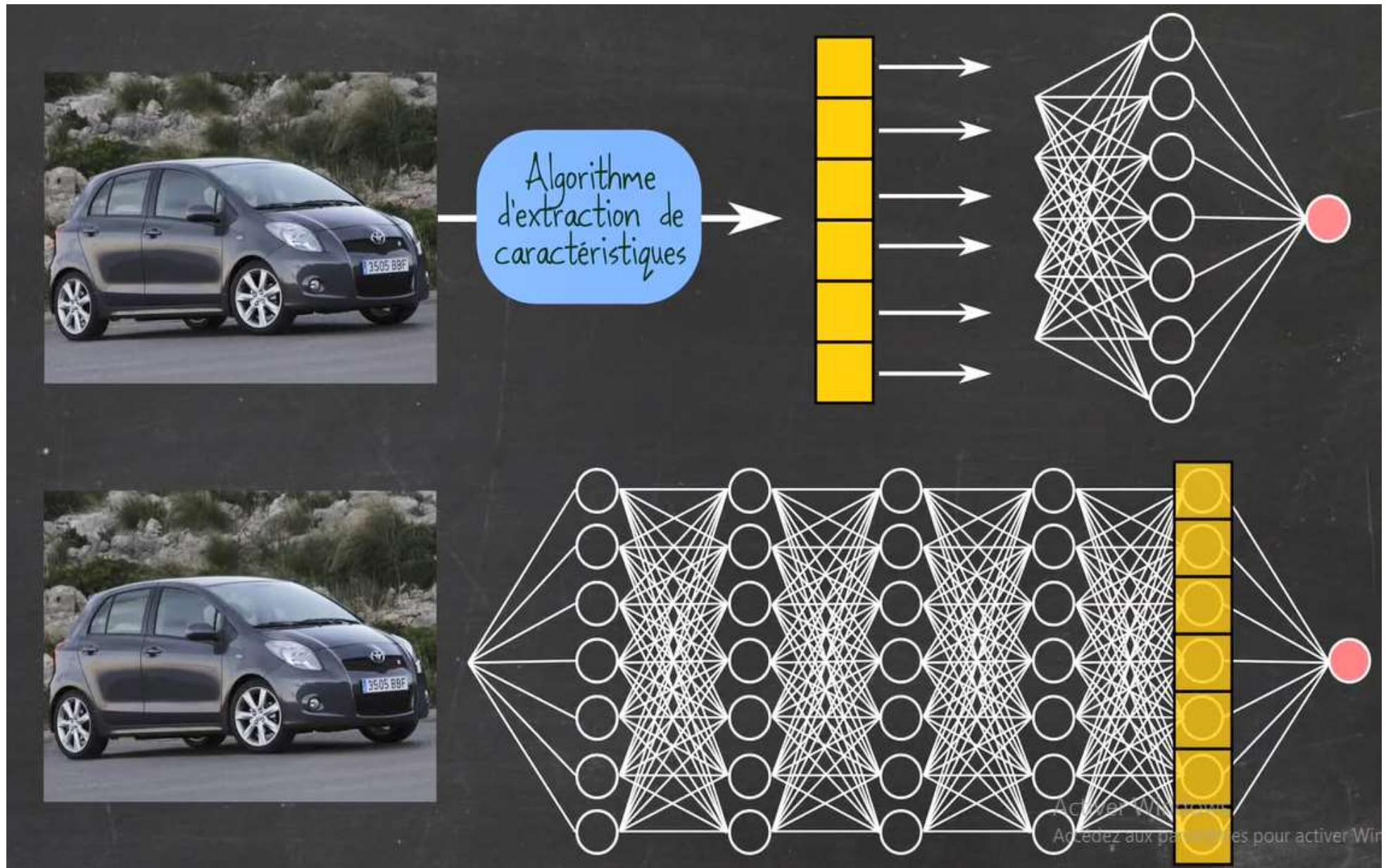
1.	SuperVision	16%
2.	ISI	26%
3.	VGG	27%
4.	XRCE	27%
5.	UV A	30%

2013

1.	Clarifai	12%
2.	NUS	13%
3.	ZeilerFergus	13%
4.	A.Howard	13%
5.	OverFeat	14%

Activer Windows
Accédez aux paramètres

Le Deep Learning



MEET THE MAN GOOGLE HIRED TO MAKE AI A REALITY



Active Windows
Activer tous les paramètres pour activer Win

MAN BEHIND THE ‘GOOGLE BRAIN’ JOINS CHINESE SEARCH GIANT BAIDU



FACEBOOK TAPS ‘DEEP LEARNING’ GIANT FOR NEW AI LAB







Stanford University





Description

Research in our lab focuses on two intimately connected branches of vision research: computer vision and human vision. In both fields, we are intrigued by visual functionalities that give rise to semantically meaningful interpretations of the visual world.

In computer vision, we aspire to develop intelligent algorithms that perform important visual perception tasks such as object recognition, scene categorization, integrative scene understanding, human motion recognition, material recognition, etc.

In human vision, our curiosity leads us to study the underlying neural mechanisms that enable the human visual system to perform high level visual tasks with amazing speed and efficiency.



Highlights



ImageNet



ImageNet Challenge



Automated Image Captioning



AI-assisted Care



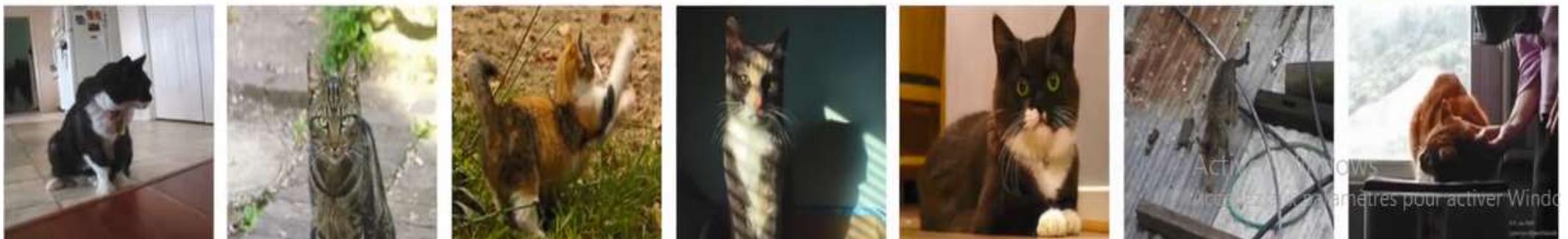
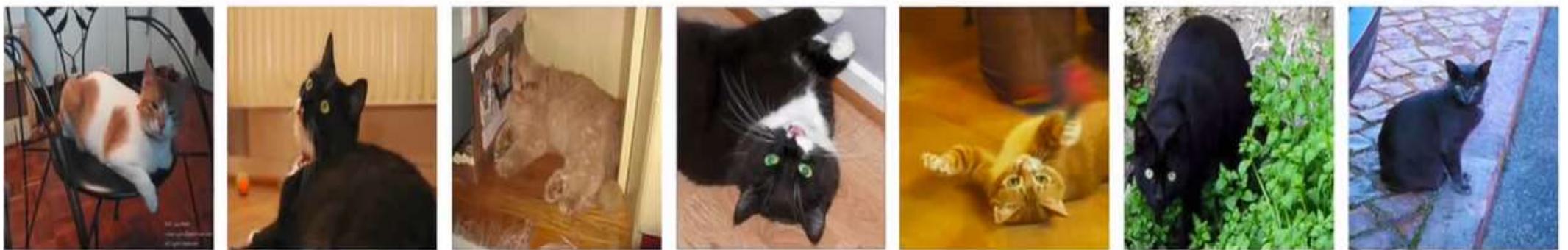
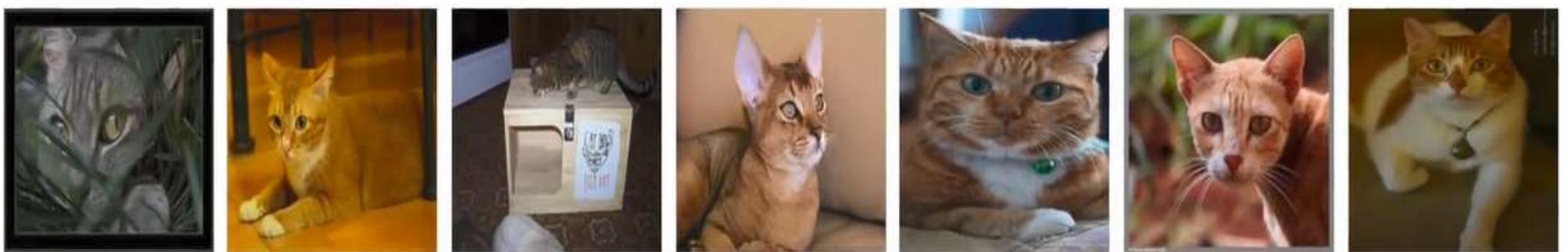
SAILORS program

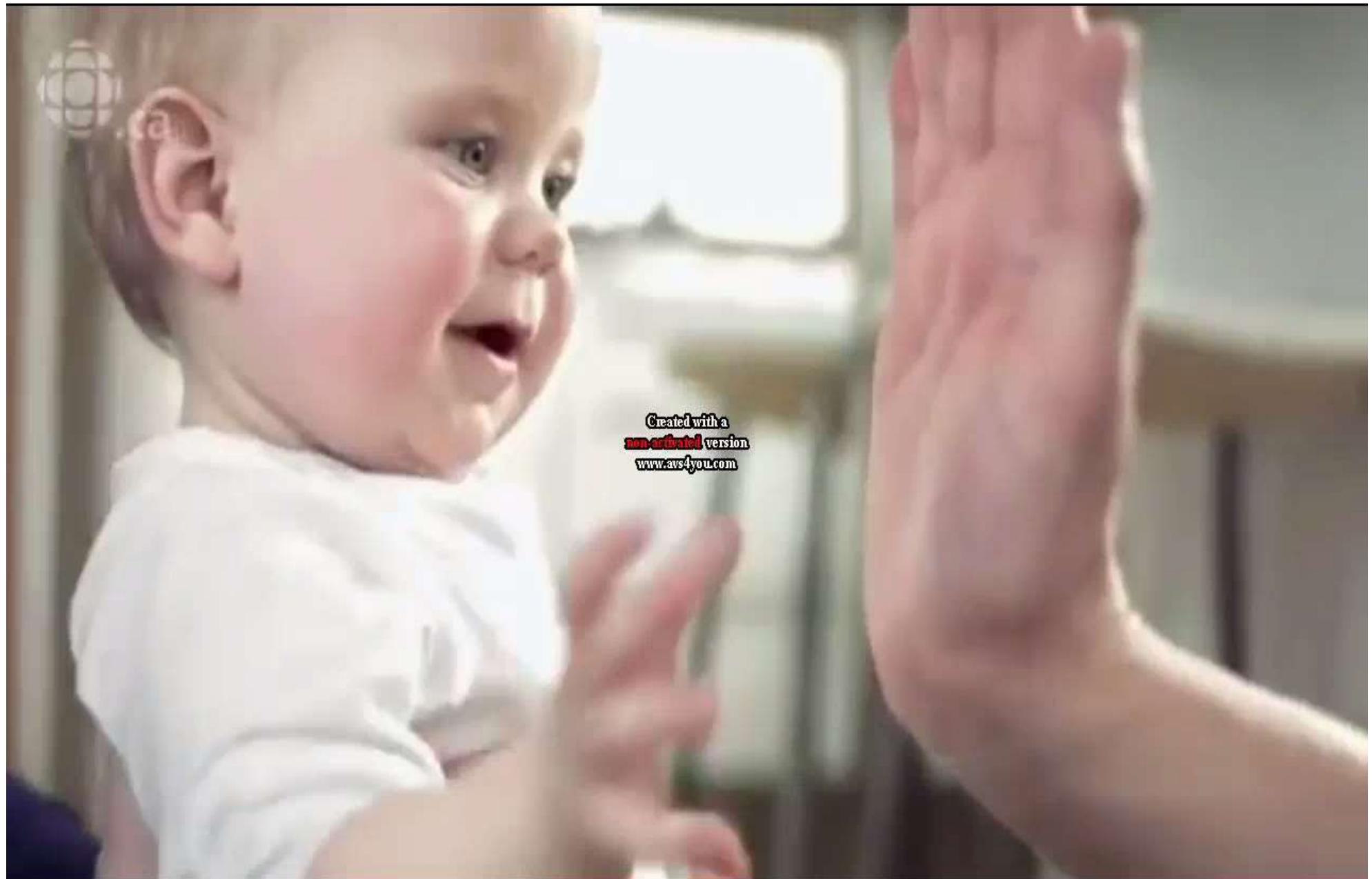
ImageNet is an image database organized according to the WordNet hierarchy (currently only the nouns), in which each node of the hierarchy is depicted by hundreds and thousands of images. Currently we have an average of over five hundred images per node. We hope ImageNet will become a useful resource for researchers, educators, students and all of you who share our passion for pictures.

[Click here](#) to learn more about ImageNet, [Click here](#) to join the ImageNet mailing list.



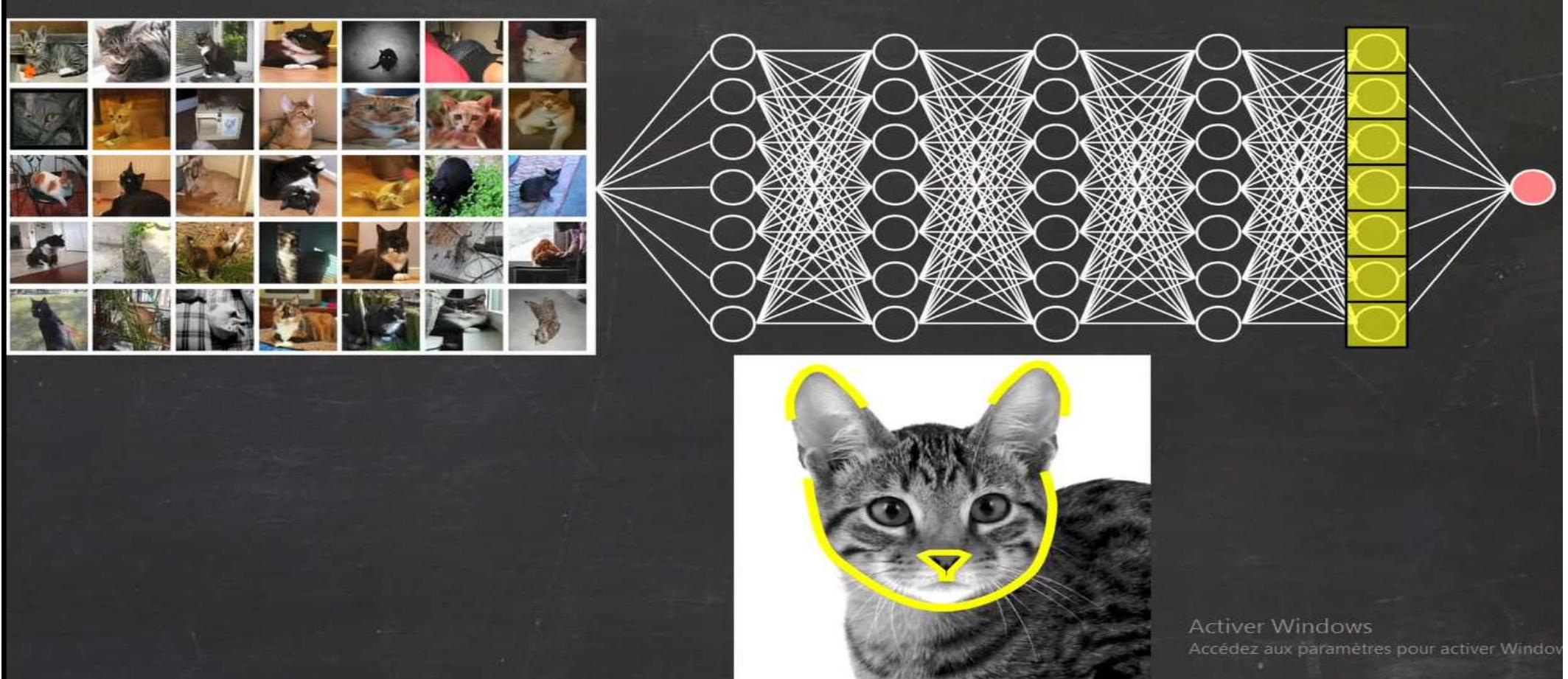
What do these images have in common? *Find out!*



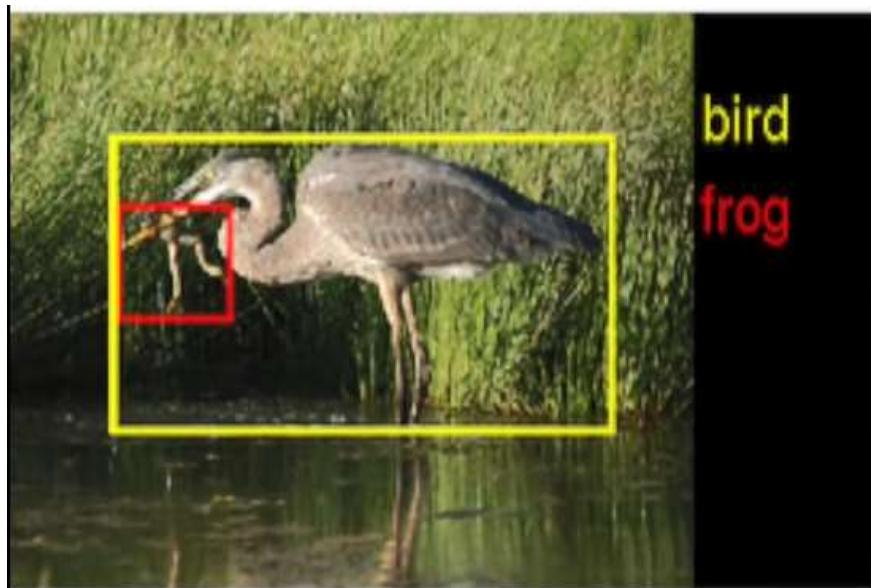


Created with a
~~non-activated~~ version
www.av4you.com

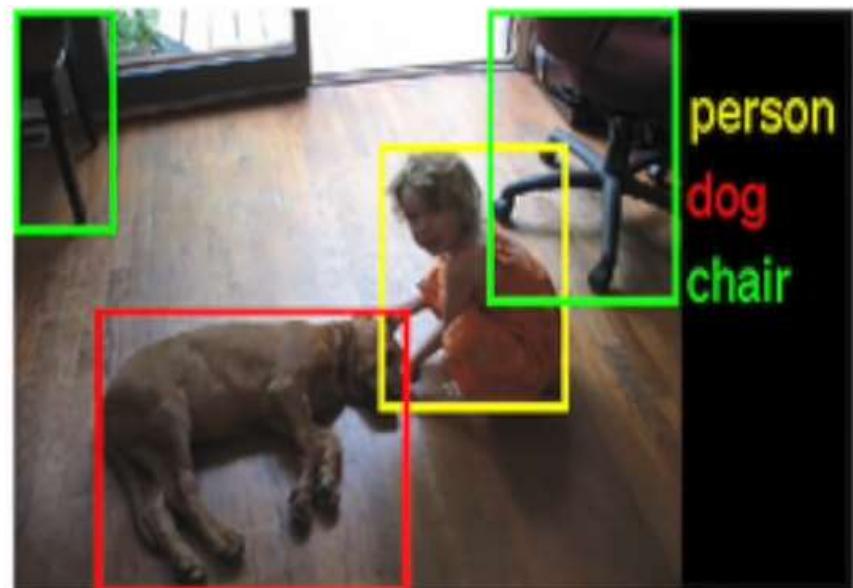
Deep Learning



1. Réseau profond plus d'une centaine de couche
2. Très loin du cerveau mais la reconnaissance d'image est assez spectulaire



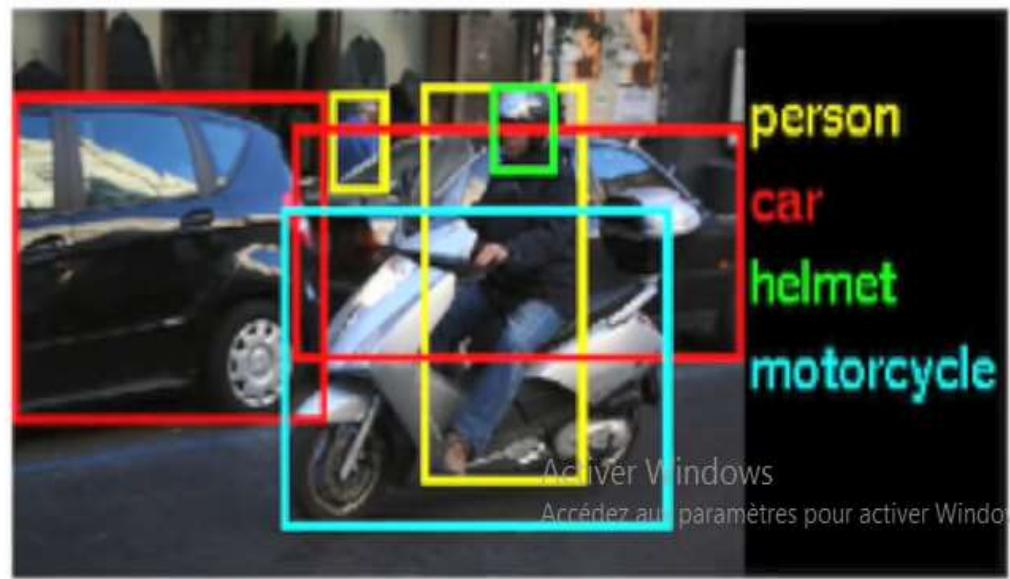
bird
frog



person
dog
chair



person
hammer
flower pot
power drill



person
car
helmet
motorcycle

Activer Windows
Accédez aux paramètres pour activer Windo



Sèche-cheveux ?



Dromadaire ?

GoogLeNet team: Christian Szegedy, Going Deeper With Convolutions, ILSVRC 2014

Activer Windows
Accédez aux paramètres pour activer

Describes without errors



A person riding a motorcycle on a dirt road.

Describes with minor errors



Two dogs play in the grass.

Analyse d'une scène et la décrire par une phrase! Très utile pour les mal voyants



A group of young people
playing a game of frisbee.



Two hockey players are fighting
over the puck.

Activer Windows
Accédez aux paramètres pour activer Wi

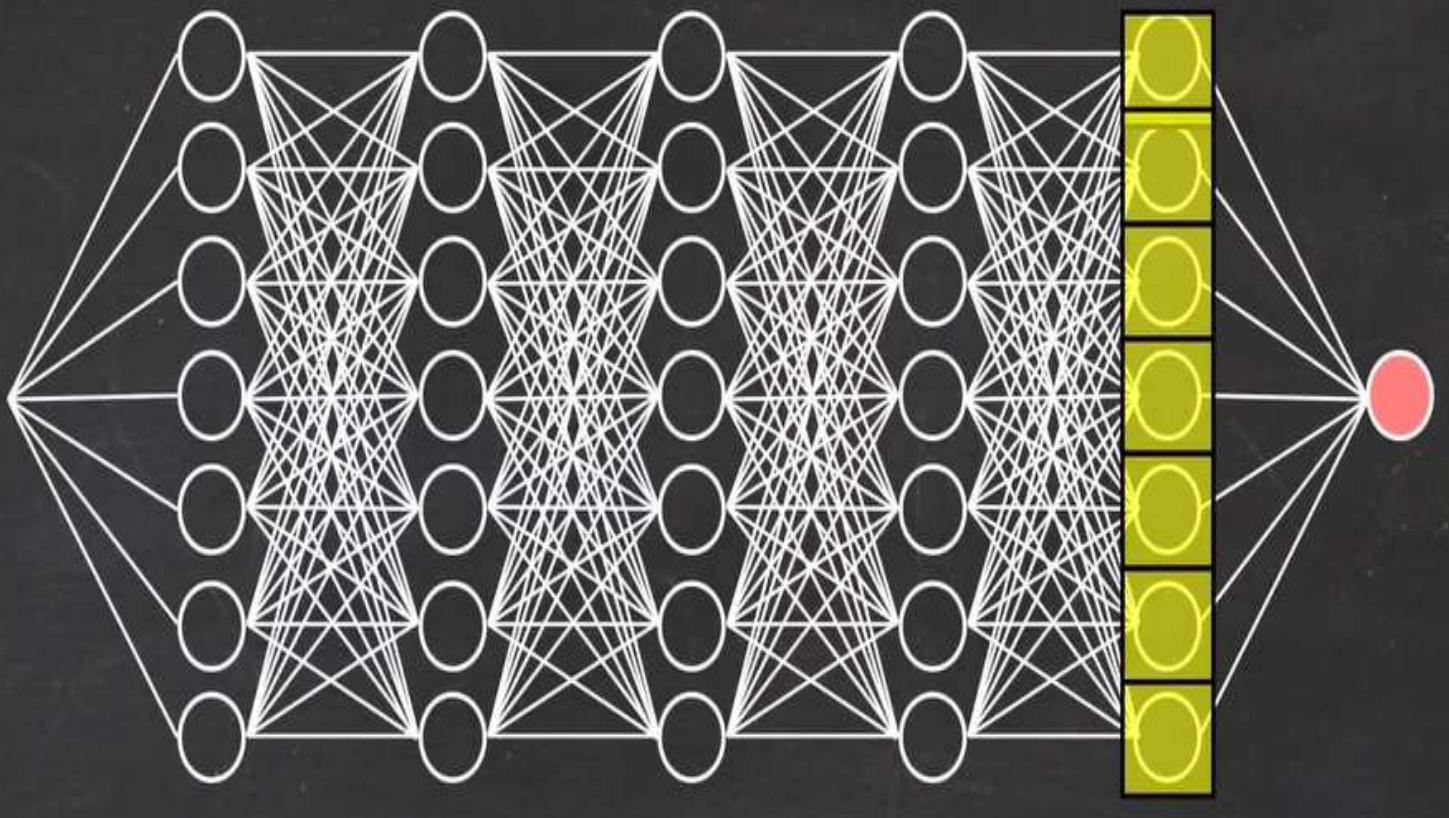


Fei Fei Li
Stanford Vision Lab

Image brute



Valeurs des
caractéristiques
essentielles



Fabrique des images

Valeurs des
caractéristiques
essentielles

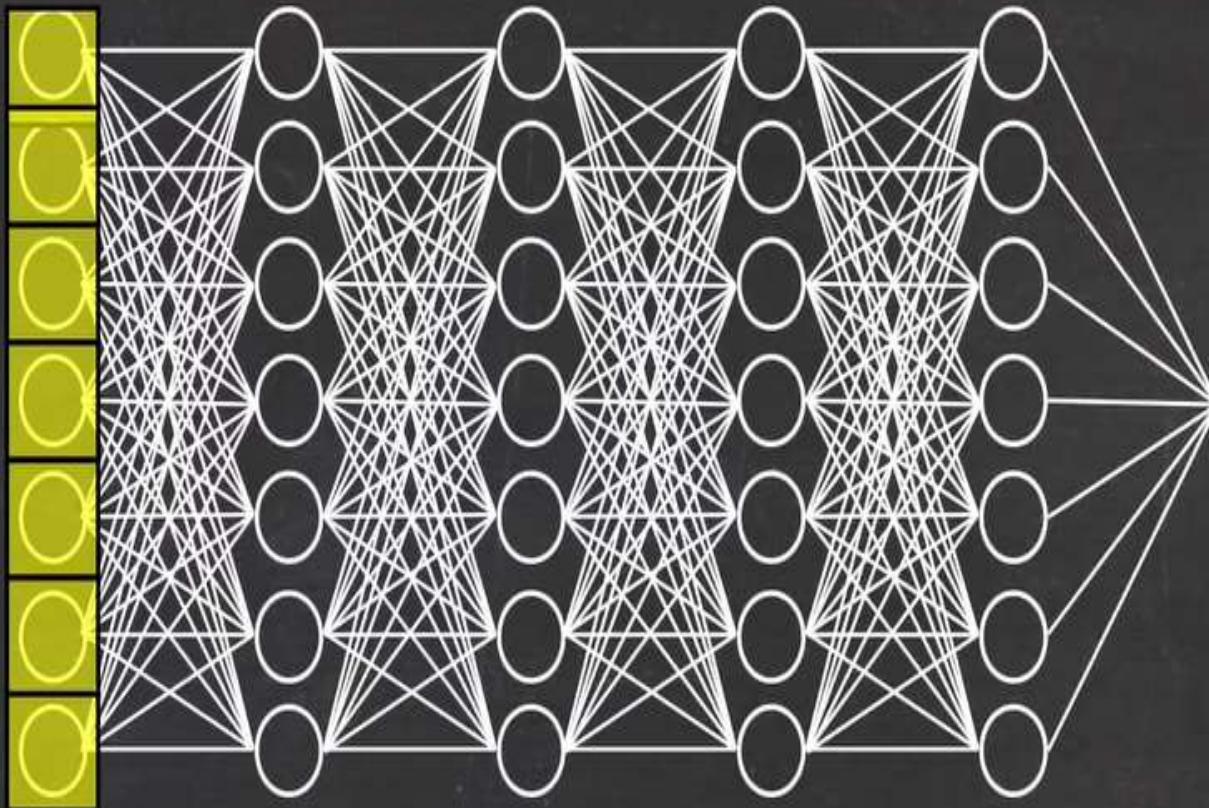
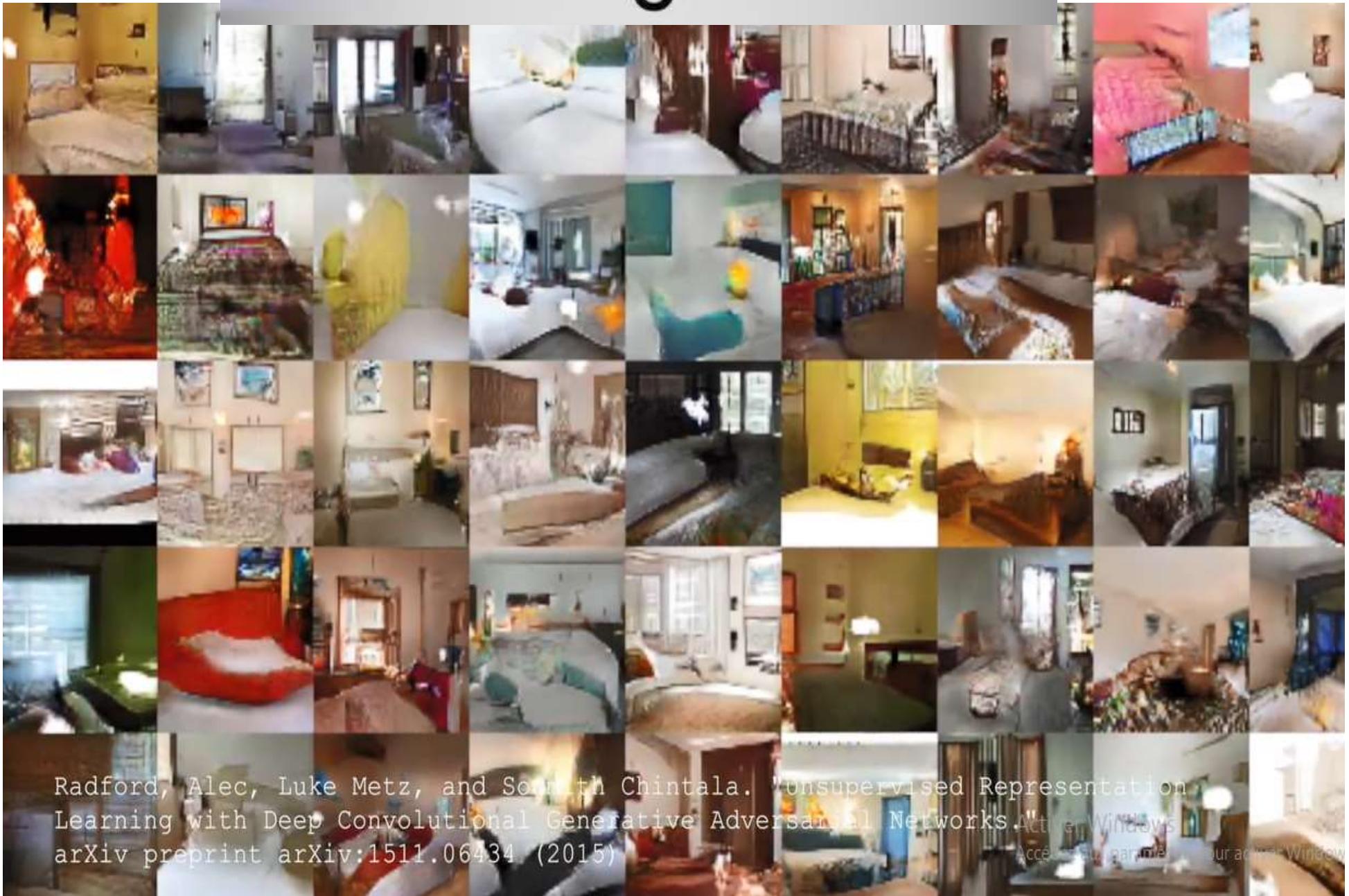


Image inventée



Modèles génératifs



Radford, Alec, Luke Metz, and Soumith Chintala. "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks." *arXiv preprint arXiv:1511.06434* (2015)

Accéder au paramètre "Your active Windows"

Modèles génératifs



Modèles génératifs

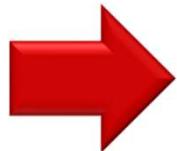
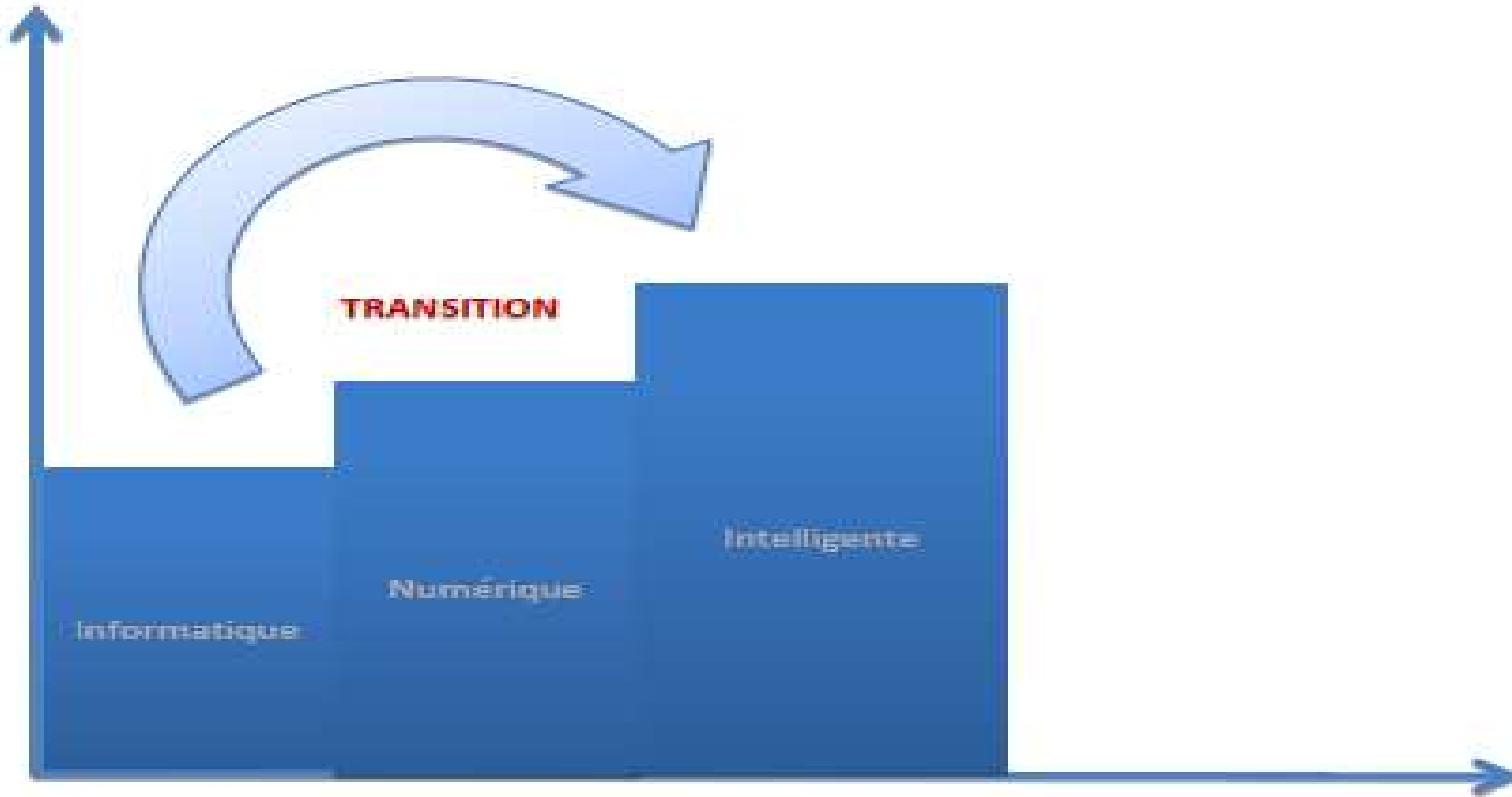


https://github.com/Newmu/dcgan/blob/master/mnist_magical_albums_128x128.png

L'EXPRESSION DE L'INTELLIGENCE ARTIFICIELLE DANS LES GRANDES ENTREPRISES



L'EXPRESSION DE L'INTELLIGENCE ARTIFICIELLE DANS LES GRANDES ENTREPRISES



L'intelligence artificielle est rattachée au *business* et l'*IT* est un support essentiel au développement

L'EXPRESSION DE L'INTELLIGENCE ARTIFICIELLE DANS LES GRANDES ENTREPRISES

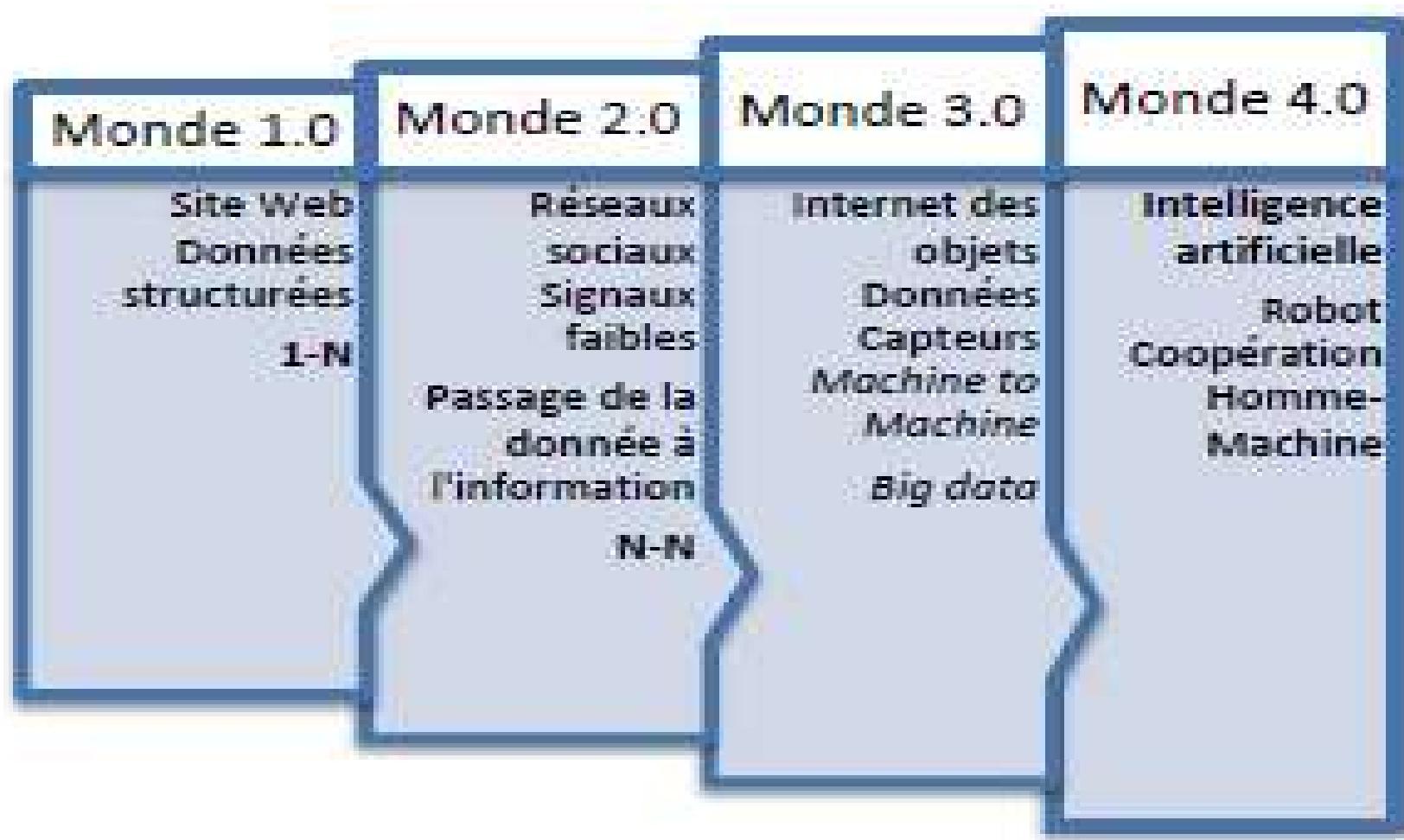


« Afin de ne pas se faire ubériser, c'est-à-dire voir sa valeur ajoutée dans la chaîne de valeur captée par un nouvel entrant qui identifierait une valeur précieuse pour nos clients à laquelle les acteurs classiques ne répondraient pas, il convient de procéder à la transformation digitale et intelligente. Elle permet d'enlever les points de douleur en interne et d'expérimenter plus facilement les services au client. »

Serge Besnard, Digital transformation manager of the Polymer B.U. of TOTAL.



