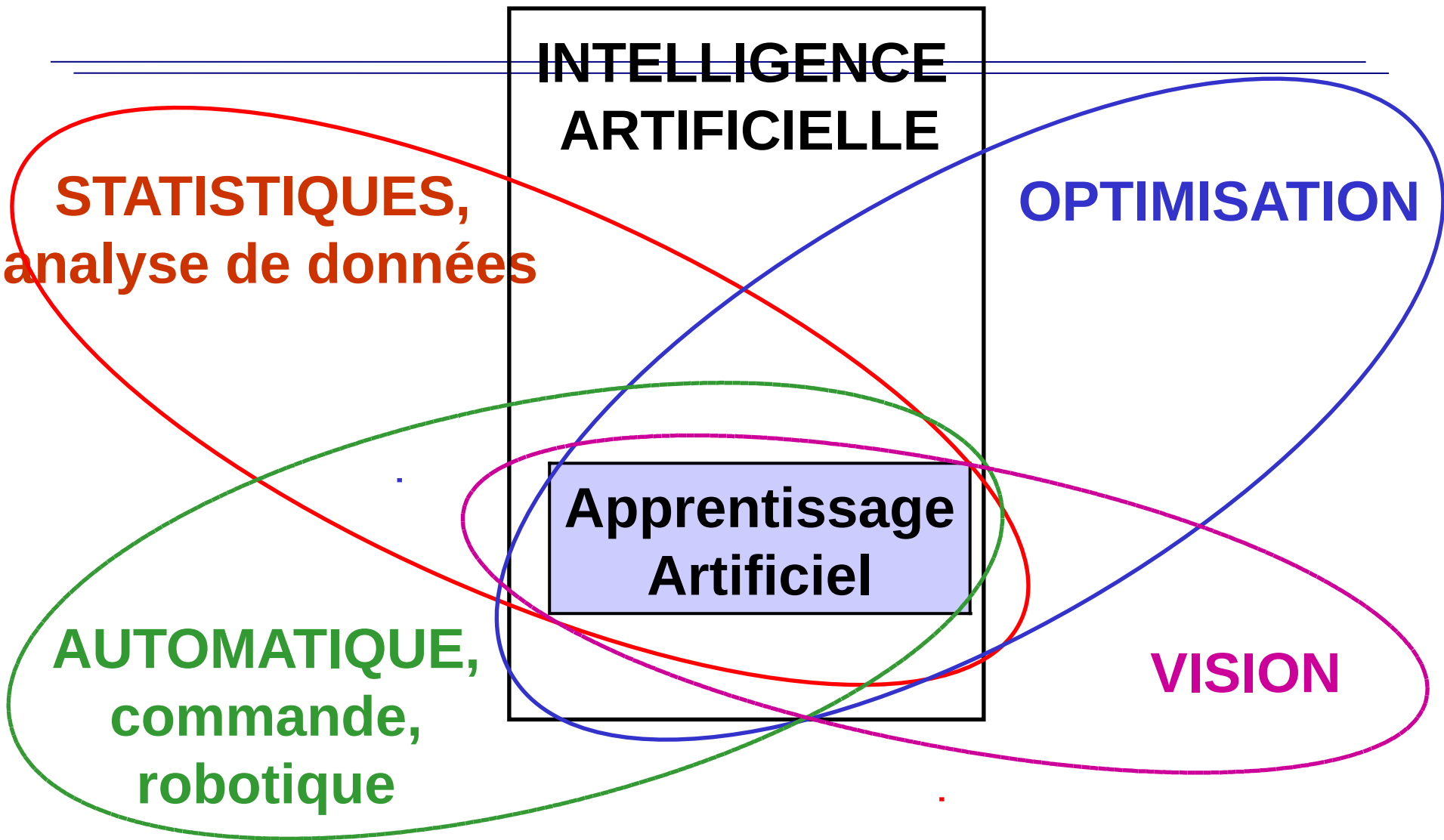

Introduction à l'Apprentissage Artificiel

Plan

- Introduction à l'Induction
 - Exemples d'applications
 - Types d'apprentissage
 - Apprentissage Supervisé
 - Apprentissage par Renforcement
 - Apprentissage Non-supervisé
 - Théorie de l'Apprentissage (Artificiel)
- Quelles questions se pose-t-on ?

