L'IA/AA dans tous les médias aujourd'hui

L'IA/AA est attendue **partout** demain

- Aide au **diagnostic médical**
- Aide aux **juges**
- Octroi de **prêts**
- Aide au **choix des employés**
- Évaluation du **risque de criminalité** avant l'acte criminel
- Calcul des **primes d'assurance**

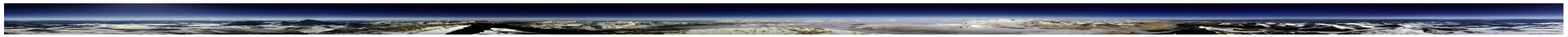
- **Assistant** personnel
- Véhicules **autonomes**
- Conduite des « **smart cities** »

De plus près

- Sommes-nous prêts ?

Qu'est-ce qu'un bon système d'apprentissage ?

La réponse a évolué avec le temps. Et demain ?



Antoine Cornuéjols

AgroParisTech – INRA MIA 518

antoine.cornuejols@agroparistech.fr

Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

Un premier cas

*Prédiction du **risque de récidive** à moins de 4 ans* ('+' ou '-')

Un premier cas

*Prédiction du **risque de récidive** à moins de 4 ans* ('+' ou '-')

- > 2200 cas provenant de 26 cours juridictionnelles européennes sur 15 ans
- Un trentaine de mesures (*âge, profession, niveau de formation, lieu de résidence, style de vie, antécédents de drogues, antécédents familiaux, …*)

Un premier cas

*Prédiction du **risque de récidive** à moins de 4 ans* ('+' ou '-')

- > 2200 cas provenant de 26 cours juridictionnelles européennes sur 15 ans
- Un trentaine de mesures (*âge, profession, niveau de formation, lieu de résidence, style de vie, antécédents de drogues, antécédents familiaux, …*)
- Méthodes :
  - Arbres de décision
  - Random forests
  - SVM

Un premier cas

*Prédiction du **risque de récidive** à moins de 4 ans* ('+' ou '-')

- > 2200 cas provenant de 26 cours juridictionnelles européennes sur 15 ans
- Un trentaine de mesures (*âge, profession, niveau de formation, lieu de résidence, style de vie, antécédents de drogues, antécédents familiaux, …*)
- Méthodes :
  - Arbres de décision
  - Random forests
  - SVM

Un juge utilise l'algorithme, qui prédit pour un sujet x_i :

- Classe '+' : une récidive aura lieu d'ici 4 ans
- (Éventuellement) avec un taux de confiance de ε% (e.g. 87%)

Que doit penser le juge?

Illustration (suite)

Le juge apprend que le taux de bonne classification de la meilleure hypothèse apprise sur les données test est de 62%

- Que doit-il penser pour le **cas du sujet x_i** ?

  Classe '+' avec probabilité estimée de 0.87

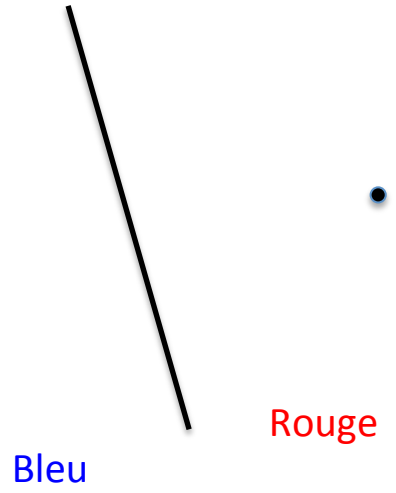
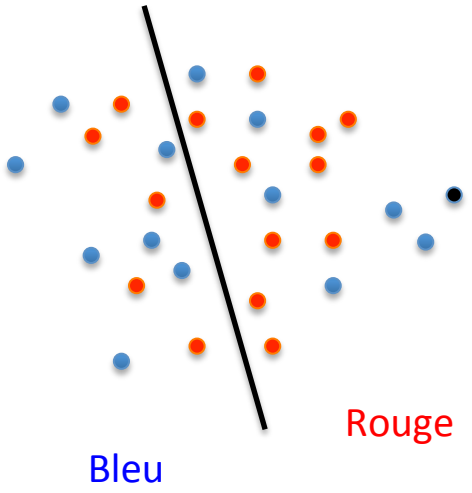


Illustration (suite)

Le juge apprend que le taux de bonne classification de la meilleure hypothèse apprise sur les données test est de 62%

- Que doit-il penser pour le **cas du sujet x_i** ?

  Classe '+' avec probabilité estimée de 0.87



Un **accident** de voiture (autonome)

Le 7 mai 2016, une voiture de la marque Tesla ***en mode « autopilot »***

percute un semi-remorque en travers de sa route

Un **accident** de voiture (autonome)

*Le 7 mai 2016, une voiture de la marque Tesla **en mode « autopilot »** percute un semi-remorque en travers de sa route*

- L'analyse révèle que :
  - Le **radar** a bien détecté le semi-remorque
    mais il y avait de nombreux panneaux routiers sur la route de « signature » radar proche
  - La **caméra** était peu sûre de ses détections en raison d'un ciel laiteux éblouissant (le semi-remorque était blanc)

Un accident de système complexe adaptatif

- L'analyse révèle que :
  - Le **radar** a bien détecté le semi-remorque
    mais …
  - La **caméra** était peu sûre de ses détections en raison de …

- **Et si** le radar avait dit qu'il avait des doutes et élevé le seuil d'alerte de la caméra, et réciproquement ? …
- **Et si** les systèmes avaient été adaptatifs ? …

Nécessité de **garanties**

1. Pouvoir « expliquer » ses préconisations
   - Prouver que le cas entre bien dans le **domaine de validité** du système de décision

Nécessité de **garanties**

1. Pouvoir « expliquer » ses préconisations
   - Prouver que le cas entre bien dans le **domaine de validité** du système de décision

2. Comme dans le génie logiciel classique
   - Pouvoir **décomposer** en sous-modules
   - Et avoir l'équivalent de **pré-conditions** et **post-conditions**

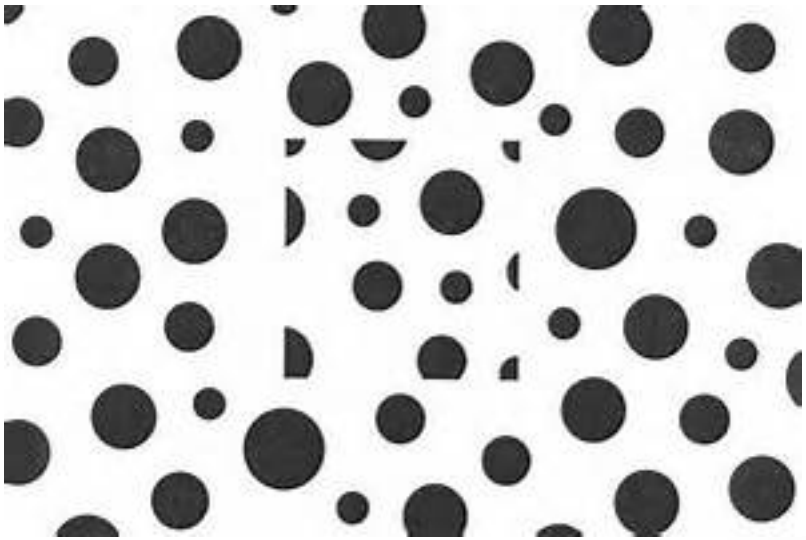
     Si je reçois cela en entrée, je garantis ceci en sortie
   - Est-ce que ce serait **suffisant** ? Faudra-t-il autre chose ?

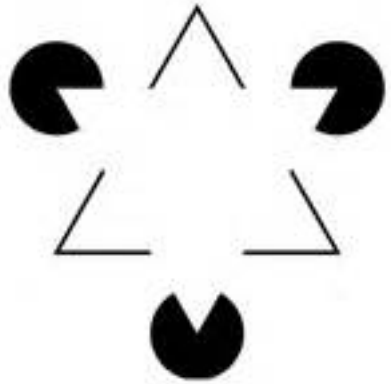
De quels outils disposons-nous pour répondre à ces questions ?

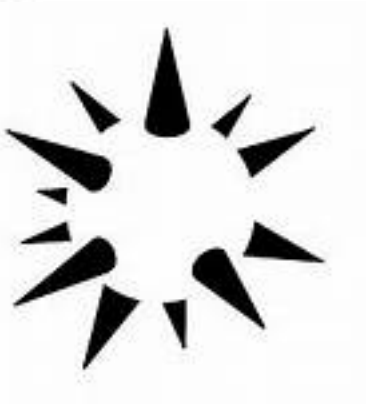
Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