L'EXPRESSION DE L'INTELLIGENCE ARTIFICIELLE DANS LES GRANDES ENTREPRISES



L'état des lieux de l'intelligence artificielle dans les grandes entreprises

Les questions suivantes ont été posées :

- Comment vous situez-vous par rapport à la transition digitale ?
 - Avez-vous des projets d'intelligence artificielle ?
 - Avez-vous un budget intelligence artificielle, un plan d'investissement ?
 - Vous sentez-vous en capacité de diriger cette transition ?
- Toutes les entreprises ont conscience de l'impact de l'intelligence artificielle et s'y préparent d'ores et déjà.



LES CHALLENGES

Les enjeux culturels

Comment anticiper cette transformation à la fois technique et culturelle, au sein d'une grande organisation ?

- Les principaux challenges culturels portent sur le développement et la mise en oeuvre du *Machine Learning*. Il faut développer une pédagogie, informer les équipes, mettre en place des systèmes de veille, etc.
- Certaines entreprises ont déjà des outils en intelligence artificielle, des applications pour lutter contre la fraude par exemple, mais n'ont pas de services centralisés.



LES CHALLENGES

Les enjeux organisationnels

- Certaines grandes entreprises sont très actives sur l'intelligence artificielle en R&D et ont parfois des équipes de prospectives dédiées, sur une période donnée, à ce sujet.

- Même si ces entités comprennent parfois peu de personnel, il y a une ambition commune qui est de faire émerger une communauté autour de l'intelligence artificielle au niveau national et international.

DE NOUVELLES MANIERE DE TRAVAILLER

- Le domaine du management de l'intelligence artificielle doit aussi s'interroger sur sa propre disparition car si l'intelligence artificielle peut renforcer l'automatisation de tâches pénibles pour l'homme, elle peut aussi remplacer ou compléter des fonctions à hautes responsabilités.
- En effet, si l'on prend comme exemple la société japonaise Hitachi, une intelligence artificielle serait capable de tenir le rôle de manager en donnant « des instructions aux employés, basées sur de grandes analyses de données et les routines des travailleurs ».
- Dans un communiqué du 4 septembre 2015, la société annonce qu'au-delà de l'amélioration de l'efficacité du travail et du gain du temps, l'intelligence artificielle est aussi capable d'anticiper d'éventuels problèmes grâce à des analyses de données extérieures en temps réel : « Si à cause d'une tempête de neige vous êtes en retard et que cela peut retarder une échéance, l'intelligence artificielle est déjà au courant du mauvais temps, a déjà procédé à des corrections et fournit des instructions de travail appropriées »



DE NOUVELLES MANIERE DE TRAVAILLER

- La dimension stratégique du management ne peut pour l'instant se soumettre à une intelligence artificielle, sans oublier l'importance du contact humain, des capacités relationnelles pour l'organisation du travail et les décisions stratégiques.
- Autrement dit, l'intelligence artificielle ne saurait trouver sa place dans les entreprises sans intelligence humaine pour la superviser. Il s'agit avant tout d'une aide à la décision.



DE NOUVELLES OPPORTUNITES BUSINESS : L'EXEMPLE BANCAIRE

À la différence de l'approche *Big Data analytics qui cherche à accumuler des connaissances sur le client en vue de « pousser des produits » vers le client, le « push product », l'IA incite à faire pivoter la relation.*



La capacité à se mettre à la place du client en se posant les bonnes questions, à considérer ses intérêts dans son propre système de valeurs, deviendra l'élément premier de la relation, pour entretenir un « pouvoir d'attraction » envers le client et pour qu'il considère à tout moment l'entreprise en question comme un acteur pertinent



Il s'agit ainsi de passer du « *push product* » au « *pull client* ».

Seeing = Believing?

- With the development of computer vision technologies, reliability of images and videos is decreasing. Fake images can be produced with technologies such as PS and generative adversarial networks (GAN), making it hard to identify whether images are true or not.
- Example:
 - A suspect provided fake evidence by forging an image in which the suspect is in a place where he has never been to or with someone he has never seen using PS technologies.
 - In advertisements for diet pills, people's appearances before and after weight loss can be changed with PS technologies to exaggerate the effect of the pills.
 - Lyrebird, a tool for simulating voice of human beings based on recording samples of minutes, may be used by criminals.
 - Household images released on rent and hotel booking platforms may be generated through GAN.

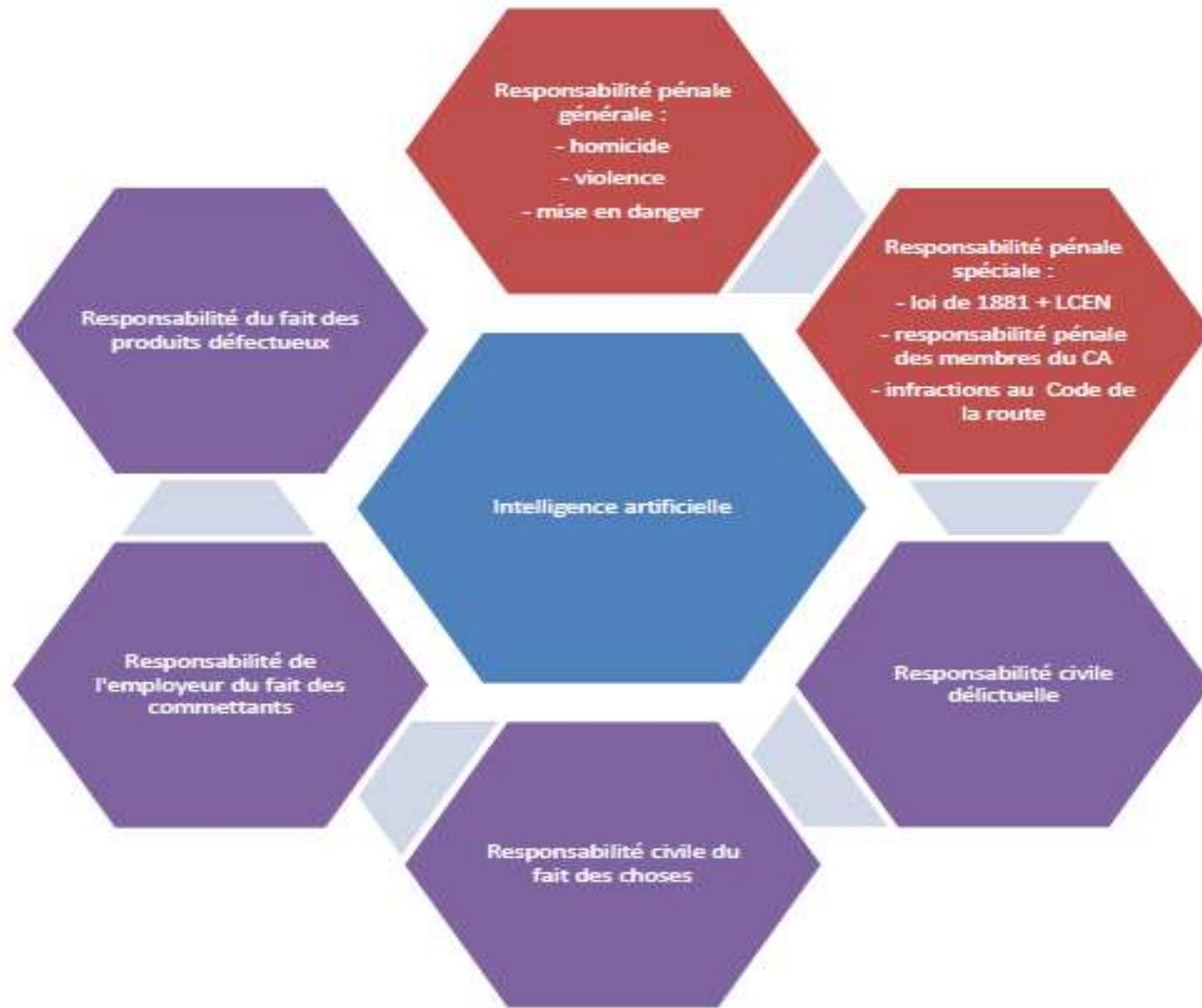
Problems to Be Solved

- Are AI-created works protected by copyright laws?
- Who gives authority to robots?
- What rights shall be authorized to robots?
- ...

Development Trends of AI Technologies

- Framework: easier-to-use development framework
- Algorithm: algorithm models with better performance and smaller size
- Computing power: comprehensive development of device-edge-cloud computing
- Data: more comprehensive basic data service industry and more secure data sharing
- Scenario: continuous breakthroughs in industry applications

L'IA et responsabilités



LE DROIT PROSPECTIF

Tel qu'il l'a été précisé précédemment, **aucun régime propre au robot** doté d'intelligence artificielle n'est encore mis en place en France ni à l'échelle européenne



- ❑ Le droit positif fait donc peser sur le concepteur de l'intelligence artificielle l'ensemble des responsabilités.
- ❑ L'apprentissage de l'intelligence artificielle n'est pas pris en considération dans la partie législative.

L'ETHIQUE DES USAGES DE L'ENTREPRISE

La protection des données personnelles est également au cœur de ces problématiques.



L'ETHIQUE BY DESIGN



Il convient d'être prudent et de faire des tests avant une mise sur le marché. On pourrait ainsi éviter une partie des risques grâce :

- **A la certification et/ou l'autorisation de mise sur le marché** ;
- **A la mise en place d'un droit à l'oubli et d'un droit au refus** : il faudrait que tout utilisateur puisse refuser de confier ses données personnelles à une intelligence artificielle. Il faut avoir la possibilité de refuser l'accès d'une intelligence artificielle à son compte Twitter, Facebook dont l'analyse des données permette déjà de déduire si une personne est solvable pour un prêt bancaire, par exemple.
Sur de nombreux sites internet, il y a déjà de l'intelligence artificielle, nos comportements sont tracés en permanence (suivi des navigations, sites précédemment visités). Comment faire pour vivre dans une société imprégnée d'intelligence artificielle ? Un individu qui exercerait ce droit au refus et/ou à l'oubli ne risquerait-il pas d'être mis au ban de cette société ?
- **A la séparation des intelligences artificielles** : dans une vision plus extrémiste, il s'agirait de rendre techniquement impossible une fusion de toutes les intelligences artificielles entre elles, afin de les empêcher d'apprendre les unes des autres.

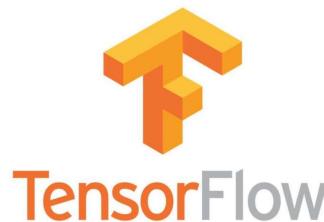
Problems to Be Solved

- Are AI-created works protected by copyright laws?
- Who gives authority to robots?
- What rights shall be authorized to robots?
- ...

Easier-to-Use Development

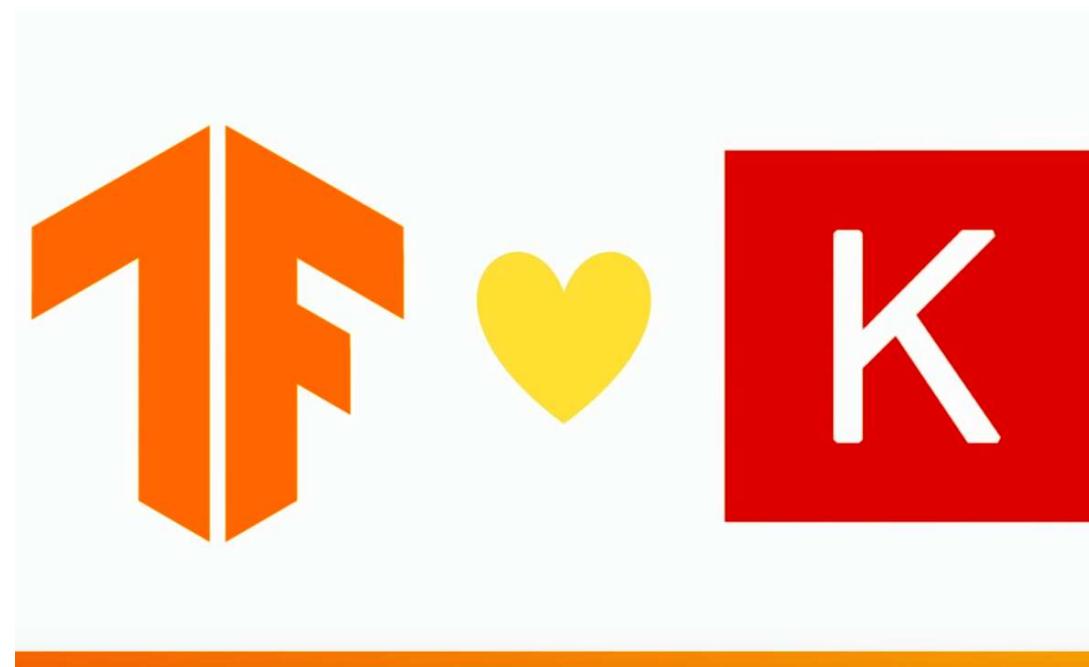
- Various AI development frameworks are evolving towards ease-of-use and omnipotent, continuously lowering the threshold for AI development.

Framework

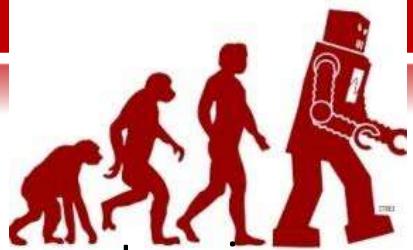


Tensorflow 2.0

- TensorFlow 2.0 has been officially released. It integrates Keras as its high-level API, greatly improving usability.



Synthèse



L'IA constitue la prochaine révolution informatique et culturelle des entreprises. Pour s'y préparer, les convictions des grandes entreprises, participantes du Cercle IA, sont :

- De ne pas hésiter à affecter des budgets spécifiques à l'IA, qui devrait dépasser le stade POC et pouvoir se développer rapidement, avec une vraie stratégie d'entreprise ;
- Anticiper l'évolution des infrastructures IT : la puissance de calcul liée à l'exécution d'algorithmes d'apprentissage nécessite de passer d'architectures séquentielles à des architectures parallèles et distribuées ;
- Attirer et valoriser les nouveaux talents : la France est leader dans le domaine des mathématiques et regorge de talents dans l'ingénierie et dans la recherche scientifique. Les grandes entreprises ont besoin de ces compétences d'excellence et doivent les valoriser dans les nouveaux métiers liés à l'IA (développeurs, roboticiens, *data scientists*) ;
- Développer le travail de prospective au sein des entreprises pour mieux orienter les stratégies à partir de différents scénarios possibles d'émergence de l'IA ;
- Dé-siloter les Métiers et développer une culture d'API au sein de l'entreprise ;
- Enfin, l'IA étant évidemment un sujet *business*, *il est important pour l'IT d'être un support, voire un pilote de ces nouveaux business models.*

Géopolitique de l'intelligence artificielle : le retour des empires ?

L'Intelligence artificielle progresse rapidement et devient un véritable outil de puissance. Ceci vaut autant pour le *hard power* (applications militaires) que pour le *soft power* (impact économique, influence politique et culturelle, etc.). Les États-Unis et la Chine dominent le marché et imposent leur pouvoir. L'Europe est à la traîne et cherche à réagir en émettant de nouvelles réglementations. Quant à l'Afrique, elle est devenue un terrain d'affrontement pour les « empires digitaux ».

Activer W



Un duopole américano-chinois



Aujourd'hui, les États-Unis et la Chine forment une sorte de duopole de l'IA de par la taille critique de leur marché, et leur politique laxiste en matière de protection des données personnelles. Leur rivalité s'illustre notamment dans une guerre commerciale qui a commencé par l'imposition par l'administration Trump de droits de douane de 25 % sur des biens chinois (y compris certains relevant de l'IA), représentant une valeur totale de 34 milliards de dollars, en réponse à ce que Trump qualifie de « vol » de propriété intellectuelle et de technologies. La Chine a répliqué en imposant des droits de douane de 25 % sur 540 produits américains. Par ailleurs, en août 2017, les États-Unis ont lancé une enquête contre la Chine, accusant cette dernière de pratiques commerciales déloyales en matière de propriété intellectuelle, touchant en particulier le domaine technologique .

China and the United States dominate investments in artificial intelligence.

Artificial-intelligence investment, 2016

North America,
\$15 billion-\$23 billion



Europe,
\$3 billion-\$4 billion



Asia,
\$8 billion-\$12 billion



● Internal corporate
investments

● External investments (venture
capital, private equity, M&A)

L'Afrique : le grand champ de bataille?

Le continent africain est pratiquement vierge en termes d'infrastructures numériques orientées vers l'IA. Le gouvernement kényan est à ce jour le seul à développer une stratégie en la matière . L'Afrique a pourtant un énorme potentiel pour explorer les applications de l'IA et inventer de nouveaux modèles d'affaires et de services. Les investissements chinois en Afrique se sont intensifiés cette dernière décennie, et la Chine est actuellement le premier partenaire commercial des pays africains, suivie de l'Inde, de la France, des États-Unis et de l'Allemagne. L'Afrique est probablement le continent où les cyber-impérialismes sont les plus flagrants.



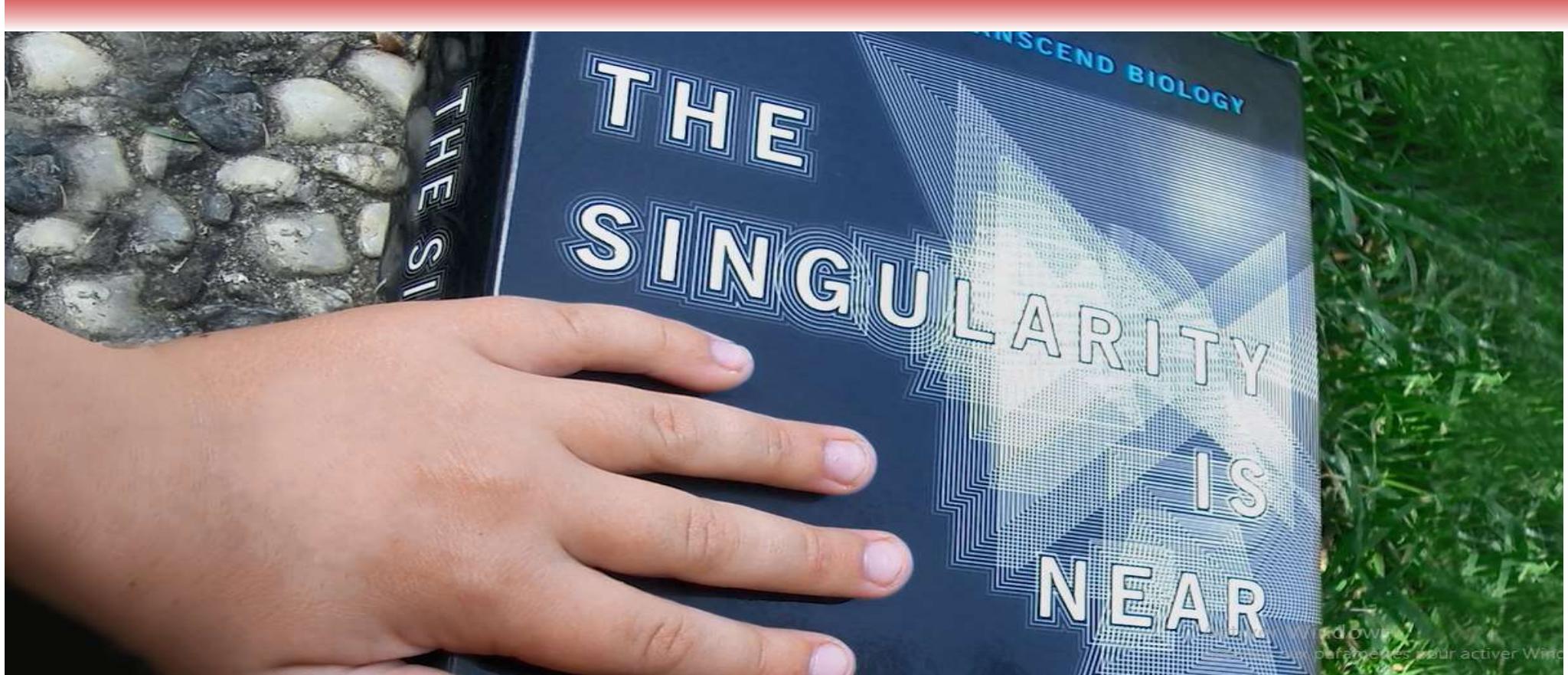
La fin de l'année 2017, deux annonces ont fait sensation :

- l'Arabie saoudite a accordé la nationalité saoudienne à un robot 47
- et la Nouvelle-Zélande a annoncé qu'elle présentera un robot au parlement en 2020



LE FUTUR

- Une question souvent entendue est la suivante : que reste-t-il à l'humain que la machine ne sache pas faire ?
 - ✓ **L'intuition** ? Mais l'intuition n'est-elle pas la qualité indispensable surtout lorsque l'on manque de données ?
 - ✓ **L'empathie** ? Mais l'informatique affective est un des grands sujets de recherche actuellement ; par exemple, le Massachusetts Institute of Technology (MIT) a consacré à ce thème un département entier, sous la direction de Rosalind Picard 40.
 - ✓ **La créativité** ? C'est aussi un sujet d'exploration de IBM Watson 41 qui, à la mi-2016, a créé une bande-annonce pour un film d'horreur



→ la croissance technologique induirait-elle des changements imprévisibles sur la société humaine ? La machine dépassera t-elle l'Homme ?

LE FUTUR

La **singularité** engendrera une rupture dans l'évolution de l'être humain. Certains parlent même d'un remplacement des humains par la machine. Les robots humanoïdes seraient alors les représentants de l'armée de demain, qui éradiquerait l'humanité et prendrait sa place. Ce phénomène est connu : plus un robot ressemble à un être humain, plus il engendre de l'inconfort





1. Les tâches qui requièrent l'humanité
2. L'authenticité de la communication humaine est irremplaçable dans l'automatisation.
3. Il n'y a pas d'intérêt à aller à un concert de Jazz si le musicien est une machine. C'est la communication des émotions
4. Le robot devrait être inculquer des valeurs universelles et humaines



1. Mariage AI et robotique : peut être une menace
2. Il ya un e espèce de peur qui vient de hollywood. C'est une projection sur la qualité et défauts de l'intelligence humaine mais l'intelligence des ordinateurs est très loin par rapport à ses motivations



Armement autonome : un robot capable de choisir une cible et l'éliminer cela soulève une question éthique
→ on n'est pas à ce niveau avec l'AI
→ Ce sont des projections psychologiques



Perte de contrôle → Ils peuvent des craintes injustifiées
Similaire à : Biotechnologie dans les années 70 modifier le génome/code génétique humain on a interdit ceci



On définit la biotechnologie comme « l'application à des organismes vivants des principes scientifiques et de l'ingénierie à la transformation de matériaux vivants ou non-vivants aux fins de la production de connaissances, de biens et de services. ».

Conclusion

- Aujourd’hui l’IA est partout sans que l’on s’en rende compte ou préoccupe.
- Rôle de plus en plus important dans la conception, les interfaces, internet, les robots, ...
- Une meilleure intégration de l’IA dans les applications informatiques
- Une démarche génie logiciel n ’est pas toujours facile. Des environnements: JAVA, Prolog, Smalltalk, etc.
- Évolution de l’IA intelligence Artificielle vers l’IA informatique avancée

Conclusion

- Nous sommes encore loin des espoirs et désespoirs prédis par les auteurs de science-fiction dans les films
- Le but ultime de l'IA n'est pas de remplacer l'humain mais bien de décharger afin qu'il puisse se concentrer sur des tâches plus créatives ou agréables.
- Timm Menzies a dit : je rêve un jour où mon processeur Word écrirait un article comme celui-ci pendant que je vais à la plage!! Y arrivera t-on un jour? Peut être...

Part 2

Seeing = Believing?

- With the development of computer vision technologies, reliability of images and videos is decreasing. Fake images can be produced with technologies such as PS and generative adversarial networks (GAN), making it hard to identify whether images are true or not.
- Example:
 - A suspect provided fake evidence by forging an image in which the suspect is in a place where he has never been to or with someone he has never seen using PS technologies.
 - In advertisements for diet pills, people's appearances before and after weight loss can be changed with PS technologies to exaggerate the effect of the pills.
 - Lyrebird, a tool for simulating voice of human beings based on recording samples of minutes, may be used by criminals.
 - Household images released on rent and hotel booking platforms may be generated through GAN.

AI Development = Rising Unemployment?

- Looking back, human beings have always been seeking ways to improve efficiency, that is, obtain more with less resources. We used sharp stones to hunt and collect food more efficiently. We used steam engines to reduce the need for horses. Every step in achieving automation will change our life and work. In the era of AI, what jobs will be replaced by AI?
- The answer is repetitive jobs that involve little creativity and social interaction.

Jobs Most Likely to Be Replaced by AI	Jobs Most Unlikely to Be Replaced by AI
Courier	Writer
Taxi driver	Management personnel
Soldier	Software engineers
Accounting	HR manager
Telesales personnel	Designer
Customer service	Activity planner
...	...

Problems to Be Solved

- Are AI-created works protected by copyright laws?
- Who gives authority to robots?
- What rights shall be authorized to robots?
- ...

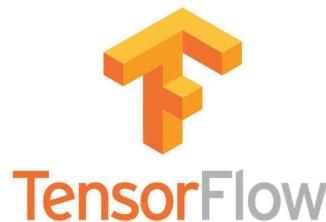
Development Trends of AI Technologies

- Framework: easier-to-use development framework
- Algorithm: algorithm models with better performance and smaller size
- Computing power: comprehensive development of device-edge-cloud computing
- Data: more comprehensive basic data service industry and more secure data sharing
- Scenario: continuous breakthroughs in industry applications

Easier-to-Use Development

- Various AI development frameworks are evolving towards ease-of-use and omnipotent, continuously lowering the threshold for AI development.

Framework



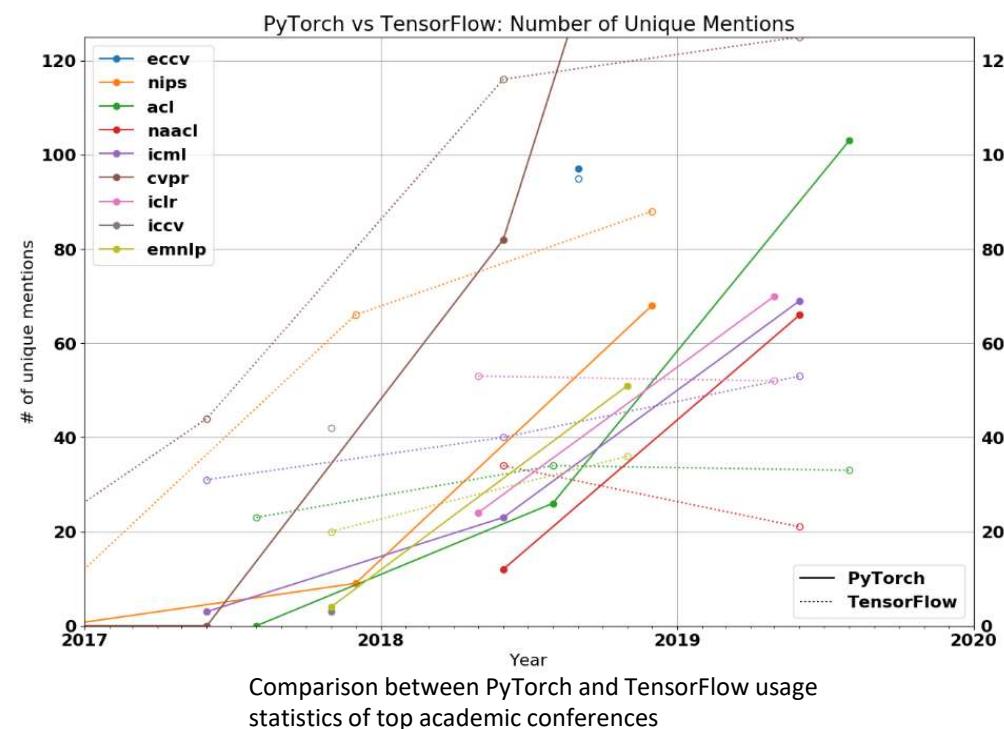
Tensorflow 2.0

- TensorFlow 2.0 has been officially released. It integrates Keras as its high-level API, greatly improving usability.



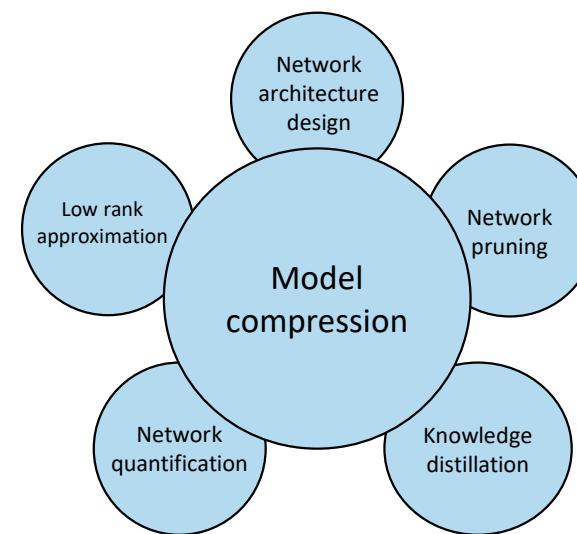
Pytorch vs Tensorflow

- PyTorch is widely recognized by academia for its ease of use.

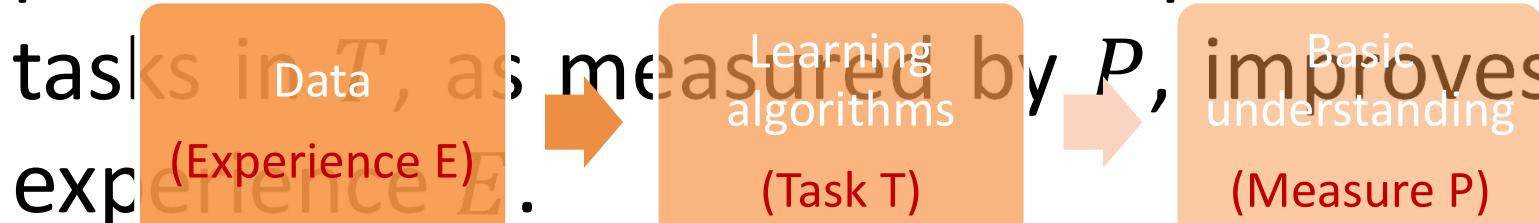


Smaller Deep Learning Models

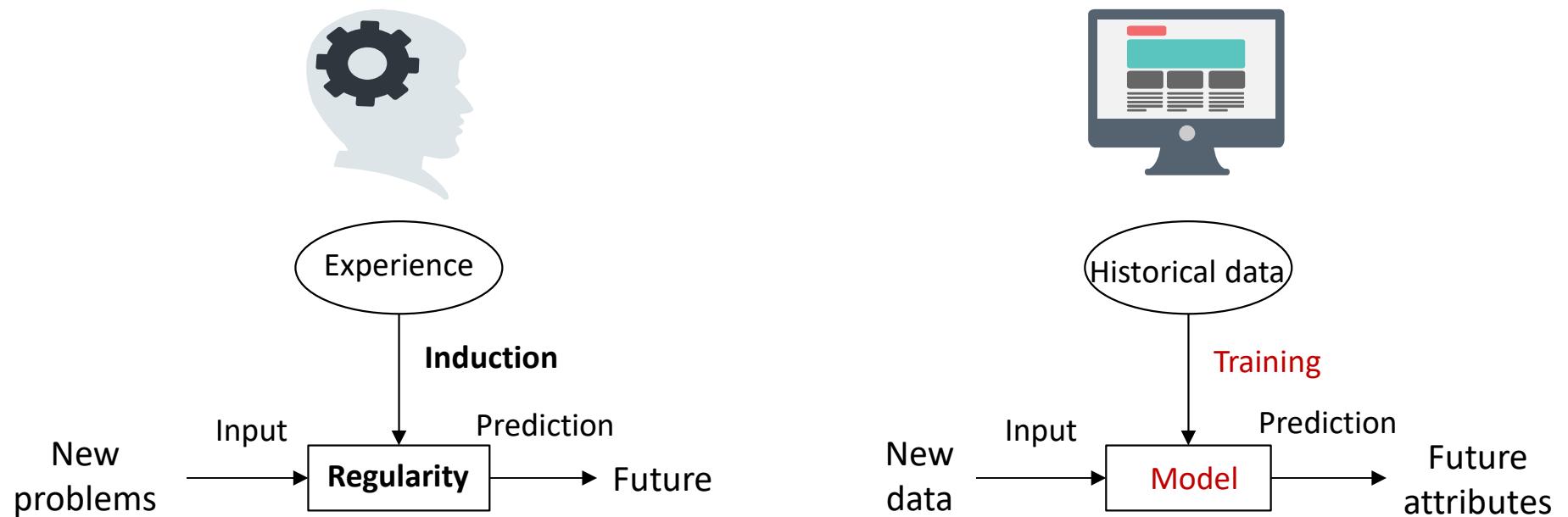
- A model with better performance usually has a larger quantity of parameters, and a large model has lower running efficiency in industrial applications. More and more model compression technologies are proposed to further compress the model size while ensuring the model performance, meeting the requirements of industrial applications.
 - Low rank approximation
 - Network pruning
 - Network quantification
 - Knowledge distillation
 - Compact network design



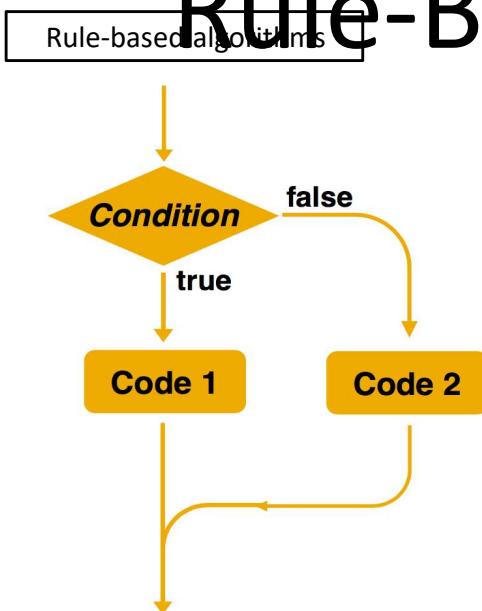
Machine Learning Algorithms (1)

- Machine learning (including deep learning) is a study of learning algorithms. A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T , as measured by P , improves with experience E .

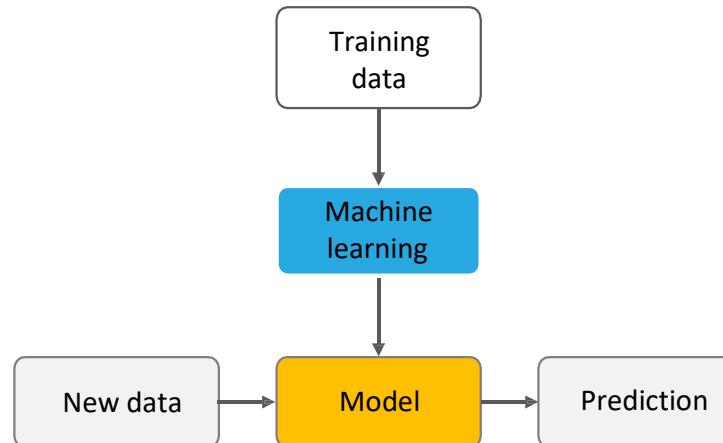
Machine Learning Algorithms (2)



Differences Between Machine Learning Algorithms and Traditional Rule-Based Algorithms



- Explicit programming is used to solve problems.
- Rules can be manually specified.

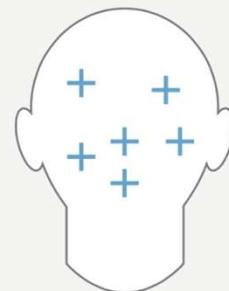


- Samples are used for training.
- The decision-making rules are complex or difficult to describe.
- Rules are automatically learned by machines.

Application Scenarios of Machine Learning

- The solution to ~~learning~~ problem(1s) complex, or the problem may involve a large amount of data without a clear data distribution function.
- Machine learning can be used in the

f Rules are complex or cannot be described, such as voice recognition.



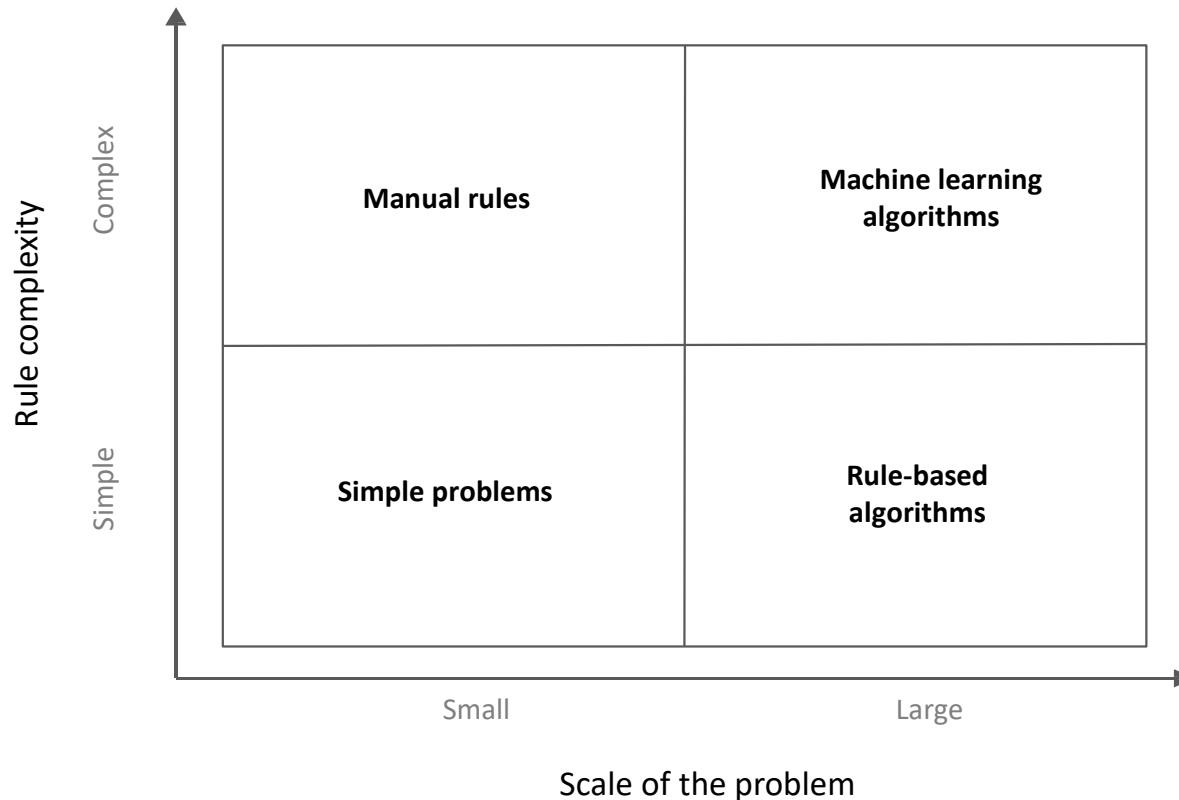
e a Task rules change over time. For example, in the part-of-speech tagging task, new words or meanings are generated at any time.