Un domaine interdisciplinaire



Qu'est ce que l'apprentissage ?

- Mémoire
 - ❑ Acquisition de connaissance
 - ❑ Neurosciences
 - A court terme (de travail)
 - ❑ rétention de 7 ± 2 objets à la fois
(exemple du joueur d'échec professionnel, plateau aléatoire, plateau structuré)
 - A long terme
 - ❑ Mémoire procédurale
 - » les enchaînements d'actions
 - ❑ Mémoire déclarative
 - » sémantique (concepts)
 - » épisodique (faits)
- Types d'apprentissage
 - ❑ Par coeur
 - ❑ Par règles
 - ❑ **Par imitation / démonstration**
 - ❑ **Par essais-erreurs**
- **Réutilisation de la connaissance**
 - ❑ Dans des situations *similaires*

APPRENTISSAGE ARTIFICIEL

**« Capacité d'un système à
améliorer ses performances via
des interactions avec son environnement »**

**Une des familles essentielles de techniques pour
l'Intelligence Artificielle (IA) : permet
conception et/ou adaptation automatisée du
modèle
et/ou du comportement d'agents « intelligents »**

Qu'est-ce que l'Apprentissage Artificiel ?

Etant donné :

- de **l'expérience** E,
- une **classe de tâches** T
- une **mesure de performance** P,

On dit d'un ordinateur qu'il **apprend** si
sa performance sur une tâche de T
mesurée par P
augmente avec l'expérience E

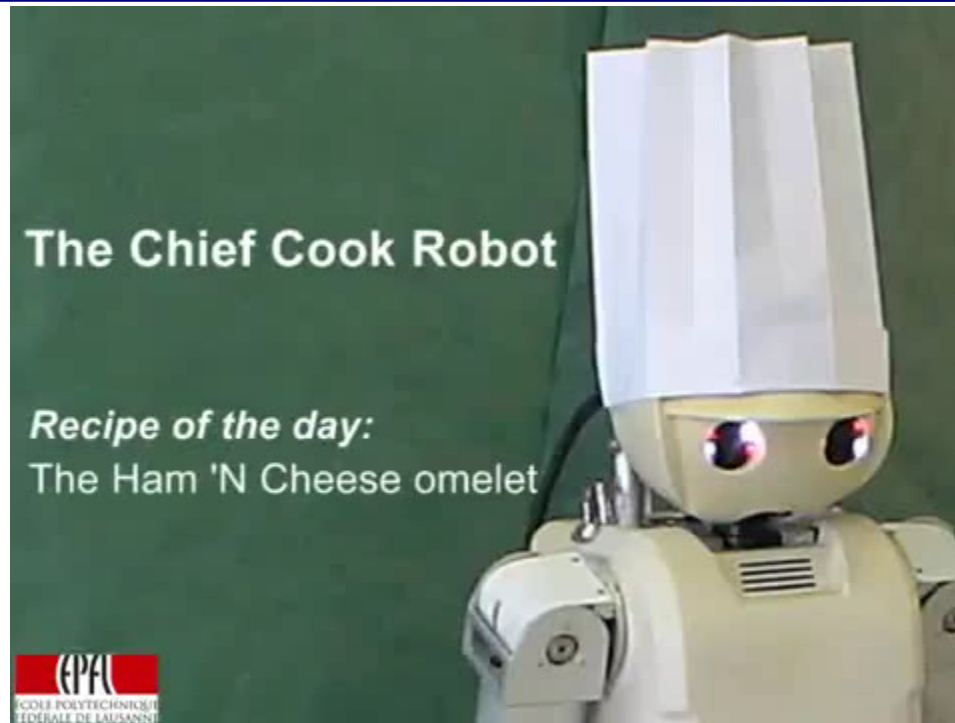
Tom Mitchell, 1997

Termes associés à l'Apprentissage Artificiel

- Robotique
 - Automatic Google Cars, Nao
- Prédiction / prévision
 - Bourse, pics de pollution, ...
- Reconnaissance
 - faciale, parole, écriture, mouvements, ...
- Optimisation
 - vitesse du métro, voyageur de commerce,
- Régulation
 - Chauffage, trafic, température du frigo, ...
- Autonomie
 - Robots, prothèses de main
- Résolution automatique de problèmes
- Adaptation
 - préférences utilisateur, Robot sur terrain accidenté, ...
- Induction
- Généralisation
- Découverte automatique
- ...