L'apprentissage – une extrapolation

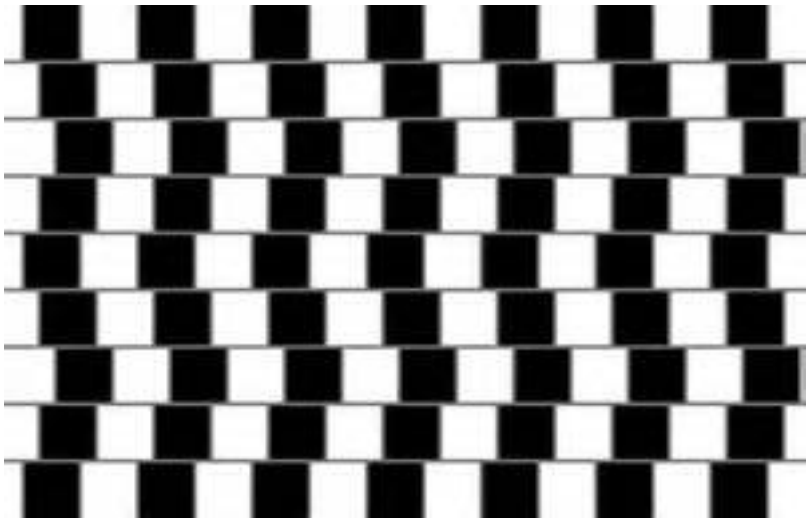




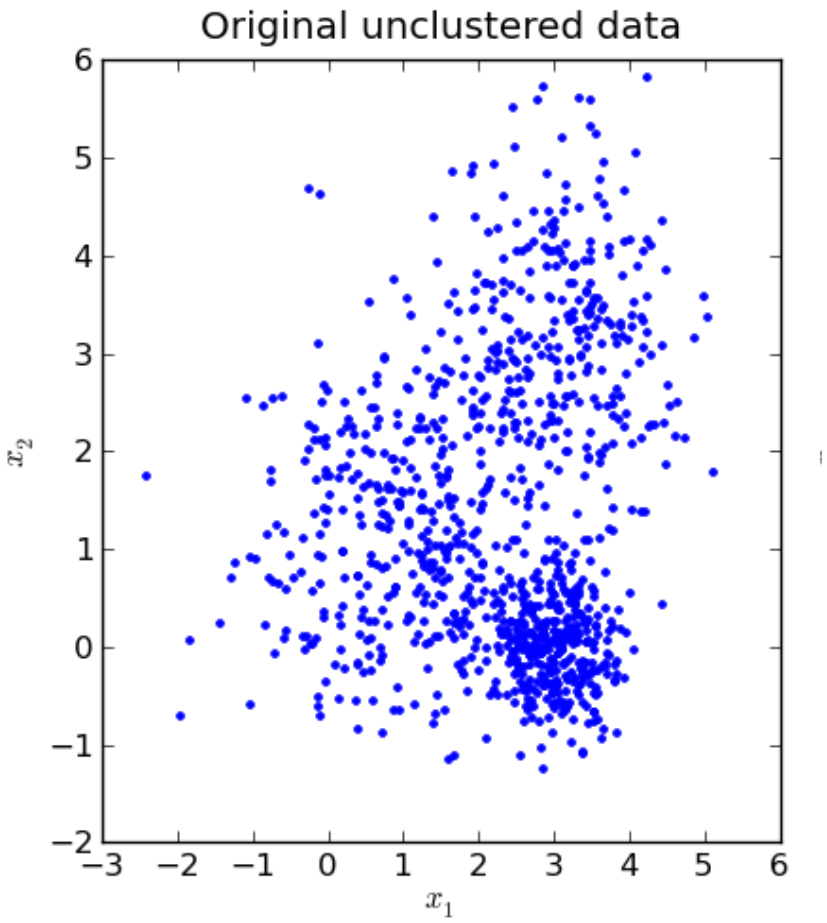


Une extrapolation – soumise à des **choix**

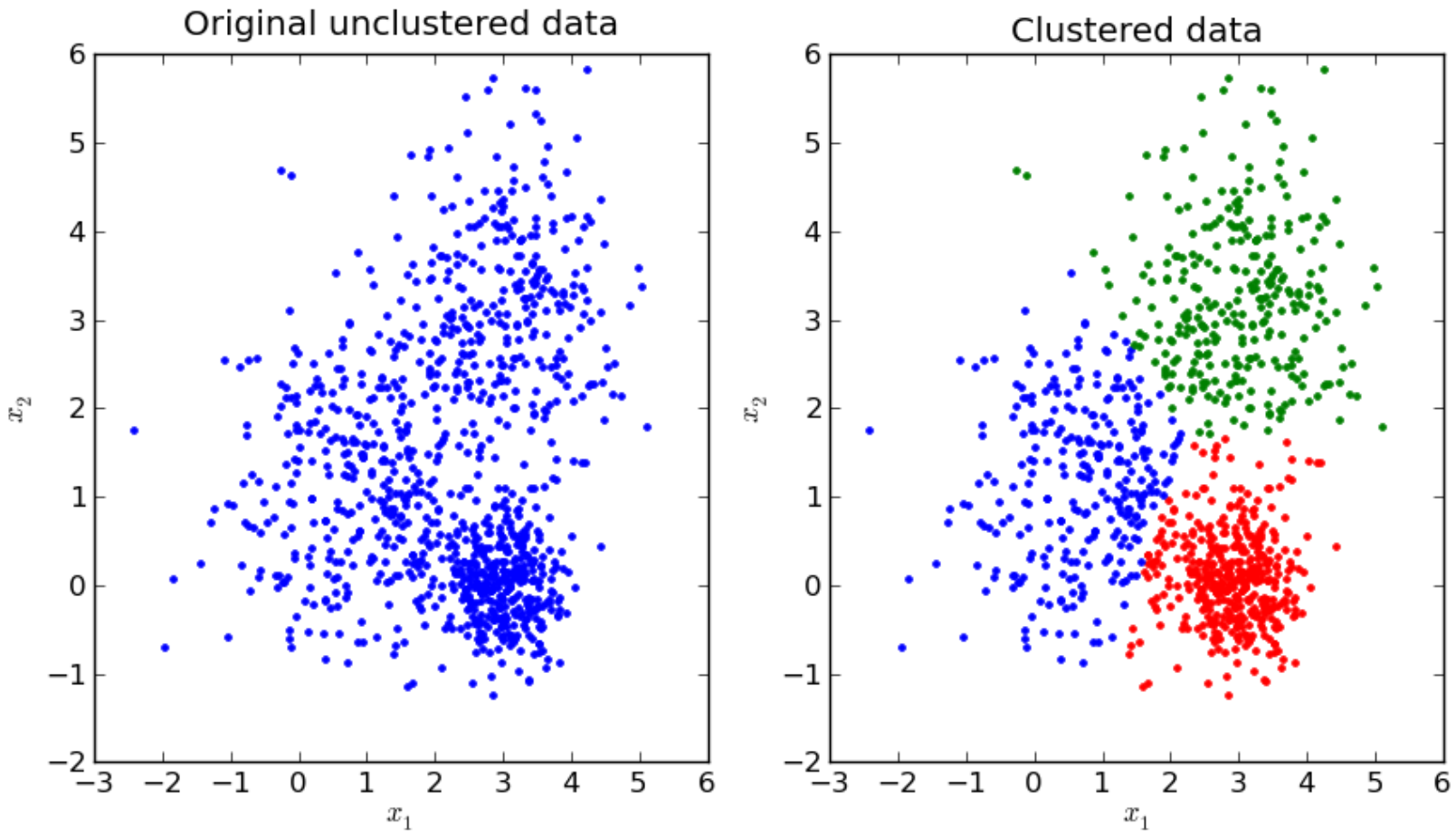
Des **biais** pouvant conduire à des illusions



Clustering

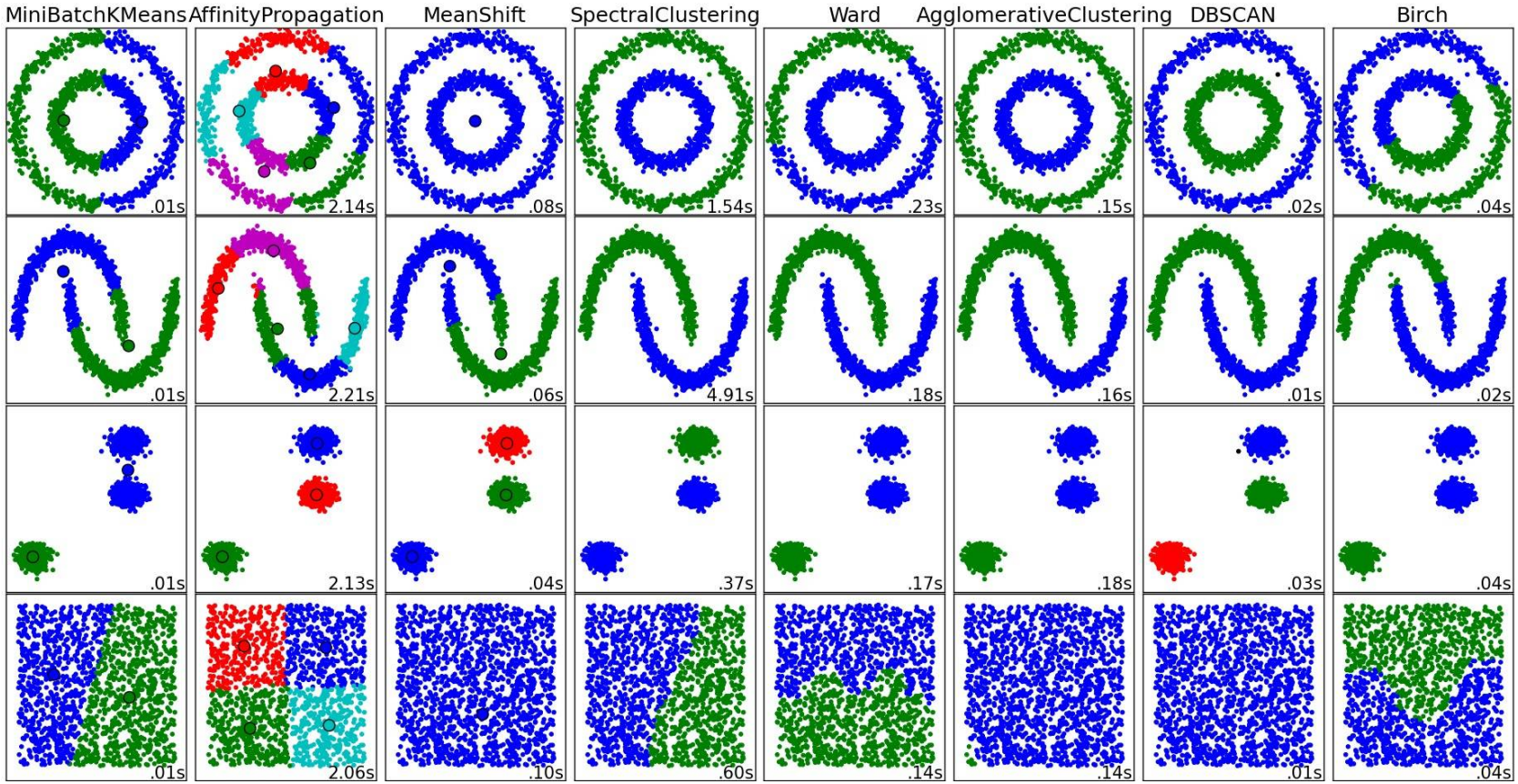


Clustering



Clustering

Dépend beaucoup des biais a priori



Comment fonder l'induction ?

Illustration : apprendre à **classer des exemples**

- Comment faire ?

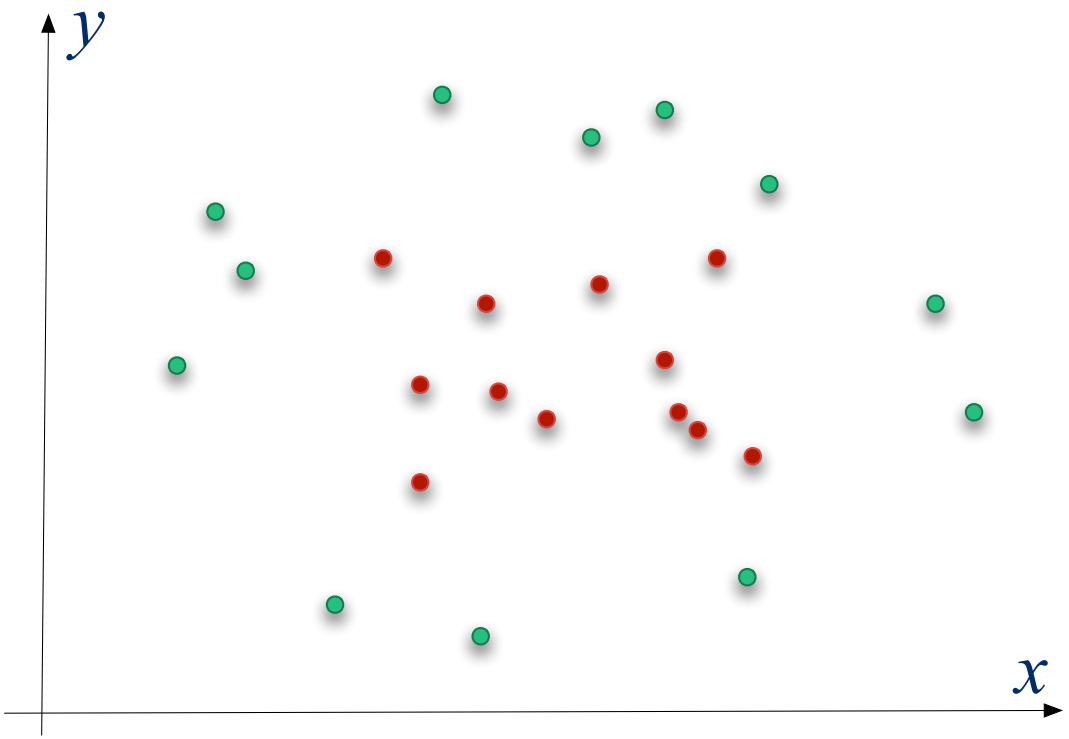


Illustration : apprendre à **classer des exemples**

- Comment faire ?