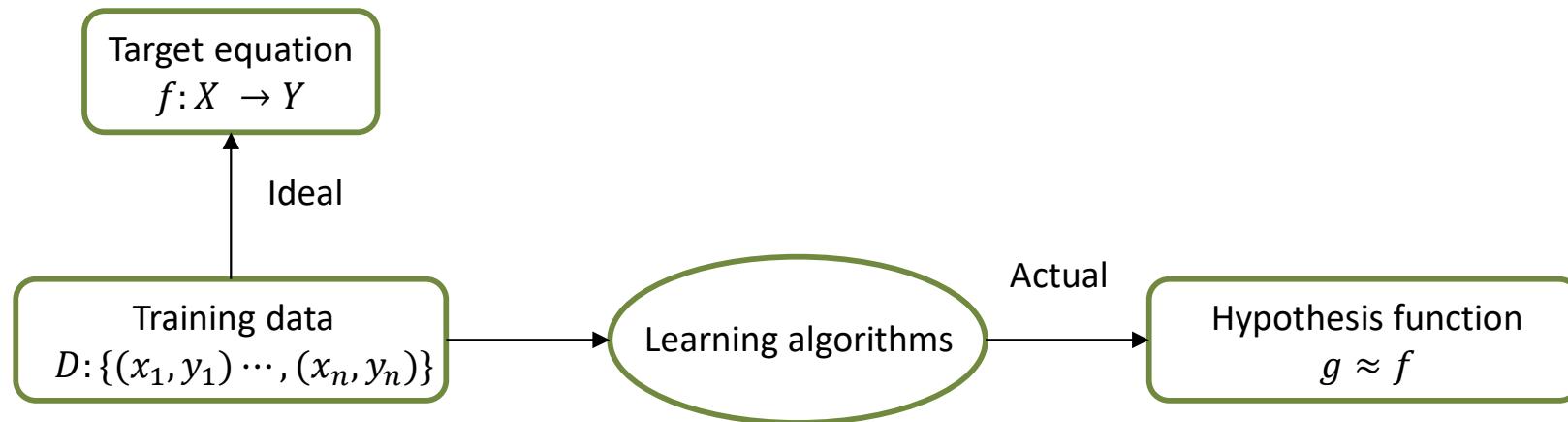
Data distribution changes over time, requiring constant readaptation of programs, such as predicting the trend of commodity sales.



Application Scenarios of Machine Learning (2)



Rational Understanding of Machine Learning Algorithms



- Target function f is unknown. Learning algorithms cannot obtain a perfect function f .
- Assume that hypothesis function g **approximates** function f , but may be different from function f .

Main Problems Solved by Machine Learning

- Machine learning can deal with many types of tasks. The following describes the most typical and common types of tasks.
 - Classification: A computer program needs to specify which of the k categories some input belongs to. To accomplish this task, learning algorithms usually output a function $f: R^n \rightarrow \{1, 2, \dots, k\}$. For example, the image classification algorithm in computer vision is developed to handle classification tasks.
 - Regression: For this type of task, a computer program predicts the output for the given input. Learning algorithms typically output a function $f: R^n \rightarrow R$. An example of this task type is to predict the claim amount of an insured person (to set the insurance premium) or predict the security price.
 - Clustering: A large amount of data from an unlabeled dataset is divided into multiple categories according to internal similarity of the data. Data in the same category is more similar than that in different categories. This feature can be used in scenarios such as image retrieval and user profile management.
- Classification and regression are two main types of prediction, accounting from 80% to 90%. The output of classification is discrete category values, and the output of regression is continuous numbers.

Contents

1. Machine Learning Definition
- 2. Machine Learning Types**
3. Machine Learning Process
4. Other Key Machine Learning Methods
5. Common Machine Learning Algorithms
6. Case study

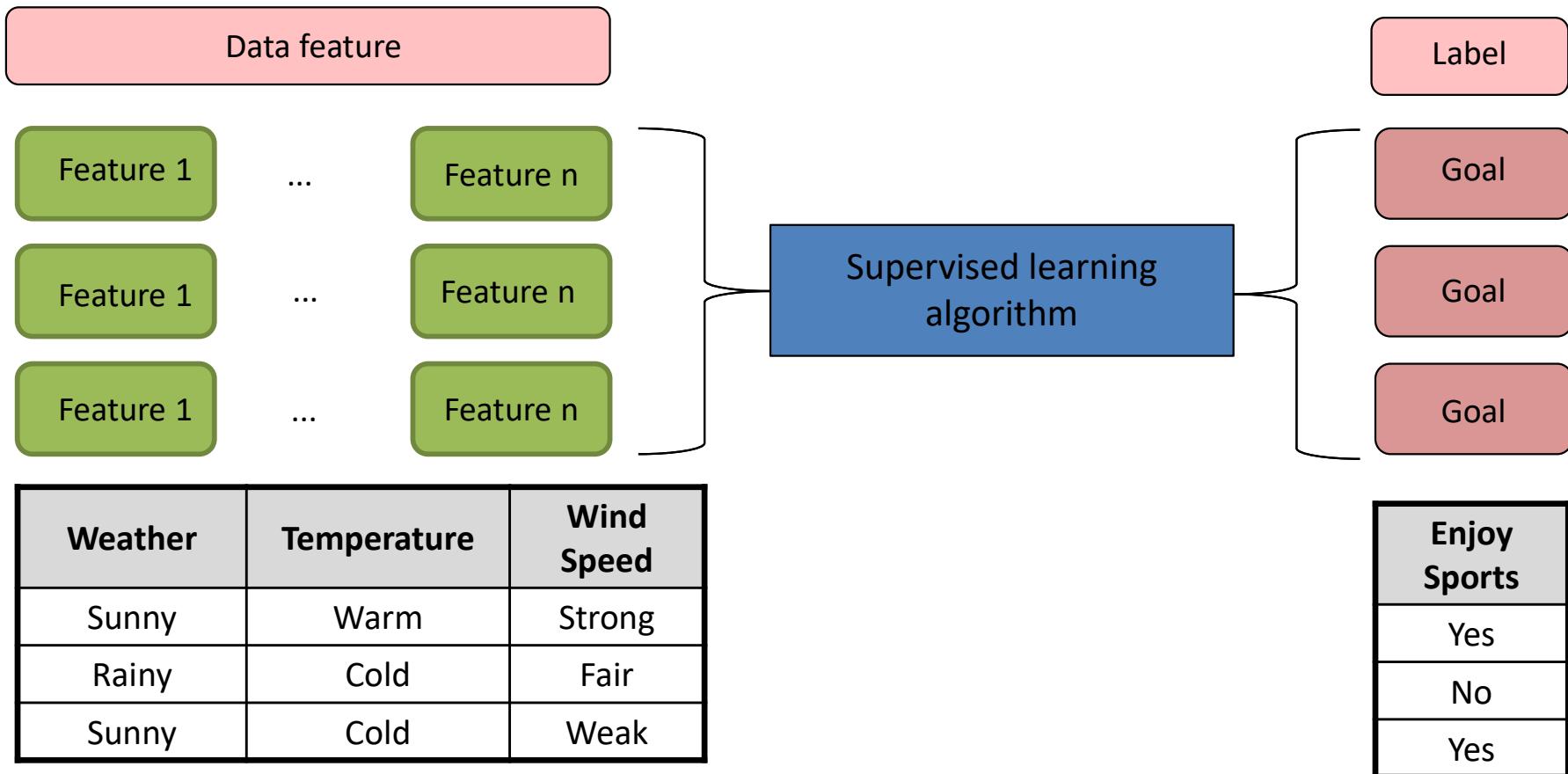
Machine Learning Classification

- **Supervised learning:** Obtain an optimal model with required performance through training and learning based on the samples of known categories. Then, use the model to map all inputs to outputs and check the output for the purpose of classifying unknown data.
- **Unsupervised learning:** For unlabeled samples, the learning algorithms directly model the input datasets. Clustering is a common form of unsupervised learning. We only need to put highly similar samples together, calculate the similarity between new samples and existing ones, and classify them by similarity.
- **Semi-supervised learning:** In one task, a machine learning model that automatically uses a large amount of unlabeled data to assist learning directly of a small amount of labeled data.
- **Reinforcement learning:** It is an area of machine learning concerned with how agents ought to take actions in an environment to maximize some notion of cumulative reward. The difference between reinforcement learning and supervised learning is the teacher signal. The reinforcement signal provided by the environment in reinforcement learning is used to evaluate the action (scalar signal) rather than telling the learning system how to perform correct actions.

Machine Learning Classification

- **Supervised learning:** Obtain an optimal model with required performance through training and learning based on the samples of known categories. Then, use the model to map all inputs to outputs and check the output for the purpose of classifying unknown data.
- **Unsupervised learning:** For unlabeled samples, the learning algorithms directly model the input datasets. Clustering is a common form of unsupervised learning. We only need to put highly similar samples together, calculate the similarity between new samples and existing ones, and classify them by similarity.
- **Semi-supervised learning:** In one task, a machine learning model that automatically uses a large amount of unlabeled data to assist learning directly of a small amount of labeled data.
- **Reinforcement learning:** It is an area of machine learning concerned with how agents ought to take actions in an environment to maximize some notion of cumulative reward. The difference between reinforcement learning and supervised learning is the teacher signal. The reinforcement signal provided by the environment in reinforcement learning is used to evaluate the action (scalar signal) rather than telling the learning system how to perform correct actions.

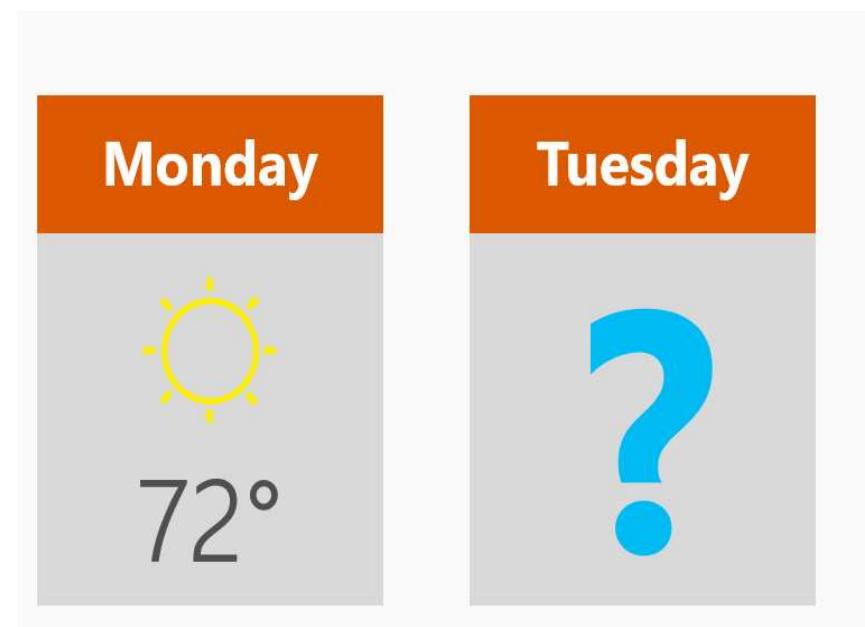
Supervised Learning



Supervised Learning - Regression

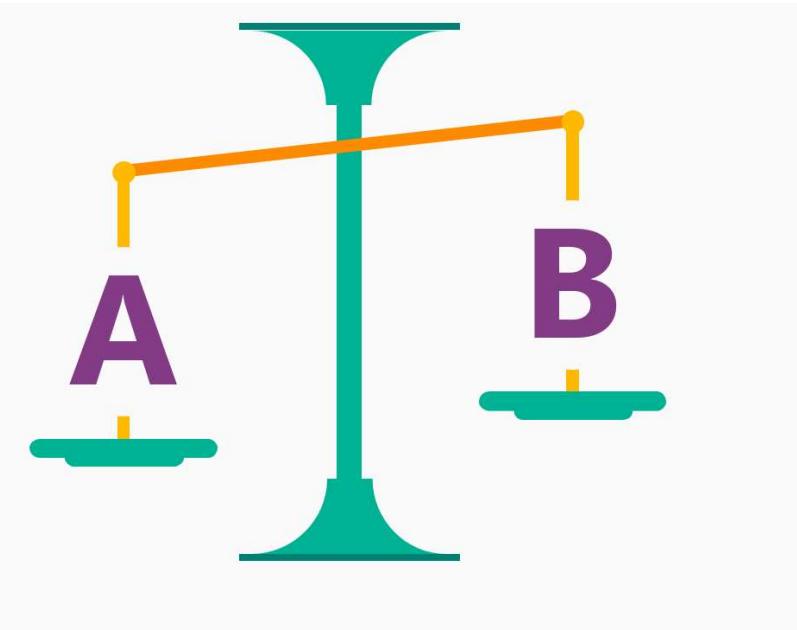
- Regression: reflects the features of attribute values of samples in a sample dataset. The dependency between attribute values is discovered by expressing the relationship of sample mapping through functions.
 - How much will I benefit from the stock next week?
 - What's the temperature on Tuesday?

Questions

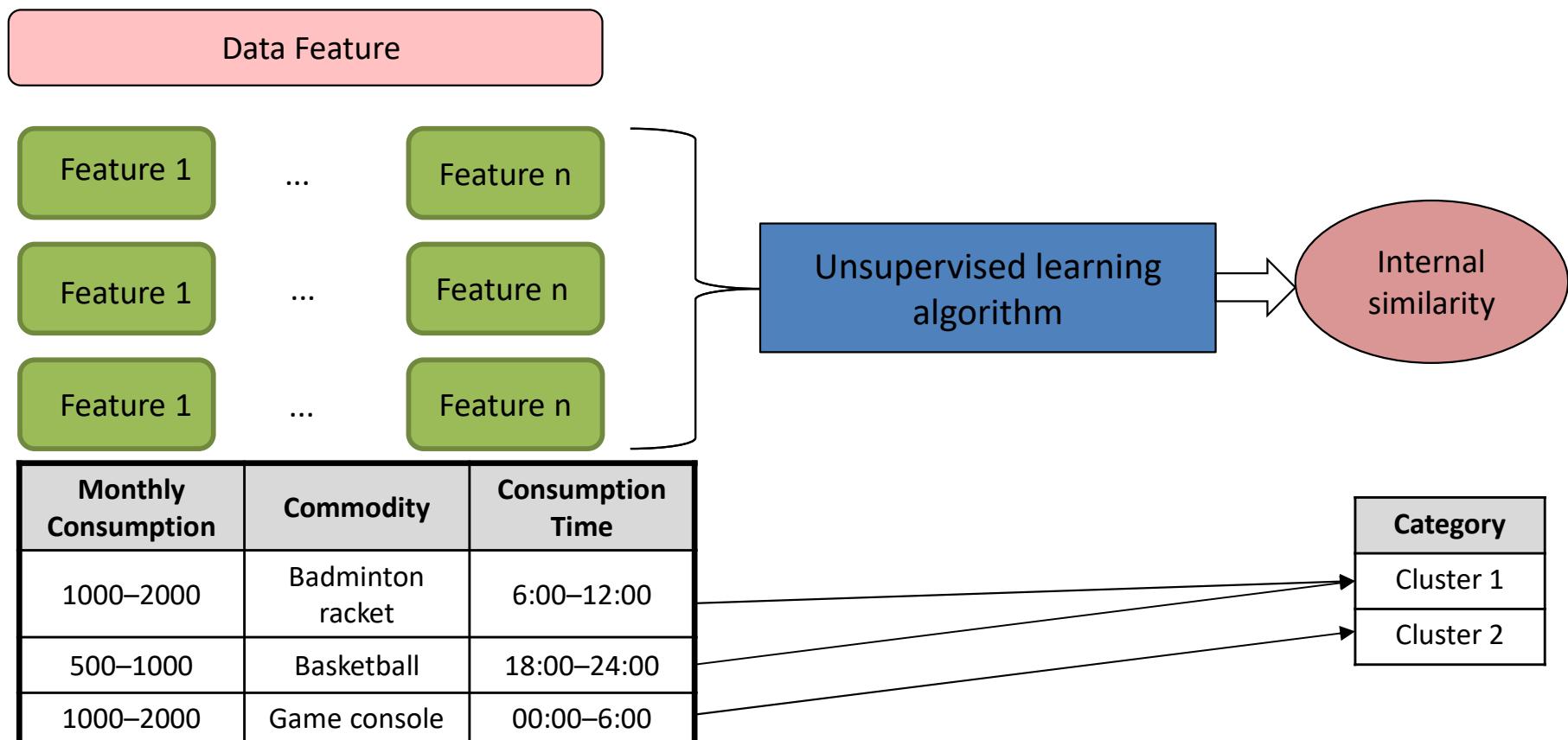


Supervised Learning - Classification

- Classification: ~~Map samples~~ ~~Answers~~ ~~samples~~ in a sample dataset to a specified category by using a classification model.
 - Will there be a traffic jam during the morning rush hour tomorrow?
 - Which method is more attractive: 5 yuan voucher or 25% off?

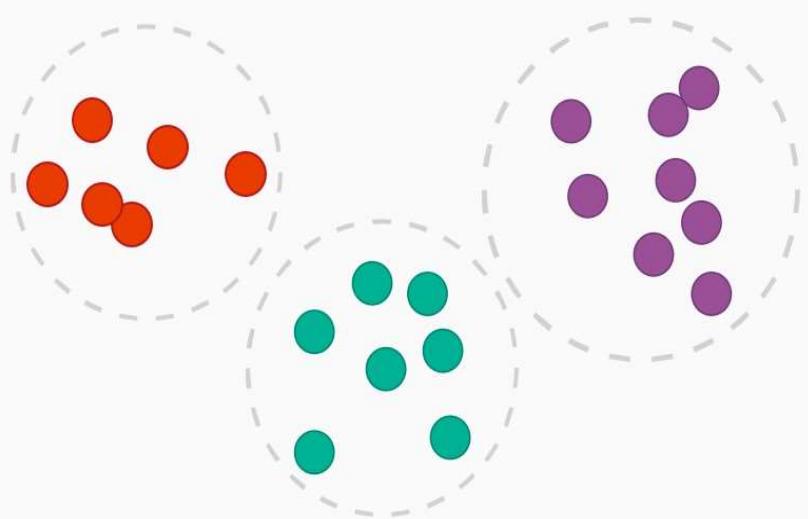


Unsupervised Learning

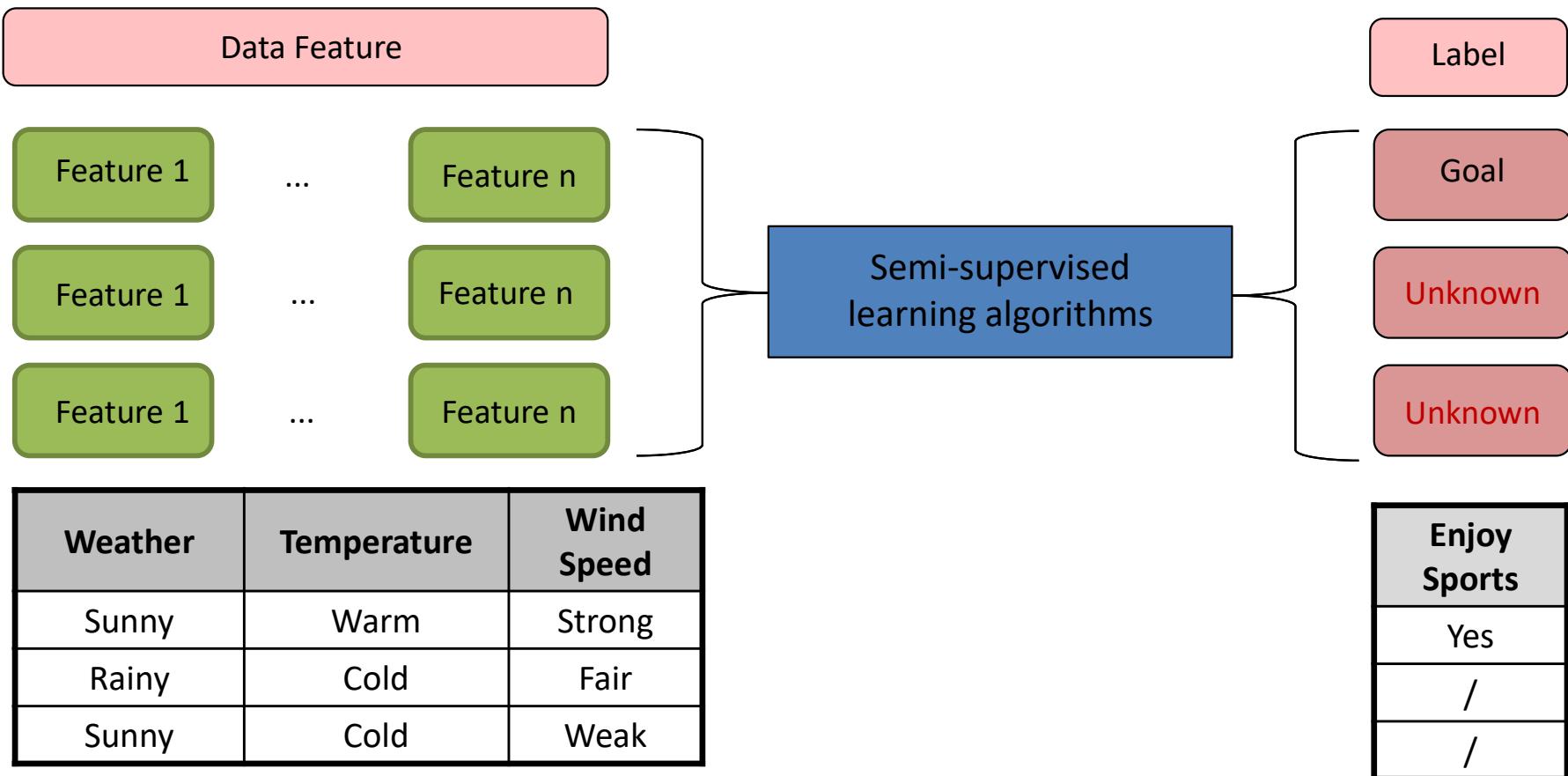


Unsupervised Learning - Clustering

- Clustering: classifies samples in a sample dataset into several categories based on the clustering model. The similarity of samples belonging to the same cluster:
 - Which audiences like the same type of content?
 - Which of these companies were damaged in a similar way?

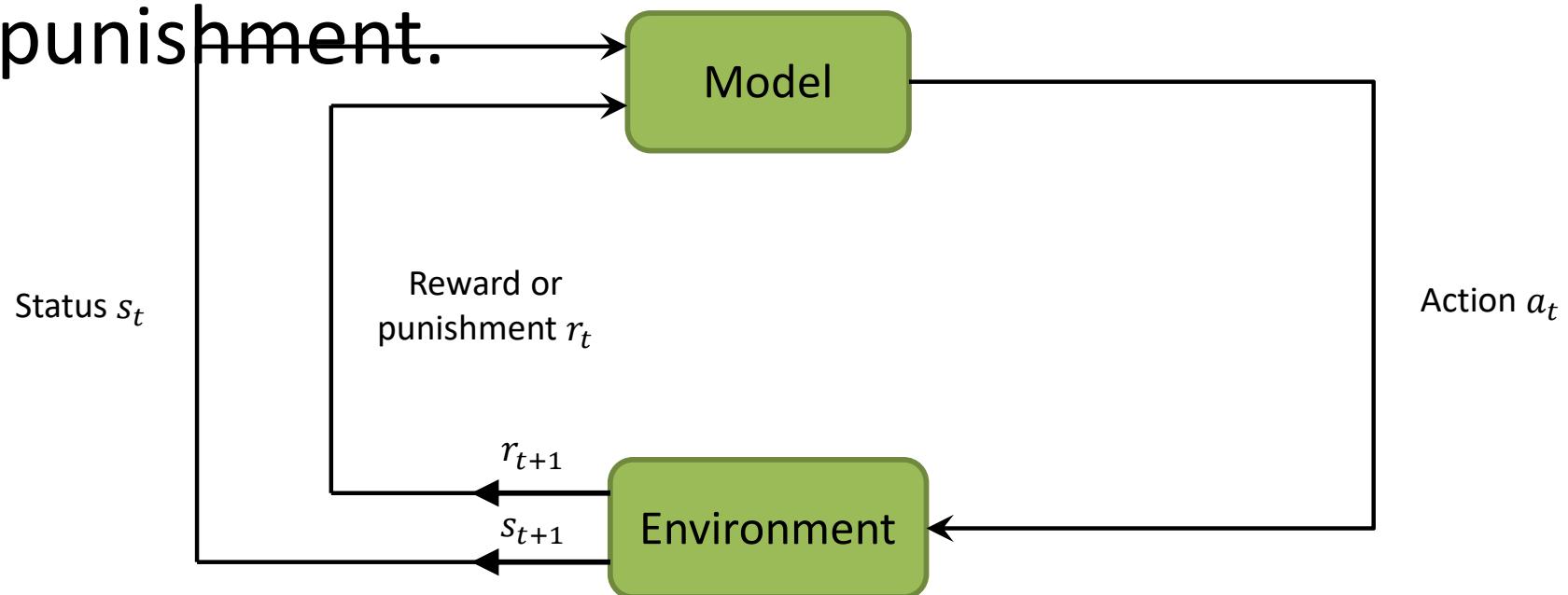


Semi-Supervised Learning



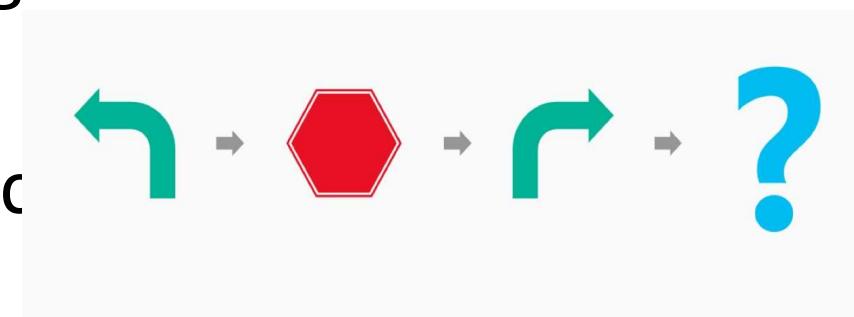
Reinforcement Learning

- The model perceives the environment, takes actions, and makes adjustments and choices based on the status and award or punishment.



Reinforcement Learning - Best

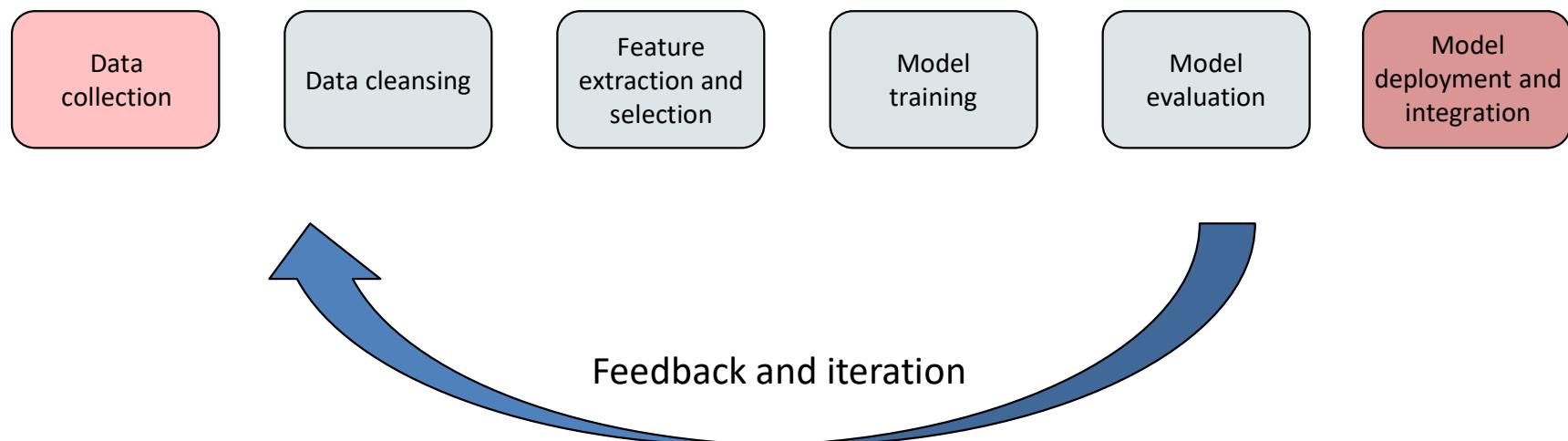
- Reinforcement learning always looks for best behaviors. Reinforcement learning is targeted at machines or robots.
 - Autopilot: Should it brake or accelerate when the yellow light starts to flash?
 - Cleaning back for cleaning or go



Contents

1. Machine learning algorithm
2. Machine Learning Classification
- 3. Machine Learning Process**
4. Other Key Machine Learning Methods
5. Common Machine Learning Algorithms
6. Case study

Machine Learning Process



Basic Machine Learning Concept –

- Dataset: a collection of data used in machine learning tasks. Each data record is called a sample. Events or attributes that reflect the performance or nature of a sample in a particular aspect are called features.
- Training set: a dataset used in the training process, where each sample is referred to as a training sample. The process of creating a model from data is called learning (training).
- Test set: Testing refers to the process of using the model obtained after learning for prediction. The dataset used is called a test set, and each sample is called a test sample.

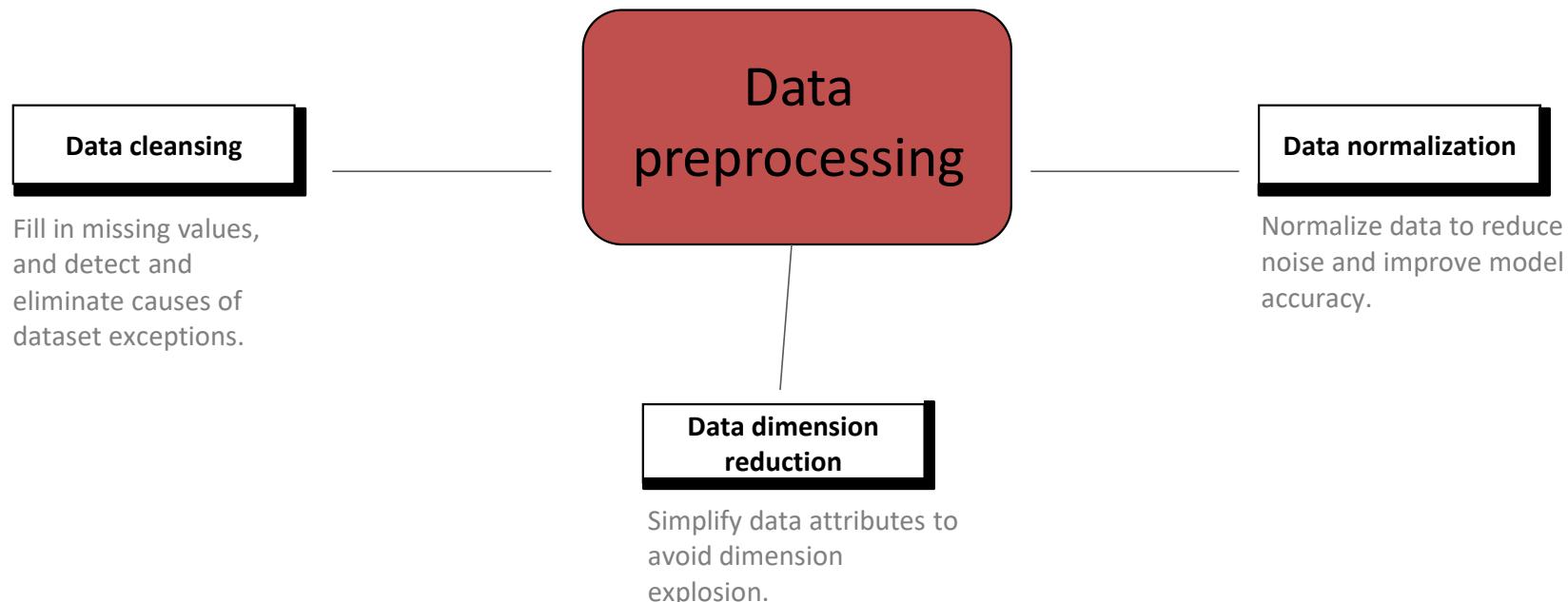
Checking Data Overview

- Typical dataset form

	Feature				Label
	1	2	3	4	
No.	Area	School Districts	Direction	House Price	
Training set	1	100	8	South	1000
	2	120	9	Southwest	1300
	3	60	6	North	700
	4	80	9	Southeast	1100
Test set	5	95	3	South	850

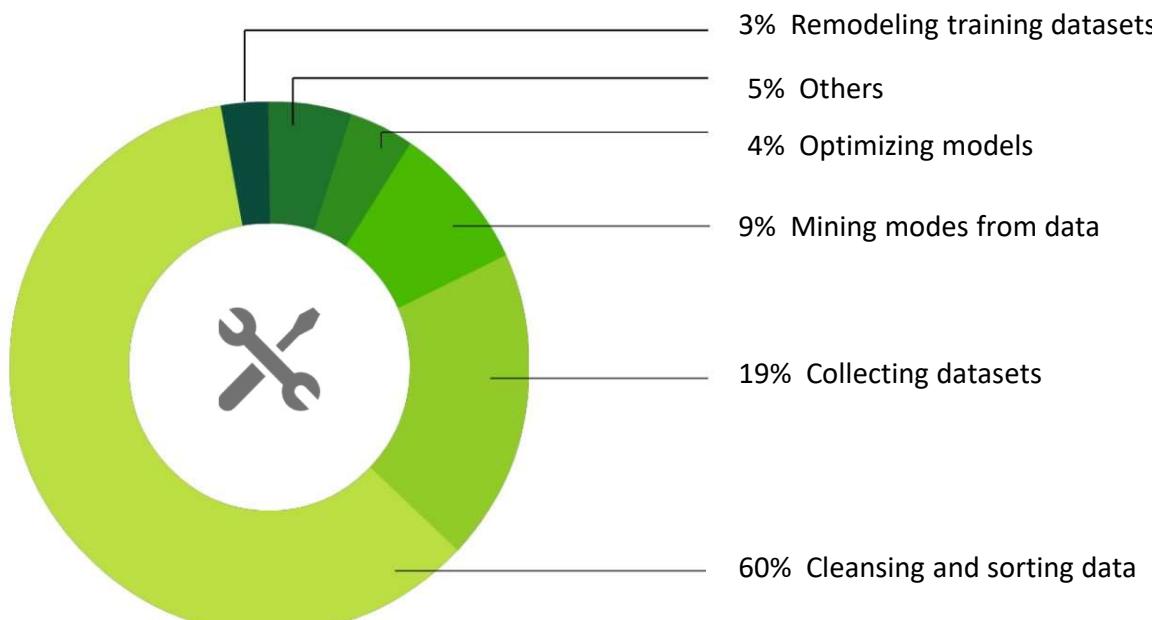
Importance of Data Processing

- Data is crucial to models. It is the ceiling of model capabilities. Without good data, there is no good model.



Workload of Data Cleansing

- Statistics on data scientists' work in machine learning



CrowdFlower Data Science Report 2016

Data Cleansing

- Most machine learning models process features, which are usually numeric representations of input variables that can be used in the model.
- In most cases, the collected data can be used by algorithms only after being preprocessed. The preprocessing operations include the following:
 - Data filtering
 - Processing of lost data
 - Processing of possible exceptions, errors, or abnormal values
 - Combination of data from multiple data sources
 - Data consolidation

Dirty Data (1)

- Generally, real data may have some quality problems.
 - Incompleteness: contains missing values or the data that lacks attributes
 - Noise: contains incorrect records or exceptions.
 - Inconsistency: contains inconsistent records.

Dirty Data (2)

#	Id	Name	Birthday	Gender	IsTeacher	#Students	Country	City
1	111	John	31/12/1990	M	0	0	Ireland	Dublin
2	222	Mery	15/10/1978	F	1	15	Iceland	
3	333	Alice	19/04/2000	F	0	0	Spain	Madrid
4	444	Mark	01/11/1997	M	0	0	France	Paris
5	555	Alex	15/03/2000	A	1	23	Germany	Berlin
6	555	Peter	1983-12-01	M	1	10	Italy	Rome
7	777	Calvin	05/05/1995	M	0	0	Italy	Italy
8	888	Roxane	03/08/1948	F	0	0	Portugal	Lisbon
9	999	Anne	05/09/1992	F	0 5		Switzerland	Geneva
10	101010	Paul	14/11/1992	M	1	26	Ytali	Rome

Annotations pointing to dirty data:

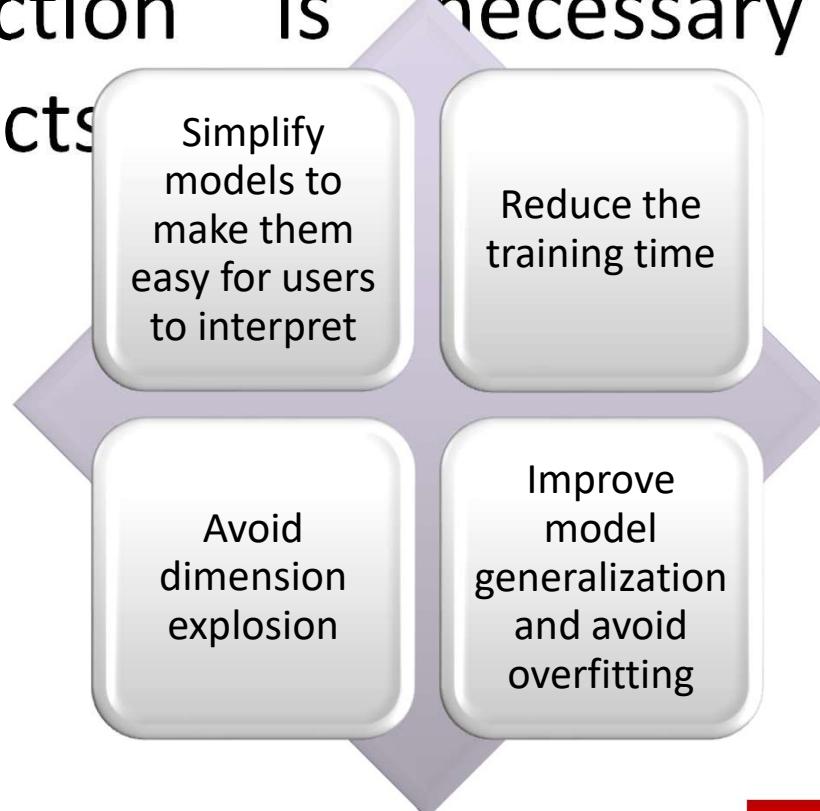
- Invalid duplicate item: Points to the Id column of row 5.
- Missing value: Points to the City column of row 2.
- Invalid value: Points to the Gender column of row 5.
- Value that should be in another column: Points to the Country column of row 7.
- Misspelling: Points to the Name column of row 10.
- Incorrect format: Points to the Birthday column of row 6.
- Attribute dependency: Points to the IsTeacher column of row 9.

Data Conversion

- After being preprocessed, the data needs to be converted into a representation form suitable for the machine learning model. Common data conversion forms include the following:
 - With respect to classification, category data is encoded into a corresponding numerical representation.
 - Value data is converted to category data to reduce the value of variables (for age segmentation).
 - Other data
 - In the text, the word is converted into a word vector through word embedding (generally using the word2vec model, BERT model, etc).
 - Process image data (color space, grayscale, geometric change, Haar feature, and image enhancement)
 - Feature engineering
 - Normalize features to ensure the same value ranges for input variables of the same model.
 - Feature expansion: Combine or convert existing variables to generate new features, such as the average.

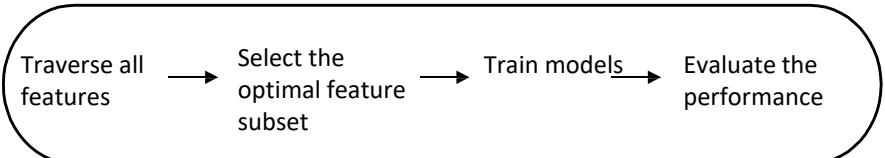
Necessity of Feature Selection

- Generally, a dataset has many features, some of which may be redundant or irrelevant to the value to be predicted.
- Feature selection is necessary in the following aspects



Feature Selection Methods - Filter

- Filter methods are independent of the model during feature selection.



Procedure of a filter method

By evaluating the correlation between each feature and the target attribute, these methods use a statistical measure to assign a value to each feature. Features are then sorted by score, which is helpful for preserving or eliminating specific features.

Common methods

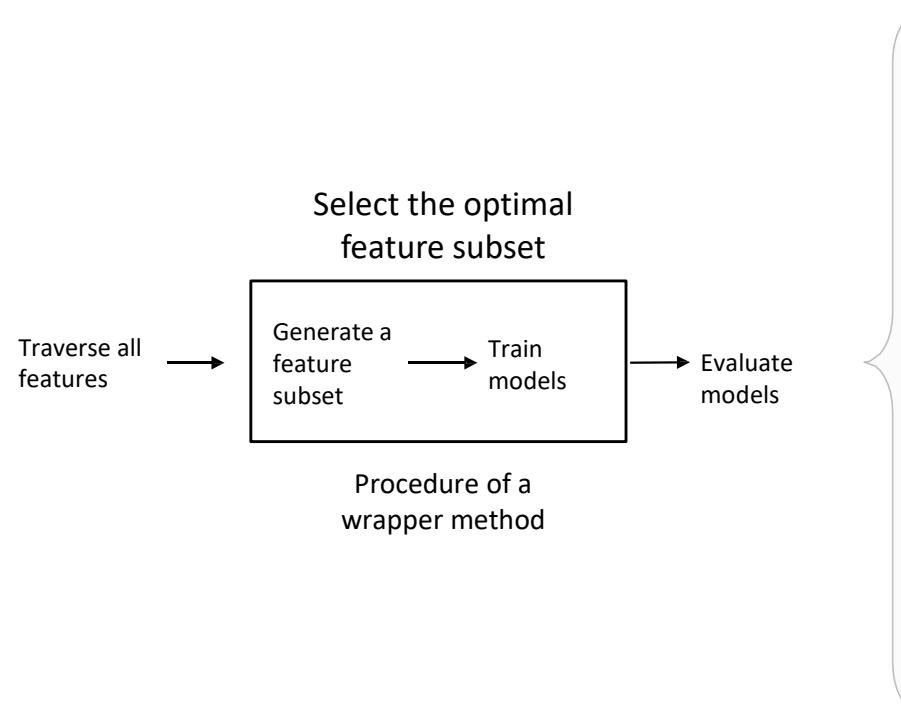
- Pearson correlation coefficient
- Chi-square coefficient
- Mutual information

Limitations

- The filter method tends to select redundant variables as the relationship between features is not considered.

