Institut intelligence et données

Intelligence artificielle, possibilités et réalité

Julien Laumônier

9 décembre 2020

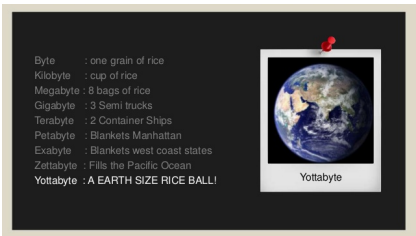
Institut intelligence et données

Introduction

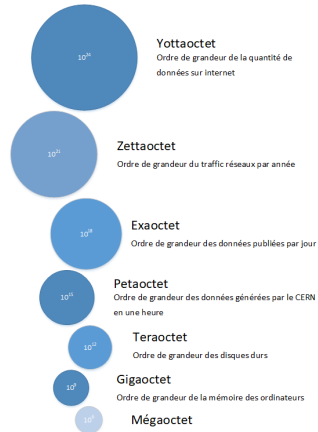
- L'intelligence artificielle connaît un essor grandissant pour un grand nombre d'usages et dans de nombreux domaines de la vie de tous les jours.
  - Disponibilité de données massives;
  - Découvertes scientifiques.
  - Évolution de la technologie du matériel;
- Ses concepts et donc ses conséquences restent difficiles à appréhender.
- Pour les démystifier, nous allons les aborder en trois sections :
  - Les données massives, la matière première de l'intelligence artificielle;
  - Les concepts de base et les possibilités;
  - Les limites et difficultés actuelles.

Données massives

- L'expression *Big Data*, en anglais, se traduit par mégadonnées ou données massives, en français.
- Nous utilisons le terme *données massives* car nous pensons, entre autres, qu'il ne se limite pas seulement à un enjeu de quantité.



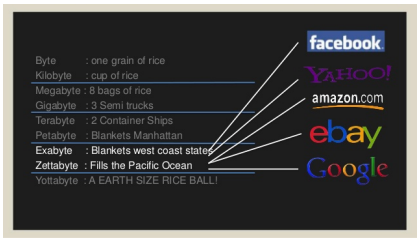
Tiré de la présentation de David Wellman http ://fr.slideshare.net/dwellman/what-is-big-data-24401517



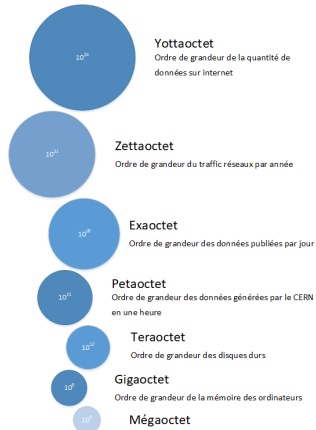
UNIVERSITÉ LAVAL

Données massives

- L'expression *Big Data*, en anglais, se traduit par mégadonnées ou données massives, en français.
- Nous utilisons le terme *données massives* car nous pensons, entre autres, qu'il ne se limite pas seulement à un enjeu de quantité.



Tiré de la présentation de David Wellman
http ://fr.slideshare.net/dwellman/what-is-big-data-24401517



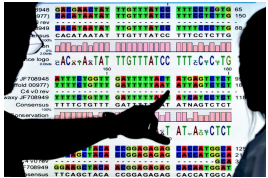
UNIVERSITÉ LAVAL

Données massives en 4V

- *Volume*
  - Quantité de données
- *Vélocité*
  - Vitesse à laquelle les données sont générées.
  - Données de plus en plus disponibles en temps-réel.
- *Variété*
  - Données provenant de diverses sources
    - Structurées ou non (images, textes, données de capteurs)
  - Données provenant de projets différents
    - avec des méthodologies non nécessairement compatibles
- *Véracité*
  - Données rapidement désuètes et non forcément correctes
  - Importance d'évaluer la qualité des données