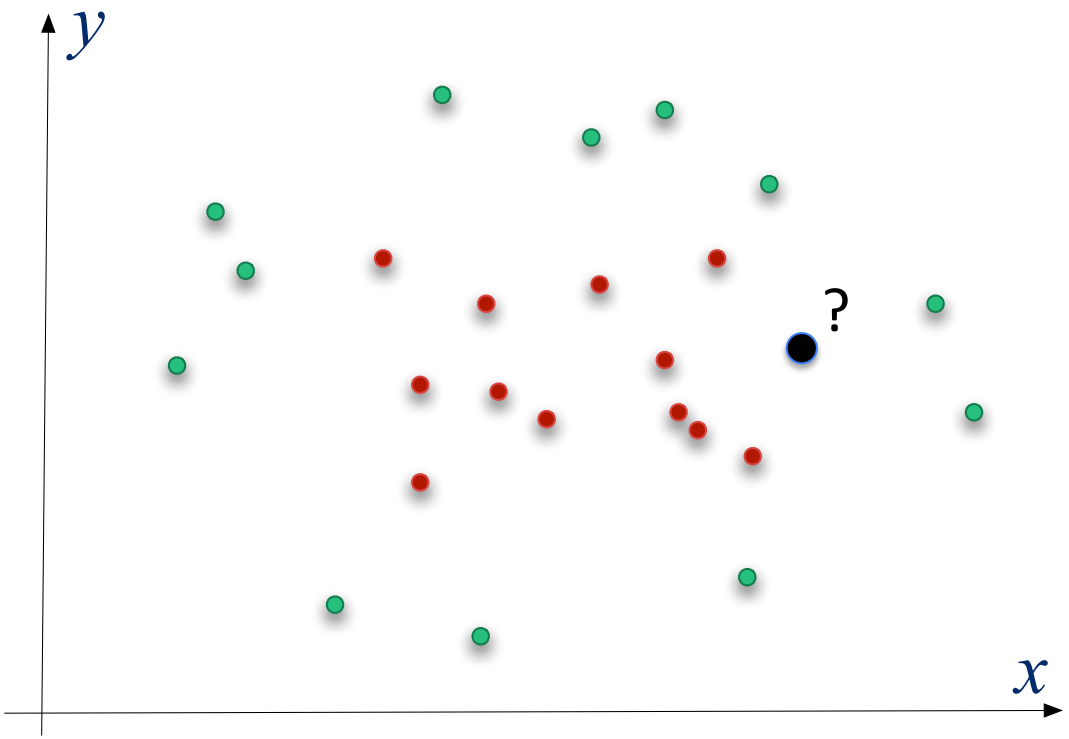
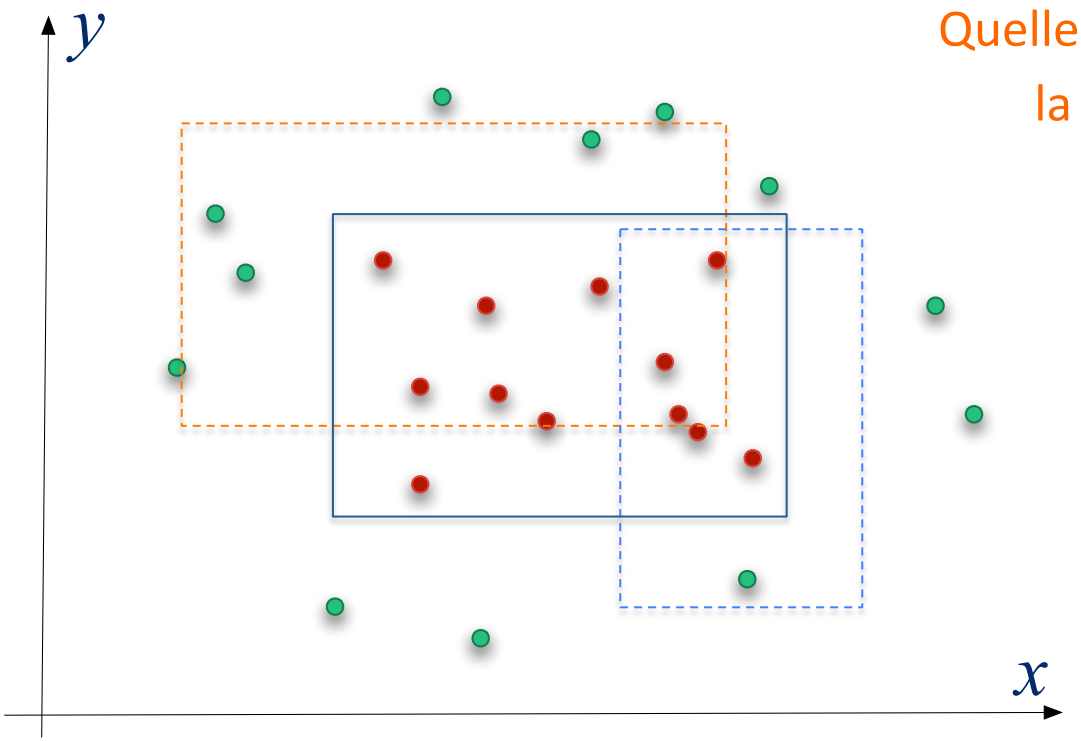


Illustration : apprendre à classer des exemples en 2D

- Comment faire ?



Quelle est l'hypothèse la meilleure ?

Quelle hypothèse choisir ?

Quelle qualité pour chaque hypothèse candidate ?

Quelle hypothèse choisir ?

Quelle performance ?

- Coût d'**une erreur** de prédiction
  - La ***fonction de perte***

$$\ell\big(h(\mathbf{x}), y\big)$$

Quelle hypothèse choisir ?

Quelle performance ?

- Coût d'**une erreur** de prédiction
  - La ***fonction de perte***

$$\ell\big(h(\mathbf{x}), y\big)$$

- Quel **coût à venir** (espérance) si je choisis *h* ?
  - Espérance de coût : le « ***risque réel*** »

$$R(h) = \int_{\mathcal{X}\times\mathcal{Y}} \ell\big(h(\mathbf{x}), y\big)\ \mathbf{p}_{\mathcal{X}\mathcal{Y}}(\mathbf{x}, y)\ d\mathbf{x}\, dy$$

Quelle hypothèse choisir ?

Comment trouver *h** (ou une bonne hypothèse) alors que l'on n'a accès qu'à un **échantillon d'apprentissage limité** ?

Quelle hypothèse choisir ?

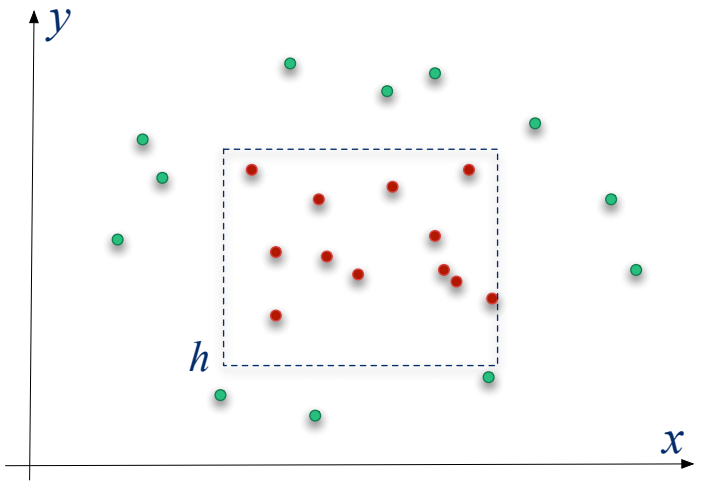
Comment trouver *h** (ou une bonne hypothèse) alors que l'on n'a accès qu'à un **échantillon d'apprentissage limité** ?

- Critère inductif : $\mathcal{H}$ x S -> valeur(h)

- Le plus naturel : ERM
  - La Minimisation du Risque Empirique

Quelle hypothèse choisir ?

- Quelle performance attendue pour *h* ?
  - Erreur moyenne sur l'échantillon d'apprentissage *S*



Le « risque empirique »

$$\hat{R}(h) = \frac{1}{m} \sum_{i=1}^{m} \ell\big(h(\mathbf{x}_i), y_i\big)$$

- A-t-on raison d'utiliser l'ERM ?

Un exemple qui dit beaucoup …

- Exemples décrits par :

  Number (1 or 2); ***size*** (small or large); ***shape*** (circle or square); ***color*** (red or green)

Description	**Your** prediction	**True** class
1 large red square		-
1 large green square		+
2 small red squares		+
2 large red circles		-
1 large green circle		+
1 small red circle		+

How many possible functions altogether from *X* to *Y* ? $2^{2^4} = 2^{16} = 65{,}536$

How many functions do remain after 6 training examples? $2^{10} = 1024$

Induction: impossible de gagner ?