Feature Selection Methods - Wrapper

- Wrapper methods use a prediction model to score feature subsets.



Wrapper methods consider feature selection as a search issue for which different combinations are evaluated and compared. A predictive model is used to evaluate a combination of features and assign a score based on model accuracy.

Common methods

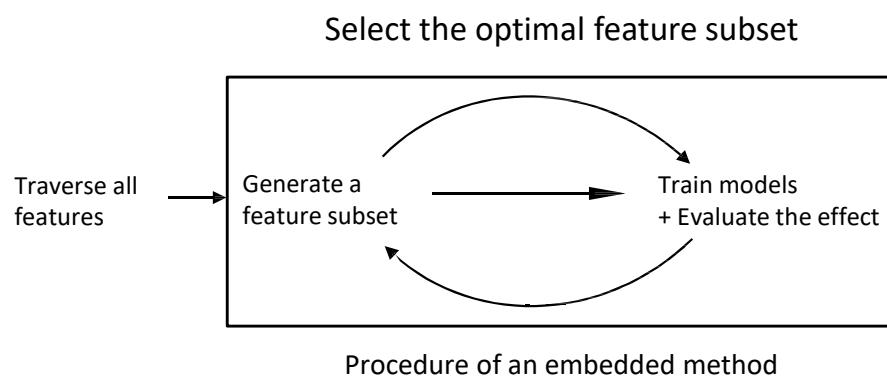
- Recursive feature elimination (RFE)

Limitations

- Wrapper methods train a new model for each subset, resulting in **a huge number of computations**.
- A feature set with the best performance is usually provided for a specific type of model.

Feature Selection Methods -

- Embedded methods consider feature selection as a part of model construction.



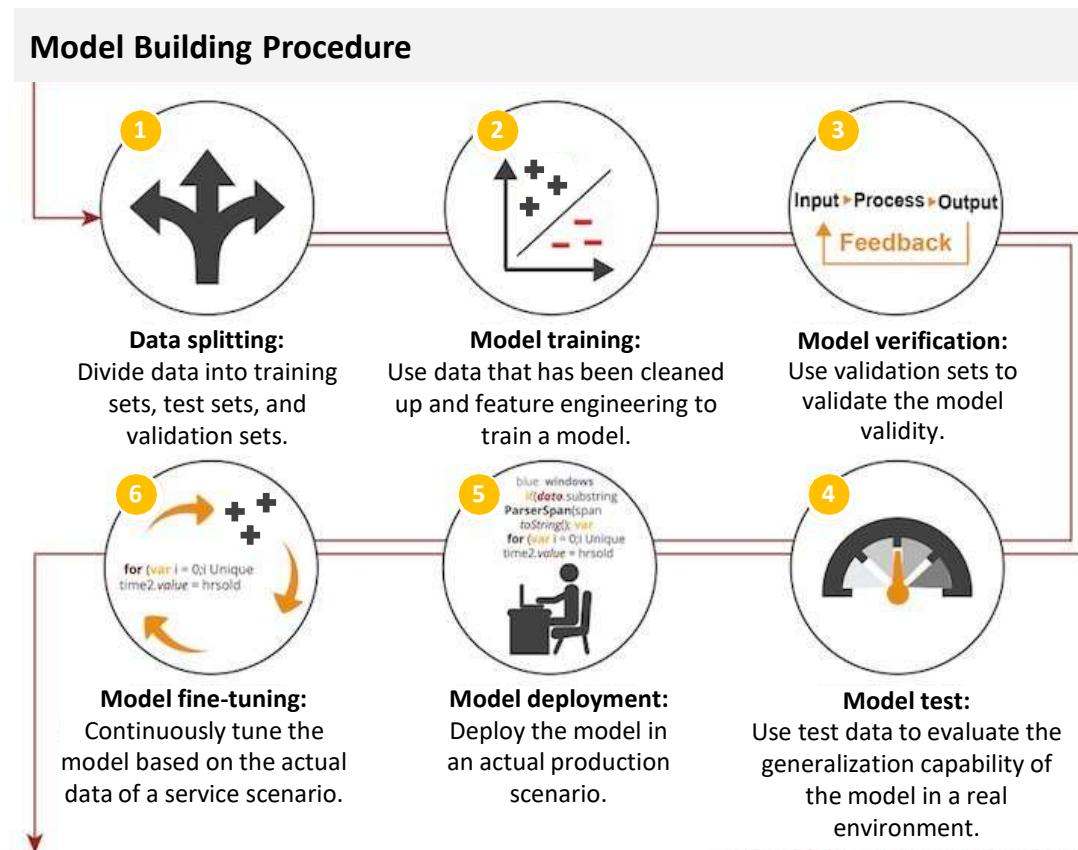
The most common type of embedded feature selection method is the **regularization method**.

Regularization methods are also called penalization methods that introduce additional constraints into the optimization of a predictive algorithm that bias the model toward lower complexity and reduce the number of features.

Common methods

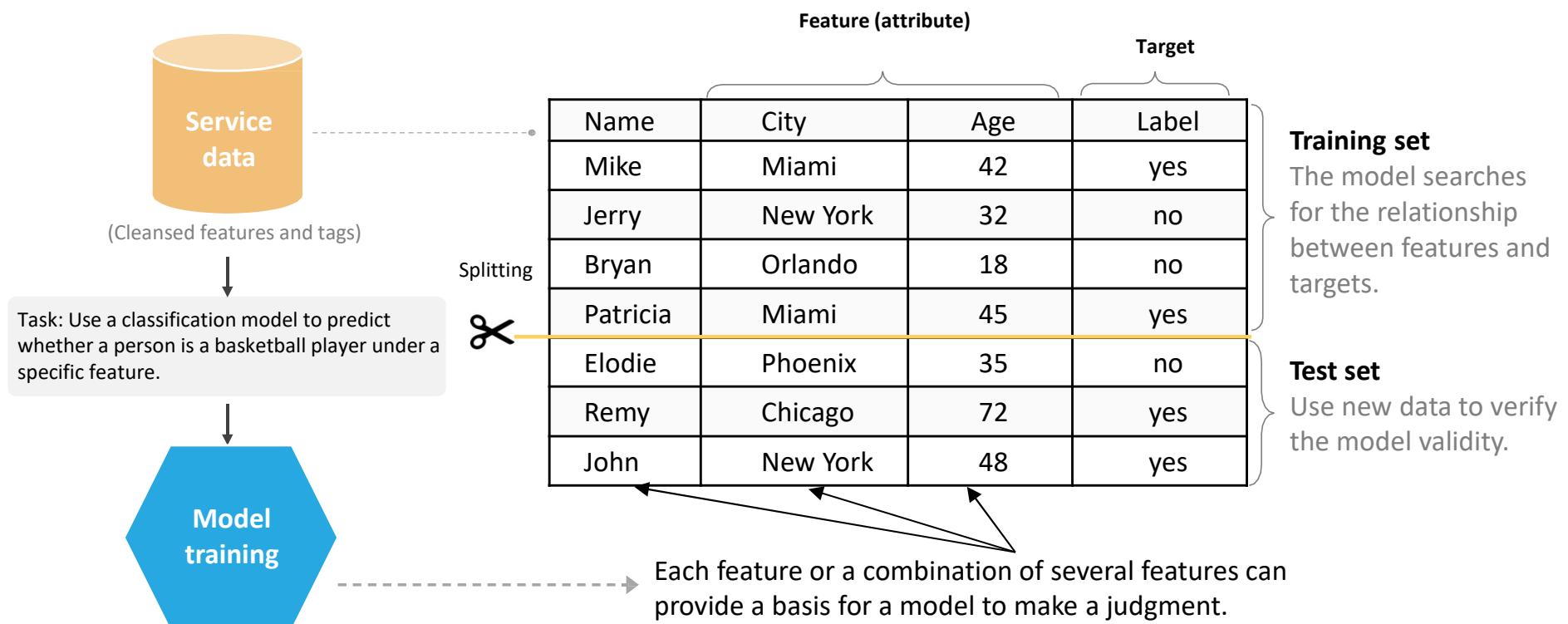
- Lasso regression
- Ridge regression

Overall Procedure of Building a Model

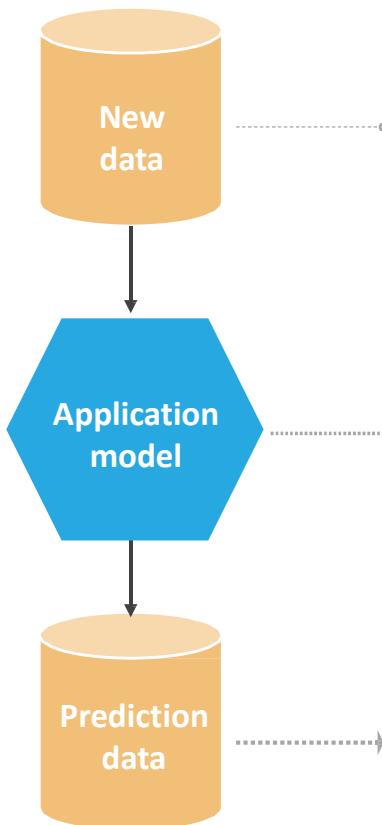


Examples of Supervised Learning -

- Use the ~~classificationPhase~~ to predict whether a person is a basketball player.



Examples of Supervised Learning - Prediction Phase



Name	City	Age	Label
Marine	Miami	45	?
Julien	Miami	52	?
Fred	Orlando	20	?
Michelle	Boston	34	?
Nicolas	Phoenix	90	?

Unknown data

Recent data, it is not known whether the people are basketball players.

IF city = Miami → Probability = +0.7
IF city= Orlando → Probability = +0.2
IF age > 42 → Probability = +0.05*age + 0.06
IF age ≤ 42 → Probability = +0.01*age + 0.02

Name	City	Age	Prediction
Marine	Miami	45	0.3
Julien	Miami	52	0.9
Fred	Orlando	20	0.6
Michelle	Boston	34	0.5
Nicolas	Phoenix	90	0.4

Possibility prediction

Apply the model to the new data to predict whether the customer will change the supplier.

What Is a Good Model?



- **Generalization capability**
Can it accurately predict the actual service data?
- **Interpretability**
Is the prediction result easy to interpret?
- **Prediction speed**
How long does it take to predict each piece of data?
- **Practicability**
Is the prediction rate still acceptable when the service volume increases with a huge data volume?

Model Validity (1)

- Generalization capability: The goal of machine learning is that the model obtained after learning should perform well on new samples, not just on samples used for training. The capability of applying a model to new samples is called generalization or robustness.
- Error: difference between the sample result predicted by the model obtained after learning and the actual sample result.
 - Training error: error that you get when you run the model on the training data.
 - Generalization error: error that you get when you run the model on new samples. Obviously, we prefer a model with a smaller generalization error.
- Underfitting: occurs when the model or the algorithm does not fit the data well enough.
- Overfitting: occurs when the training error of the model obtained after learning is small but the generalization error is large (poor generalization capability).

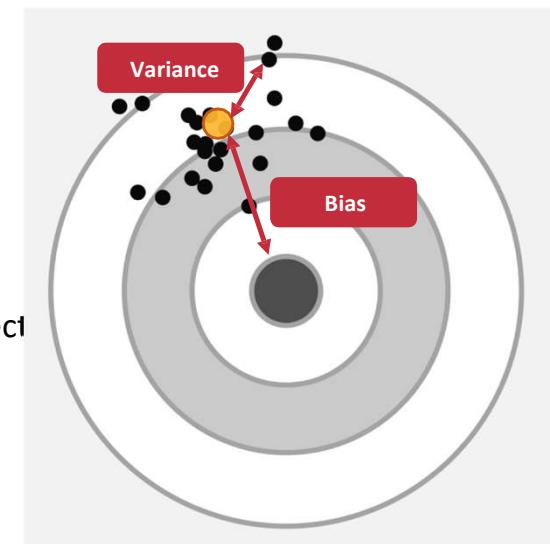
Model Validity (2)

- Model capacity: model's capability of fitting functions, which is also called model complexity.
 - When the capacity suits the task complexity and the amount of training data provided, the algorithm effect is usually optimal.
 - Models with insufficient capacity cannot solve complex tasks and underfitting may occur.
 - A high-capacity model can solve complex tasks, but overfitting may occur if the capacity is higher than that required by a task.



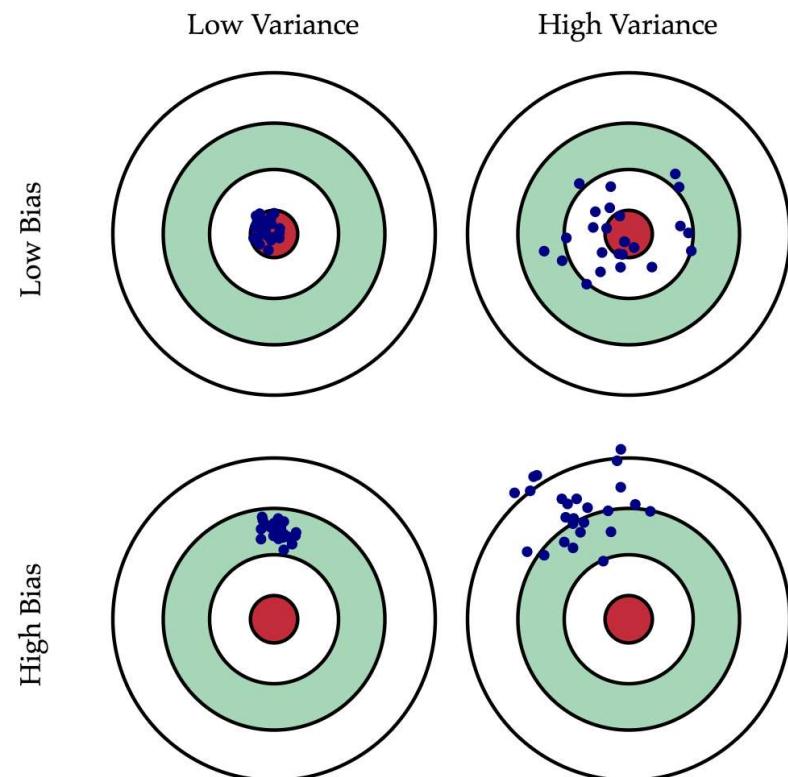
Overfitting Cause – Error

- Total error of final prediction = Bias² + Variance + Irreducible error
- Generally, the prediction error can be divided into two types:
 - Error caused by "bias"
 - Error caused by "variance"
- Variance:
 - Offset of the prediction result from the average value
 - Error caused by the model's sensitivity to small fluctuations in the training set
- Bias:
 - Difference between the expected (or average) prediction value and the correct value we are trying to predict.



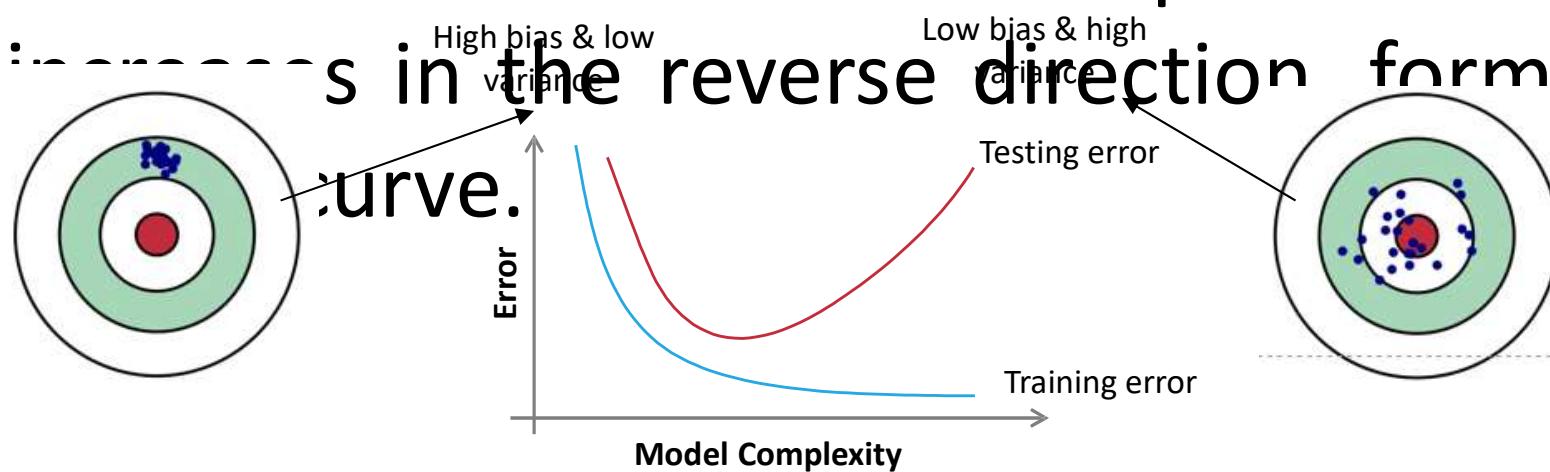
Variance and Bias

- Combinations of variance and bias are as follows:
 - Low bias & low variance → Good model
 - Low bias & high variance
 - High bias & low variance
 - High bias & high variance → Poor model
- Ideally, we want a model that can accurately capture the rules in the training data and summarize the invisible data (new data). However, it is usually impossible for the model to complete both tasks at the same time.



Model Complexity and Error

- As the model complexity increases, the training error decreases.
- As the model complexity increases, the test error decreases to a certain point and then increases in the reverse direction forming a curve.



Machine Learning Performance

- The closer the Mean Absolute Error (MAE) is to 0, the better the model can fit the training data.

Evaluation - Regression

$$MAE = \frac{1}{m} \sum_{i=1}^m |y_i - \hat{y}_i|$$

- Mean Square Error (MSE)

$$MSE = \frac{1}{m} \sum_{i=1}^m (y_i - \hat{y}_i)^2$$

- The value range of R^2 is $(-\infty, 1]$. A larger value indicates that the model can better fit the training data. TSS indicates the difference between samples. RSS indicates the difference between the predicted value and sample value.

$$R^2 = 1 - \frac{RSS}{TSS} = 1 - \frac{\sum_{i=1}^m (y_i - \hat{y}_i)^2}{\sum_{i=1}^m (y_i - \bar{y}_i)^2}$$

Machine Learning Performance Evaluation - Classification (1)

- Terms and definitions:
 - P : positive, indicating the number of real positive cases in the data.
 - N : negative, indicating the number of real negative cases in the data.
 - TP : true positive, indicating the number of positive cases that are correctly classified by the classifier.
 - TN : true negative, indicating the number of negative cases that are correctly classified by the classifier.
 - FP : false positive, indicating the number of positive cases that are incorrectly classified by the classifier.
 - FN : false negative, indicating the number of negative cases that are incorrectly classified by the classifier.
- Confusion matrix: at least an $m \times m$ table. $CM_{i,j}$ of the first m rows and m columns indicates the number of cases that actually belong to class i but are classified into class j by the classifier.
 - Ideally, for a high accuracy classifier, most prediction values should be located in the diagonal from $CM_{1,1}$ to $CM_{m,m}$ of the table while values outside the diagonal are 0 or close to 0. That is, FP and FN are close to 0.

Estimated amount		yes	no	Total
Actual amount	yes	TP	FN	P
no	FP	TN	N	Total

Confusion matrix

Machine Learning Performance Evaluation - Classification (2)

Measurement	Ratio
Accuracy and recognition rate	$\frac{TP + TN}{P + N}$
Error rate and misclassification rate	$\frac{FP + FN}{P + N}$
Sensitivity, true positive rate, and recall	$\frac{TP}{P}$
Specificity and true negative rate	$\frac{TN}{N}$
Precision	$\frac{TP}{TP + FP}$
F_1 , harmonic mean of the recall rate and precision	$\frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$
F_β , where β is a non-negative real number	$\frac{(1 + \beta^2) \times \text{precision} \times \text{recall}}{\beta^2 \times \text{precision} + \text{recall}}$

Example of Machine Learning Performance Evaluation

- We have trained a machine learning model to identify whether the object in an image is a cat. Now we use 200 pictures to verify the model performance. Among the 200 images, objects in 170 images are cats, while others are not. The identification result of the model is that objects in 160 images are cats, while others are not.

Precision: $P = \frac{TP}{TP+FP} = \frac{140}{140+20} = 87.5\%$

Recall: $R = \frac{TP}{P} = \frac{140}{170} = 82.4\%$

Accuracy: $ACC = \frac{TP+TN}{P+N} = \frac{140+30}{170+30} = 75\%$

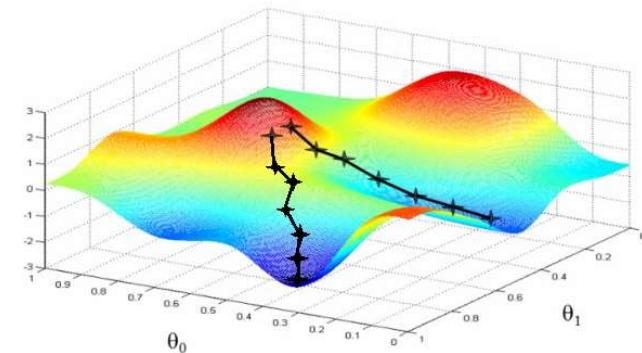
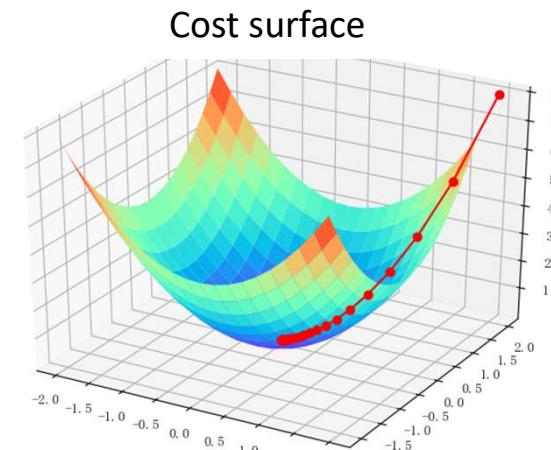
Actual amount Estimated amount	yes	no	Total
yes	140	30	170
no	20	10	30
Total	160	40	200

Contents

1. Machine Learning Definition
2. Machine Learning Types
3. Machine Learning Process
- 4. Other Key Machine Learning Methods**
5. Common Machine Learning Algorithms
6. Case study

Machine Learning Training Method - Gradient Descent (1)

- The gradient descent method uses the negative gradient direction of the current position as the search direction, which is the steepest direction. The formula is as follows:
- In the formula, η indicates the learning rate and i indicates the data record number. The weight parameter w indicates the change in each iteration.
- Convergence: The value of the objective function changes very little, or the maximum number of iterations is reached.

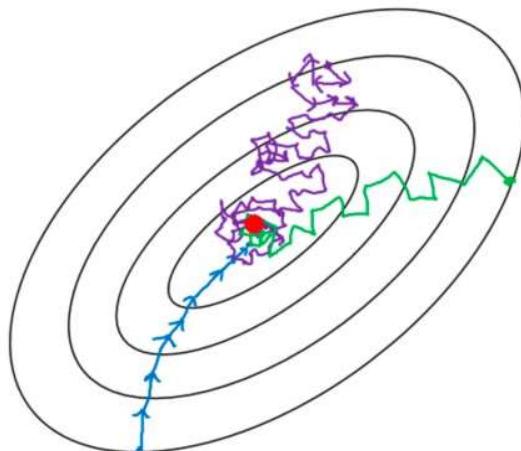


Machine Learning Training Method -

- Batch Gradient Descent (BGD) uses all samples (m in total) in all datasets to update the weight parameter based on the gradient value at the current point.
$$w_{k+1} = w_k - \eta \frac{1}{m} \sum_{i=1}^m \nabla f_{w_k}(x^i)$$
- Stochastic Gradient Descent (SGD) randomly selects a sample in a dataset to update the weight parameter based on the gradient value at the current point.
$$w_{k+1} = w_k - \eta \nabla f_{w_k}(x)$$
- Mini-Batch Gradient Descent (MBGD) combines the features of BGD and SGD and selects the gradients of n samples in a dataset to update the weight parameter.
$$w_{k+1} = w_k - \eta \frac{1}{n} \sum_{i=1}^{n+1} \nabla f_{w_k}(x')$$

Machine Learning Training Method - Gradient Descent (3)

- Comparison of three gradient descent methods
 - In the SGD, samples selected for each training are stochastic. Such instability causes the loss function to be unstable or even causes reverse displacement when the loss function decreases to the lowest point.
 - BGD has the highest stability but consumes too many computing resources. MBGD is a method that balances SGD and BGD.



BGD

Uses **all** training samples for training each time.

SGD

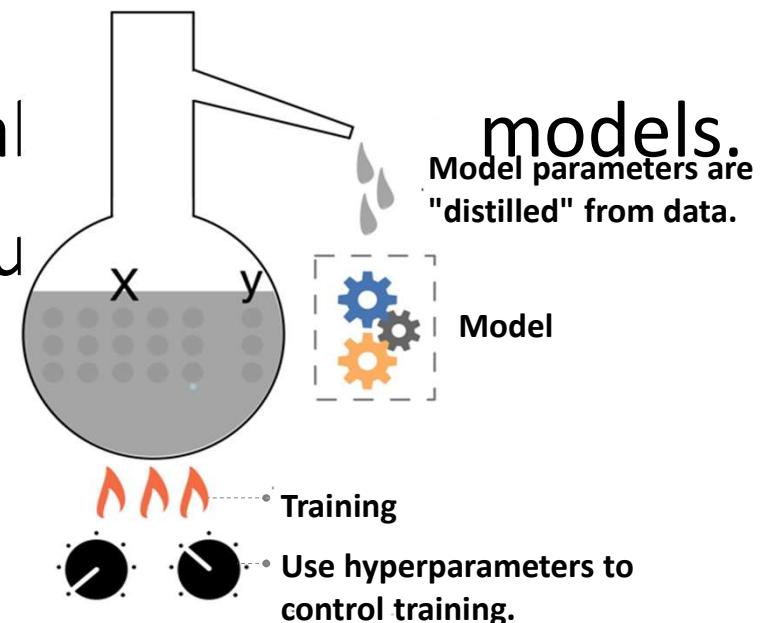
Uses **one** training sample for training each time.

MBGD

Uses a certain number of training samples for training each time.

Parameters and Hyperparameters in

- The model contains ~~Model~~ only parameters but also hyperparameters. The purpose is to enable the model to learn the optimal parameters.
 - Parameters are automatical
 - Hyperparameters are manu



Hyperparameters of a Model

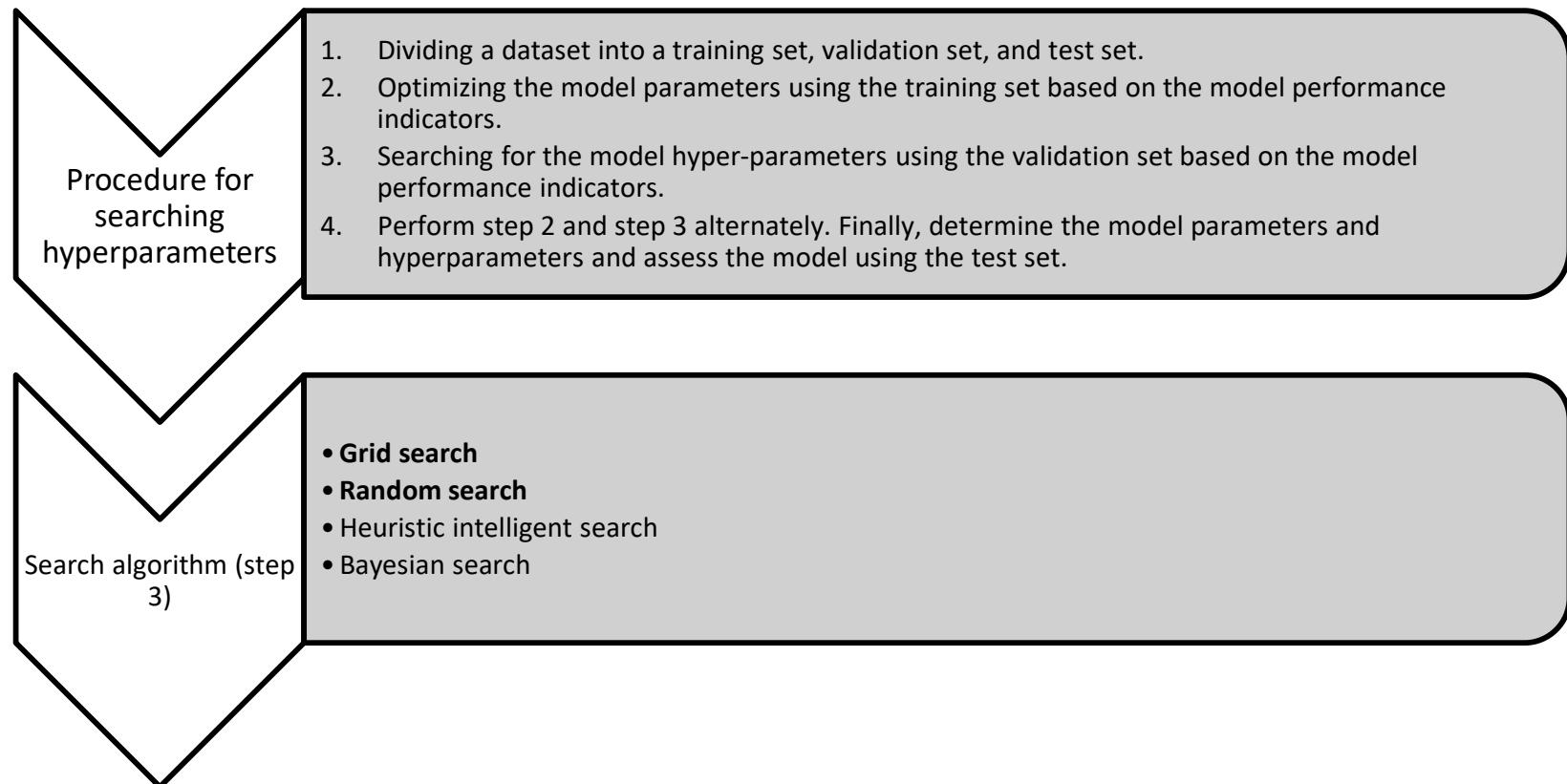
- Often used in model parameter estimation processes.
- Often specified by the practitioner.
- Can often be set using heuristics.
- Often tuned for a given predictive modeling problem.

Model hyperparameters are external configurations of models.

- λ during Lasso/Ridge regression
- Learning rate for training a neural network, number of iterations, batch size, activation function, and number of neurons
- C and σ in support vector machines (SVM)
- K in k-nearest neighbor (KNN)
- Number of trees in a random forest

Common model hyperparameters

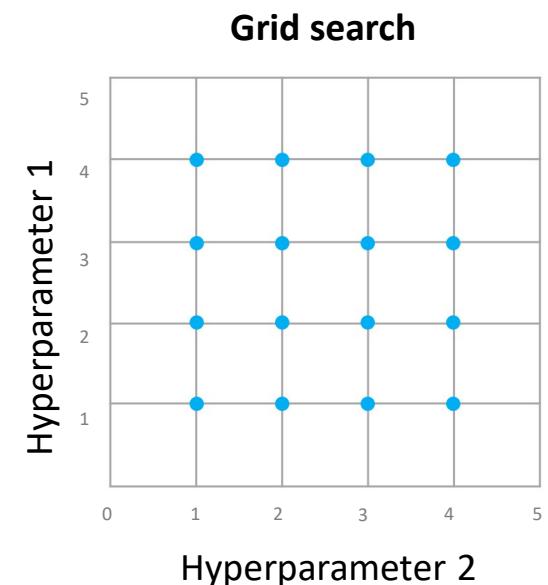
Hyperparameter Search Procedure and Method



Hyperparameter Searching Method

- Grid Search

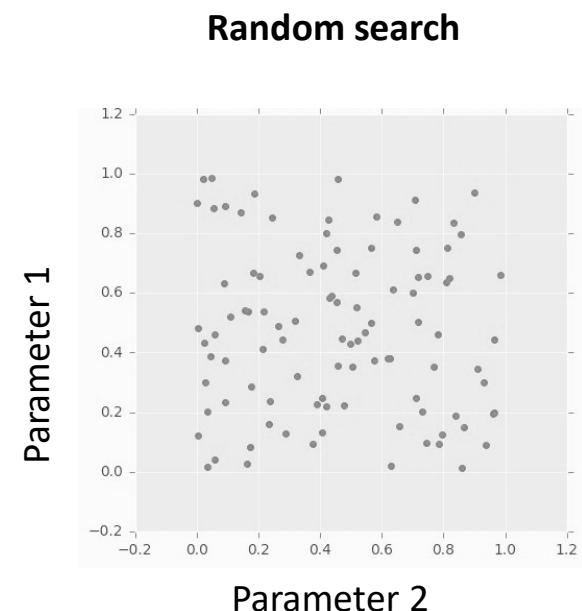
- Grid search attempts to **exhaustively search** all possible hyperparameter combinations to form a hyperparameter value grid.
- In practice, the range of hyperparameter values to search is specified manually.
- Grid search is an expensive and time-consuming method.
 - This method works well when the number of hyperparameters is relatively small. Therefore, it is applicable to generally machine learning algorithms but inapplicable to neural networks (see the deep learning part).



Hyperparameter Searching Method

- Random Search

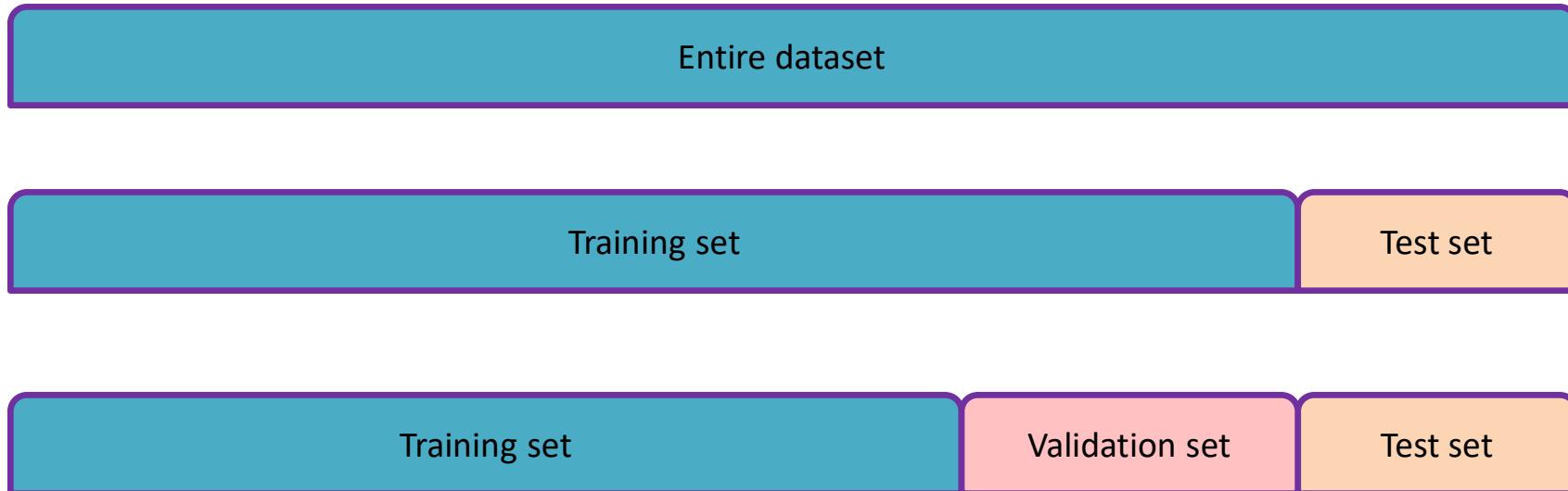
- When the hyperparameter search space is large, **random search** is better than grid search.
- In random search, each setting is sampled from the distribution of possible parameter values, in an attempt to find the best subset of hyperparameters.
- Note:
 - Search is performed within a coarse range, which then will be narrowed based on where the best result appears.
 - Some hyperparameters are more important than others, and the search deviation will be affected during random search.



Cross Validation (1)

- **Cross validation:** It is a statistical analysis method used to validate the performance of a classifier. The basic idea is to divide the original dataset into two parts: training set and validation set. Train the classifier using the training set and test the model using the validation set to check the classifier performance.
- **k-fold cross validation ($K - CV$):**
 - Divide the raw data into k groups (generally, evenly divided).
 - Use each subset as a validation set, and use the other $k - 1$ subsets as the training set. A total of k models can be obtained.
 - Use the mean classification accuracy of the final validation sets of k models as the performance indicator of the $K - CV$ classifier.

Cross Validation (2)

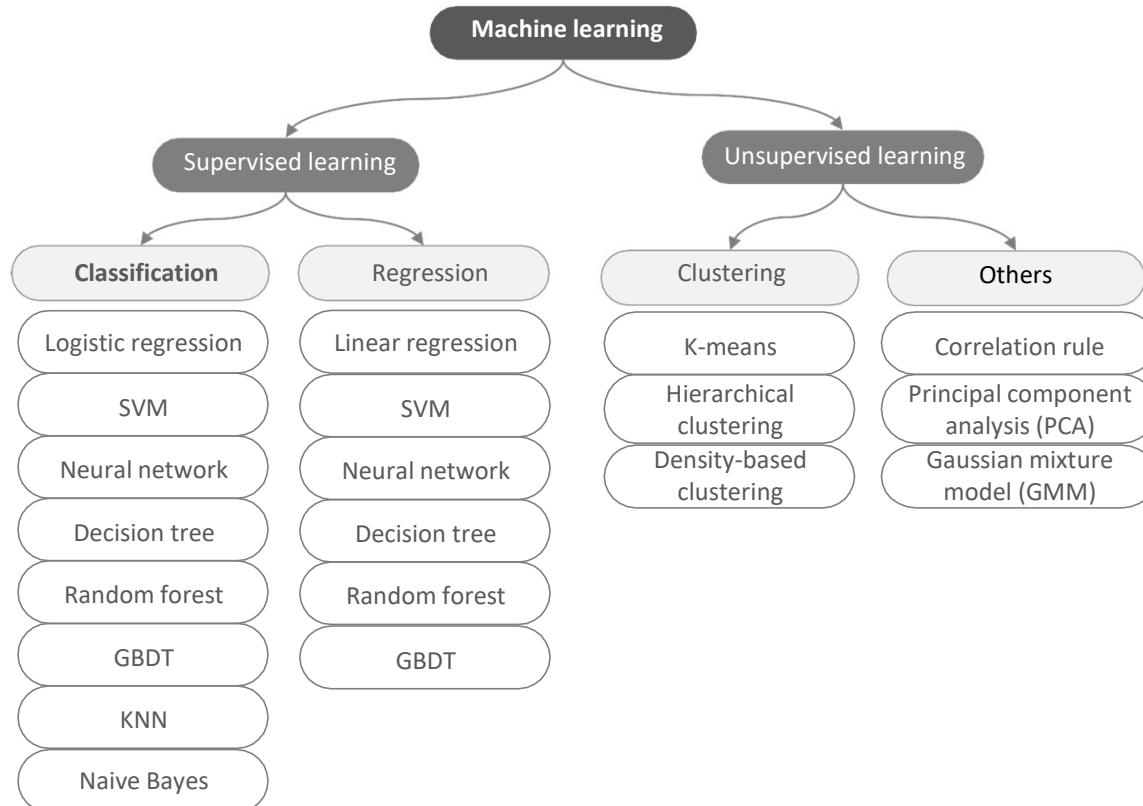


- Note: The K value in K-fold cross validation is also a hyperparameter.