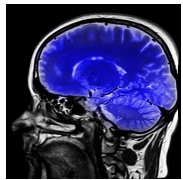
Données massives

Exemple de données hétérogènes et non structurées

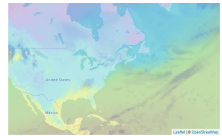


Interprétation de données « omics »

combinées avec des données cliniques



des données d'imageries

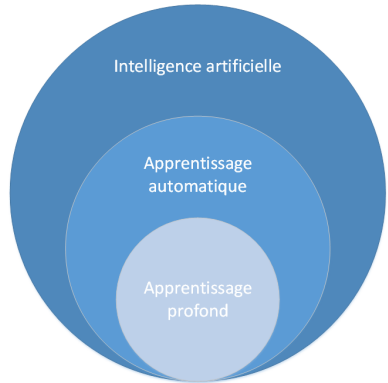


et des données environnementales

UNIVERSITÉ LAVAL

Qu'est-ce qu'on en fait ?

- Parfois on ajoute un 5e V : la *Valeur*
- Comment transformer/analyser pour trouver la valeur de ces données ?
- C'est là que l'intelligence artificielle entre en ligne de compte



Inspirée de « Why Deep Learning Matters and what's next for Artificial Intelligence », Algorithmia, Novembre 2016

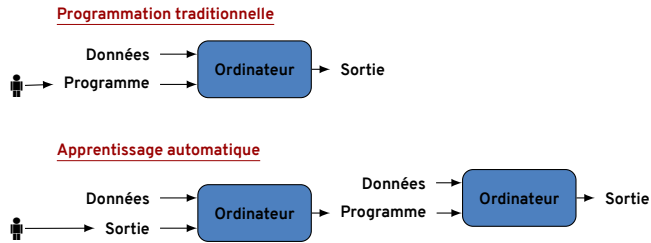
UNIVERSITÉ LAVAL

Apprentissage automatique 101

Champ d'étude qui donne à un ordinateur la capacité à apprendre sans être explicitement programmé

Arthur Samuel (1959)

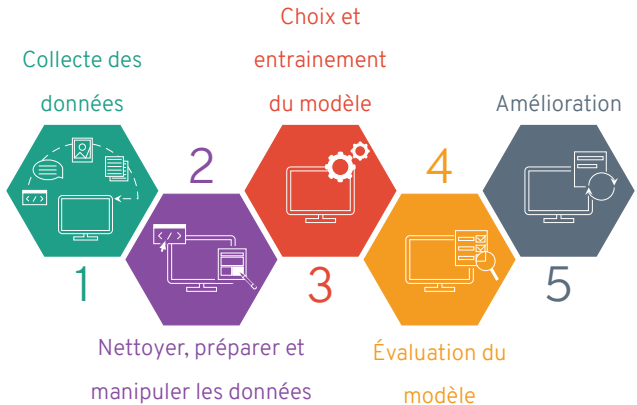
L'apprentissage se fait à partir d'exemples ou d'interaction avec l'environnement.