- **Un biais est nécessaire**

- **Types** de biais
  - **De représentation** (déclaratif)
  - **De recherche** (procédural)

One example that tells a lot …

- Examples described using:

  ~~***Number***~~ (1 or 2); ***size*** (small or large); ~~***shape***~~ (circle or square); ***color*** (red or green)

Description	**Your** prediction	**True** class
~~1~~ large red ~~square~~		-
~~1~~ large green ~~square~~		+
~~2~~ small red ~~squares~~		+
~~2~~ large red ~~circles~~		-
~~1~~ large green ~~circle~~		+
~~1~~ small red ~~circle~~		+

How many possible functions with 2 descriptors from *X* to *Y* ? $2^{2^2} = 2^4 = 16$

How many functions do remain after 3 ≠ training examples? $2^1 = 2$

L'analyse « PAC learning »

- On arrive à :

$$\forall h \in \mathcal{H}, \forall \delta \leq 1 : \quad \mathbf{P}^m \left[R_{\text{Réel}}(h) \leq R_{\text{Emp}}(h) + \overbrace{\frac{\log |\mathcal{H}| + \log \frac{1}{\delta}}{m}}^{\varepsilon} \right] > 1 - \delta$$

Le principe de minimisation du risque empirique

n'est sain **que si** il y a des contraintes sur l'espace des hypothèses

Recette pour … **concevoir des algorithmes** d'apprentissage

1. Définir un **critère inductif régularisé**
   a. Exprimer le coût d'erreur de prédiction en une fonction de perte
   b. Définir un **terme de régularisation** qui exprime
      les attendus sur les régularités du monde
   c. Si possible, rendre convexe le problème d'**optimisation** résultant

$$h_{opt} = \underset{h \in \mathcal{H}}{\text{ArgMin}} \left[\underbrace{\frac{1}{m} \sum_{i=1}^{m} l(h(\mathbf{x}_i), y_i)}_{\text{empirical risk}} + \lambda \underbrace{reg(\mathcal{H})}_{\text{bias on the world}} \right]$$

2. Utiliser ou développer un **algorithme d'optimisation efficace**

Learning **sparse linear** approximator

- The **hypothesis** is of the form $h(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x}$
- A priori assumption: few non zero coefficients

Ridge regression

$$\mathbf{w}^*_{\text{ridge}} = \underset{\mathbf{w}}{\text{Argmin}} \left\{ \sum_{i=1}^{m} (y_i - \mathbf{w}\,\mathbf{x}_i)^2 + \lambda \, ||\mathbf{w}||_2^2 \right\}$$

Lasso regression

$$\mathbf{w}^*_{\text{lasso}} = \underset{\mathbf{w}}{\text{Argmin}} \left\{ \sum_{i=1}^{m} (y_i - \mathbf{w}\,\mathbf{x}_i)^2 + \lambda \, ||\mathbf{w}||_1 \right\}$$

3.3 du chapitre 3. Ainsi, étant donnés un échantillon source étiqueté $S = \{(x_i^s, y_i^s)\}_{i=1}^m$ constitué de m exemples *i.i.d.* selon P_S et un échantillon cible non étiqueté $T = \{(x_i^t)\}_{i=1}^m$ composé de m exemples *i.i.d.* selon D_T, en posant $S_u = \{x_i^s\}_{i=1}^m$ l'échantillon S privé de ses étiquettes, on veut minimiser :

Risque empirique régularisé

$$\min_{\mathbf{w}} \; c\,m\,\mathrm{R}_S(G_{\rho_\mathbf{w}}) + a\,m\,\mathrm{dis}_{\rho_{\mathbf{w}^2}}(S_u, T_u) + \mathrm{KL}(\rho_\mathbf{w} \| \pi_0), \tag{7.5}$$

où $\mathrm{dis}_{\rho_{\mathbf{w}^2}}(S_u, T_u) = \left| \mathop{\mathrm{E}}_{(h,h')\sim\rho_{\mathbf{w}^2}} \mathrm{R}_{S_u}(h,h') - \mathop{\mathrm{E}}_{(h,h')\sim\rho_{\mathbf{w}^2}} \mathrm{R}_{T_u}(h,h') \right|$ est le désaccord empirique entre S_u et T_u spécialisé à une distribution $\rho_\mathbf{w}$ sur l'espace $\mathcal{H}$ des classifieurs linéaires considéré. Les réels $a > 0$ et $c > 0$ sont des hyperparamètres de l'algorithme. Notons que les constantes A et C du théorème 7.7 peuvent être retrouvées à partir de n'importe quelle valeur de a et c. Étant donnée la fonction $\ell_{\mathrm{dis}}(x) = 2\,\ell_{\mathbf{Erf}}(x)\,\ell_{\mathbf{Erf}}(-x)$ (illustrée sur la figure 7.1) , pour toute distribution D sur X, on a :

Expression de **substitution** du risque régularisé

$$\begin{aligned}
\mathop{\mathrm{E}}_{(h,h')\sim\rho_{\mathbf{w}^2}} \mathrm{R}_D(h,h') &= \mathop{\mathrm{E}}_{\mathbf{x}\sim D} \mathop{\mathrm{E}}_{(h,h')\sim\rho_{\mathbf{w}^2}} \mathrm{I}\left[h(\mathbf{x}) \neq h'(\mathbf{x})\right] \\
&= 2 \mathop{\mathrm{E}}_{\mathbf{x}\sim D} \mathop{\mathrm{E}}_{(h,h')\sim\rho_{\mathbf{w}^2}} \mathrm{I}\left[h(\mathbf{x}) = 1\right] \mathrm{I}\left[h'(\mathbf{x}) = -1\right] \\
&= 2 \mathop{\mathrm{E}}_{\mathbf{x}\sim D} \mathop{\mathrm{E}}_{h\sim\rho_\mathbf{w}} \mathrm{I}\left[h(\mathbf{x}) = 1\right] \mathop{\mathrm{E}}_{h'\sim\rho_\mathbf{w}} \mathrm{I}\left[h'(\mathbf{x}) = -1\right] \\
&= 2 \mathop{\mathrm{E}}_{\mathbf{x}\sim D} \ell_{\mathbf{Erf}}\left(\frac{\langle \mathbf{w}, \mathbf{x}\rangle}{\|\mathbf{x}\|}\right) \ell_{\mathbf{Erf}}\left(-\frac{\langle \mathbf{w}, \mathbf{x}\rangle}{\|\mathbf{x}\|}\right) \\
&= \mathop{\mathrm{E}}_{\mathbf{x}\sim D} \ell_{\mathrm{dis}}\left(\frac{\langle \mathbf{w}, \mathbf{x}\rangle}{\|\mathbf{x}\|}\right).
\end{aligned}$$

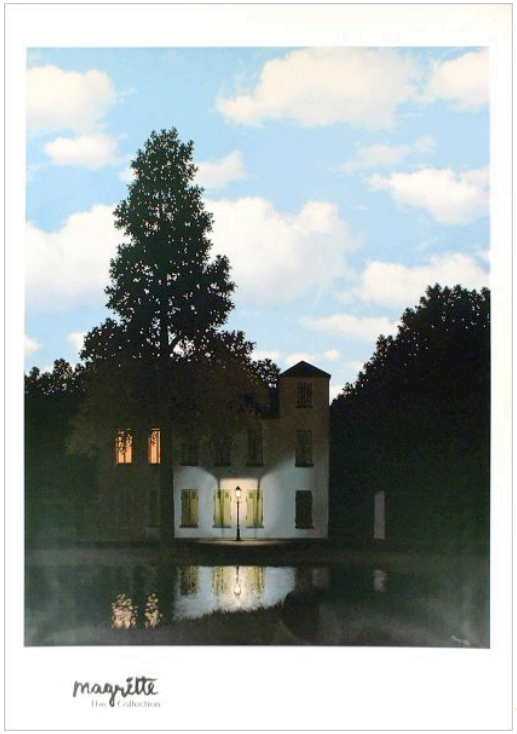
Ainsi, trouver la solution optimale de l'équation (7.5) revient à chercher le vecteur $\mathbf{w}$ qui minimise :

$$c \sum_{i=1}^m \ell_{\mathbf{Erf}}\left(y_i^s \frac{\langle \mathbf{w}, \mathbf{x}_i^s\rangle}{\|\mathbf{x}_i^s\|}\right) + a \left| \sum_{i=1}^m \left[\ell_{\mathrm{dis}}\left(\frac{\langle \mathbf{w}, \mathbf{x}_i^s\rangle}{\|\mathbf{x}_i^s\|}\right) - \ell_{\mathrm{dis}}\left(\frac{\langle \mathbf{w}, \mathbf{x}_i^t\rangle}{\|\mathbf{x}_i^t\|}\right) \right] \right| + \frac{\|\mathbf{w}\|^2}{2}. \tag{7.6}$$

Optimisation

L'équation précédente est fortement non convexe. Afin de rendre sa résolution plus facilement contrôlable, nous remplaçons la fonction $\ell_{\mathbf{Erf}}(\cdot)$ par sa relaxation convexe $\ell_{\mathbf{Erf}_{\mathrm{cvx}}}(\cdot)$ (comme pour PBGD3 et illustrée sur la figure 7.1). L'optimisation se réalise ensuite par une descente de gradient. Le gradient de l'équation 7.6 étant :

Des garanties « de lampadaire »



Des garanties « de lampadaire »

(*Quasi*) garantie que :

- **Si** le monde satisfait **mes attentes** sur lui
- **Alors** l'algorithme d'apprentissage produira une bonne hypothèse (proche de la vraie)

Des garanties « de lampadaire »

(*Quasi*) garantie que :

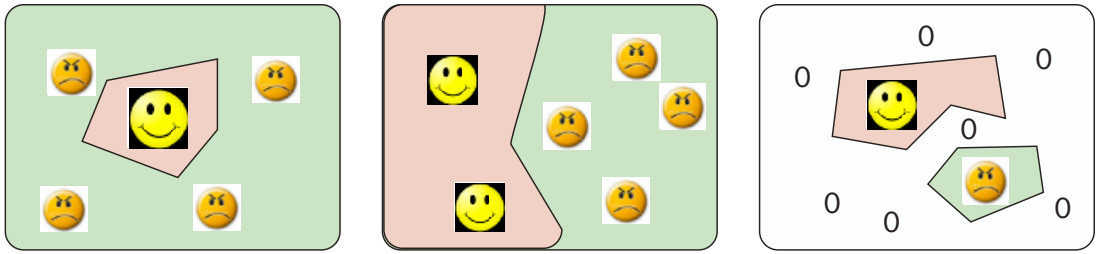
- **Si** le monde satisfait **mes attentes** sur lui
- **Alors** l'algorithme d'apprentissage produira une bonne hypothèse (proche de la vraie)

- **Autrement** l'apprentissage peut conduire à de très mauvaises hypothèses

  (ex. *Si le monde **n'est pas** parcimonieux*)

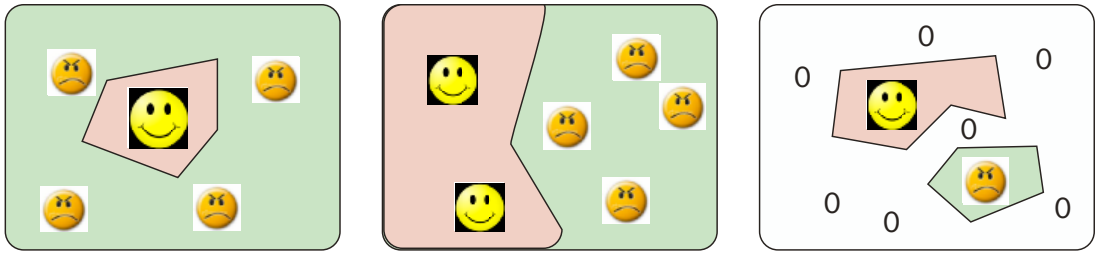
Le no-free-lunch theorem

Possible

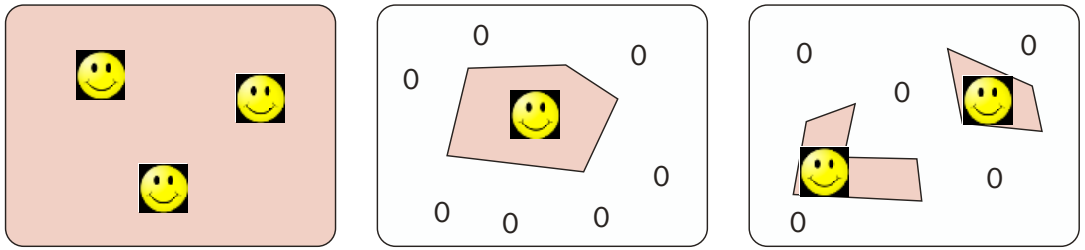


Le no-free-lunch theorem

Possible



Impossible



Il faut **choisir** le **bon algorithme** pour la **classe de problèmes** étudiée

- Très mathématisé et sophistiqué
- Conduit à l'invention de nouveaux algorithmes

Est-ce que cela permet de répondre aux **nouveaux défis** ?