Contents

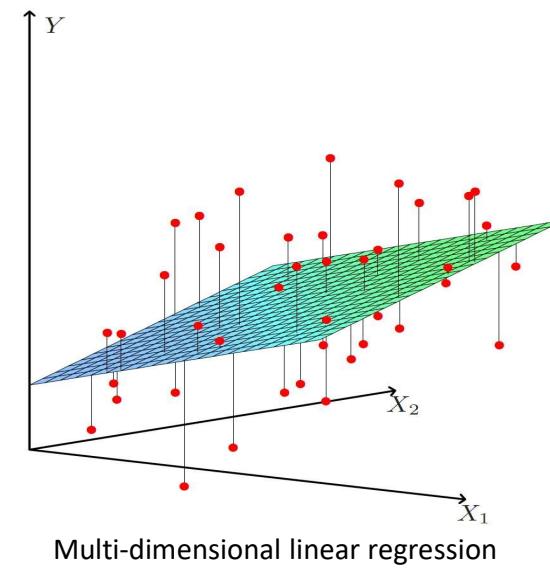
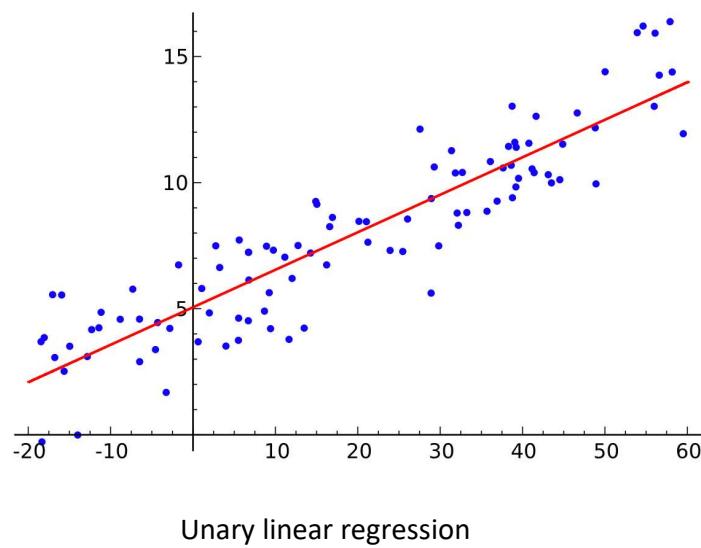
1. Machine Learning Definition
2. Machine Learning Types
3. Machine Learning Process
4. Other Key Machine Learning Methods
- 5. Common Machine Learning Algorithms**
6. Case study

Machine Learning Algorithm Overview



Linear Regression (1)

- Linear regression: a statistical analysis method to determine the quantitative relationships between two or more variables through regression analysis in mathematical statistics.
- Linear regression is a type of supervised learning.



Linear Regression (2)

- The model function of linear regression is as follows, where w indicates the weight parameter, b indicates the bias, and x indicates the sample attribute.
- The relationship between the value predicted by the model and actual value is as follows, where y indicates the actual value, and ε indicates the error.
- The error ε is influenced by many factors independently. According to the central limit theorem, the error ε follows normal distribution. According to the normal distribution function and maximum likelihood estimation, the loss function of linear regression is as follows:
- To make the predicted value close to the actual value, we need to minimize the loss value. We can use the gradient descent method to calculate the weight parameter w when the loss function reaches the minimum, and then complete model building.

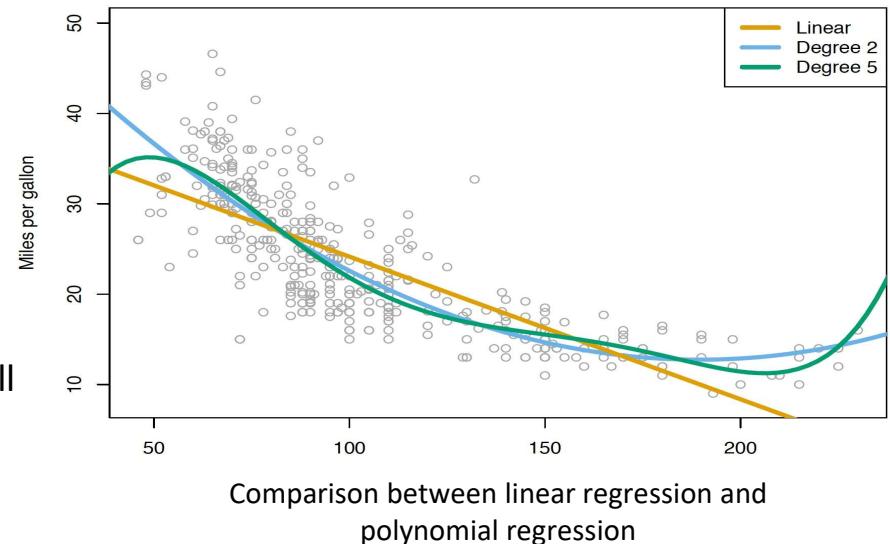
$$J(w) = \frac{1}{2m} \sum (h_w(x) - y)^2$$

Linear Regression Extension -

- Polynomial regression is an extension of linear regression. Generally, the complexity of a dataset exceeds the possibility of fitting by a straight line. That is, obvious underfitting occurs if the original linear regression model is used. The solution is to use polynomial regression.

$$h_w(x) = w_1x + w_2x^2 + \dots + w_nx^n + b$$

- where, the nth power is a polynomial regression dimension (degree).
- Polynomial regression belongs to linear regression as the relationship between its weight parameters w is still linear while its nonlinearity is reflected in the feature dimension.



Linear Regression and Overfitting

- Regularization terms can be used to reduce overfitting. The value of w cannot be too large or too small in the sample space. You can add a square sum loss to the target function.
- Regularization terms (norm): The regularization term here is called L2-norm. Linear regression that uses this loss function is also called Ridge regression.

$$J(w) = \frac{1}{2m} \sum (h_w(x) - y)^2 + \lambda \sum \|w\|_2^2$$

- Linear regression with absolute ~~loss~~ is called Lasso regression.

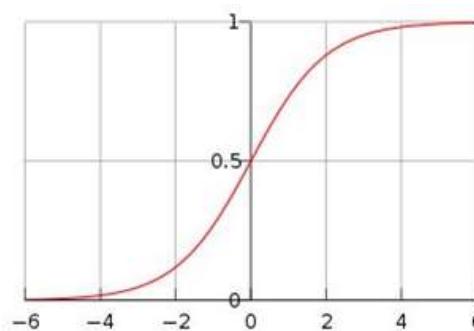
$$J(w) = \frac{1}{2m} \sum (h_w(x) - y)^2 + \lambda \sum \|w\|_1$$

Logistic Regression (1)

- Logistic regression: The logistic regression model is used to solve classification problems. The model is defined as follows:

$$P(Y = 1|x) = \frac{e^{wx+b}}{1 + e^{wx+b}}$$
$$P(Y = 0|x) = \frac{1}{1 + e^{wx+b}}$$

where w indicates the weight, b indicates the bias, and $wx + b$ is regarded as the linear function of x . Compare the preceding two probability values. The class with a higher probability value is the class of x .



Logistic Regression (2)

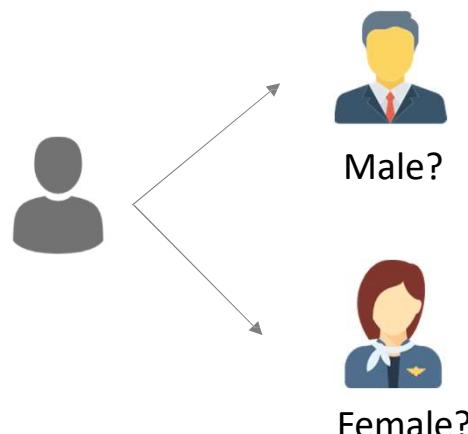
- Both the logistic regression model and linear regression model are generalized linear models. Logistic regression introduces nonlinear factors (the sigmoid function) based on linear regression and sets thresholds, so it can deal with binary classification problems.
- According to the model function of logistic regression, the loss function of logistic regression can be estimated as follows by using the maximum likelihood estimation:
- where w indicates the weight parameter, m indicates the number of samples, x indicates the sample, and y indicates the real value. The values of all the weight parameters w can also be obtained through the gradient descent algorithm.

$$J(w) = -\frac{1}{m} \sum (y \ln h_w(x) + (1-y) \ln(1-h_w(x)))$$

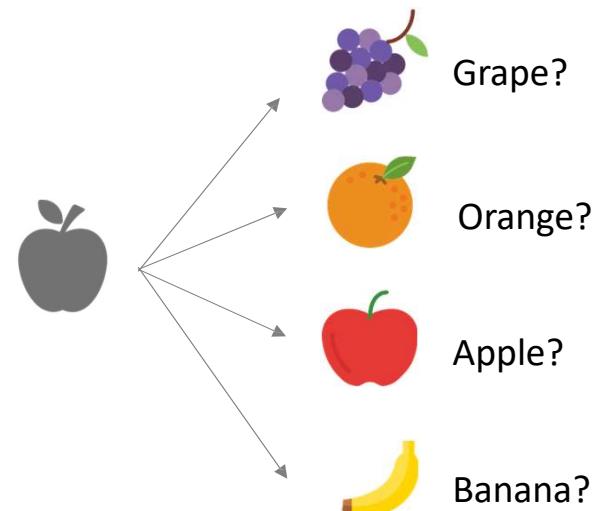
Logistic Regression Extension -

- Logistic ~~Sigmoid Function~~ ~~Classification Function~~ to binary classification problems. For multi-class classification problems, use the Softmax function.

Binary classification problem



Multi-class classification problem



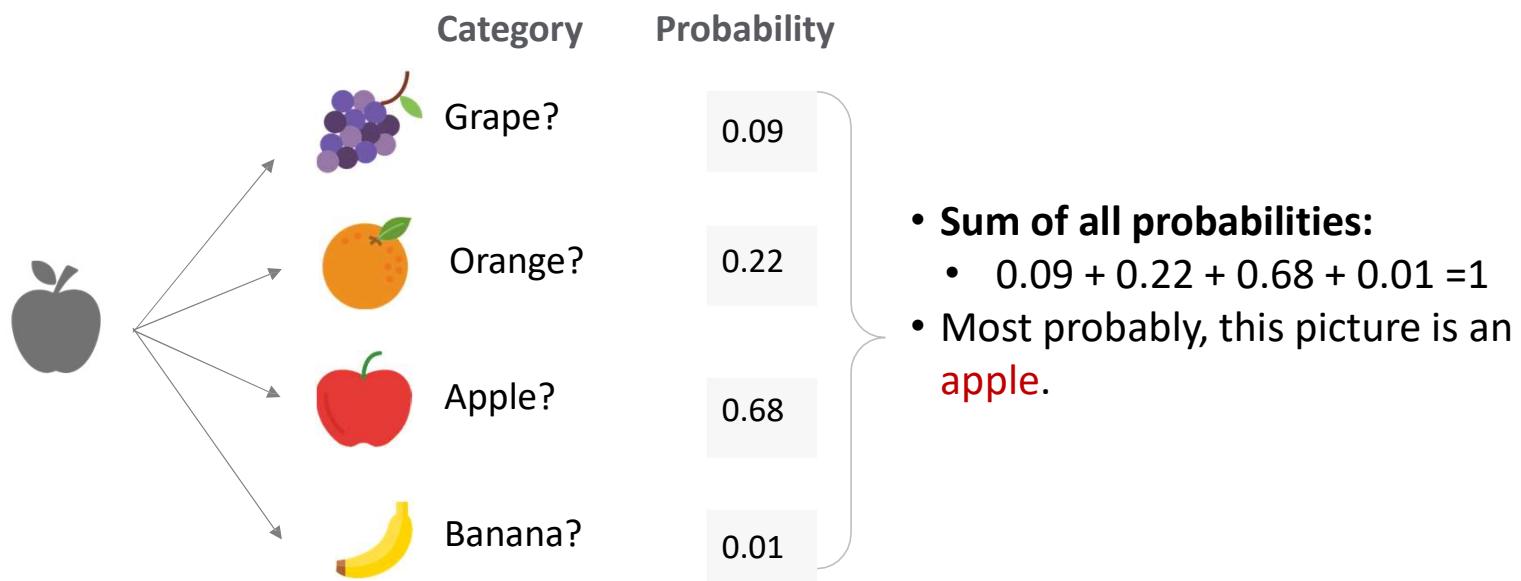
Logistic Regression Extension -

- Softmax ~~Softmax Function is a generalization of~~ logistic regression that we can use for K-class classification.
- The Softmax function is used to map a K-dimensional vector of arbitrary real values to another K-dimensional vector of real values, where each vector element is in the interval $(0, 1)$.
$$p(y = k | x; w) = \frac{e^{w_k^T x}}{\sum_{l=1}^K e^{w_l^T x}}, k = 1, 2, \dots, K$$
- The probability function of Softmax is as follows:

Logistic Regression Extension -

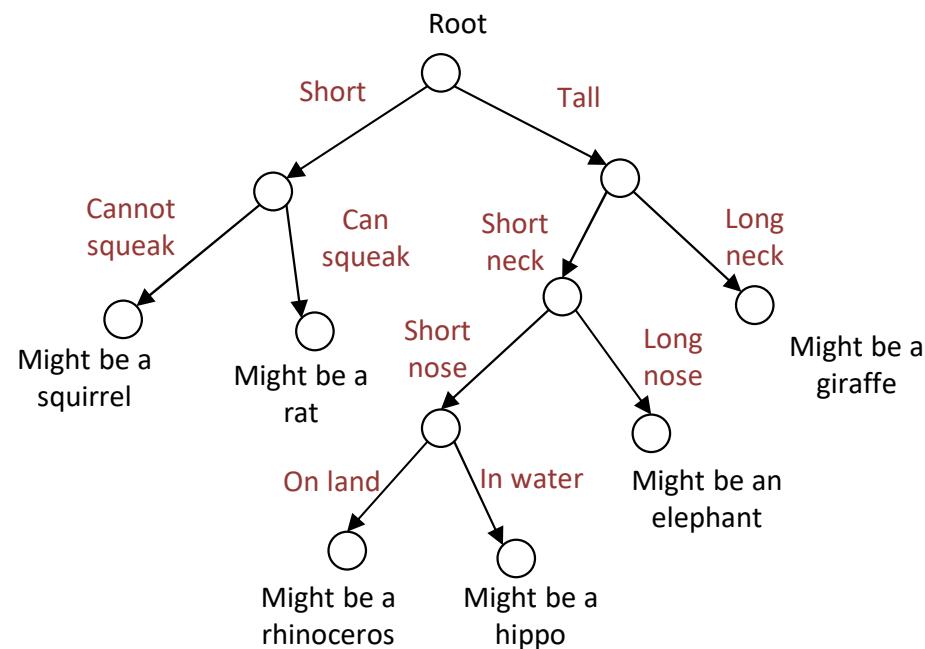
- Softmax assigns a probability to each class in a multi-class problem. These probabilities must add up to 1.
 - Softmax may produce a form belonging to a particular class. Example:

Softmax Function (3)

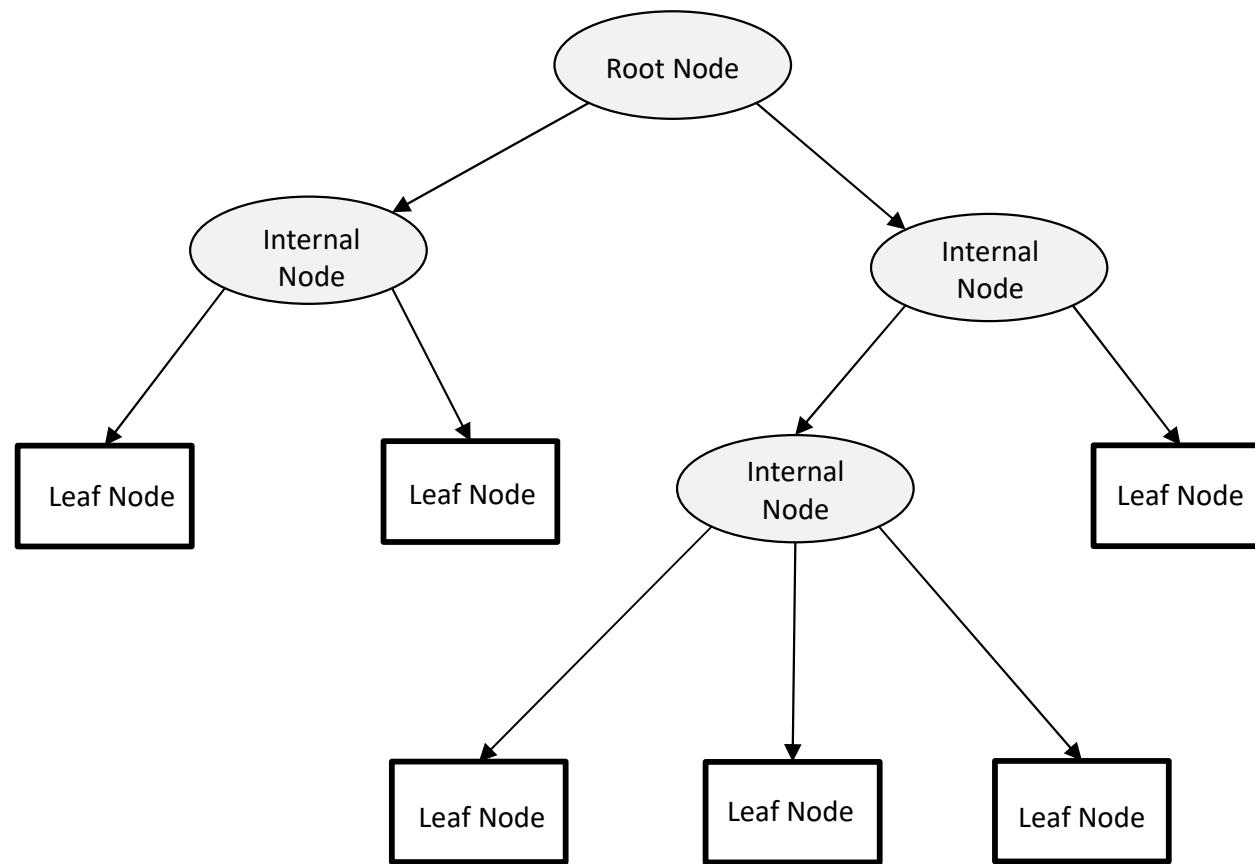


Decision Tree

- A decision tree is a tree structure (a binary tree or a non-binary tree). Each non-leaf node represents a test on a feature attribute. Each branch represents the output of a feature attribute in a certain value range, and each leaf node stores a category. To use the decision tree, start from the root node, test the feature attributes of the items to be classified, select the output branches, and use the category stored on the leaf node as the final result.



Decision Tree Structure



Key Points of Decision Tree

- To create a decision tree, we need to select attributes and determine the tree structure between feature attributes. The key step of constructing a decision tree is to divide data of all feature attributes, compare the result sets in terms of 'purity', and select the attribute with the highest 'purity' as the data point for dataset division.
- The metrics to quantify the 'purity' include the information entropy and GINI Index. The formula is as follows:
- where p_k indicates the probability that the sample belongs to class k (there are K classes in total). A greater difference between purity before segmentation and that after segmentation indicates a better decision tree.
- Common decision tree algorithms include ID3, C4.5, and CART.

$$H(X) = -\sum_{k=1}^K p_k \log_2(p_k) \quad Gini = 1 - \sum_{k=1}^K p_k^2$$

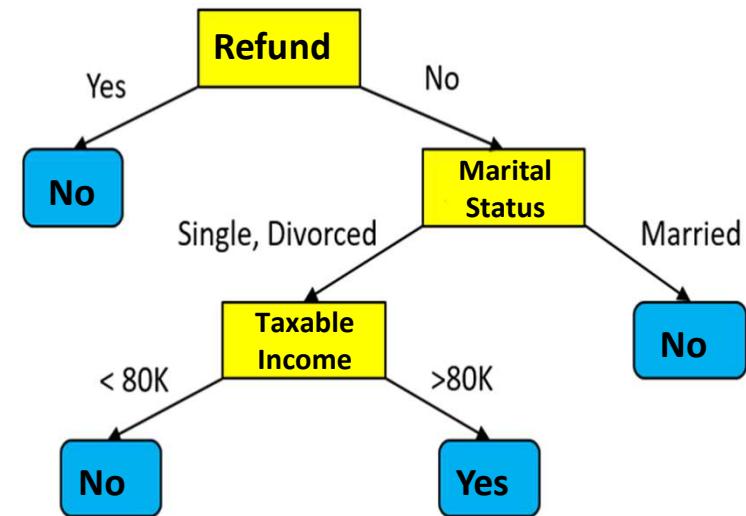
Decision Tree Construction Process

- **Feature selection:** Select a feature from the features of the training data as the split standard of the current node. (Different standards generate different decision tree algorithms.)
- **Decision tree generation:** Generate internal node upside down based on the selected features and stop until the dataset can no longer be split.
- **Pruning:** The decision tree may easily become overfitting unless necessary pruning (including pre-pruning and post-pruning) is performed to reduce the tree size and optimize its node structure.

Decision Tree Example

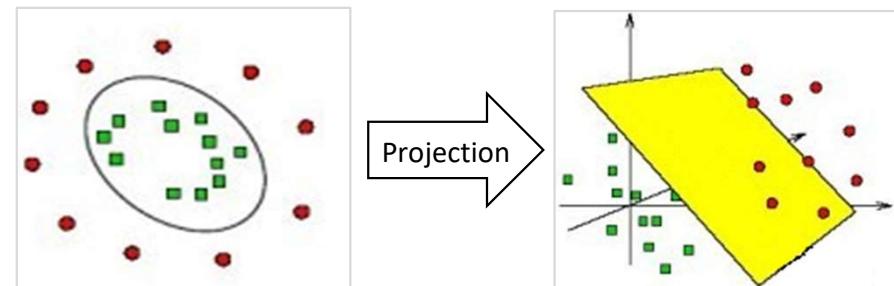
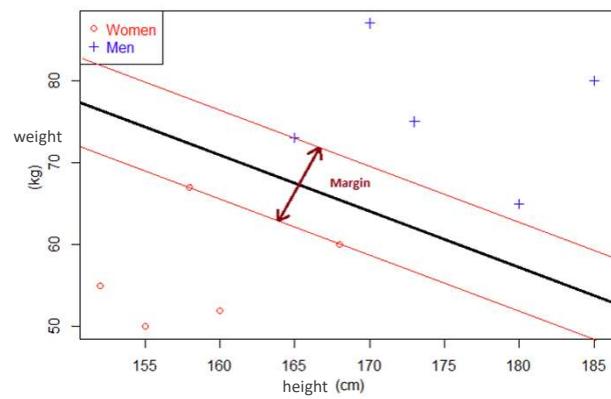
- The following figure shows a classification when a decision tree is used. The classification result is impacted by three attributes: Refund, Marital Status, and Taxable Income.

Tid	Refund	Marital Status	Taxable Income	Cheat
1	Yes	Single	125,000	No
2	No	Married	100,000	No
3	No	Single	70,000	No
4	Yes	Married	120,000	No
5	No	Divorced	95,000	Yes
6	No	Married	60,000	No
7	Yes	Divorced	220,000	No
8	No	Single	85,000	Yes
9	No	Married	75,000	No
10	No	Single	90,000	Yes



SVM

- SVM is a binary classification model whose basic model is a linear classifier defined in the eigenspace with the largest interval. SVMs also include kernel tricks that make them nonlinear classifiers. The SVM learning algorithm is the optimal solution to convex quadratic programming.

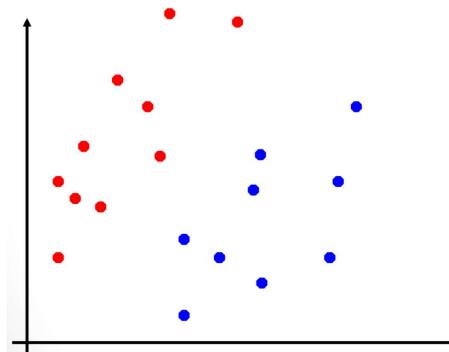


Complex segmentation
in low-dimensional
space

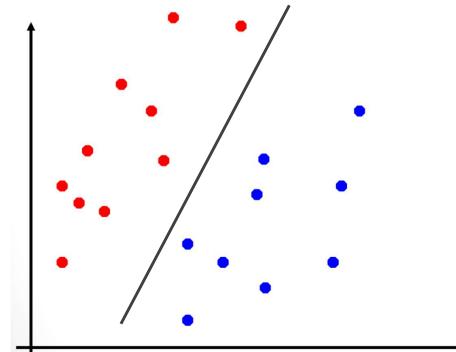
Easy segmentation in
high-dimensional space

Linear SVM (1)

- How do we split the red and blue datasets by a straight line?

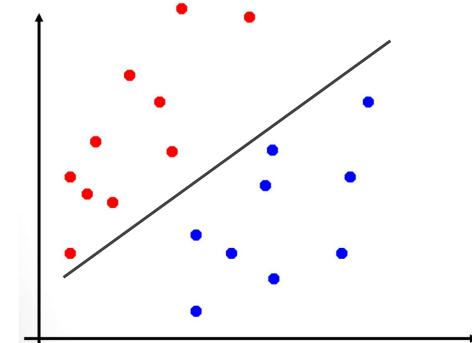


With binary classification
Two-dimensional dataset



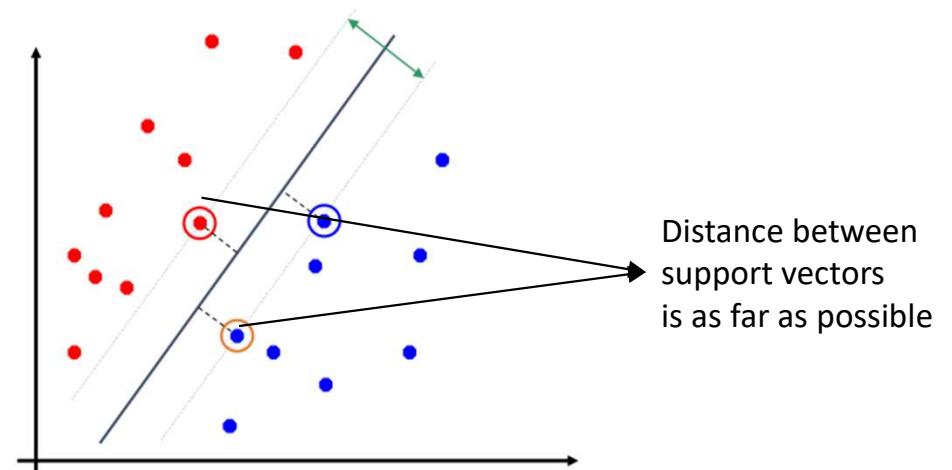
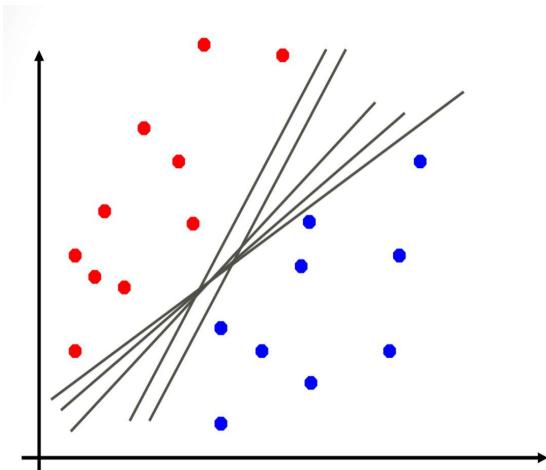
Both the left and right methods can be used to divide datasets. Which of them is correct?

or



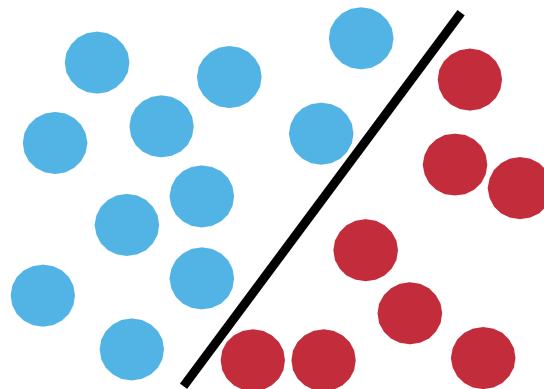
Linear SVM (2)

- Straight lines are used to divide data into different classes. Actually, we can use multiple straight lines to divide data. The core idea of the SVM is to find a straight line and keep the point close to the straight line as **far** as possible from the straight line. This can enable strong generalization capability of the model. These points are called **support vectors**.
- In two-dimensional space, we use straight lines for segmentation. In high-dimensional space, we use **hyperplanes** for segmentation.

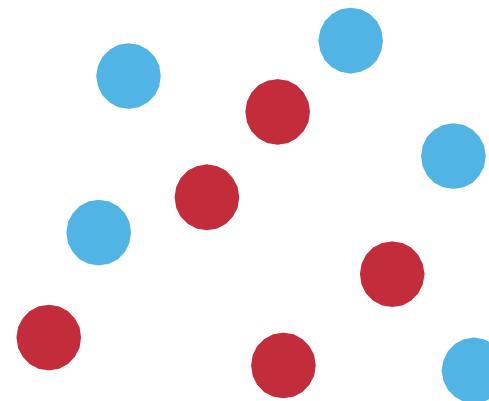


Nonlinear SVM (1)

- How do we classify a nonlinear separable dataset?



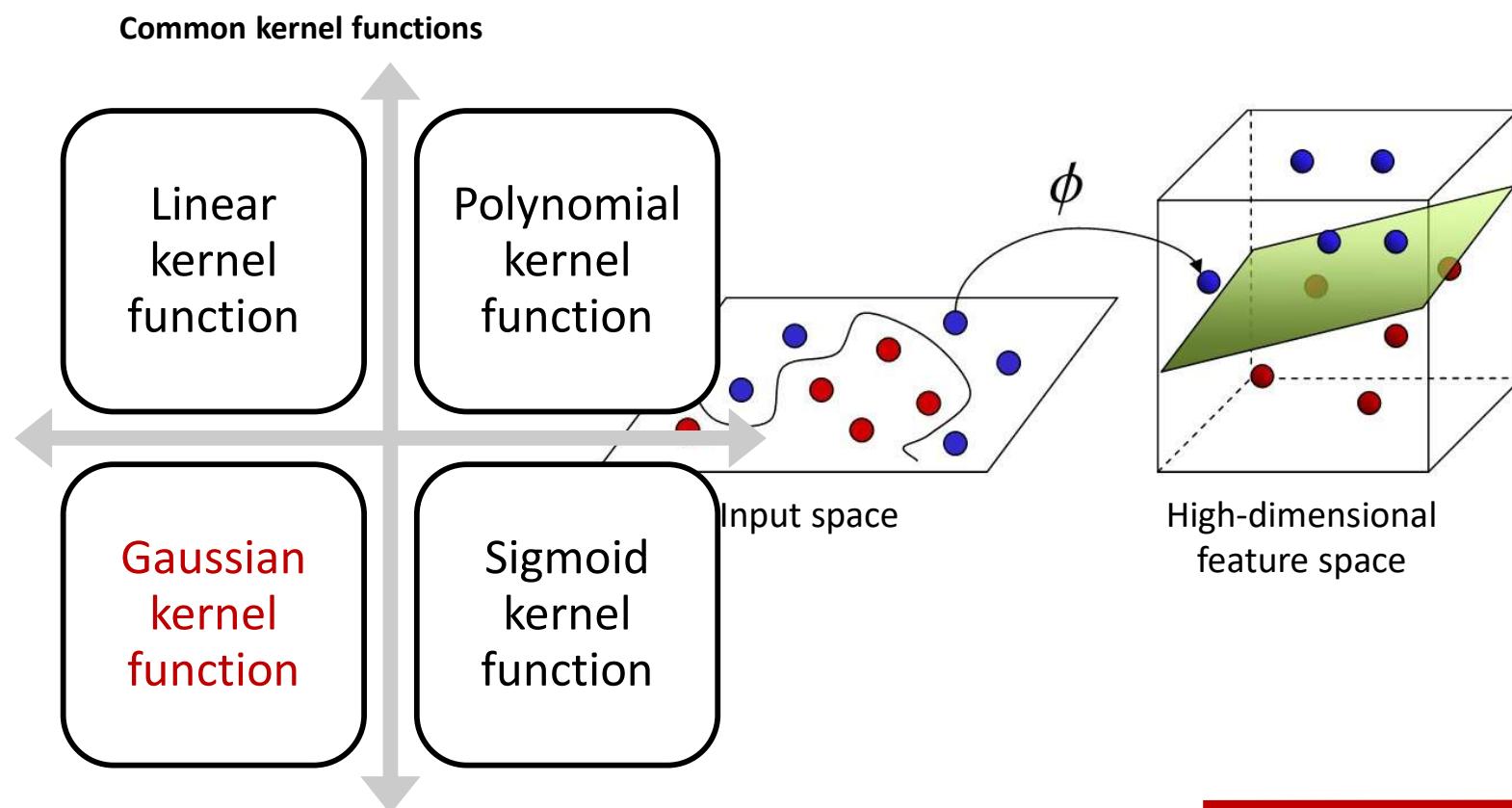
Linear SVM can function well for linear separable datasets.



Nonlinear datasets cannot be split with straight lines.

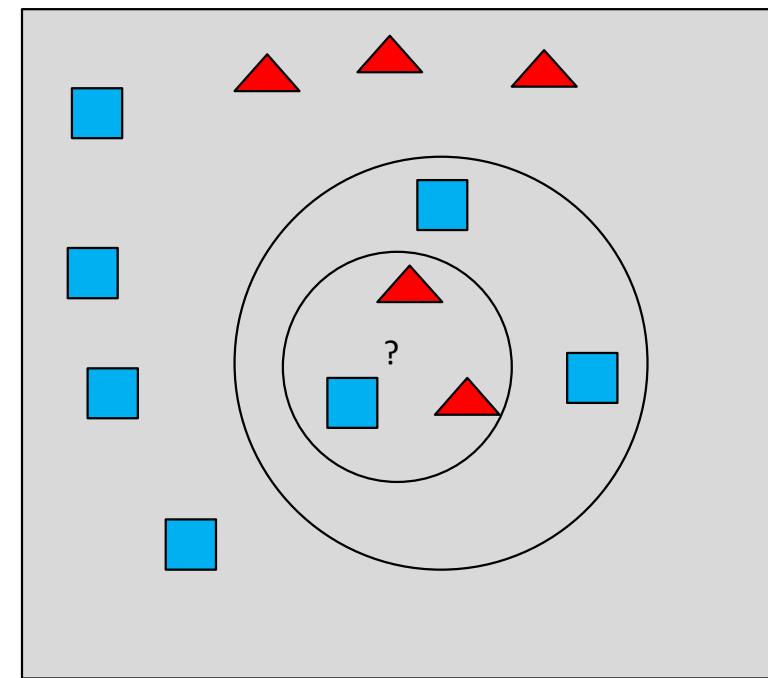
Nonlinear SVM (2)

- Kernel functions are used to construct nonlinear SVMs.
- Kernel functions allow algorithms to fit the largest hyperplane in a transformed high-dimensional feature space.



KNN Algorithm (1)

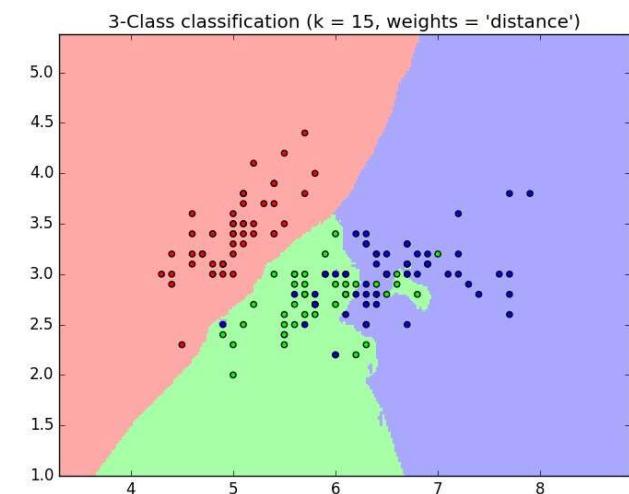
- The KNN classification algorithm is a theoretically mature method and one of the simplest machine learning algorithms. According to this method, if the majority of k samples most similar to one sample (nearest neighbors in the eigenspace) belong to a specific category, this sample also belongs to this category.



The target category of point ? varies with the number of the most adjacent nodes.

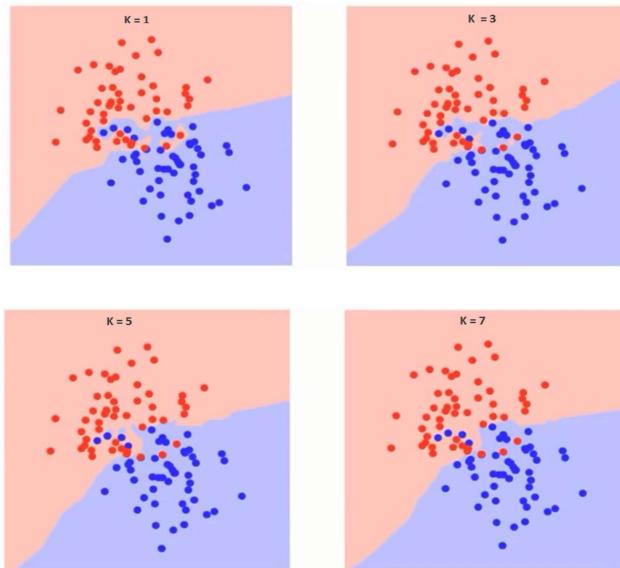
KNN Algorithm (2)

- As the prediction result is determined based on the number and weights of neighbors in the training set, the KNN algorithm has a simple logic.
- KNN is a non-parametric method which is usually used in datasets with irregular decision boundaries.
 - The KNN algorithm generally adopts the majority voting method for classification prediction and the average value method for regression prediction.
- KNN requires a huge number of computations.



KNN Algorithm (3)

- Generally, a larger k value reduces the impact of noise on classification, but obscures the boundary between classes.
 - A larger k value means a higher probability of underfitting because the segmentation is too rough. A smaller k value means a higher probability of overfitting because the segmentation is too refined.



- The boundary becomes smoother as the value of k increases.
- As the k value increases to infinity, all data points will eventually become all blue or all red.

Naive Bayes (1)

- Naive Bayes algorithm: a simple multi-class classification algorithm based on the Bayes theorem. It assumes that features are independent of each other. For a given sample feature X , the probability that a sample belongs to a category H is:
 - X_1, \dots, X_n are data features, which are usually described by measurement values of m attribute sets.
 - For example, the color feature may have three attributes: red, yellow, and blue.
 - C_k indicates that the data belongs to a specific category C_k .
 - $P(C_k|X_1, \dots, X_n)$ is a posterior probability or a posterior probability of under condition C_k .
 - $P(C_k)$ is a prior probability that is independent of X_1, \dots, X_n
 - $P(X_1, \dots, X_n)$ is the priori probability of X .

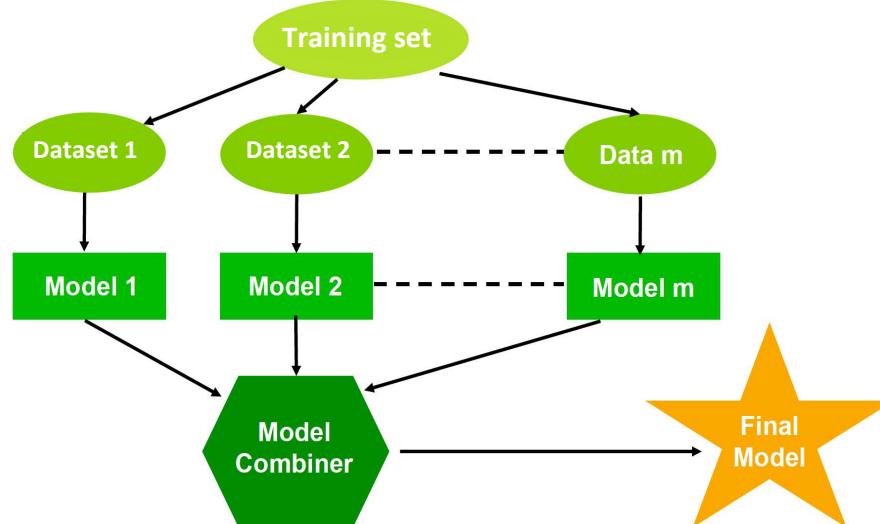
Naive Bayes (2)

- Independent assumption of features.
 - For example, if a fruit is red, round, and about 10 cm (3.94 in.) in diameter, it can be considered an apple.
 - A Naive Bayes classifier considers that each feature independently contributes to the probability that the fruit is an apple, regardless of any possible correlations between the color, roundness, and diameter.