UNIVERSITÉ LAVAL

Apprentissage automatique 101

Processus

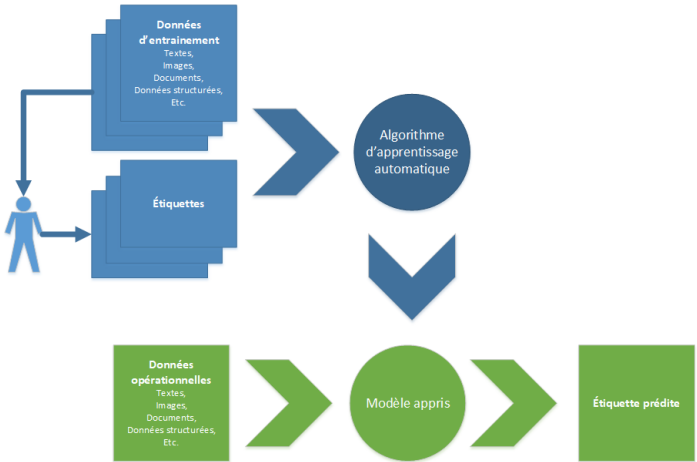


Source : inspiré de https ://cio-wiki.org/wiki/Machine_Learning, Kimberly Cook

UNIVERSITÉ LAVAL

Apprentissage automatique 101

Choix et entraînement du modèle



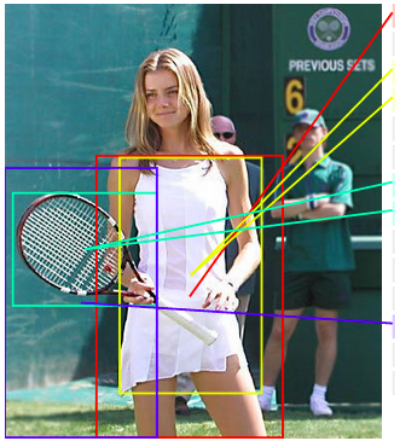
UNIVERSITÉ LAVAL

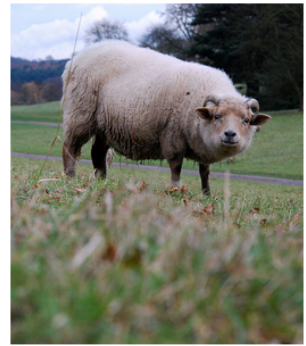
Résultat – Étiquetage de scènes par réseaux profonds

[Farabet et al. ICML, 2012, PAMI, 2013]

UNIVERSITÉ LAVAL

L’apprentissage automatique, un outil pour percevoir les informations





a sheep is standing in a field of grass
logprob: -9.13

http ://cs.stanford.edu/people/karpathy/deepimagesent/

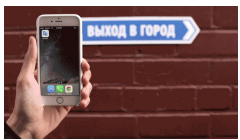
UNIVERSITÉ LAVAL

Apprentissage automatique

Réalisations

[Google car]

[Amazon Go]



[Google translate app]

[Boston Dynamics]

[Deep Mind AlphaGo]

UNIVERSITÉ LAVAL

L’apprentissage automatique, un outil pour « percevoir » les informations

a bathroom with a toilet and a sink
logprob: -7.17

a woman sitting on a bench with a laptop
logprob: -8.55

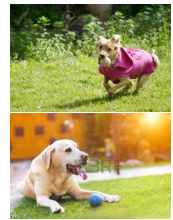
[https ://cs.stanford.edu/people/karpathy/deepimagesent/generationdemo/]

UNIVERSITÉ LAVAL

Quand la collecte peut causer des problèmes

Corrélation n'est pas causalité

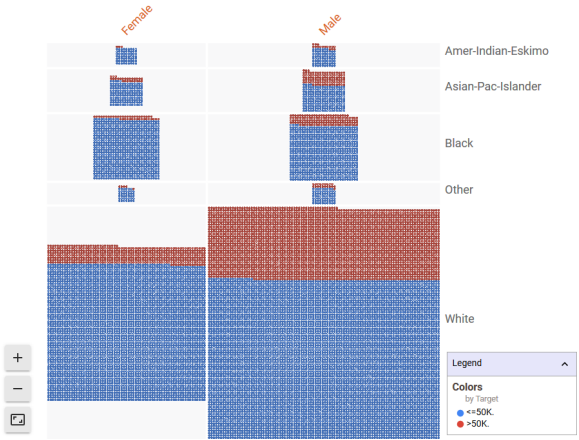
- Les données d'entraînement doivent être obtenues de façon iid.
  - i.e., chaque exemple des données d'entraînement est censé avoir été obtenu par un tirage d'une unique distribution inconnue et indépendamment des autres données obtenues.
- Idem pour les exemples « à venir »



UNIVERSITÉ LAVAL

Quand la collecte peut causer des problèmes

Équité



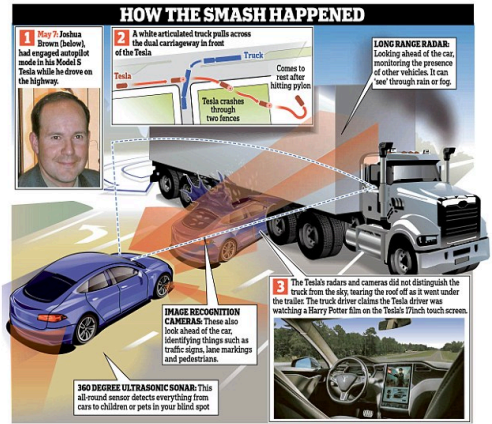
Source : https ://pair-code.github.io/facets

Le modèle d'apprentissage automatique est aussi « bon » que les données sur lesquelles il a été entraîné.