Est-ce que l'on a **toujours été** dans ce paradigme ?

- **Paradigme** :

*Manière jugée cohérente de **percevoir** le monde et de le **représenter**,*

*ensemble de **valeurs** et **techniques** qui sont **partagées** par les membres d'une*

*communauté scientifique, au cours d'une **période de consensus** théorique*

Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

Objectifs et méthode

- Question

  Le paradigme : centré sur **l'espérance de coût d'usage**

  1. De **quand** ça date ?
  2. Y a-t-il eu un **avant** ? Et, si oui, lequel ?
  3. Peut-on détecter des **changements de paradigmes** ?

- Méthode
  - Examiner les publications depuis ~1950
    - Western Joint Computer Conference (1955)
    - IJCAI 1969-2016
    - ICML
  - Que cherche t-on à **prouver** ?
  - Quels **critères d'évaluation** ?

Perspective historique : apprentissage automatique

1950s

- Expériences de pensée sous contrainte de réalisabilité computationnelle
  - **Opérateurs** sur des représentation
  - Recherche dans un **espace d'états**. Buts / sous-buts
  - **Apprentissage** par mutations aléatoires (mais guidée par ressemblance) ~ AG
  - Ivresse : comprendre la pensée
  - « *Our problem, our joint problem, is to discover what transformations must be made on the available data in order to preserve intact the significant features and to discard the irrelevant details* ».

1960s

- Principes, théorèmes et démonstrations (Checker. Problèmes « jouets »)
  - Reconnaissance des formes. Plutôt numérique (bayésien, perceptron)

1970s

Perspective historique : apprentissage automatique

1950s

- Expériences de pensée sous contrainte de réalisabilité computationnelle
  - **Opérateurs** sur des représentation
  - Recherche dans un **espace d'états**. Buts / sous-buts
  - **Apprentissage** par mutations aléatoires (mais guidée par ressemblance) ~ AG
  - Ivresse : comprendre la pensée
  - « *Our problem, our joint problem, is to discover what transformations must be made on the available data in order to preserve intact the significant features and to discard the irrelevant details* ».

1960s

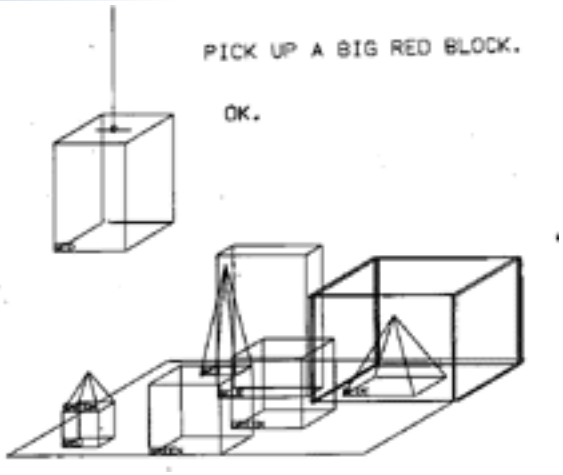
- Principes, théorèmes et démonstrations (Checker. Problèmes « jouets »)
  - Reconnaissance des formes. Plutôt numérique (bayésien, perceptron)

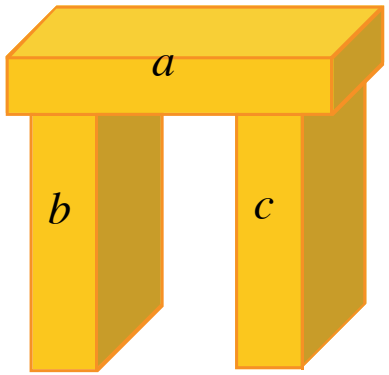
1970s

- Expertise. Sciences cognitives : plausibilité. Intégration dans le raisonnement
  - **Modèles de mémoire**. Réseaux sémantiques. Représentation des connaissances
  - **Règles** de production. Moteur d'inférence.
  - **Mécanismes** d'apprentissage et de **généralisation**
  - **Apprentissage et raisonnement** : heuristiques, macro-opérateurs, chunking

ARCH [Winston, 1970]

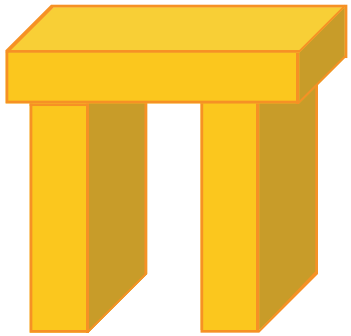
- **Apprentissage** de **concept** (e.g. arche) dans un monde de blocs

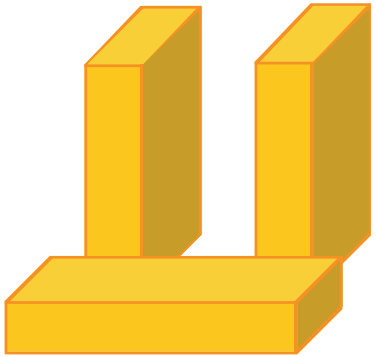




ARCH [Winston, 1970]

- Les exemples ne sont **pas choisis au hasard**



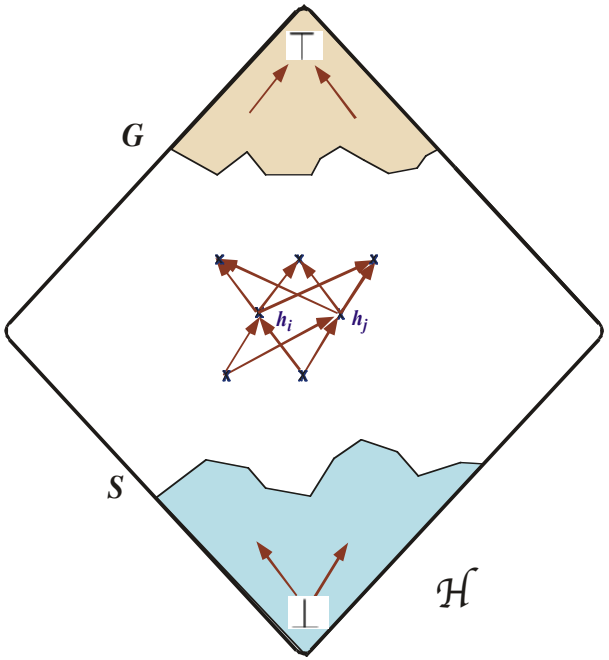


Apprentissage de l'espace des versions [Tom Mitchell, 1979]

Observation fondamentale :

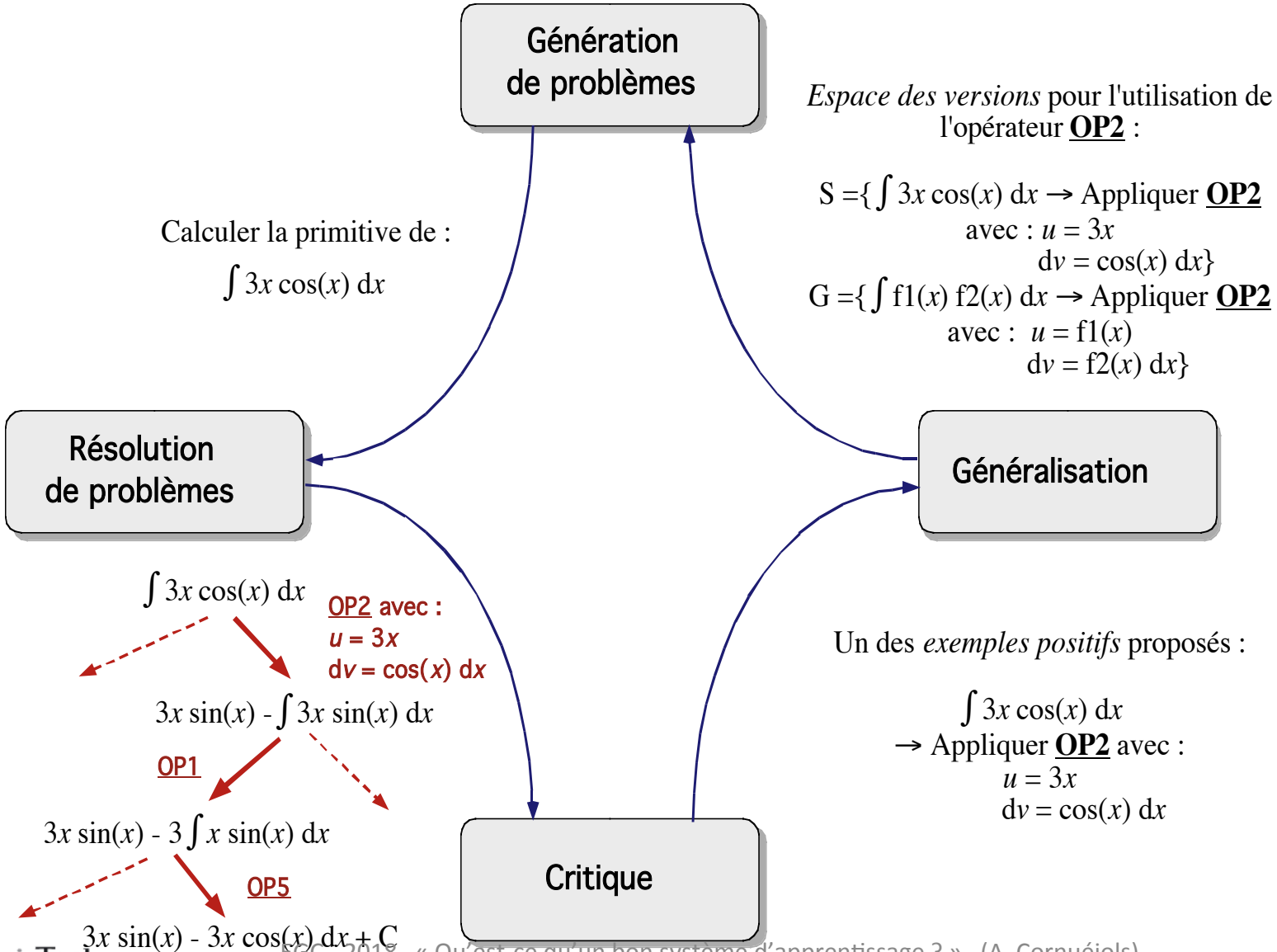
L'espace des versions structuré par une relation d'ordre partiel peut être représenté par :