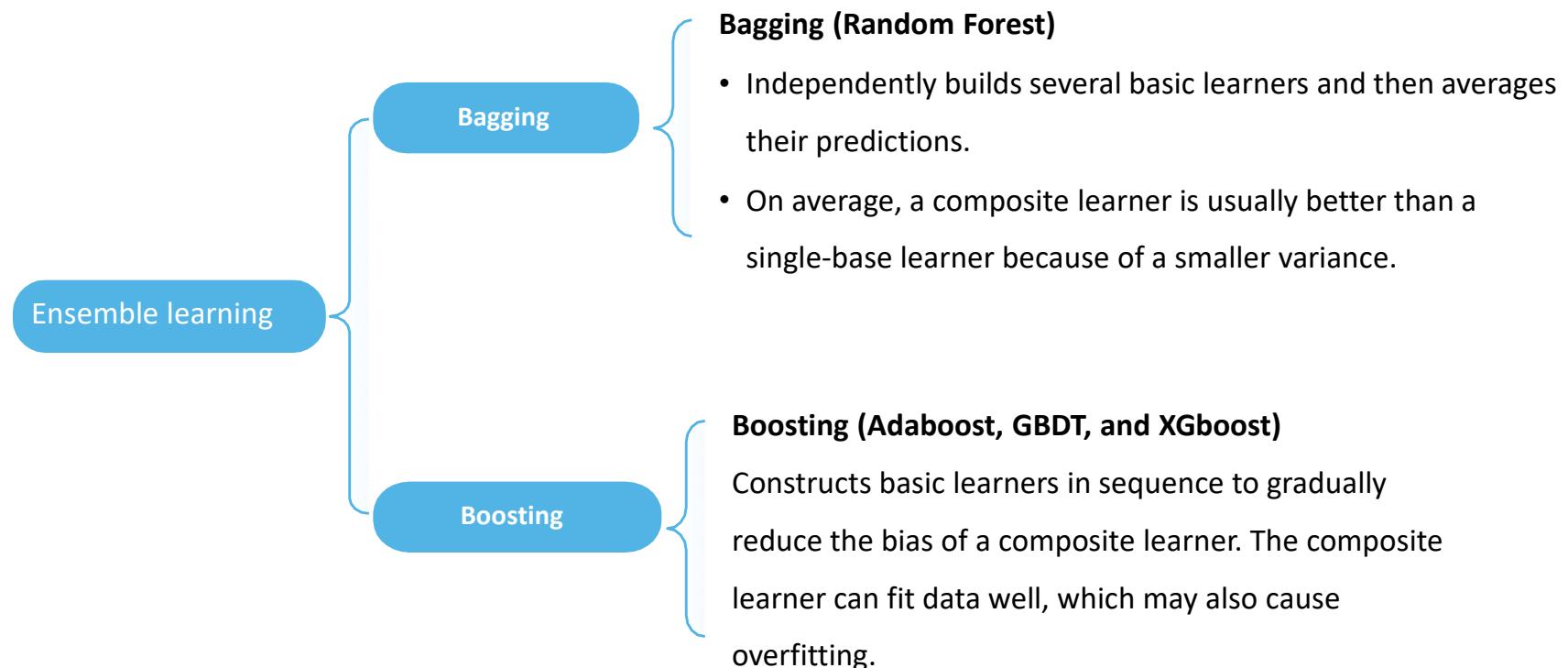


Ensemble Learning

- Ensemble learning is a machine learning paradigm in which multiple learners are trained and combined to solve the same problem. When multiple learners are used, the integrated generalization capability can be much stronger than that of a single learner.
- If you ask a complex question to thousands of people at random and then summarize their answers, the summarized answer is better than an expert's answer in most cases. This is the wisdom of the masses.

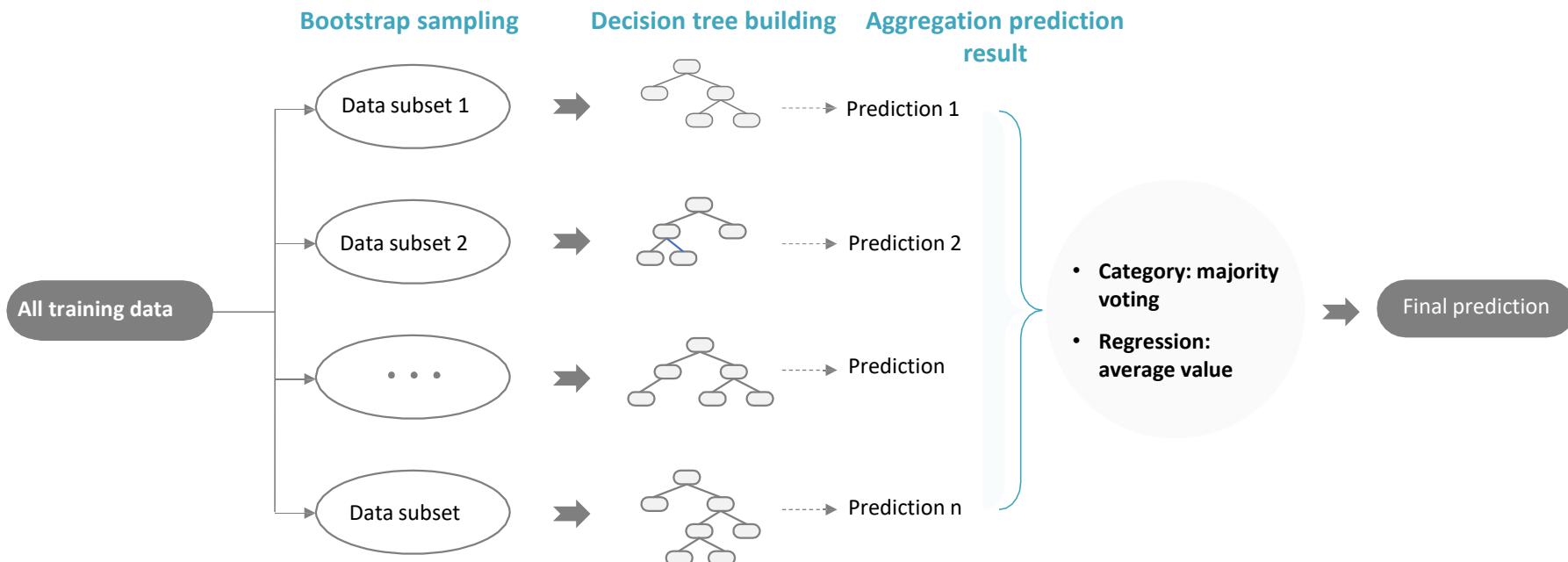


Classification of Ensemble Learning



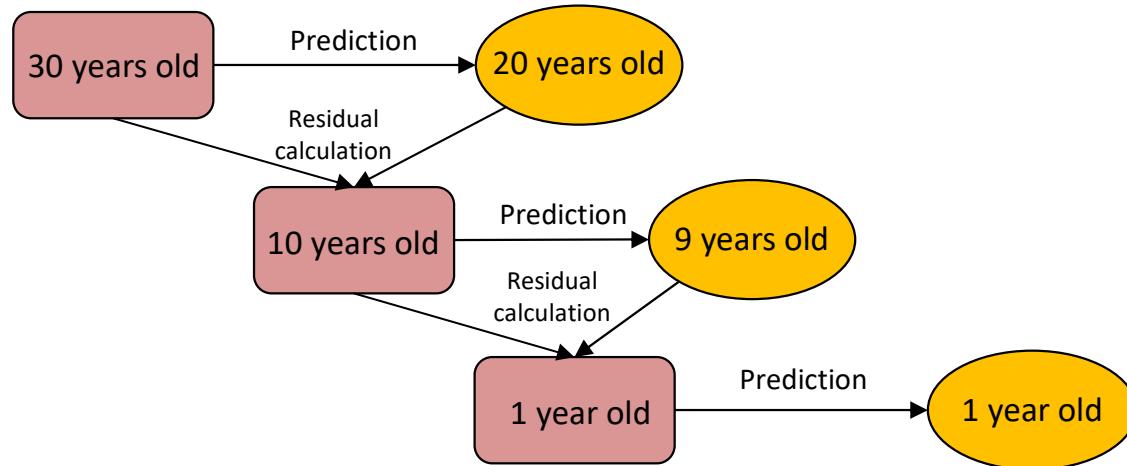
Ensemble Methods in Machine Learning (1)

- Random forest = Bagging + CART decision tree
- Random forests build multiple decision trees and merge them together to make predictions more accurate and stable.
 - Random forests can be used for classification and regression problems.



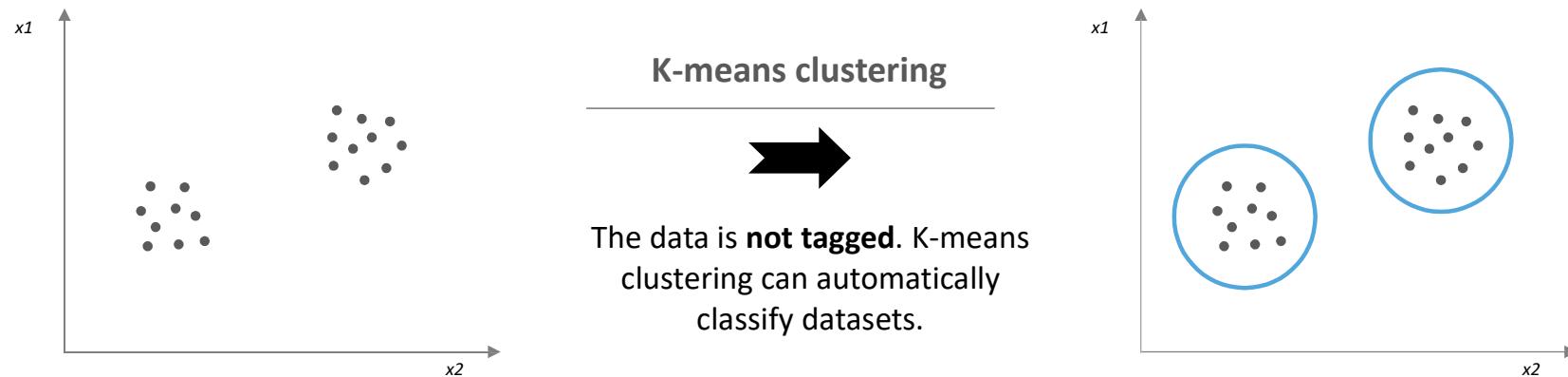
Ensemble Methods in Machine Learning (2)

- GBDT is a type of boosting algorithm.
- For an aggregative mode, the sum of the results of all the basic learners equals the predicted value. In essence, the residual of the error function to the predicted value is fit by the next basic learner. (The residual is the error between the predicted value and the actual value.)
- During model training, GBDT requires that the sample loss for model prediction be as small as possible.



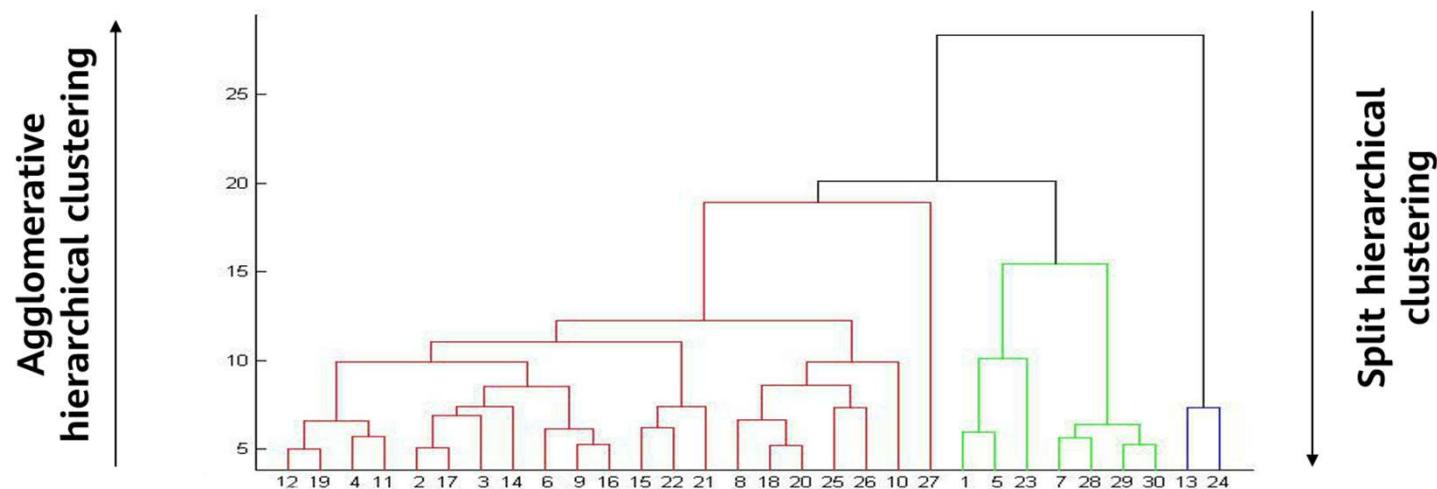
Unsupervised Learning - K-means

- K-means clustering aims to partition n observations into k clusters in which each observation belongs to the cluster with the nearest mean, serving as a prototype of the cluster.
- For the k-means algorithm, specify the final number of clusters (k). Then, divide n data objects into k clusters. The clusters obtained meet the following conditions: (1) Objects in the same cluster are highly similar. (2) The similarity of objects in different clusters is small.



Unsupervised Learning - Hierarchical Clustering

- Hierarchical clustering divides a dataset at different layers and forms a tree-like clustering structure. The dataset division may use a "bottom-up" aggregation policy or a "top-down" splitting policy. The hierarchy of clustering is represented in a tree graph. The root is the unique cluster of all samples, and the leaves are the cluster of only a sample.



Contents

1. Machine Learning Definition
2. Machine Learning Types
3. Machine Learning Process
4. Other Key Machine Learning Methods
5. Common Machine Learning Algorithms
- 6. Case study**

Comprehensive Case

- Assume that there is a dataset containing the house areas and prices of 21,613 housing units sold in a city. Based on this data, we can predict the prices of other houses in the city.

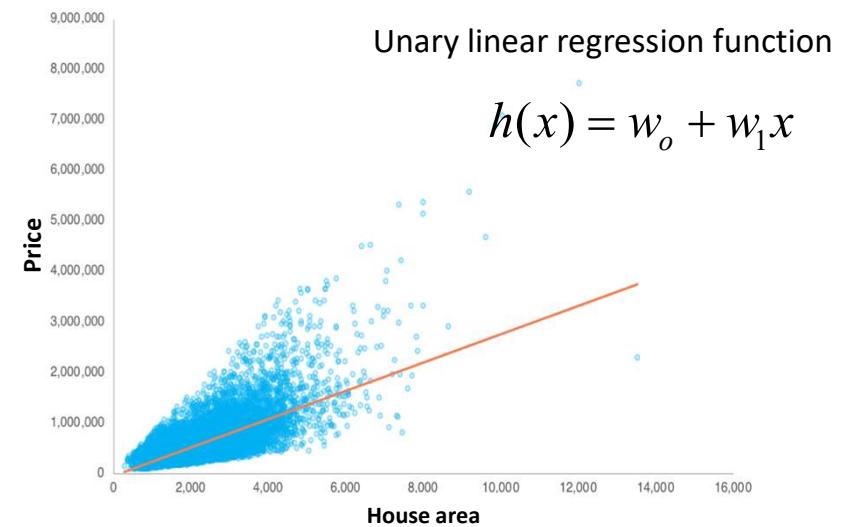
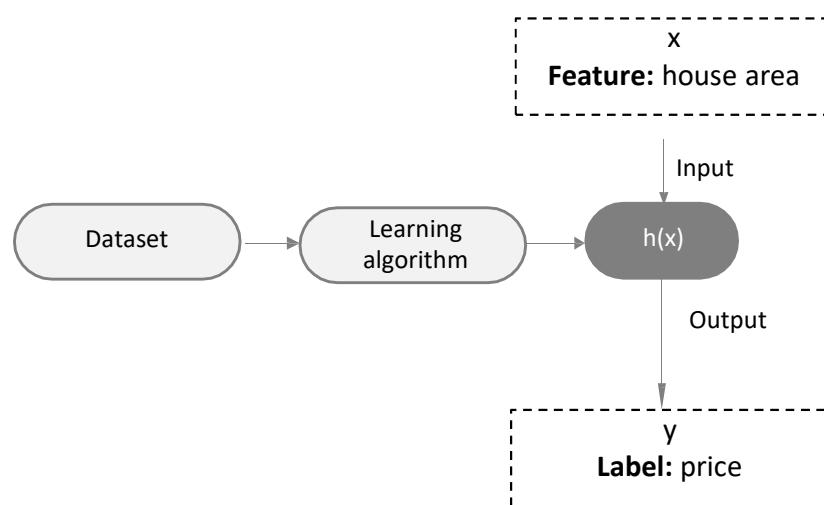
House Area	Price
1,180	221,900
2,570	538,000
770	180,000
1,960	604,000
1,680	510,000
5,420	1,225,000
1,715	257,500
1,060	291,850
1,160	468,000
1,430	310,000
1,370	400,000
1,810	530,000
...	...

Dataset



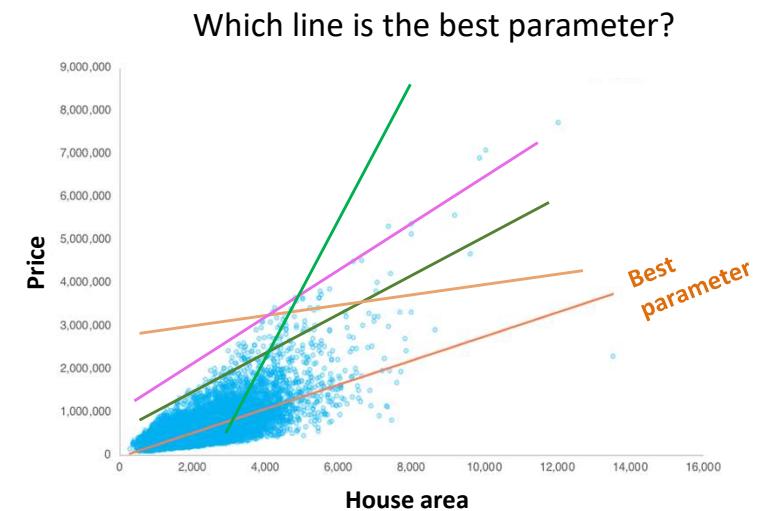
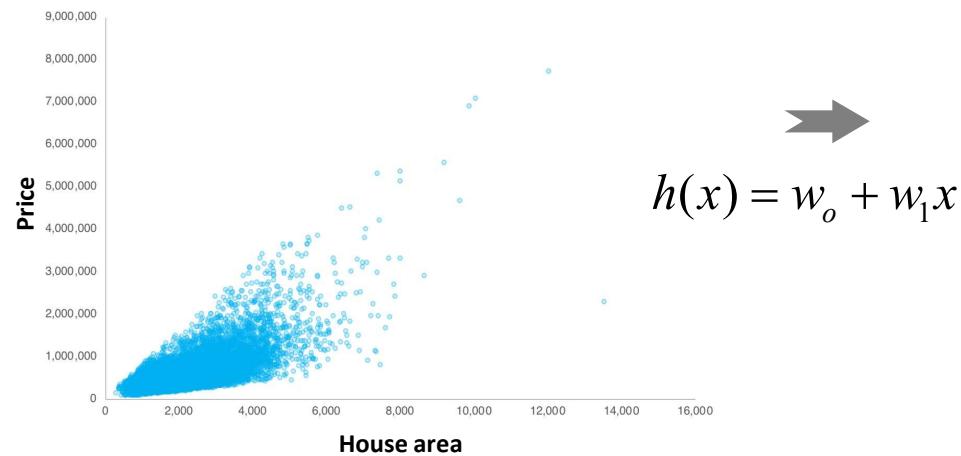
Problem Analysis

- This case contains a large amount of data, including input x (house area), and output y (price), which is a continuous value. We can use **regression of supervised learning**. Draw a scatter chart based on the data and use **linear regression**.
- Our goal is to build a model function $h(x)$ that infinitely approximates the function that expresses true distribution of the dataset.
- Then, use the model to predict unknown price data.



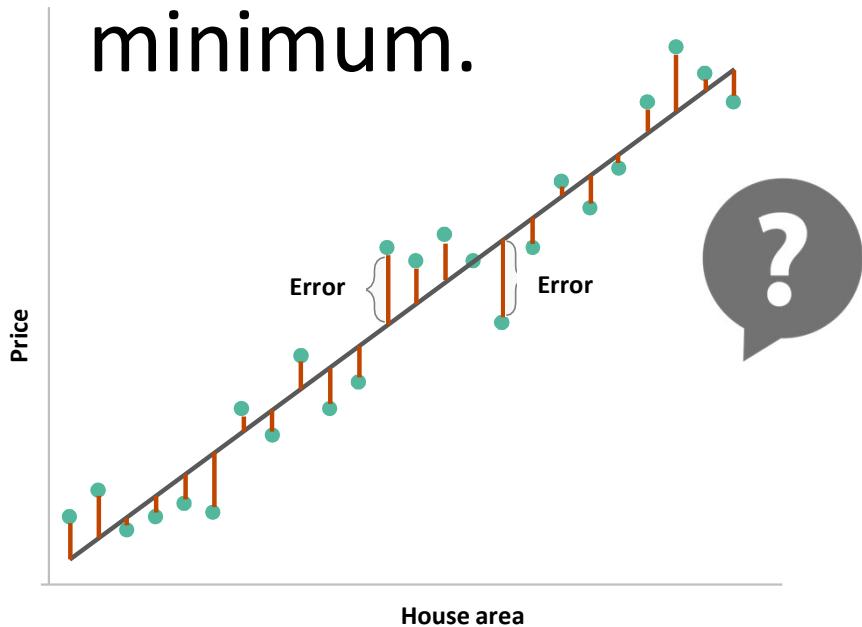
Goal of Linear Regression

- Linear regression aims to find a straight line that best fits the dataset.
- Linear regression is a parameter-based model. Here, we need learning parameters w_0 and w_1 . When these two parameters are found, the best model appears.



Loss Function of Linear Regression

- To find the optimal parameter, construct a loss function and find the parameter values when the loss function becomes the minimum.



Loss function of linear regression: $J(w) = \frac{1}{2m} \sum (h(x) - y)^2$

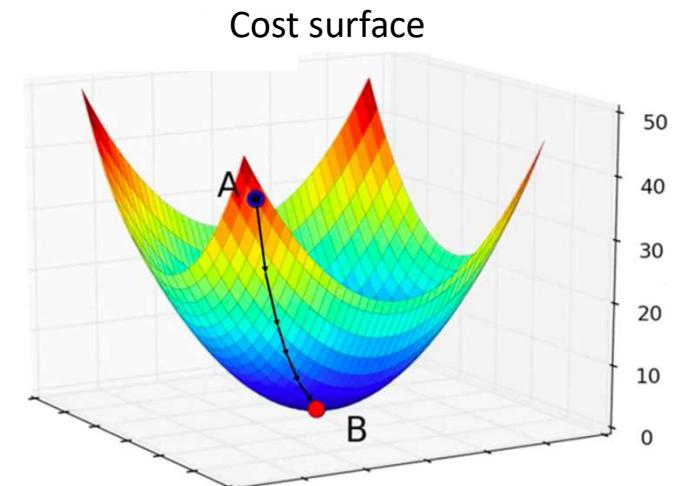
Goal:

$$\arg \min_w J(w) = \frac{1}{2m} \sum (h(x) - y)^2$$

- where, m indicates the number of samples,
- $h(x)$ indicates the predicted value, and y indicates the actual value.

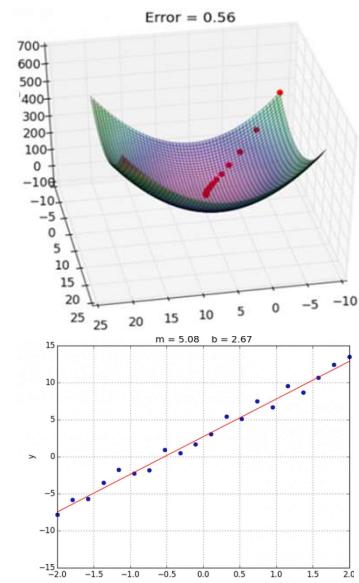
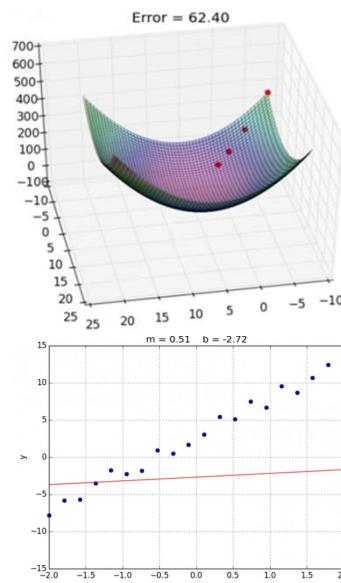
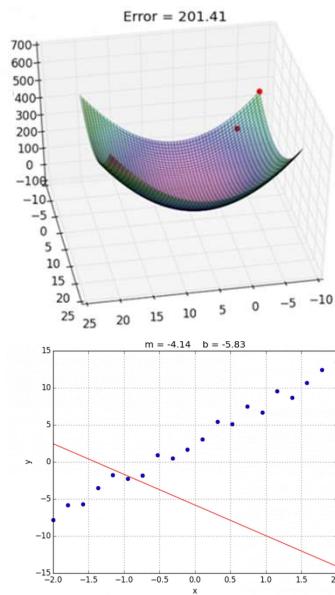
Gradient Descent Method

- The gradient descent algorithm finds the minimum value of a function through iteration.
- It aims to randomize an initial point on the loss function, and then find the global minimum value of the loss function based on the negative gradient direction. Such parameter value is the optimal parameter value.
 - **Point A:** the position of w_0 and w_1 after random initialization.
 w_0 and w_1 are the required **parameters**.
 - **A-B connection line:** a path formed based on descents in a negative gradient direction. Upon each descent, values w_0 and w_1 **change**, and the regression line also changes.
 - **Point B:** global minimum value of the loss function.
Final values of w_0 and w_1 are also found.



Iteration Example

- The following is an example of a gradient descent iteration. We can see that as red points on the loss function surface gradually approach a lowest point, fitting of the linear regression red line with data becomes better and better. At this time, we can get the best parameters.

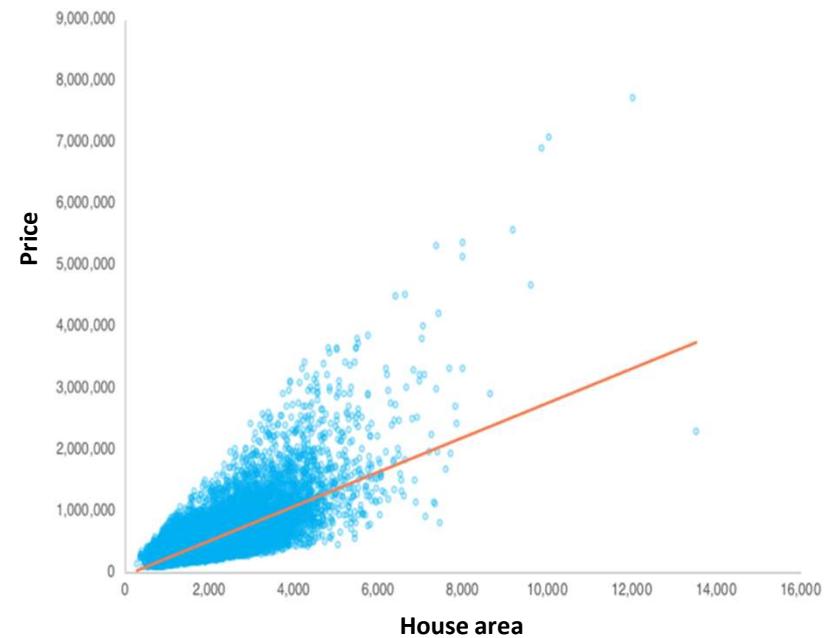


Model Debugging and Application

- After the model is trained, test it with the test set to ensure the generalization capability.
- If overfitting occurs, use Lasso regression or Ridge regression with regularization terms and tune the hyperparameters.
- If underfitting occurs, use a more complex regression model, such as GBDT.
- Note:
 - For real data, pay attention to the functions of data cleansing and feature engineering.

The final model result is as follows:

$$h(x) = 280.62x - 43581$$



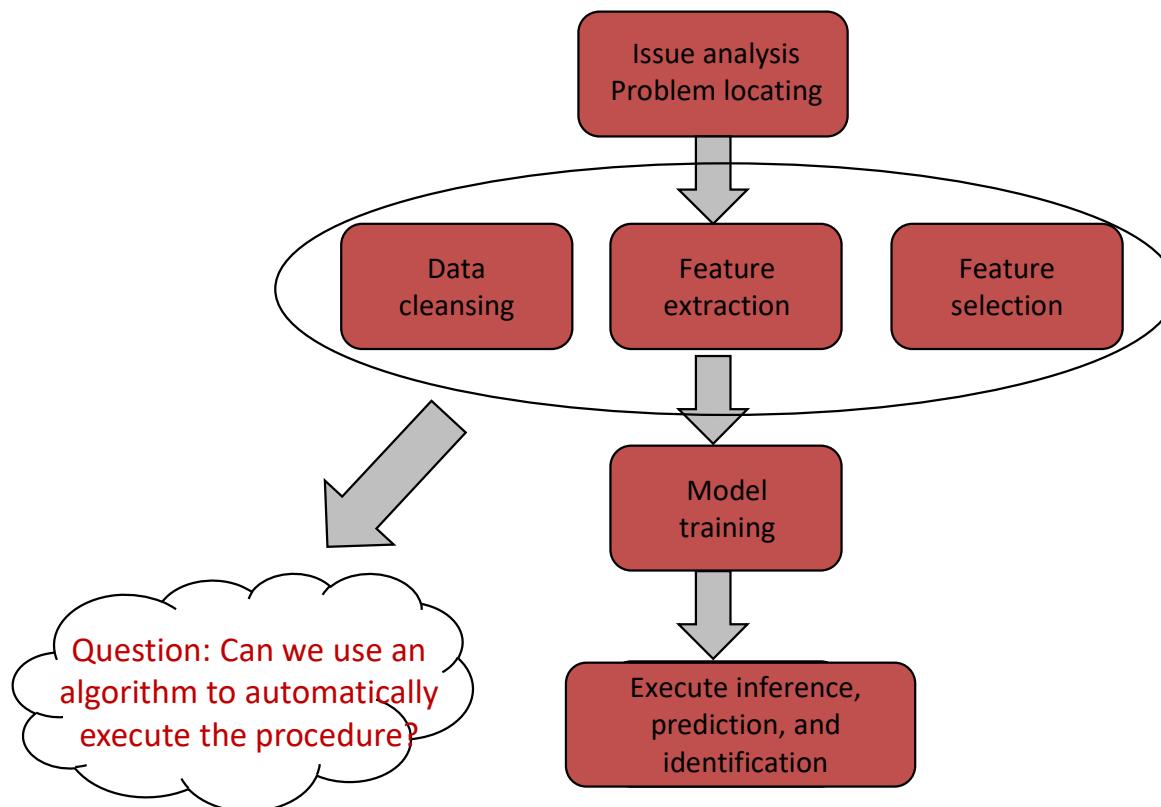
Traditional Machine Learning and

Deep Learning

- As a model based on unsupervised feature learning and feature hierarchy learning, deep learning has great advantages in fields such as computer vision, speech recognition, and natural language processing.

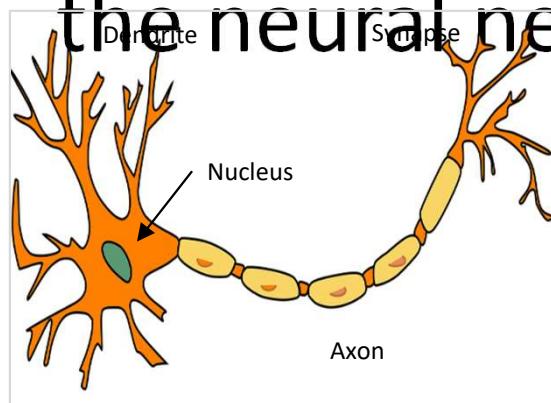
Traditional Machine Learning	Deep Learning
Low hardware requirements on the computer: Given the limited computing amount, the computer does not need a GPU for parallel computing generally.	Higher hardware requirements on the computer: To execute matrix operations on massive data, the computer needs a GPU to perform parallel computing.
Applicable to training under a small data amount and whose performance cannot be improved continuously as the data amount increases.	The performance can be high when high-dimensional weight parameters and massive training data are provided.
Level-by-level problem breakdown	E2E learning
Manual feature selection	Algorithm-based automatic feature extraction
Easy-to-explain features	Hard-to-explain features

Traditional Machine Learning

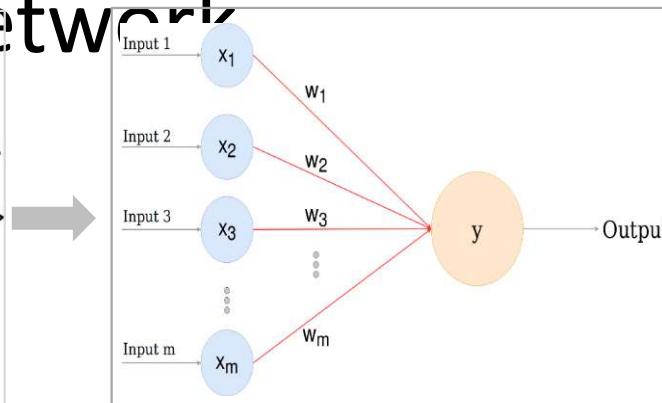


Deep Learning

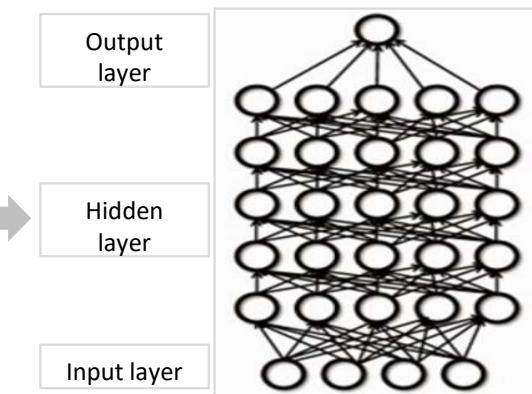
- Generally, the deep learning architecture is a deep neural network. "Deep" in "deep learning" refers to the number of layers of the neural network



Human neural network



Perceptron

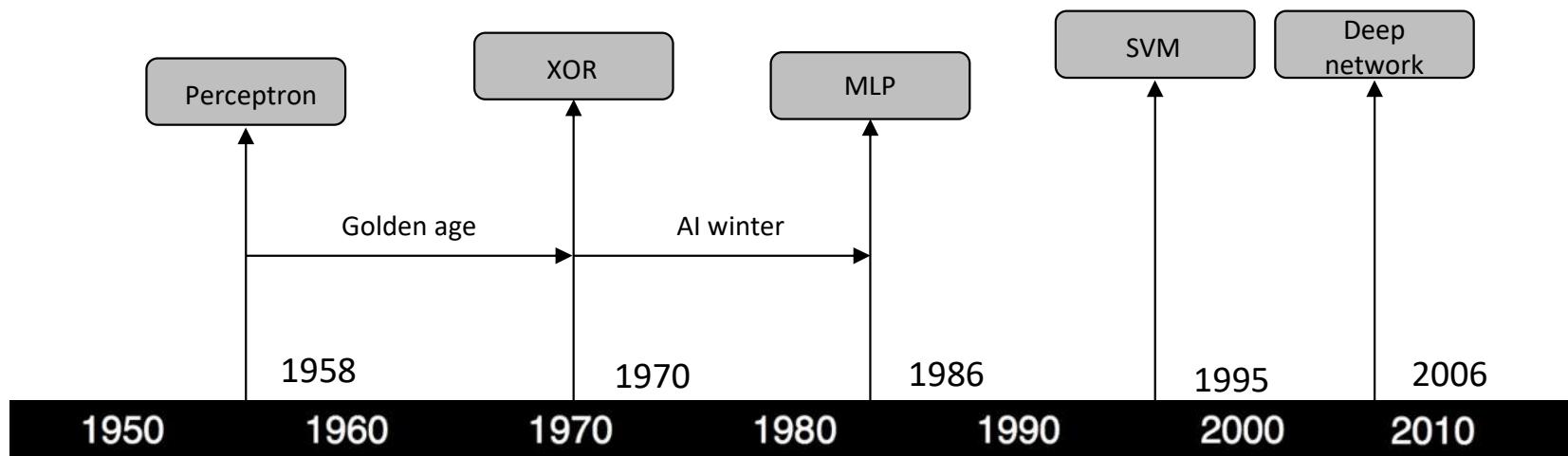


Deep neural network

Neural Network

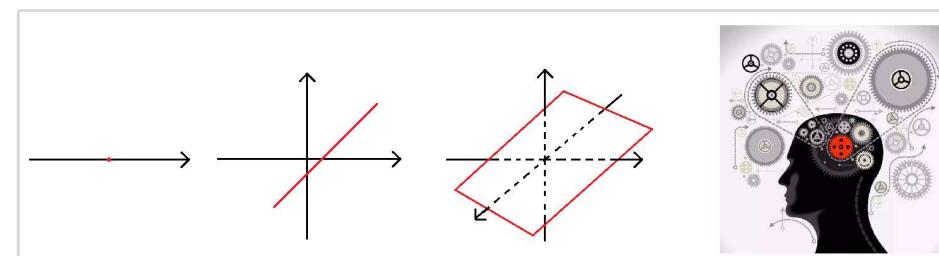
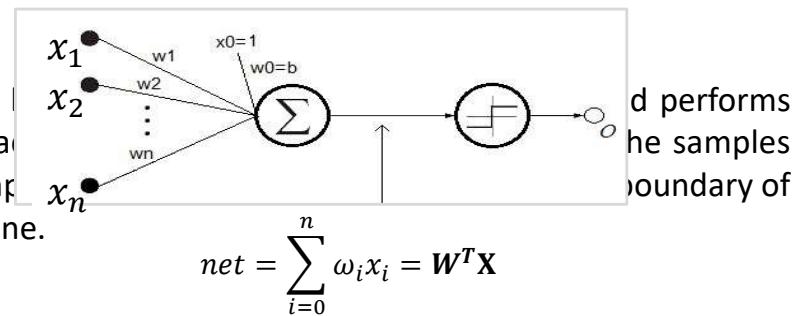
- Currently, the definition of the neural network has not been determined yet. Hecht Nielsen, a neural network researcher in the U.S., defines a neural network as a computer system composed of simple and highly interconnected processing elements, which process information by dynamic response to external inputs.
- A neural network can be simply expressed as an information processing system designed to imitate the human brain structure and functions based on its source, features, and explanations.
- Artificial neural network (neural network): Formed by artificial neurons connected to each other, the neural network extracts and simplifies the human brain's microstructure and functions. It is an important approach to simulate human intelligence and reflect several basic features of human brain functions, such as concurrent information processing, learning, association, model classification, and memory.

Development History of Neural Networks



Single-Layer Perceptron

- Input vector: $X = [x_0, x_1, \dots, x_n]^T$
- Weight: $W = [\omega_0, \omega_1, \dots, \omega_n]^T$, in which ω_0 is the offset.
- Activation function: $O = sign(net) = \begin{cases} 1, & net > 0, \\ -1, & otherwise. \end{cases}$
- The preceding perceptron is equivalent to a classifier. It uses the binary classification on input samples in the high-dimensional space. Samples are classified into a type. Otherwise, $O = -1$. In this case, the sample belongs to one of these two types is $W^T X = 0$, which is a high-dimensional hyperplane.