UNIVERSITÉ LAVAL

Quand la collecte peut causer des problèmes

Évènements rares



L'apprentissage automatique a besoin d'avoir une vision complète du problème à résoudre.

Source : https ://www.dailymail.co.uk/news/article-3715336/Tesla-engineers-say-car-involved-fatal-crash-autopilot-seen-tractor-trailer-blocking-road-chose-ignore-it.html

Quand la technique peut causer des problèmes

Robustesse

Source : Intriguing properties of neural networks, Szegedy et al., 2013, arXiv :1312.6199

UNIVERSITÉ LAVAL

Quand la technique peut causer des problèmes

Robustesse

Source : Intriguing properties of neural networks, Szegedy et al., 2013, arXiv :1312.6199

Source : Robust Physical-World Attacks on Deep Learning Models, Eykholt et al., 2017, arXiv :1707.08945

UNIVERSITÉ LAVAL

Quand la technique peut causer des problèmes

Confidentialité des données

- Possibilité de recouper des bases de données pour retrouver des informations personnelles : le cas Sweeney
- Possibilité de retrouver des informations personnelles à partir du modèle :

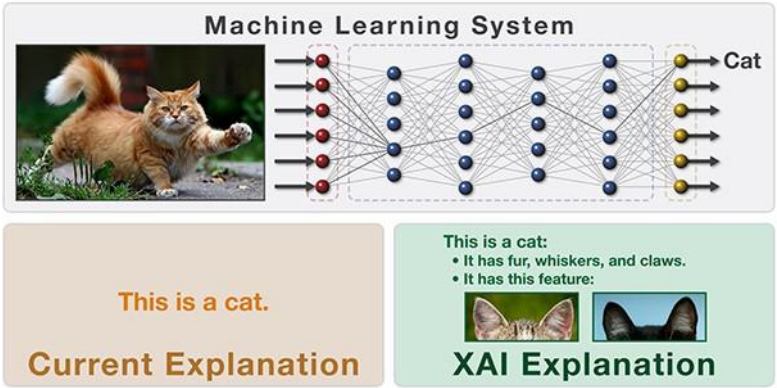
Figure 1: An image recovered using a new model inversion attack (left) and a training set image of the victim (right). The attacker is given only the person's name and access to a facial recognition system that returns a class confidence score.

Source : *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, M. Fredrikson, S. Jha, T. Ristenpart, CCS'15, 2015

UNIVERSITÉ LAVAL

Quand la technique peut causer des problèmes

Explicabilité



Source : https ://becominghuman.ai/interpretable-machine-learning-an-overview-10684eaa1fd7

Vers la certification

- Avant de pouvoir certifier les modèles d'apprentissage automatique, il faut améliorer leur robustesse, leur explicabilité et garantir la confidentialité.
- Développer la confiance dans les modèles.
  - Cette confiance dépend de la criticité du système.
- Plusieurs initiatives sont en cours.

UNIVERSITÉ LAVAL

Conclusion

- L'apprentissage automatique s'appuie sur les données pour prédire et proposer des décisions.
- Afin d'utiliser cet outil au mieux, il ne faut pas oublier :
  - Ces techniques offrent de grandes possibilités dans de nombreux domaines.
  - Les enjeux techniques et éthiques existent, il faut en avoir conscience et en faire prendre conscience.
  - Il faut bien réfléchir aux objectifs que l'on souhaite atteindre.
  - Renoncer aux données, c'est se couper de grandes possibilités !
  - Dans le cas général, on doit chercher un compromis entre la protection du citoyen et l'intérêt collectif.
  - D'autres enjeux peuvent également survenir (organisationnels, culture, gouvernance, ...).

Institut intelligence et données

POUR PLUS D'INFORMATIONS

julien.laumonier@iid.ulaval.ca
https://iid.ulaval.ca/
@iid.ulaval
iid-ulaval
@IID_ULaval
iid_ulaval