- sa **borne supérieure** : le *G-set*
- sa **borne inférieure** : le *S-set*

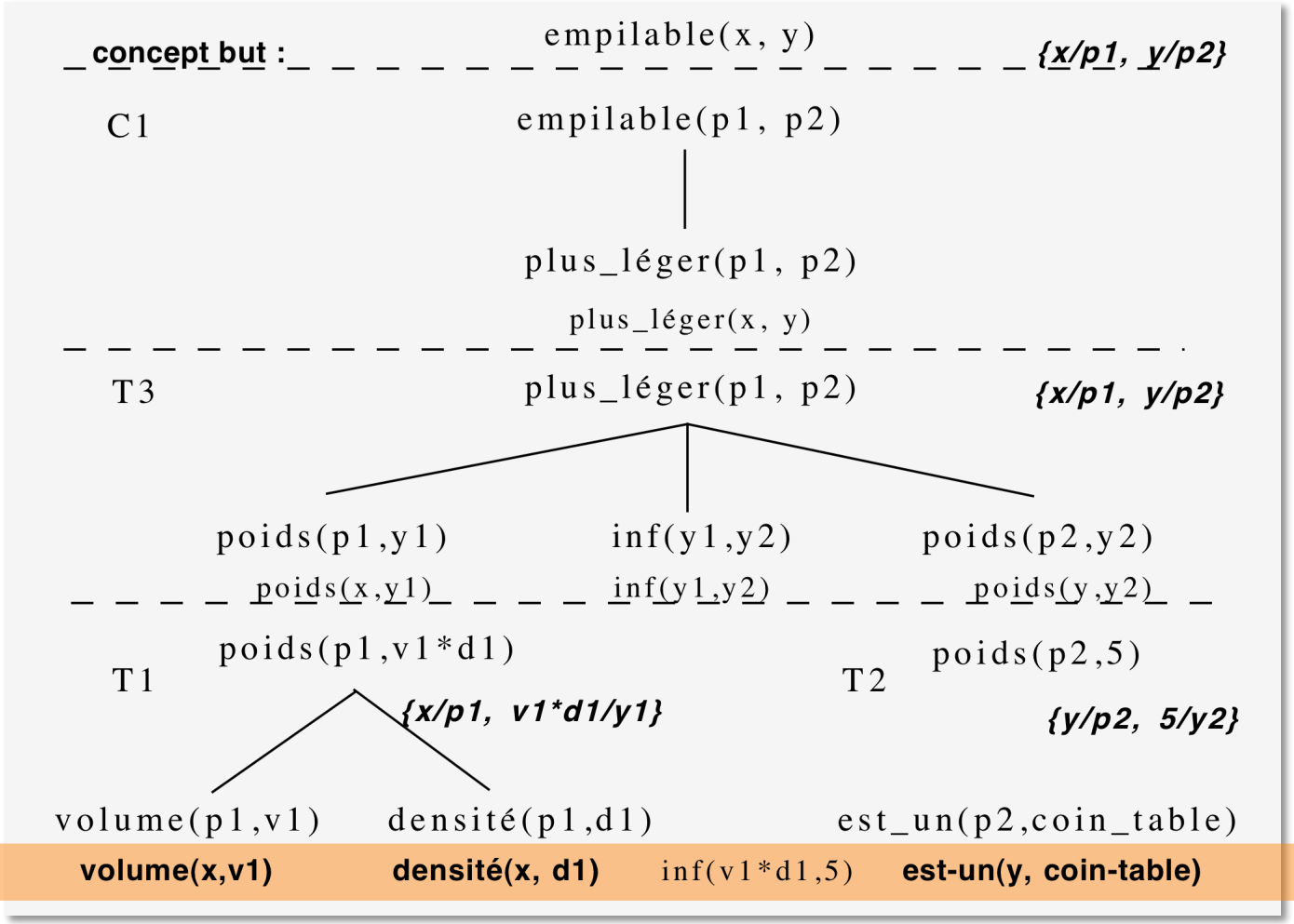


- *G-set = Ensemble de toutes les hypothèses **les plus** **générales** cohérentes avec les exemples connus*
- *S-set = Ensemble de toutes les hypothèses **les plus** **spécifiques** cohérentes avec les exemples connus*

Le système LEX [Tom Mitchell, 1983]



Explanation-Based Learning



Generalized search tree resulting from regression of the target concept in the proof tree by computing at each step the most general literals allowing this step.

Perspective historique : apprentissage automatique

1990s

- Espérance d'erreur de prédiction
  - Bases de données supposées i.i.d.
  - Données bruitées
  - Espérance du coût de prédiction
  - Théorie : quels principes inductifs ? Donc quel problème d'optimisation
  - Comment accélérer le processus d'optimisation : convexification
  - Nouvelles méthodes : SVM / Boosting / random forests / Lasso, …
  - Plus de raisonnement !!!

2000s

2010s

- Applications à des problèmes « réels »

2020s

Perspective historique : apprentissage automatique

1990s

- Espérance d'erreur de prédiction
  - Bases de données supposées i.i.d.
  - Données bruitées
  - Espérance du coût de prédiction
  - Théorie : quels principes inductifs ? Donc quel problème d'optimisation
  - Comment accélérer le processus d'optimisation : convexification
  - Nouvelles méthodes : SVM / Boosting / random forests / Lasso, …
  - Plus de raisonnement !!!

2000s

- Applications à des problèmes « réels »

2010s

- L'apprentissage « profond » : apprendre les (hiérarchies de) descripteurs
  - Performances en prédiction
  - Exhiber les descripteurs (et espaces « sémantiques »)
  - Transfert

2020s

- … ?

Changements de paradigmes

- Changements de **paradigme**
  - Très **progressifs** !!
  - Au début : signaux faibles

Changements de paradigmes

- Changements de **paradigme**
  - Très **progressifs** !!
  - Au début : signaux faibles

- Changements de **méthodes**
  - Très **rapides** (modes) !!
  - **Au sein** d'un paradigme
    - SVM ; Boosting
  - Facilitant une **charnière**
    - RNs profonds ???

Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

Sait-on finalement **expliquer**

les capacités de généralisation ?

Quelque chose de troublant

– C. Zhang, S. Bengio, M. Hardt, B. Recht, O. Vinyals (ICLR, **May 2017**).

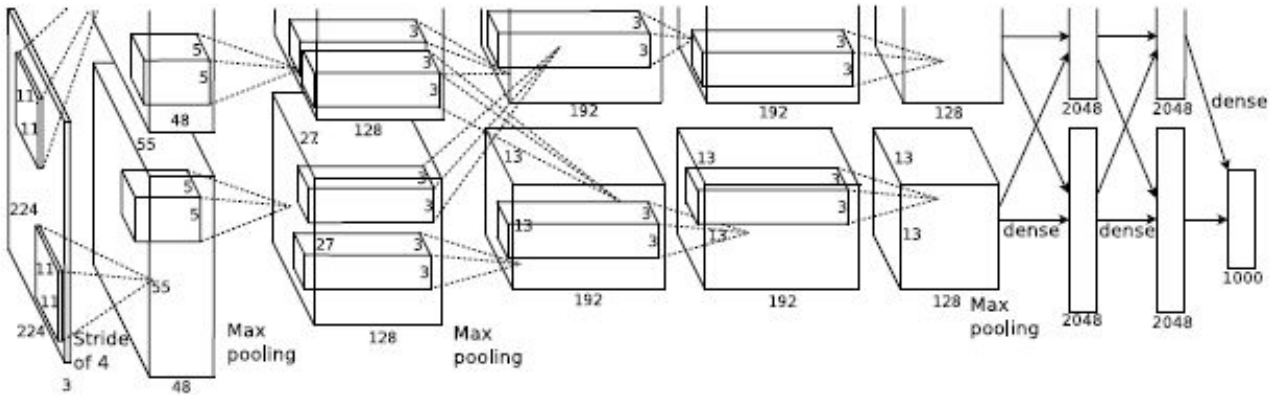
"Understanding deep learning requires rethinking generalization"

Quelque chose de troublant

– C. Zhang, S. Bengio, M. Hardt, B. Recht, O. Vinyals (ICLR, **May 2017**).
"Understanding deep learning requires rethinking generalization"

Extensive experiments on the classification of images

– The AlexNet (**> 1,000,000 parameters**) + 2 other architectures



– The **CIFAR-10 data set**:

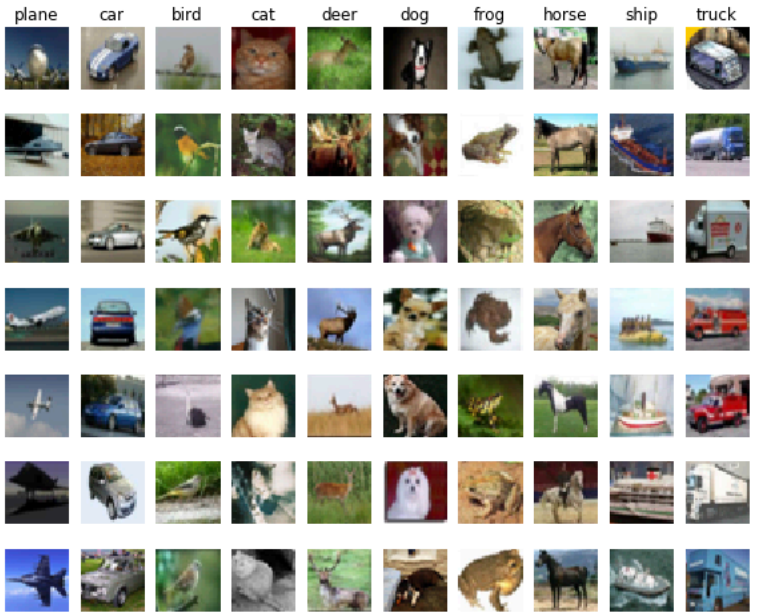
- **60,000** images categorized in **10 classes** (50,000 for training and 10,000 for testing)
- Images: 32x32 pixels in 3 color channels

Quelque chose de troublant

Experiments

1. **Original dataset** without modification

- Results ?
  - **Training** accuracy = 100% ; **Test** accuracy = 89%
  - Speed of convergence ~ 5,000 steps



Quelque chose de troublant

Experiments

1. **Original dataset** without modification

   - Results ?
     - **Training** accuracy = 100% ; **Test** accuracy = 89%
     - Speed of convergence ~ 5,000 steps

Expected behavior if the **capacity** of the hypothesis space is **limited**

i.e. the system **cannot** fit any (arbitrary) training data

$$\forall h \in \mathcal{H}, \forall \delta \leq 1 : \quad P^m \left[R(h) \leq \widehat{R}(h) + 2\,\widehat{Rad}_m(\mathcal{H}) + 3\sqrt{\frac{\ln(2/\delta)}{m}} \right] > 1 - \delta$$

Troubling findings

Experiments

1. **Original dataset** without modification
   - Results ?
     - **Training** accuracy = 100% ; **Test** accuracy = 89%
     - Speed of convergence ~ 5,000 steps

2. Random **labels**

!!!