Classification point
 $Ax + B = 0$

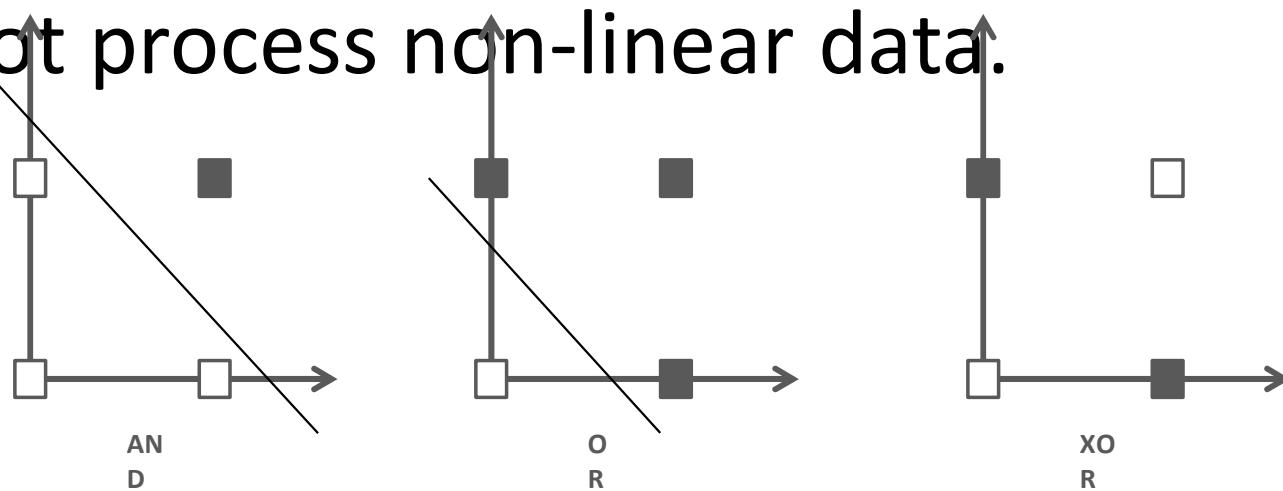
Classification line
 $Ax + By + C = 0$

Classification plane
 $Ax + By + Cz + D = 0$

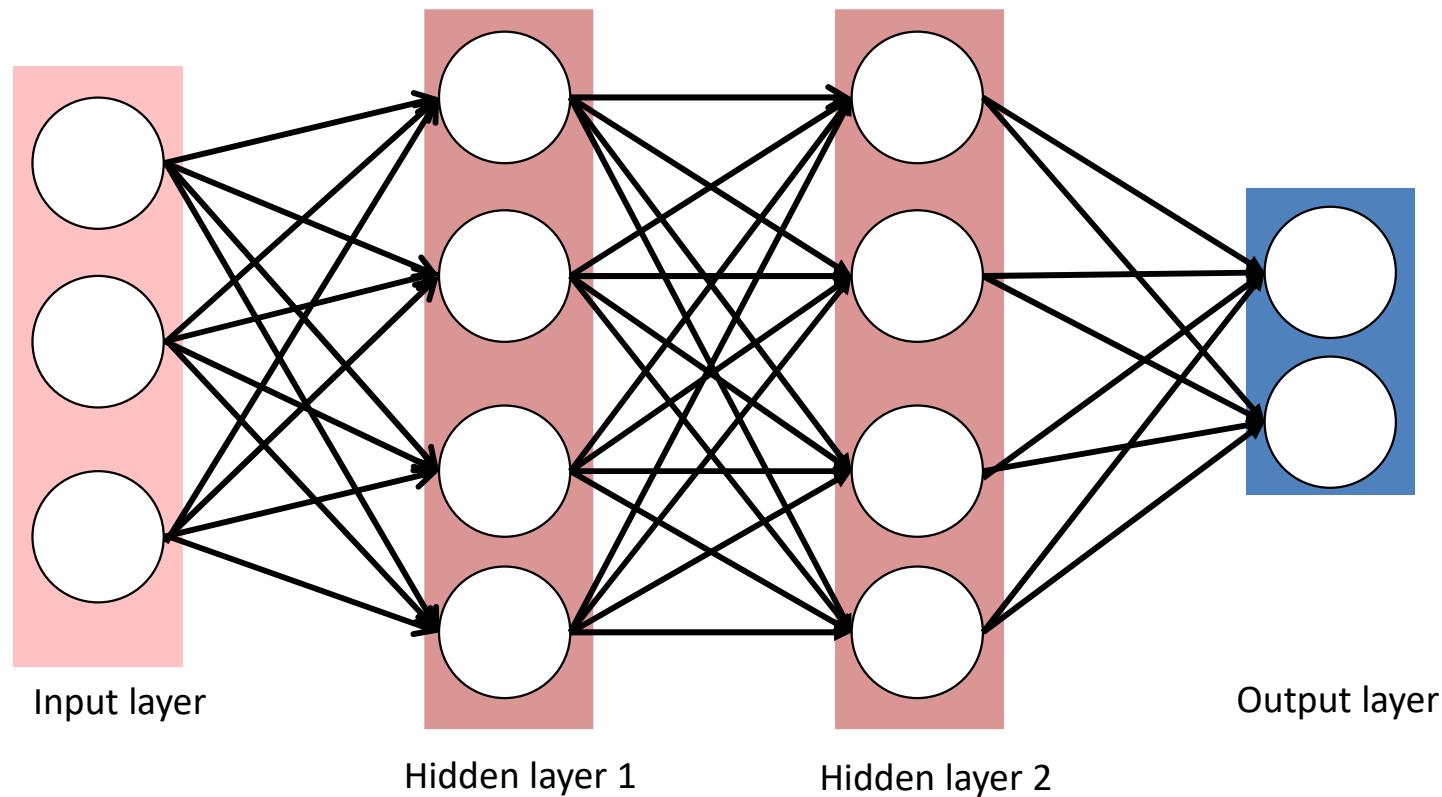
Classification hyperplane
 $W^T X + b = 0$

XOR Problem

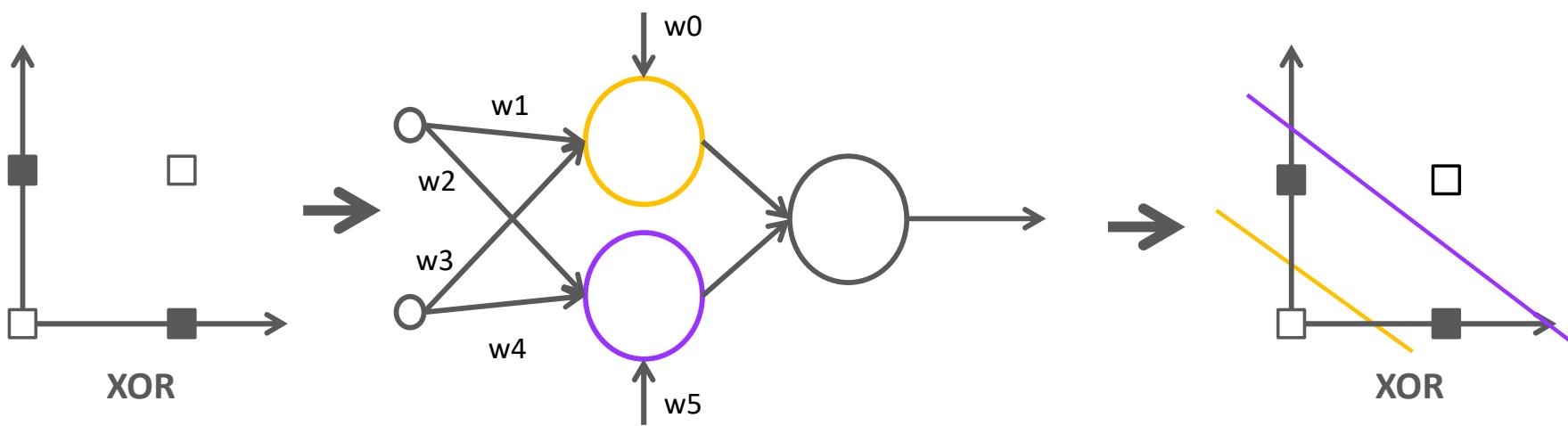
- In 1969, Minsky, an American mathematician and AI pioneer, proved that a perceptron is essentially a linear model that can only deal with linear classification problems, but cannot process non-linear data.



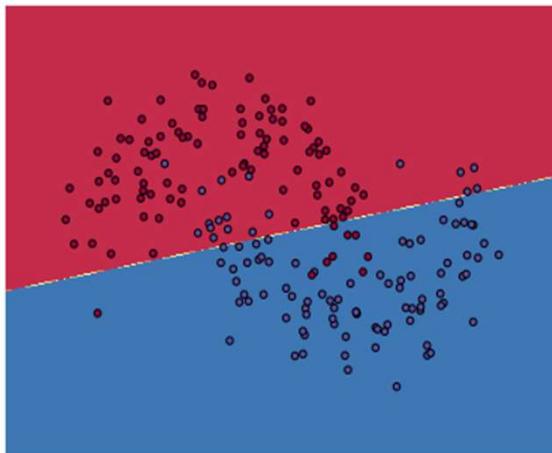
Feedforward Neural Network



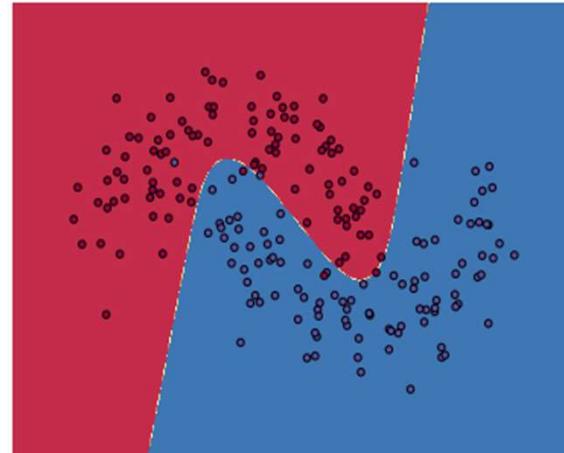
Solution of XOR



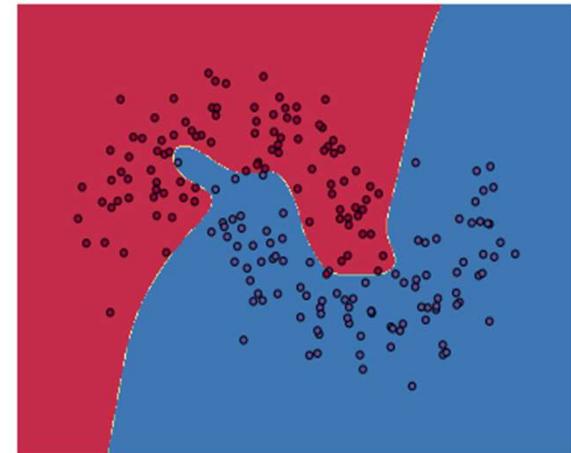
Impacts of Hidden Layers on A Neural Network



0 hidden layers



3 hidden layers



20 hidden layers

Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks



Gradient Descent and Loss

- The gradient of the multivariate function $o = f(x) = f(x_0, x_1, \dots, x_n)$ at $X' = [x_0', x_1', \dots, x_n']^T$ is shown as follows:

$$\nabla f(x_0', x_1', \dots, x_n') = [\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}]^T|_{X=X'},$$

The direction of the gradient vector is the fastest growing direction of the function. As a result, the direction of the negative gradient vector $-\nabla f$ is the fastest descent direction of the function.

- During the training of the deep learning network, target classification errors must be parameterized. **A loss function (error function)** is used, which reflects the error between the target output and actual output of the perceptron. For a single training sample x , the most common error function is the **Quadratic cost function**.

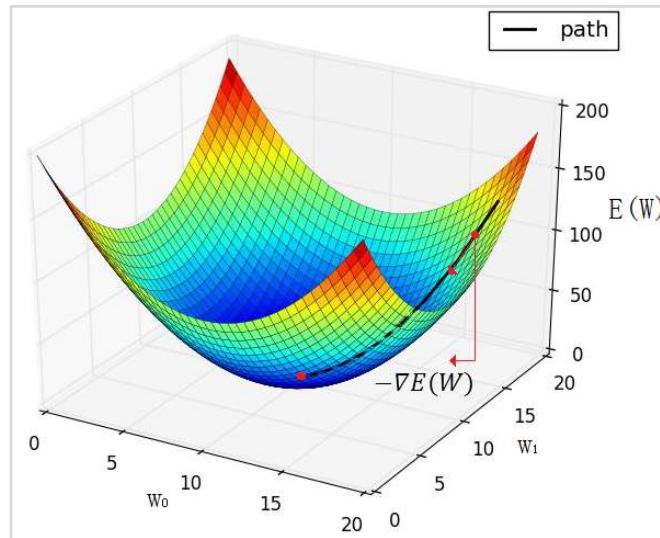
$$E(w) = \frac{1}{2} \sum_{d \in D} (t_d - o_d)^2,$$

In the preceding function, d is one neuron in the output layer, D is all the neurons in the output layer, t_d is the target output, and o_d is the actual output.

- The gradient descent method enables the loss function to search along the negative gradient direction and update the parameters iteratively, finally minimizing the loss function.

Extrema of the Loss Function

- Purpose: The loss function $E(W)$ is defined on the weight space. The objective is to search for the weight vector W that can minimize $E(W)$.
- Limitation: No effective method can solve the extremum in mathematics on the complex high-dimensional surface of $E(W) = \frac{1}{2} \sum_{d \in D} (t_d - o_d)^2$.



Example of gradient descent of binary paraboloid

Common Loss Functions in Deep Learning

- Quadratic cost function:

$$E(W) = \frac{1}{2} \sum_{d \in D} (t_d - o_d)^2$$

- Cross entropy error function:

$$E(W) = - \sum_{d \in D} t_d \ln o_d$$

- The cross entropy error function depicts the distance between two probability distributions, which is a widely used loss function for classification problems.
- Generally, the mean square error function is used to solve the regression problem, while the cross entropy error function is used to solve the classification problem.

Batch Gradient Descent Algorithm

- In the training sample set X , each sample is recorded as $\langle x, t \rangle$, in which x is the input vector, t the target output, o the actual output, and η the learning rate.
 – Initializes each w_i to a random value with a smaller absolute value.
 – Before the end condition is met:
 - Initializes each Δw_i to zero.
 - For each iteration:
 - Input all the x to this unit and calculate the output o_x .
 - For each w_i in this unit: $\Delta w_i += -\eta \frac{1}{n} \sum_{x \in X} \frac{\partial C(t_x, o_x)}{\partial w_i}$.
 - For each w_i in this unit: $w_i += \Delta w_i$.
- The gradient descent algorithm of this version is not commonly used because:
 - The convergence process is very slow as all training samples need to be calculated every time the weight is updated.

Stochastic Gradient Descent Algorithm

- To address the BGD algorithm defect, a common variant called Incremental Gradient Descent algorithm is used, which is also called the Stochastic Gradient Descent (SGD) algorithm. One implementation is called Online Learning, which updates the gradient based on each sample:

$$\Delta w_i = -\eta \frac{1}{n} \sum_{x \in X} \frac{\partial C(t_x, o_x)}{\partial w_i} \Rightarrow \Delta w_i = -\eta \frac{\partial C(t_x, o_x)}{\partial w_i}.$$

- ONLINE-GRADIENT-DESCENT**

- Initializes each w_i to a random value with a smaller absolute value.
- Before the end condition is met:
- Generates a random $\langle x, t \rangle$ from X and does the following calculation:
 - Input X to this unit and calculate the output o_x .
 - For each w_i in this unit: $w_i += -\eta \frac{\partial C(t_x, o_x)}{\partial w_i}$.

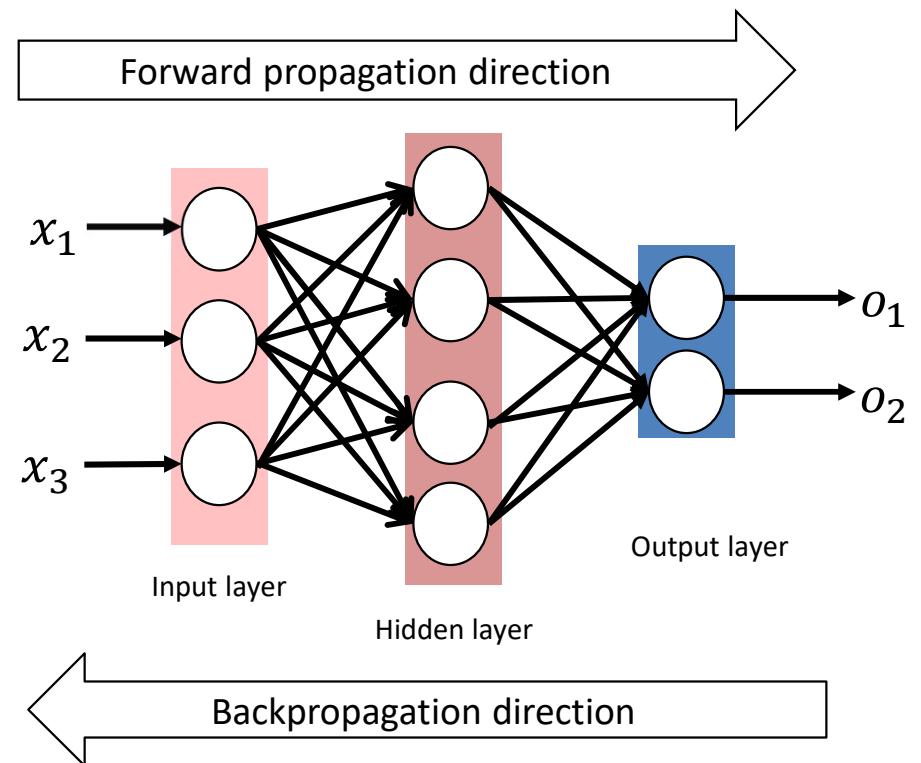
Mini-Batch Gradient Descent

- To address the defects of the previous two gradient descent algorithms, the Mini-batch Gradient Descent Algorithm (MBGD) was proposed, and has been most widely used. A small number of Batch Size (BS) samples are used at a time to calculate Δw_i , and then the weight is updated accordingly.
- Batch-gradient-descent
 - Initializes each w_i to a random value with a smaller absolute value.
 - Before the end condition is met:
 - Initializes each Δw_i to zero.
 - For each $\langle x, t \rangle$ in the BS samples in the next batch in B :
 - Input x to this unit and calculate the output o_x .
 - For each w_i in this unit: $\Delta w_i += -\eta \frac{1}{n} \sum_{x \in B} \frac{\partial C(t_x, o_x)}{\partial w_i}$
 - For each w_i in this unit: $w_i += \Delta w_i$
 - For the last batch, the training samples are mixed up in a random order.

Backpropagation Algorithm (1)

- Signals are propagated in forward direction, and errors are propagated in backward direction.
- In the training sample set D, each sample is recorded as $\langle X, t \rangle$, in which X is the input vector, t the target output, o the actual output, and w the weight coefficient.
- Loss function:

$$E(w) = \frac{1}{2} \sum_{(d \in D)} (t_d - o_d)^2$$



Backpropagation Algorithm (2)

- According to the following formulas, errors in the input, hidden, and output layers are accumulated to generate the error in the loss function.
- w_c is the weight coefficient between the hidden layer and the output layer, while w_b is the weight coefficient between the input layer and the hidden layer. f is the activation function, D is the output layer set, and C and B are the hidden layer set and input layer set respectively. Assume that the loss function is a quadratic cost function:

□ Output layer error:

$$E = \frac{1}{2} \sum_{(d \in D)} (t_d - o_d)^2$$

□ Expanded hidden
layer error:

$$E = \frac{1}{2} \sum_{(d \in D)} [t_d - f(\text{net}_d)]^2 = \frac{1}{2} \sum_{(d \in D)} \left[t_d - f\left(\sum_{(c \in C)} w_c y_c\right) \right]^2$$

□ Expanded input

$$E = \frac{1}{2} \sum_{(d \in D)} \left[t_d - f\left(\sum_{(c \in C)} w_c f(\text{net}_c)\right) \right]^2 =$$

layer error:

$$\frac{1}{2} \sum_{(d \in D)} \left[t_d - f\left(\sum_{(c \in C)} w_c f\left(\sum_{b \in B} w_b x_b\right)\right) \right]^2$$

Backpropagation Algorithm (3)

- To minimize error E, the gradient descent iterative calculation can be used to solve W_c and W_b , that is, calculating W_c and W_b to minimize error E.
- Formula:

$$\Delta w_c = -\eta \frac{\partial E}{\partial w_c}, c \in C$$

$$\Delta w_b = -\eta \frac{\partial E}{\partial w_b}, b \in B$$

- If there are multiple hidden layers, chain rules are used to take a derivative for each layer to obtain the optimized parameters by iteration.

Backpropagation Algorithm (4)

- For a neural network with any number of layers, the arranged formula for training is as follows:
$$\Delta w_{ik}^l = -\eta \delta_k^{l+1} f'(z_i^l)$$
- The BP algorithm is used to train the network as follows:
 - Takes out the next training sample $x^{(t)}$ (inputs x to the network and obtains the actual output o).
 - Calculates output layer δ according to the output layer error formula (1).
 - Calculates δ of each hidden layer from output to input (z_j^l) by iteration according to the hidden layer error propagation formula (2).
 - According to the δ of each layer, the weight values of all the layer are updated.

Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks

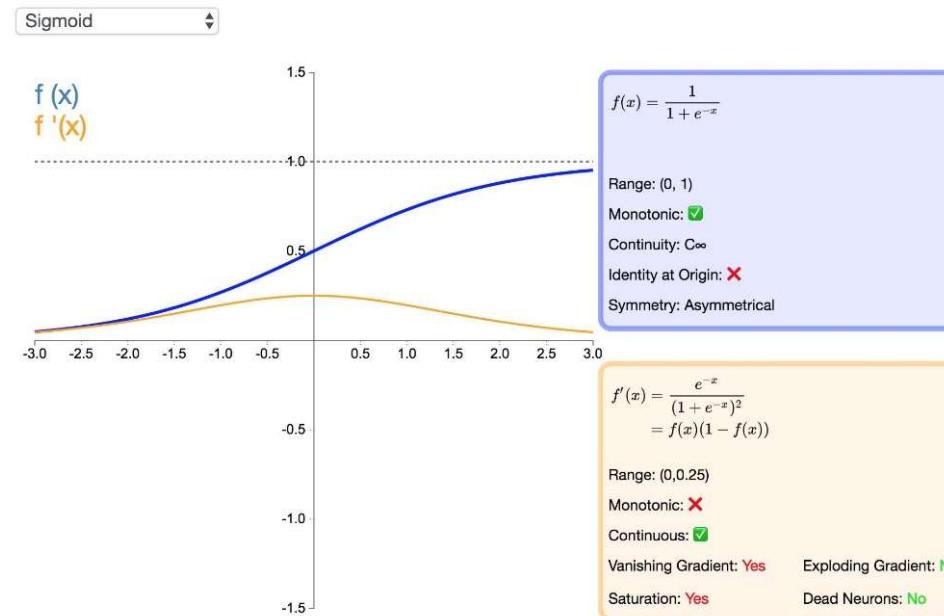


Activation Function

- Activation functions are important for the neural network model to learn and understand complex non-linear functions. They allow introduction of non-linear features to the network.
- Without activation functions, output signals are only simple linear functions. The complexity of linear functions is limited, and the capability of learning complex function mappings from data is low.

Sigmoid

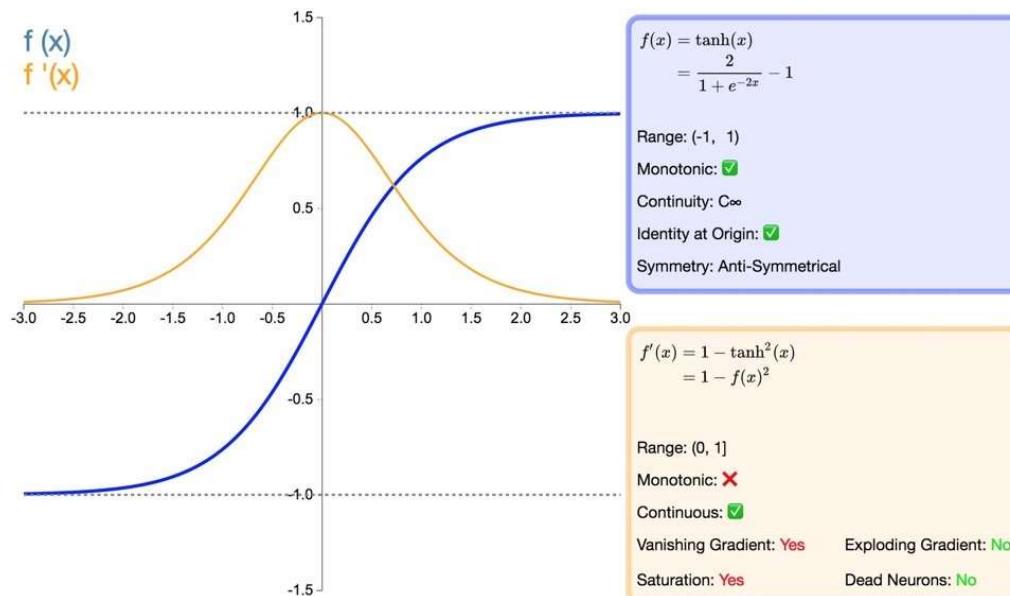
$$f(x) = \frac{1}{1 + e^{-x}}$$



Tanh

$$\tanh x = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

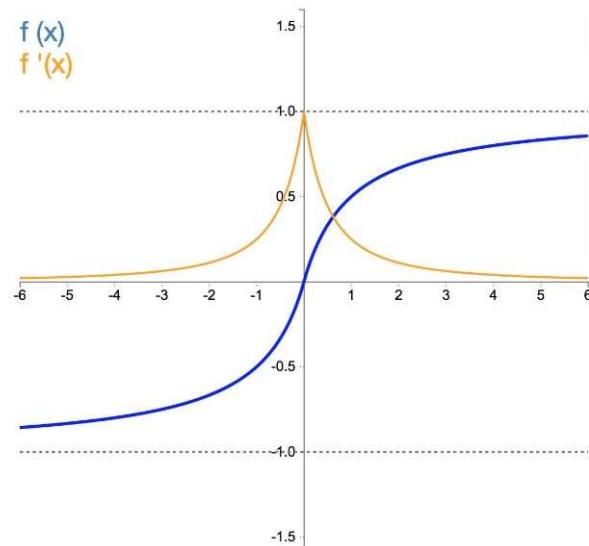
Tanh



Softsign

$$f(x) = \frac{x}{|x| + 1}$$

SoftSign



$$f(x) = \frac{x}{1+|x|}$$

Range: $(0, \infty)$

Monotonic:

Continuity: C^1

Identity at Origin:

Symmetry: Anti-Symmetrical

Reference

$$f'(x) = \frac{1}{(1+|x|)^2}$$

Range: $(0, 1]$

Monotonic:

Continuous:

Vanishing Gradient: Yes

Exploding Gradient: No

Saturation: Yes

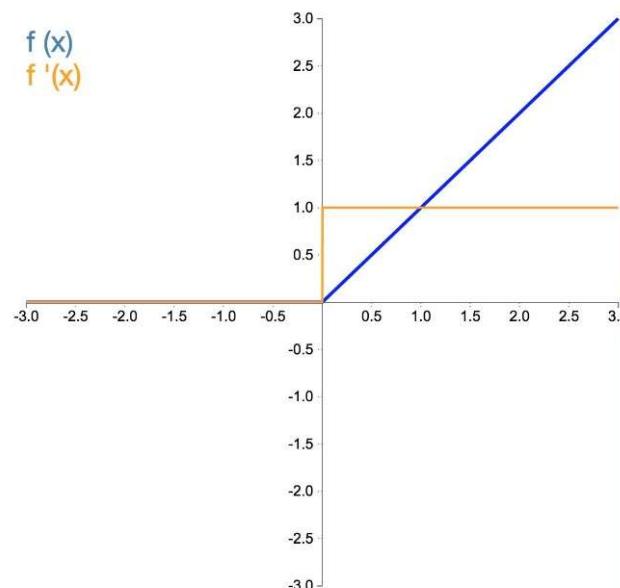
Dead Neurons: No

Rectified Linear Unit (ReLU)

$$y = \begin{cases} x, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

ReLU

$f(x)$
 $f'(x)$



$$f(x) = \begin{cases} x & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$$

Range: $[0, \infty)$

Monotonic:

Continuity: C^0

Identity at Origin:

Symmetry: Asymmetrical

Reference

$$f'(x) = \begin{cases} 1 & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$$

Range: $\{0,1\}$

Monotonic:

Continuous:

Vanishing Gradient: No

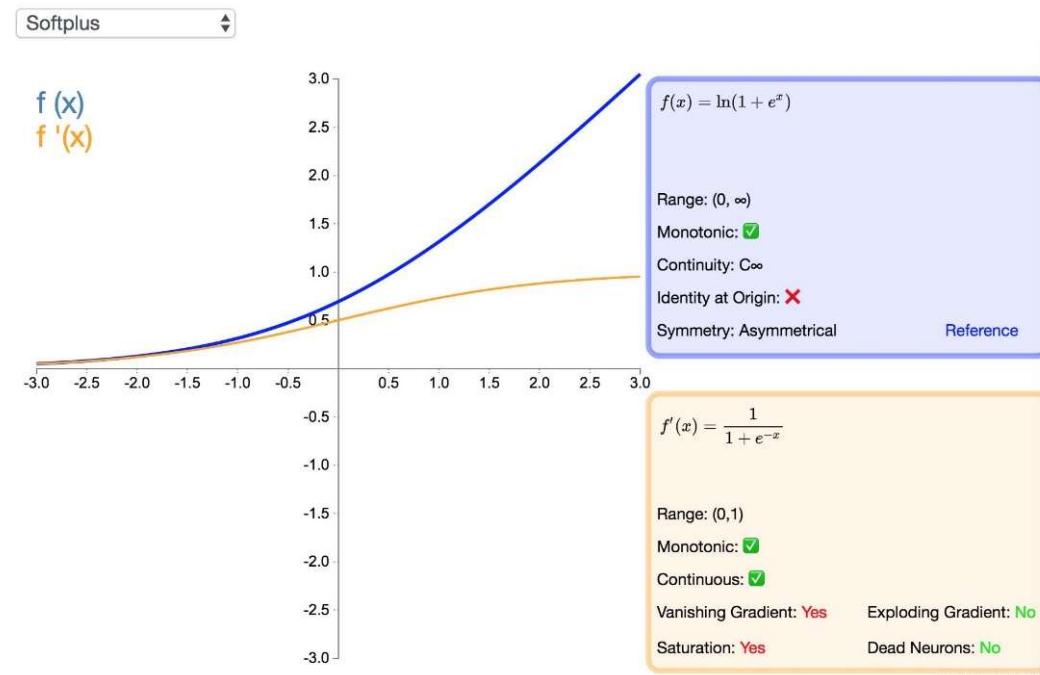
Exploding Gradient: No

Saturation: Yes

Dead Neurons: Yes

Softplus

$$f(x) = \ln(e^x + 1)$$



Softmax

- Softmax function:

$$\sigma(z)_j = \frac{e^{z_j}}{\sum_k e^{z_k}}$$

- The Softmax function is used to map a K-dimensional vector of arbitrary real values to another K-dimensional vector of real values, where each vector element is in the interval (0, 1). All the elements add up to 1.
- The Softmax function is often used as the output layer of a multiclass classification task.

Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks



Normalizer

- Regularization is an important and effective technology to reduce generalization errors in machine learning. It is especially useful for deep learning models that tend to be over-fit due to a large number of parameters. Therefore, researchers have proposed many effective technologies to prevent over-fitting, including:
 - Adding constraints to parameters, such as L_1 and L_2 norms
 - Expanding the training set, such as adding noise and transforming data
 - Dropout
 - Early stopping

Penalty Parameters

- Many regularization methods restrict the learning capability of models by adding a penalty parameter $\Omega(\theta)$ to the objective function J . Assume that the target function after regularization is \tilde{J} .

$$\tilde{J}(\theta; X, y) = J(\theta; X, y) + \alpha\Omega(\theta),$$

- Where $\alpha \in [0, \infty)$ is a hyperparameter that weights the relative contribution of the norm penalty term Ω and the standard objective function $J(X; \theta)$. If α is set to 0, no regularization is performed. The penalty in regularization increases with α .

L_1 Regularization

- Add L_1 norm constraint to model parameters, that is,

$$\tilde{J}(w; X, y) = J(w; X, y) + \alpha \|w\|_1,$$

- If a gradient method is used to resolve the value, the parameter gradient is

$$\nabla \tilde{J}(w) = \alpha \text{sign}(w) + \nabla J(w).$$

L_2 Regularization

- Add norm penalty term L_2 to prevent overfitting.

$$\tilde{J}(w; X, y) = J(w; X, y) + \frac{1}{2}\alpha\|w\|_2^2,$$

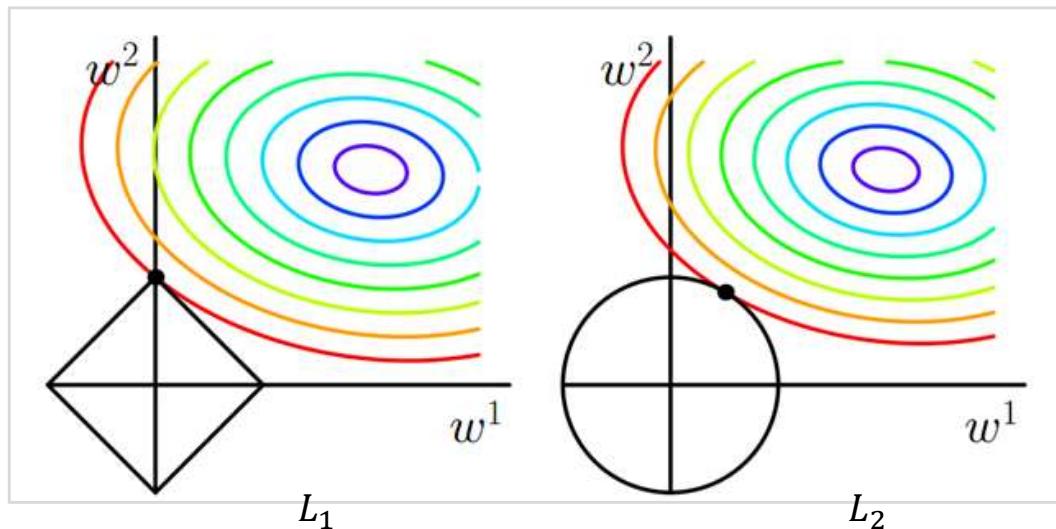
- A parameter optimization method can be inferred using an optimization technology (such as a gradient method):

$$w = (1 - \varepsilon\alpha)\omega - \varepsilon\nabla J(w),$$

- where ε is the learning rate. Compared with a common gradient optimization formula, this formula multiplies the parameter by a reduction factor.

L_1 v.s. L_2

- The major differences between L_2 and L_1 :
 - According to the preceding analysis, L_1 can generate a more sparse model than L_2 . When the value of parameter w is small, L_1 regularization can directly reduce the parameter value to 0, which can be used for feature selection.
 - From the perspective of probability, many norm constraints are equivalent to adding prior probability distribution to parameters. In L_2 regularization, the parameter value complies with the Gaussian distribution rule. In L_1 regularization, the parameter value complies with the Laplace distribution rule.

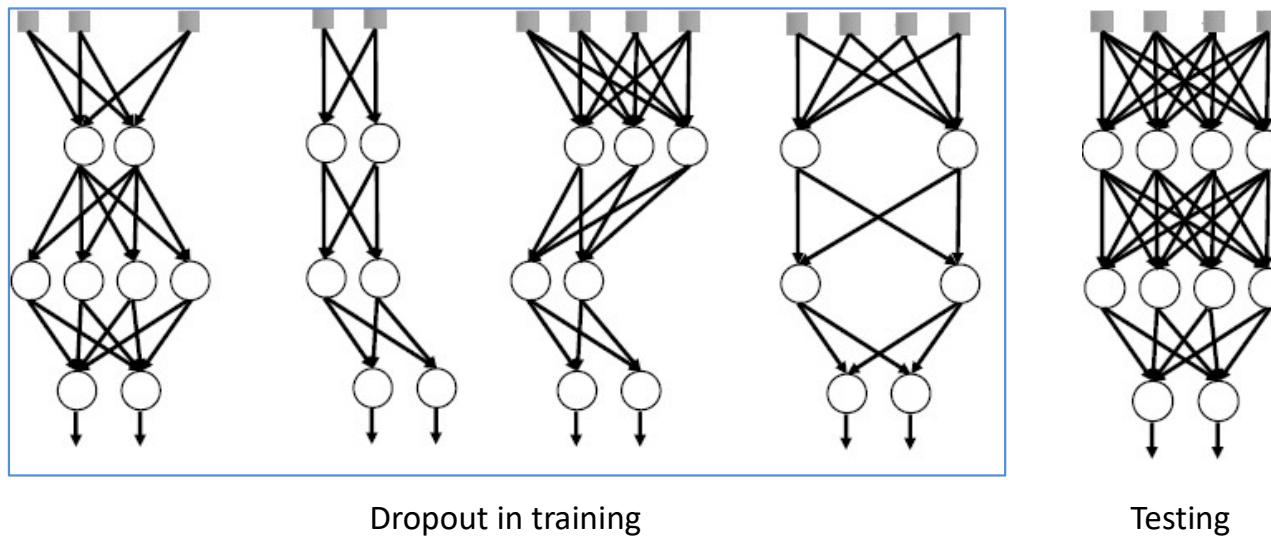


Dataset Expansion

- The most effective way to prevent over-fitting is to add a training set. A larger training set has a smaller over-fitting probability. Dataset expansion is a time-saving method, but it varies in different fields.
 - A common method in the object recognition field is to rotate or scale images. (The prerequisite to image transformation is that the type of the image cannot be changed through transformation. For example, for handwriting digit recognition, categories 6 and 9 can be easily changed after rotation).
 - Random noise is added to the input data in speech recognition.
 - A common practice of natural language processing (NLP) is replacing words with their synonyms.
 - Noise injection can add noise to the input or to the hidden layer or output layer. For example, for Softmax classification, noise can be added using the label smoothing technology. If noise is added to categories 0 and 1, the corresponding probabilities are changed to $\frac{\varepsilon}{k}$ and $1 - \frac{k-1}{k}\varepsilon$ respectively.

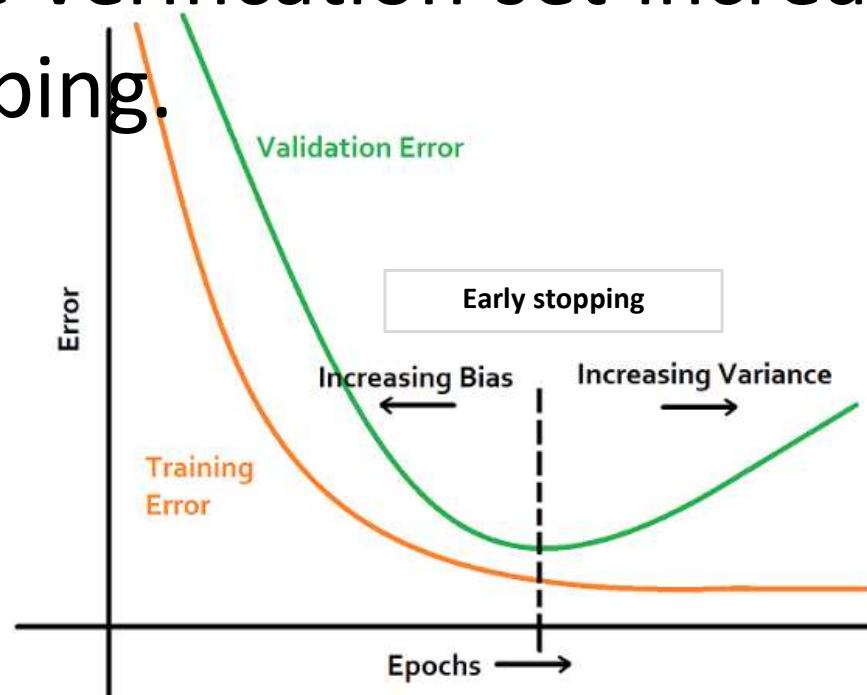
Dropout

- Dropout is a common and simple regularization method, which has been widely used since 2014. Simply put, Dropout randomly discards some inputs during the training process. In this case, the parameters corresponding to the discarded inputs are not updated. As an integration method, Dropout combines all sub-network results and obtains sub-networks by randomly dropping inputs. See the figures below:



Early Stopping

- A test on data of the validation set can be inserted during the training. When the data loss of the verification set increases, perform early stopping.



Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks

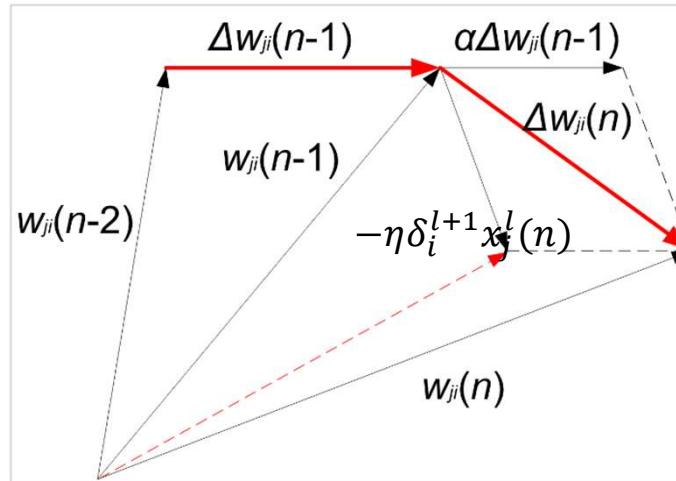


Optimizer

- There are various optimized versions of gradient descent algorithms. In object-oriented language implementation, different gradient descent algorithms are often encapsulated into objects called optimizers.
- Purposes of the algorithm optimization include but are not limited to:
 - Accelerating algorithm convergence.
 - Preventing or jumping out of local extreme values.
 - Simplifying manual parameter setting, especially the learning rate (LR).
- Common optimizers: common GD optimizer, momentum optimizer, Nesterov, AdaGrad, AdaDelta, RMSProp, Adam, AdaMax, and Nadam.

Momentum Optimizer

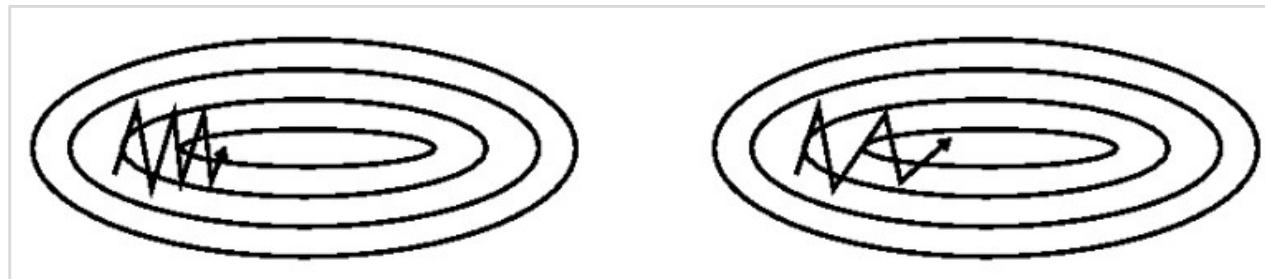
- A most basic improvement is to add momentum terms for Δw_{ji} . Assume that the weight correction of the n -th iteration is $\Delta w_{ji}(n)$. The weight correction rule is:
- $\Delta w_{ji}^l(n) = -\eta \delta_i^{l+1} x_j^l(n) + \alpha \Delta w_{ji}^l(n-1)$
- where α is a constant ($0 \leq \alpha < 1$) called Momentum Coefficient and $\alpha \Delta w_{ji}(n-1)$ is a momentum term.
- Imagine a small ball rolls down from a random point on the error surface. The introduction of the momentum term is equivalent to giving the small ball inertia.



Advantages and Disadvantages of

Momentum Optimizer

- Advantages:
 - Enhances the stability of the gradient correction direction and reduces mutations.
 - In areas where the gradient direction is stable, the ball rolls faster and faster (there is a speed upper limit because $\alpha < 1$), which helps the ball quickly overshoot the flat area and accelerates convergence.
 - A small ball with inertia is more likely to roll over some narrow local extrema.
- Disadvantages:
 - The learning rate η and momentum α need to be manually set, which often requires more experiments to determine the appropriate value.



AdaGrad Optimizer (1)

- The common feature of the random gradient descent algorithm (SGD), small-batch gradient descent algorithm (MBGD), and momentum optimizer is that each parameter is updated with the same LR.
- According to the approach of AdaGrad, different learning rates need to be set for different parameters.

$$g_t = \frac{\partial C(t, o)}{\partial w}$$

Gradient calculation

- g_t indicates the t -th gradient, r_t is a gradient accumulation variable, and the initial value of r is 0, which **increases continuously**. η indicates the global LR, which needs to be set manually. ϵ is a small constant, and is set to about 10^{-7} for numerical stability.

Square gradient accumulation

$$\Delta w_t = -\frac{\eta}{\epsilon + \sqrt{r_t}} g_t$$

Computing update

$$w_{t+1} = w_t + \Delta w_t$$

Application update

AdaGrad Optimizer (2)

- The AdaGrad optimization algorithm shows that the r continues increasing while the overall learning rate keeps decreasing as the algorithm iterates. This is because we hope LR to decrease as the number of updates increases. In the initial learning phase, we are far away from the optimal solution to the loss function. As the number of updates increases, we are closer to the optimal solution, and therefore LR can decrease.
- Pros:
 - The learning rate is automatically updated. As the number of updates increases, the learning rate decreases.
- Cons:
 - The denominator keeps accumulating so that the learning rate will eventually become very small, and the algorithm will become ineffective.

RMSProp Optimizer

- The RMSProp optimizer is an improved AdaGrad optimizer. It introduces an attenuation coefficient to ensure a certain attenuation ratio for r in each round.
- The RMSProp optimizer solves the problem that the AdaGrad optimizer ends the optimization process too early. It is suitable for non-stable target handling and has good effects on the RNN.

- $g_t = \frac{\partial C(t, o)}{\partial w}$ indicates the t th gradient, r is a gradient accumulation variable, and the initial value of r is 0, which **may not increase and needs to be adjusted using a parameter**. β is the attenuation factor, η indicates the global LR, which needs to be set manually. ε is a small constant, and is set to about 10^{-7} for numerical stability.

$$\Delta w_t = -\frac{\eta}{\varepsilon + \sqrt{r_t}} g_t$$

Gradient calculation

Square gradient accumulation

Computing update

$$w_{t+1} = w_t + \Delta w_t$$

Application update

Adam Optimizer (1)

- Adaptive Moment Estimation (Adam): Developed based on AdaGrad and AdaDelta, Adam maintains two additional variables m_t and v_t for each variable to be trained:

$$\begin{aligned}m_t &= \beta_1 m_{t-1} + (1 - \beta_1) g_t \\v_t &= \beta_2 v_{t-1} + (1 - \beta_2) g_t^2\end{aligned}$$

- Where t represents the t -th iteration and g_t is the calculated gradient. m_t and v_t are moving averages of the gradient and square gradient. From the statistical perspective, m_t and v_t are estimates of the first moment (the average value) and the second moment (the uncentered variance) of the gradients

Adam Optimizer (2)

- If m_t and v_t are initialized using the zero vector, m_t and v_t are close to 0 during the initial iterations, especially when β_1 and β_2 are close to 1. To solve this problem, we use \hat{m}_t and \hat{v}_t :

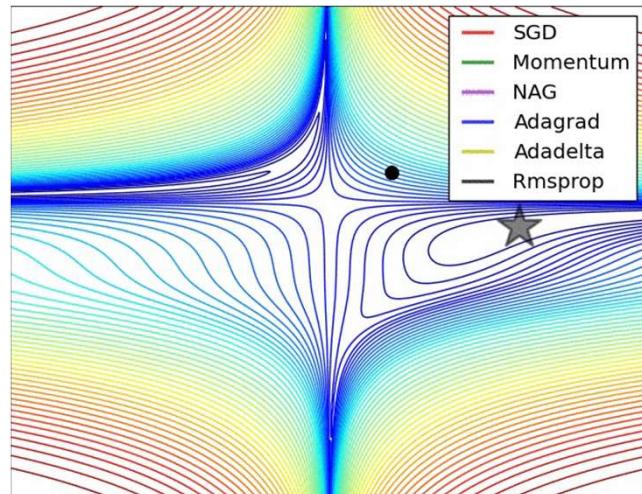
$$\begin{aligned}\hat{m}_t &= \frac{m_t}{1 - \beta_1^t} \\ \hat{v}_t &= \frac{v_t}{1 - \beta_2^t}\end{aligned}$$

- The weight update rule of Adam is as follows:

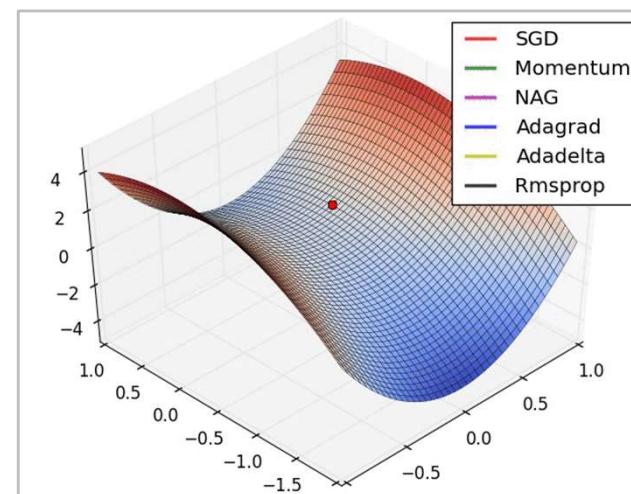
$$w_{t+1} = w_t - \frac{\eta}{\sqrt{\hat{v}_t} + \epsilon} \hat{m}_t$$

- Although the rule involves manual setting of η , β_1 , and β_2 , the setting is much simpler. According to experiments, the default settings are $\beta_1 = 0.9$, $\beta_2 = 0.999$, $\epsilon = 10^{-8}$, and $\eta = 0.001$. In practice, Adam will converge quickly. When convergence saturation is reached, η can be reduced. After several times of reduction, a satisfying local extremum will be obtained. Other parameters do not need to be adjusted.

Optimizer Performance Comparison



Comparison of optimization algorithms in contour maps of loss functions



Comparison of optimization algorithms at the saddle point

Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks

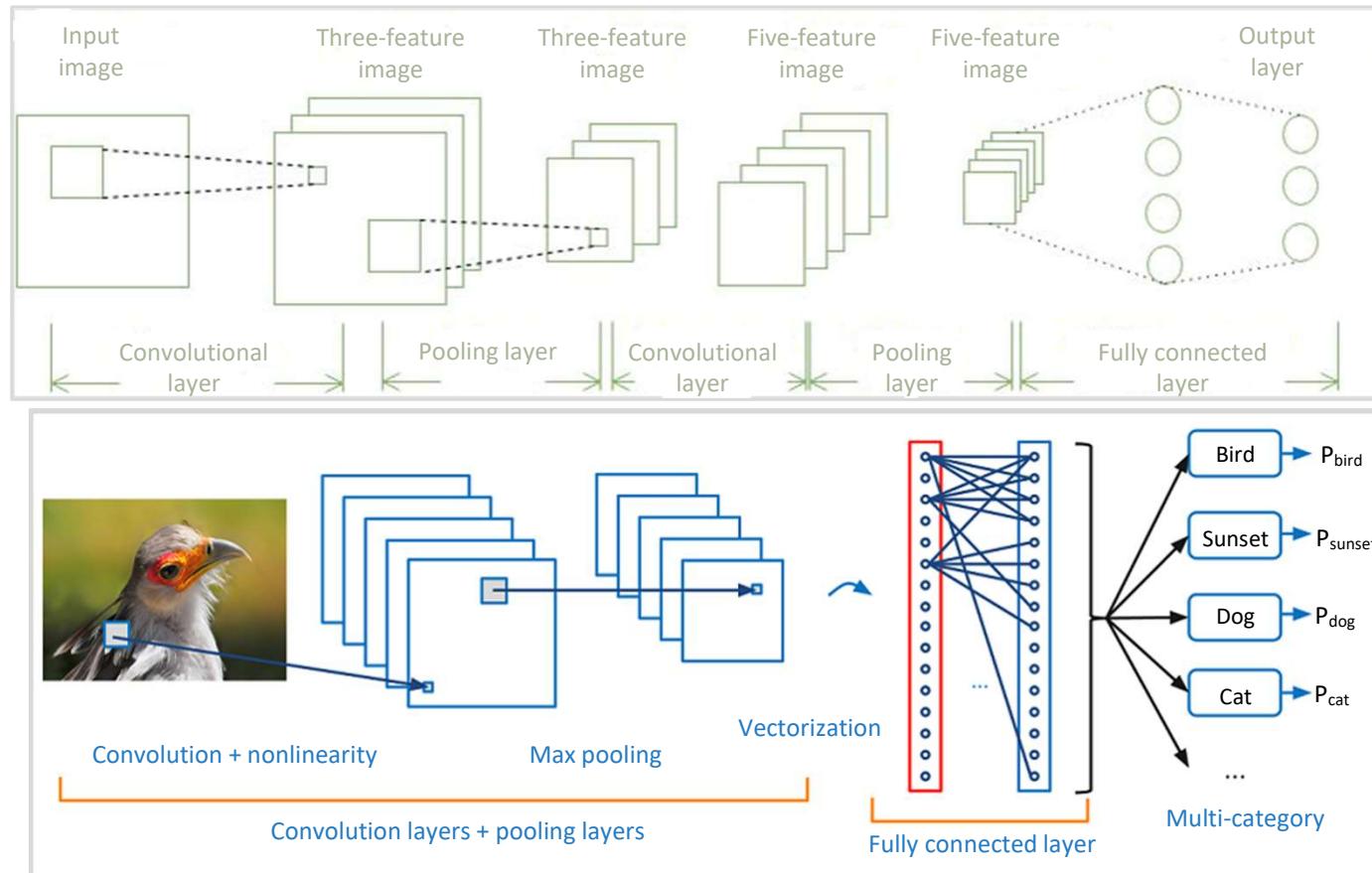
Convolutional Neural Network

- A convolutional neural network (CNN) is a feedforward neural network. Its artificial neurons may respond to **surrounding units within the coverage range**. CNN excels at image processing. It includes a **convolutional layer**, a **pooling layer**, and a **fully connected layer**.
- In the 1960s, Hubel and Wiesel studied cats' cortex neurons used for local sensitivity and direction selection and found that their unique network structure could simplify feedback neural networks. They then proposed the CNN.
- Now, CNN has become one of the research hotspots in many scientific fields, especially in the pattern classification field. The network is widely used because it can avoid complex pre-processing of images and directly input original images.

Main Concepts of CNN

- **Local receptive field:** It is generally considered that human perception of the outside world is from local to global. **Spatial correlations among local pixels of an image are closer than those among distant pixels.** Therefore, each neuron does not need to know the global image. It only needs to know the local image. The local information is combined at a higher level to generate global information.
- **Parameter sharing:** One or more filters/kernels may be used to scan input images. Parameters carried by the filters are weights. In a layer scanned by filters, each filter uses the same parameters during weighted computation. Weight sharing means that when each filter scans an entire image, parameters of the filter are fixed.

Architecture of Convolutional Neural Network



Single-Filter Calculation (1)

- Description of convolution calculation

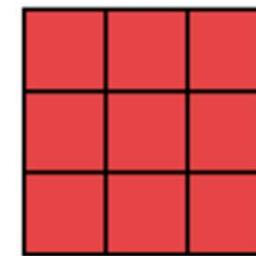
1	1	1	0	0
0	1	1	1	0
0	0	1	1	1
0	0	1	1	0
0	1	1	0	0

image 5*5

1	0	1
0	1	0
1	0	1

bias=0

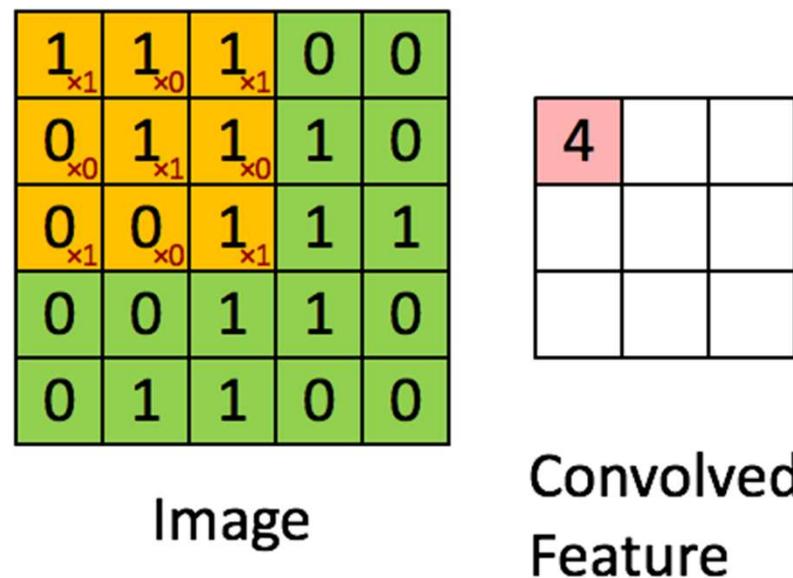
filter 3*3



feature map 3*3

Single-Filter Calculation (2)

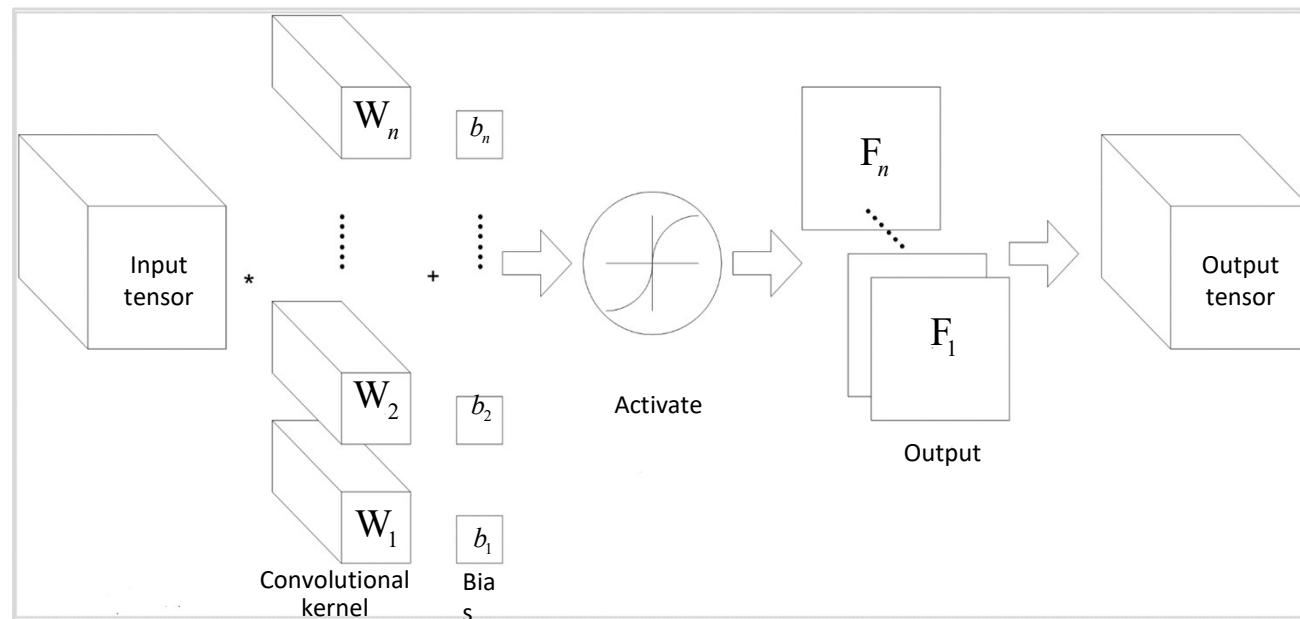
- Demonstration of the convolution calculation



Han Bingtao, 2017, Convolutional Neural Network

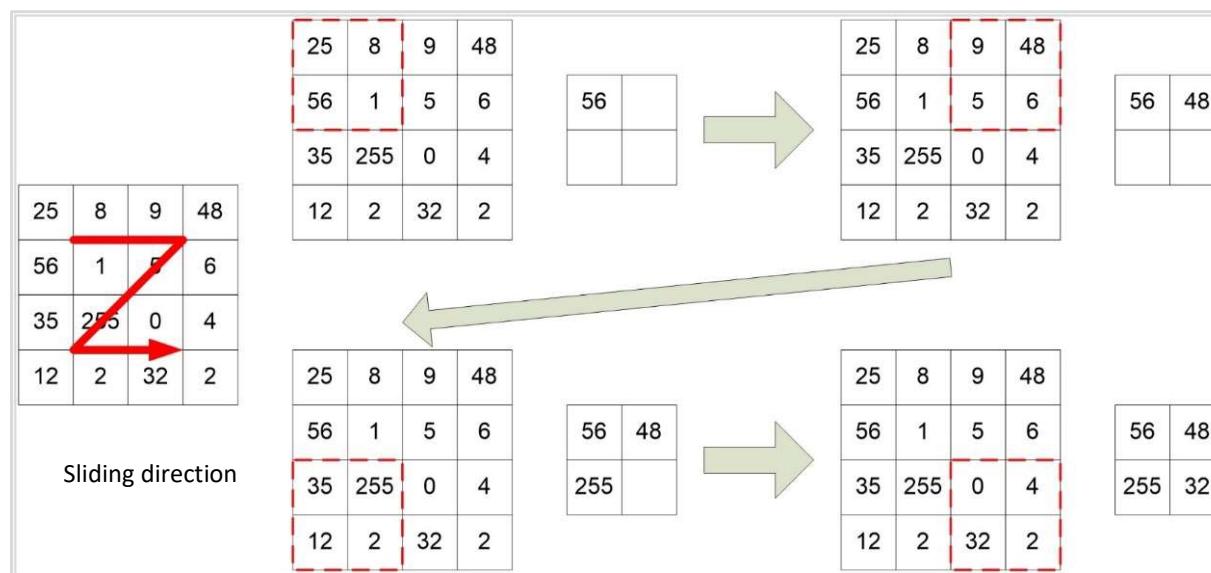
Convolutional Layer

- The basic architecture of a CNN is multi-channel convolution consisting of multiple single convolutions. The output of the previous layer (or the original image of the first layer) is used as the input of the current layer. It is then convolved with the filter in the layer and serves as the output of this layer. The convolution kernel of each layer is the weight to be learned. Similar to FCN, after the convolution is complete, the result should be biased and activated through activation functions before being input to the next layer.



Pooling Layer

- Pooling combines nearby units to reduce the size of the input on the next layer, reducing dimensions. Common pooling includes max pooling and average pooling. When max pooling is used, the maximum value in a small square area is selected as the representative of this area, while the mean value is selected as the representative when average pooling is used. The side of this small area is the pool window size. The following figure shows the max pooling operation whose pooling window size is 2.



Fully Connected Layer

- The fully connected layer is essentially a classifier. The features extracted on the convolutional layer and pooling layer are straightened and placed at the fully connected layer to output and classify results.
- Generally, the Softmax function is used as the activation function of the final fully connected output layer to combine all local features into global features and calculate the score of each type.

$$\sigma(z)_j = \frac{e^{z_j}}{\sum_k e^{z_k}}$$

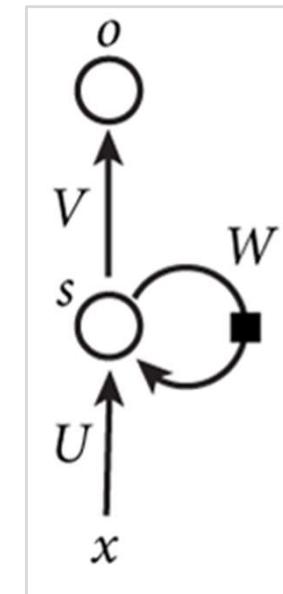
Recurrent Neural Network

- The recurrent neural network (RNN) is a neural network that captures dynamic information in sequential data through periodical connections of hidden layer nodes. It can classify sequential data.
- Unlike other forward neural networks, the RNN can keep a context state and even store, learn, and express related information in context windows of any length. Different from traditional neural networks, it is not limited to the space boundary, but also supports time sequences. In other words, there is a side between the hidden layer of the current moment and the hidden layer of the next moment.
- The RNN is widely used in scenarios related to sequences, such as videos consisting of image frames, audio consisting of clips, and sentences consisting of words.

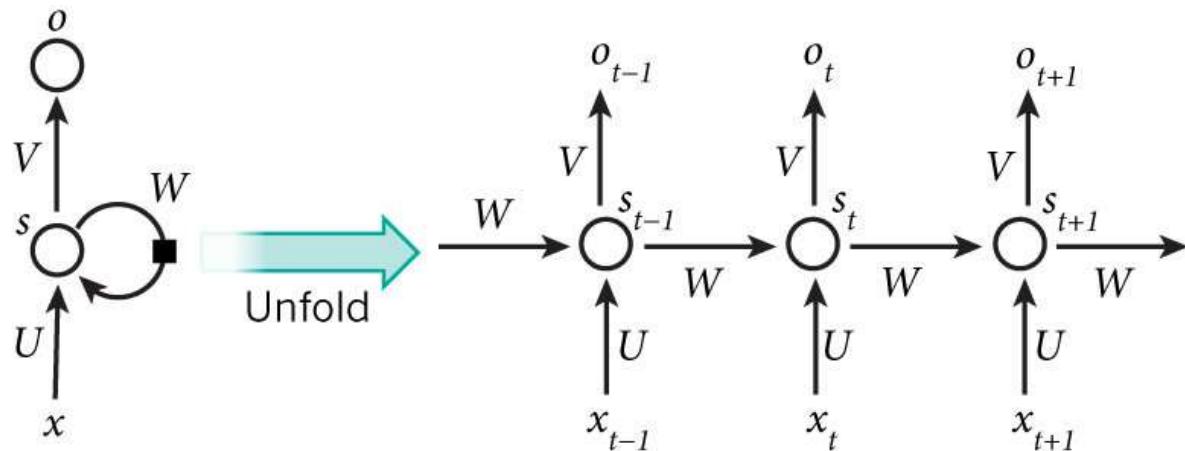
Recurrent Neural Network

Architecture (1)

- X_t is the input of the input sequence at time t.
- S_t is the memory unit of the sequence at time t and caches previous information.
$$S_t = \tanh(UX_t + WS_{t-1}).$$
- O_t is the output of the hidden layer of the sequence at time t.
$$O_t = \tanh(VS_t)$$
- O_t after through multiple hidden layers, it can get the final output of the sequence at time t.

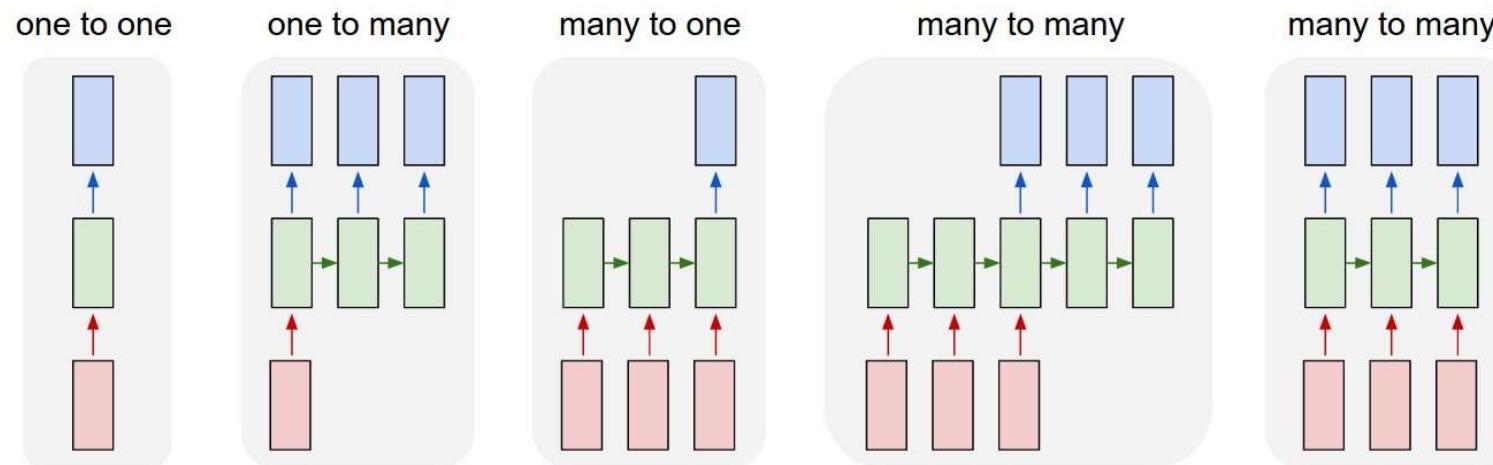


Recurrent Neural Network Architecture (2)



LeCun, Bengio, and G. Hinton, 2015, A Recurrent Neural Network and the Unfolding in Time of the Computation Involved in Its Forward Computation

Types of Recurrent Neural Networks



Andrej Karpathy, 2015, The Unreasonable Effectiveness of Recurrent Neural Networks

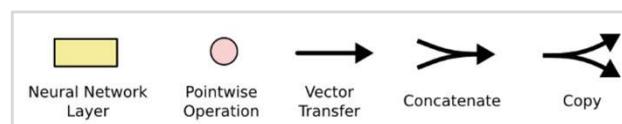
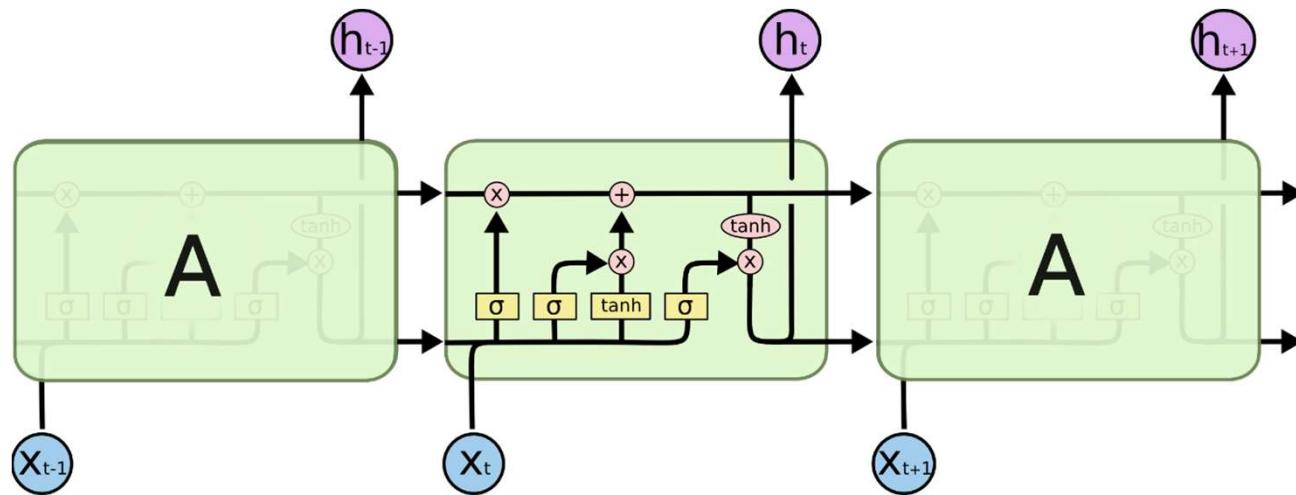
Backpropagation Through Time (BPTT)

- BPTT:
 - Traditional backpropagation is the extension on the time sequence.
 - There are two sources of errors in the sequence at time of memory unit: first is from the hidden layer output error at t time sequence; the second is the error from the memory cell at the next time sequence $t + 1$.
 - The longer the time sequence, the more likely the loss of the last time sequence to the gradient of w in the first time sequence causes the vanishing gradient or exploding gradient problem.
 - The total gradient of weight w is the accumulation of the gradient of the weight at all time sequence.
- Three steps of BPTT:
 - Computing the output value of each neuron through forward propagation.
 - Computing the error value of each neuron through backpropagation δ_j .
 - Computing the gradient of each weight.
- Updating weights using the SGD algorithm.

Recurrent Neural Network Problem

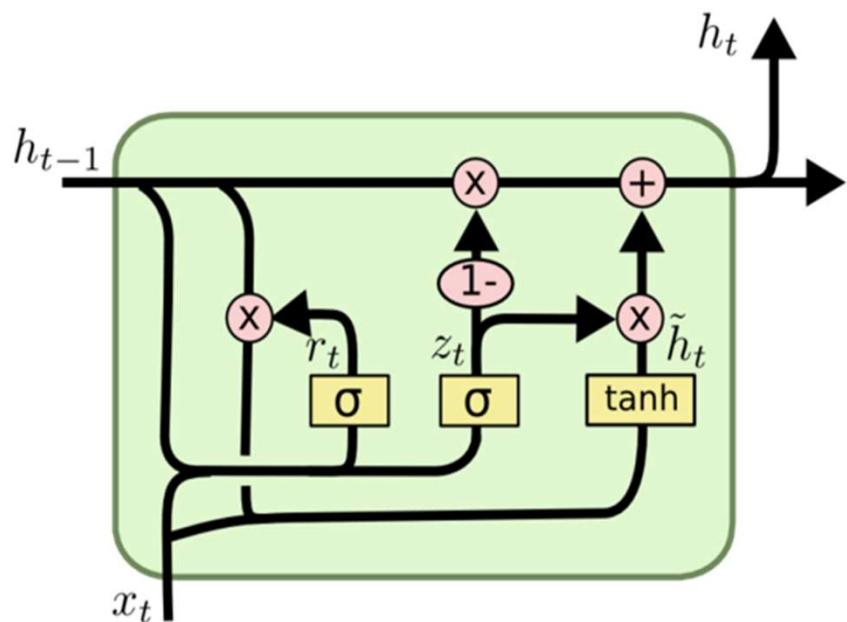
- $S_t = \sigma(UX_t + WS_{t-1})$ is extended on the time sequence.
- $$S_t = \sigma\left(UX_t + W \left(\sigma \left(UX_{t-1} + W \left(\sigma \left(UX_{t-2} + W(\dots) \right) \right) \right) \right) \right)$$
- Despite that the standard RNN structure solves the problem of information memory, the information attenuates during long-term memory.
- Information needs to be saved long time in many tasks. For example, a hint at the beginning of a speculative fiction may not be answered until the end.
- The RNN may not be able to save information for long due to the limited memory unit capacity.
- We expect that memory units can remember key information.

Long Short-term Memory Network



Colah, 2015, Understanding LSTMs Networks

Gated Recurrent Unit (GRU)



$$z_t = \sigma (W_z \cdot [h_{t-1}, x_t])$$

$$r_t = \sigma (W_r \cdot [h_{t-1}, x_t])$$

$$\tilde{h}_t = \tanh (W \cdot [r_t * h_{t-1}, x_t])$$

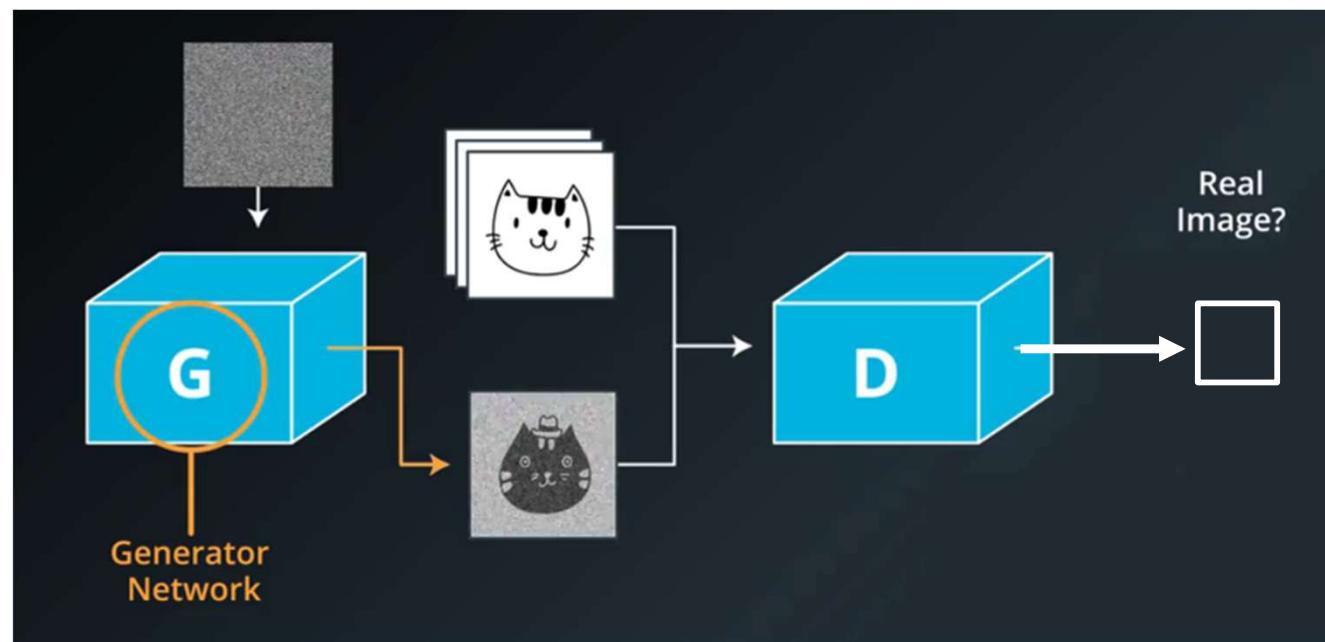
$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t$$

Generative Adversarial Network (GAN)

- Generative Adversarial Network is a framework that trains generator G and discriminator D through the adversarial process. Through the adversarial process, the discriminator can tell whether the sample from the generator is fake or real. GAN adopts a mature BP algorithm.
- (1) Generator G: The input is noise z , which complies with manually selected prior probability distribution, such as even distribution and Gaussian distribution. The generator adopts the network structure of the multilayer perceptron (MLP), uses maximum likelihood estimation (MLE) parameters to represent the derivable mapping $G(z)$, and maps the input space to the sample space.
- (2) Discriminator D: The input is the real sample x and the fake sample $G(z)$, which are tagged as real and fake respectively. The network of the discriminator can use the MLP carrying parameters. The output is the probability $D(G(z))$ that determines whether the sample is a real or fake sample.
- GAN can be applied to scenarios such as image generation, text generation, speech enhancement, image super-resolution.

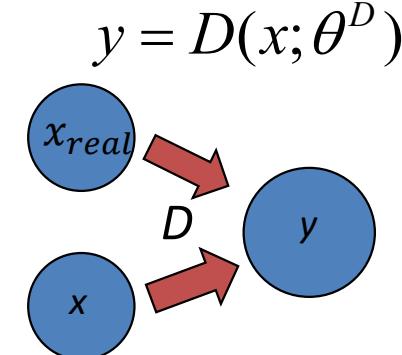
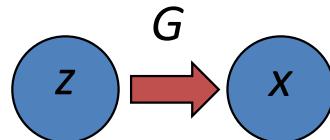
GAN Architecture

- Generator/Discriminator



Generative Model and Discriminative Model

- Generative network
 - Generates sample data
 - Input: Gaussian white noise vector z
 - Output: sample data vector x
- Discriminator network
 - Determines whether sample data is real
 - Input: real sample data x_{real} and generated sample data $x = G(z)$
 - Output: probability that determines whether the sample is real



Training Rules of GAN

- Optimization objective:
 - Value function

$$\min_G \max_D V(D, G) = E_{x \sim p_{data}(x)}[\log D(x)] + E_{z \sim p_z(z)}[\log(1 - D(G(z)))]$$

– In the early training stage, when the outcome of G is very poor, D determines that the generated sample is fake with high confidence, because the sample is obviously different from training data. In this case, $\log(1 - D(G(z)))$ is saturated (where the gradient is 0, and iteration cannot be performed). Therefore, we choose to train G only by minimizing $[-\log(D(G(z)))]$.

Contents

1. Deep Learning Summary

2. Training Rules

3. Activation Function

4. Normalizer

5. Optimizer

6. Types of Neural Networks



Data Imbalance (1)

- Problem description: In the dataset consisting of various task categories, the number of samples varies greatly from one category to another. One or more categories in the predicted categories contain very few samples.
- For example, in an image recognition experiment, more than 2,000 categories among a total of 4251 training images contain just one image each. Some of the others have 2-5 images.
- Impacts:
 - Due to the unbalanced number of samples, we cannot get the optimal real-time result because model/algorithm never examines categories with very few samples adequately.
 - Since few observation objects may not be representative for a class, we may fail to obtain adequate samples for verification and test.

Data Imbalance (2)

Random undersampling

- Deleting redundant samples in a category

Random oversampling

- Copying samples

Sy
Mi
Overs
Tec

- Sampling
- Merging

Data Imbalance (2)

Random undersampling

- Deleting redundant samples in a category

Random oversampling

- Copying samples

Sy
Mi
Overs
Tec

- Sampling
- Merging

Vanishing Gradient and Exploding

- Vanishing gradient: As network layers increase, the derivative value of backpropagation decreases, which causes a vanishing gradient problem.
- Exploding gradient: As network layers increase, the derivative value of backpropagation increases, which causes an exploding gradient problem.
 $y_i = \sigma(w_i^T x + b_i)$ Where σ is sigmoid function.
- Cause:



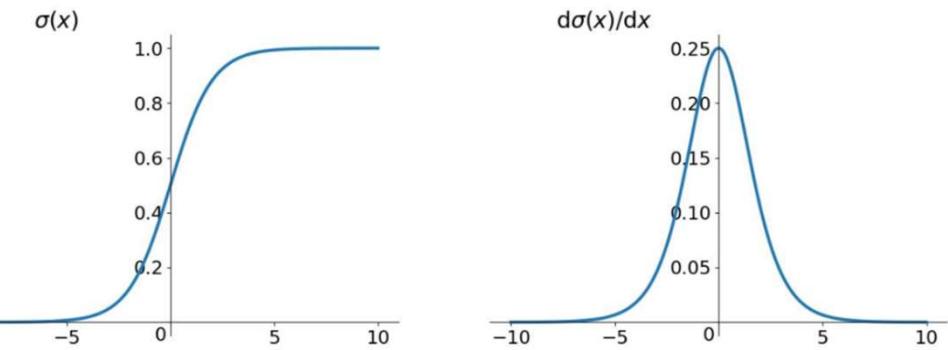
$$\frac{\partial C}{\partial b_1} = \frac{\partial C}{\partial y_4} \frac{\partial y_4}{\partial z_4} \frac{\partial z_4}{\partial x_4} \frac{\partial x_4}{\partial z_3} \frac{\partial z_3}{\partial x_3} \frac{\partial x_3}{\partial z_2} \frac{\partial z_2}{\partial x_2} \frac{\partial x_2}{\partial z_1} \frac{\partial z_1}{\partial b_1}$$

- Backpropagation can be deduced as follows:

Vanishing Gradient and Exploding Gradient Problem (2)

- The maximum value of $\sigma'(0)$ is $\frac{1}{4}$.

- However, the network weight $|w|$ is usually smaller. As $|w|$ increases, the derivation result $\frac{\partial C}{\partial b_1}$ decreases, resulting in a vanishing gradient.
- When the network weight $|w|$ is large, resulting in $|w| \gg 1$, the derivative value is very small.
- Solution: For example, gradient clipping is used to alleviate the vanishing gradient problem. LSTM are used to alleviate the exploding gradient problem.



Overfitting

- Problem description: The model performs well in the training set, but badly in the test set.
- Root cause: There are too many feature dimensions, model assumptions, and parameters, too much noise, but very few training data. As a result, the fitting function perfectly predicts the training set, while the prediction result of the test set of new data is poor. Training data is over-fitted without considering generalization capabilities.
- Solution: For example, data augmentation, regularization, early stopping, and dropout

Overfitting

- Problem description: The model performs well in the training set, but badly in the test set.
- Root cause: There are too many feature dimensions, model assumptions, and parameters, too much noise, but very few training data. As a result, the fitting function perfectly predicts the training set, while the prediction result of the test set of new data is poor. Training data is over-fitted without considering generalization capabilities.
- Solution: For example, data augmentation, regularization, early stopping, and dropout