   - **Training** accuracy = 100% !!?? ; **Test** accuracy = 9.8%
   - Speed of convergence = similar behavior (~ 10,000 steps)

Troubling findings

Experiments

1. **Original dataset** without modification
   - Results ?
     - **Training** accuracy = 100% ; **Test** accuracy = 89%
     - Speed of convergence ~ 5,000 steps

2. Random **labels**
   - **Training** accuracy = 100% !!?? ; **Test** accuracy = 9.8%
   - Speed of convergence = similar behavior (~ 10,000 steps)

3. Random **pixels**
   - **Training** accuracy = 100% !!?? ; **Test** accuracy ~ 10%
   - Speed of convergence = similar behavior (~ 10,000 steps)

Now, we are in trouble!!

Troubling findings

- Deep NNs can accommodate ANY training set

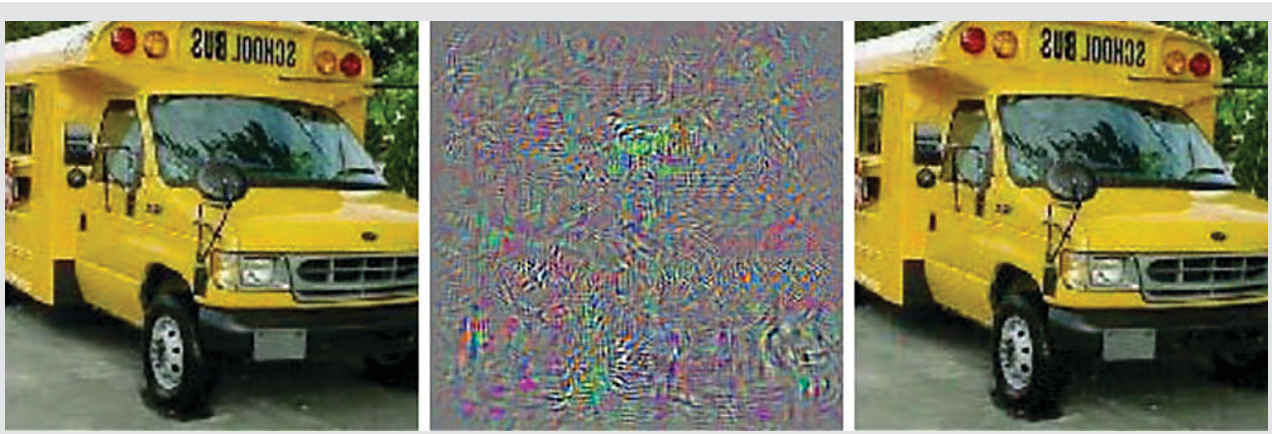
Can grow without limit!!

$$\forall h \in \mathcal{H}, \forall \delta \leq 1 : \quad P^m \left[R(h) \leq \widehat{R}(h) + 2\,\widehat{Rad}_m(\mathcal{H}) + 3\sqrt{\frac{\ln(2/\delta)}{m}} \right] > 1 - \delta$$

But then,

why are deep NNs ***so good on image classification tasks?***

Adversarial learning



Adversarial input can fool a machine-learning algorithm into misperceiving images.

Sait-on expliquer une conclusion ?

Voiture dans une piscine

- … ou pas de voiture … ?

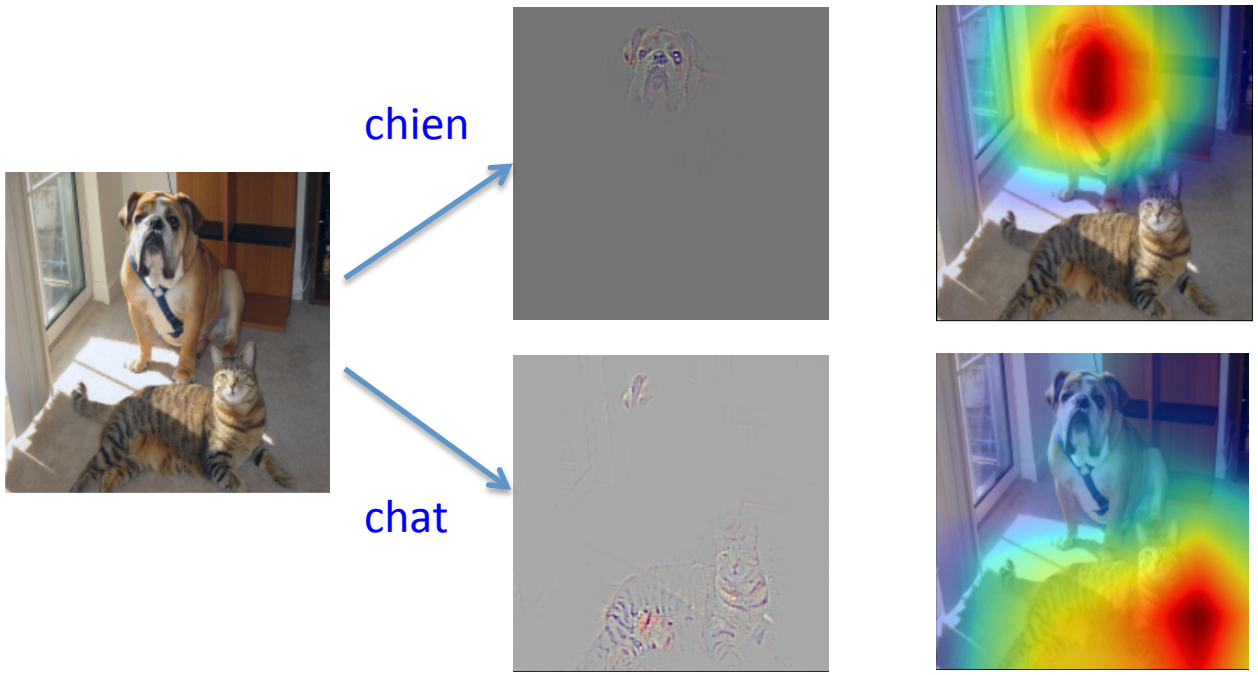
Is this less of a car
because the context is wrong?

[Léon Bottou (ICML-2015, invited talk) « *Two big challenges in Machine Learning* »]

Explication et réseaux de neurones profonds

Identification de classes d'objets dans une image

- Ici deux classes : « **chien** » et « **chat tigré** »



[Selvaraju et al. (2017) « *Grad-CAM: Visual explanations from deep networks via gradient-based localization* »]

Explication et réseaux de neurones profonds

Protocole d'évaluation : comparaison entre explications

- À quel robot faites-vous le plus confiance ?

What do you see?

Your options:

- ○ Horse
- ○ Person

Both robots predicted: Person

Robot A based it's decision on

Robot B based it's decision on

Which robot is more reasonable?

- ○ **Robot A** seems clearly more reasonable than **robot B**
- ○ **Robot A** seems slightly more reasonable than **robot B**
- ○ Both robots seem equally reasonable
- ○ **Robot B** seems slightly more reasonable than **robot A**
- ○ **Robot B** seems clearly more reasonable than **robot A**

54 sujets sur Amazon Turk -> robot B évalué à 1.27 (entre -2 et +2)

[Selvaraju et al. (2017) « *Grad-CAM: Visual explanations from deep networks via gradient-based localization* »]

Explication et réseaux de neurones profonds

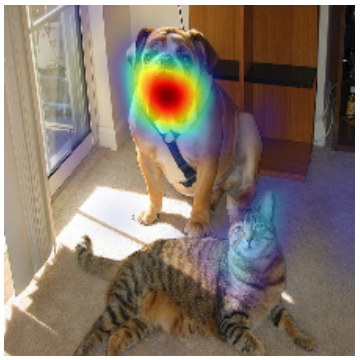
Illusions d'optique : quelle explication ?

Boxer: 0.40 Tiger Cat: 0.18

(a) Original image

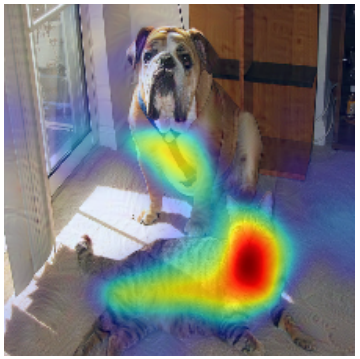
Airliner: 0.9999

(b) Adversarial image



Boxer: 1.1e-20

(c) Grad-CAM "Dog"



Tiger Cat: 6.5e-17

(d) Grad-CAM "Cat"

!!??

[Selvaraju et al. (2017) « *Grad-CAM: Visual explanations from deep networks via gradient-based localization* »]

Détecter des **biais**

Ground-Truth: Nurse

(a) Original image

Predicted: Nurse

(b) Grad-CAM for biased model

Predicted: Nurse

(c) Grad-CAM for unbiased model

Ground-Truth: Doctor

(d) Original Image

Predicted: Nurse

(e) Grad-CAM for biased model

Predicted: Doctor

(f) Grad-CAM for unbiased model

Ground-Truth: Doctor

(g) Original Image

Predicted: Nurse

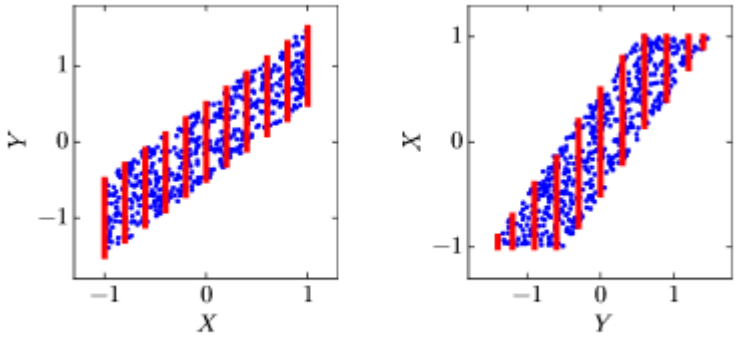
(h) Grad-CAM for biased model

Predicted: Doctor

(i) Grad-CAM for unbiased model

L'identification de relations causales

- Dans les images



(a) ANM $X \to Y$. (b) ANM $Y \to X$

[David Lopez-Paz, Robert Nishihara, Soumith Chintala, Bernhard Schölkopf, and Léon Bottou.
« *Discovering causal signals in images* ». *arXiv preprint arXiv :1605.08179*, 2016.]

Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

Retour sur les défis

Est-ce que cela suffira ?

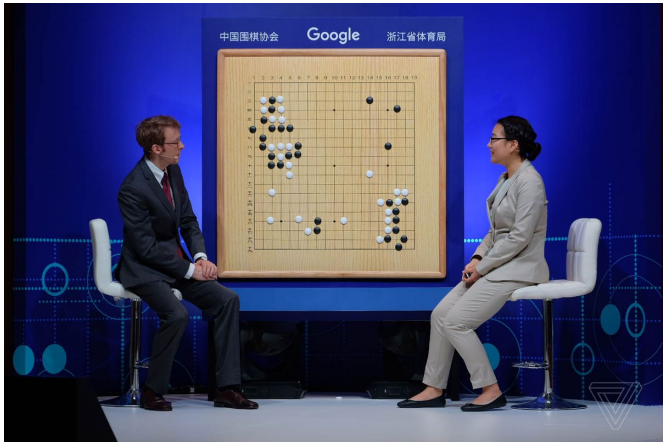
Le cas AlphaGo

- Un joueur « extraterrestre »
- Un jeu stupéfiant
- Révolutionne la manière de jouer
- Effervescence dans les écoles de go

Le cas AlphaGo : comprendre

Fan Hui, Gu Li, Zhou Ruyang (très forts joueurs de Go) se reconvertissent dans l'analyse des parties jouées par AlphaGo

- Sorte d'exégèse. Explications a posteriori
- Nécessaire pour
  - La communication
  - L'enseignement



Et même AlphaGo peut se tromper

Les explications des SEs

MYCIN : L'infection du malade a t-elle été contractée à l'hôpital ?

Utilisateur : pourquoi ?

TEIRESIAS : [pourquoi est-ce important de savoir cela ?]

Cela aidera à déterminer la catégorie à laquelle appartient l'organisme responsable de l'infection :

- il a déjà été établi que 1° l'organisme est à Gram négatif, 2° c'est un bâtonnet, 3° il se développe à l'air ou sans air,

- donc si l'infection par cet organisme n'a pas été contactée lors du séjour à l'hôpital

alors il est presque certain (0,8) que l'organisme est de la catégorie des enterobactoriaceae; de plus, il se peut (0,1 ; règle 37) que ce soit la pseudomonia aeruginosa.

Utilisateur : pourquoi n'avez-vous pas envisagé la possibilité que l'organisme soit un streptocoque ?

TEIRESIAS : la règle 33 aurait du être utilisée pour identifier l'organisme comme un streptocoque, mais la seconde clause "la morphologie est de type coque" était déjà connue comme fausse et la règle 33 n'a jamais été essayée.

Les explications des SEs

- Quel est l'âge du patient ?
- ** Pourquoi
- Pour déterminer si on peut prescrire de la tétracycline
  - Si le patient a moins de 8 ans
  - Alors on ne peut pas prescrire de tétracycline
  - [Règle 122]
- ** Pourquoi ?
- …

Pourquoi ne faut-il pas prescrire de tétracycline à un enfant de moins de 8 ans ?

Les explications des SEs

Pourquoi ne faut-il pas prescrire de tétracycline à un enfant de moins de 8 ans ?

Connaissances justificatives

Dépôt de la drogue sur les **os en développement**

→ **Noircissement** définitif des dents

→ Coloration socialement **indésirable**

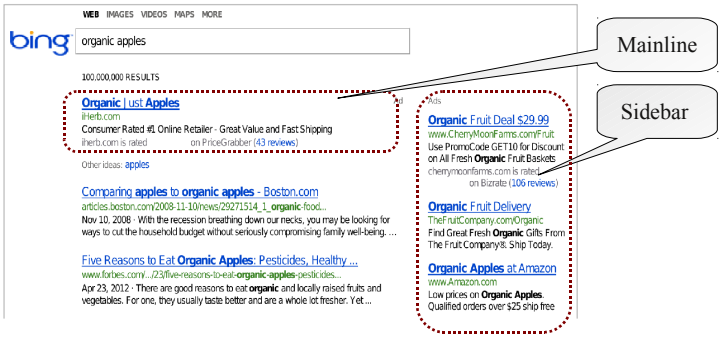
→ **Ne pas administrer** de tétracycline aux enfants de moins de 8 ans

Notion d'**effets secondaires** indésirables

Relations de **causalité**

Système adaptatif de placement de publicité

- Deux **sous-systèmes**
  - L'un plaçant les **liens publicitaires**
  - L'autre choisissant les **publicités**



- Qui **s'influencent mutuellement**
  - Chacun s'appuie sur les données de clicks
  - Qui dépendent aussi de l'intervention de l'autre systèmes
  - Et d'autres facteurs non contrôlés (prix, requête de l'utilisateur, …)

[L. Bottou et al. «*Counterfactual Reasoning and Learning Systems: The Example of Computational Advertising* », JMLR, 14, (2013), 3207-3260]

Le paradoxe de Simpson

- Les médecins voudraient savoir si le traitement A est plus performant ou moins performant que le traitement B
- Deux groupes de 350 patients sont sélectionnés, l'un recevant le traitement A, l'autre le traitement B

	Overall
Treatment A: Open surgery	78% (273/350)
Treatment B: Percutaneous nephrolithotomy	**83%** (289/350)

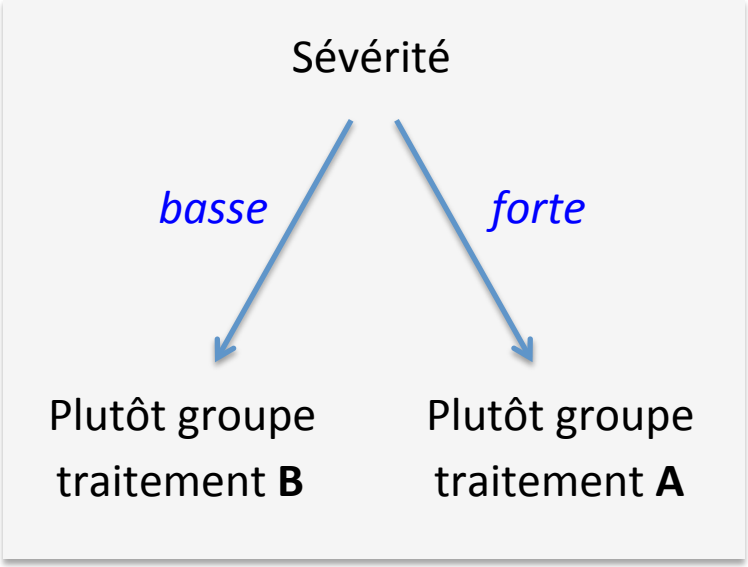
B est meilleur ?

Le paradoxe de Simpson

	Overall	Patients with small stones	Patients with large stones
Treatment A: Open surgery	78% (273/350)	**93%** (81/87)	**73%** (192/263)
Treatment B: Percutaneous nephrolithotomy	**83%** (289/350)	87% (234/270)	69% (55/80)

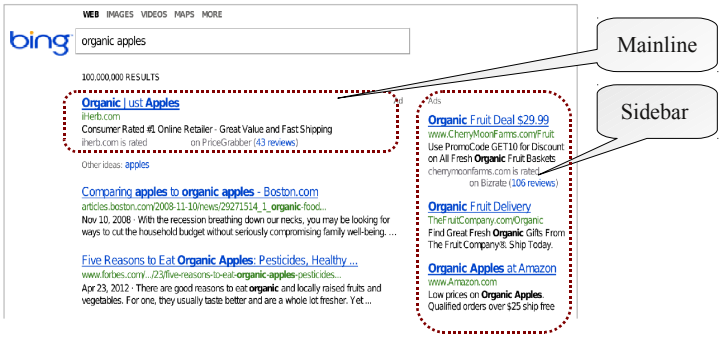
- Variable influençante

  Le choix des patients entrant dans les deux groupes dépendait de la sévérité de la pathologie



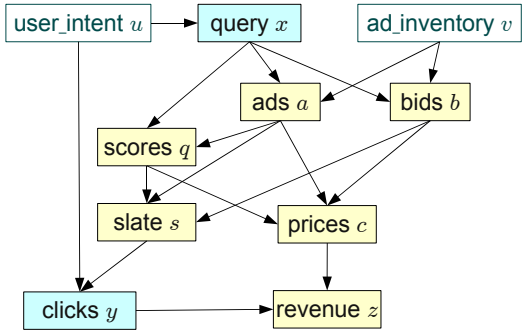
Système adaptatif de placement de publicité

- Deux **sous-systèmes**
  - L'un plaçant les **liens publicitaires**
  - L'autre choisissant les **publicités**



- Qui **s'influencent mutuellement**
  - Chacun s'appuie sur les données de clicks
  - Qui dépendent aussi de l'intervention de l'autre systèmes
  - Et d'autres facteurs non contrôlés (prix, requête de l'utilisateur, …)

Importance de l'identification
du **graphe causal**



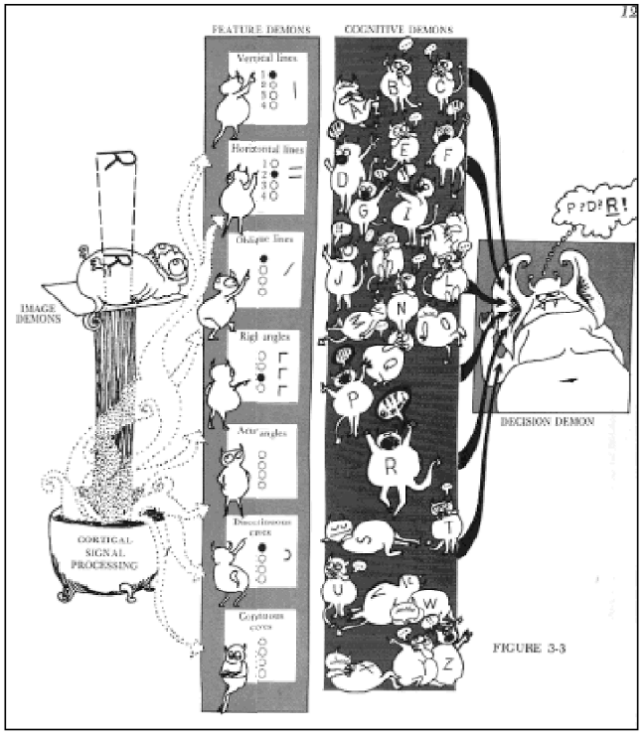
[L. Bottou et al. «*Counterfactual Reasoning and Learning Systems: The Example of Computational Advertising* », JMLR, 14, (2013), 3207-3260]

Dartmouth Summer School on Artificial Intelligence (1956)

- Oliver Selfridge : « Pandemonium: A Paradigm for Learning ».

  Une architecture hiérarchique de « démons » pour résoudre des problèmes + la suggestion d'un mécanisme d'apprentissage

- L'architecture « blackboard » (1975)



Plan

1. L'IA est **attendue partout**
2. Quelles **garanties** sur l'induction
3. Un peu d'**histoire**
4. Et **demain** ? Prémisses de changement de paradigme
5. Retour sur les **défis**
6. Conclusions … et ouverture

Pour généraliser l'usage de systèmes apprenants et adaptatifs

1. Savoir **expliquer** et **justifier** des décisions pour chaque cas particulier
2. **Sous-systèmes en interaction** ni chaotiques, ni s'égarant

- **Aller au-delà** de l'apprentissage statistique
  - Les **explications** … entre nouveauté et revisite ?
  - Sous-systèmes **en interaction**
    - Graphes de dépendances causales et conditions d'indépendance conditionnelle
    - Contrefactuelles
  - La **causalité** : fondamental

Question

- Quels **critères** de **performance** ?

Un pari

Aller vers des systèmes capables d'enseigner

1. **Expliquer** un cas
2. **Synthétiser**
3. Organiser un **curriculum**

➢ Vers une **évaluation** des systèmes **par la performance de leurs élèves ?**