Quelques applications

Apprendre à cuisiner



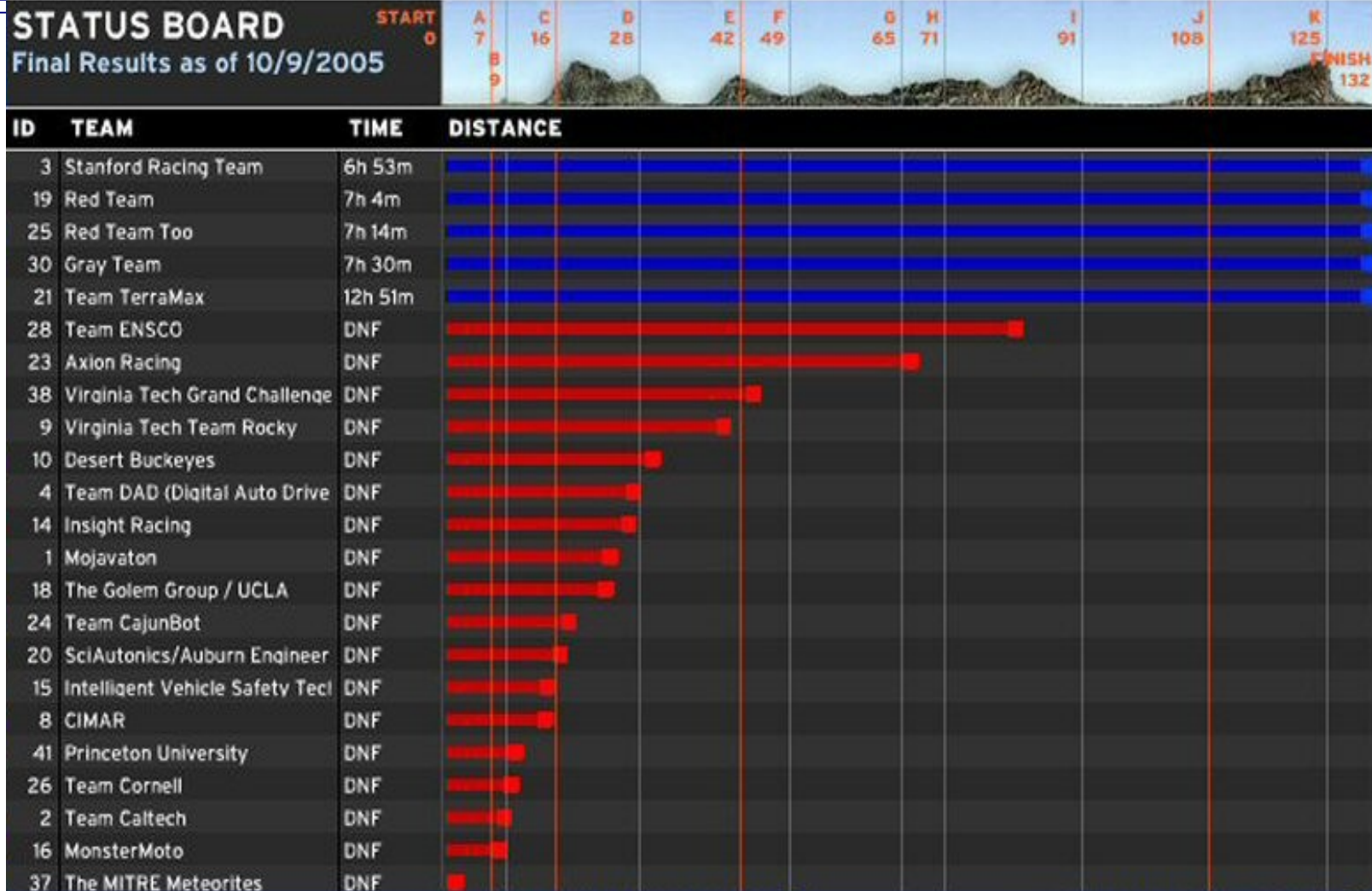
- Apprentissage par imitation / démonstration
- Apprentissage procédural (précision motrice)
- Reconnaissance d'objets

DARPA Grand challenge (2005)

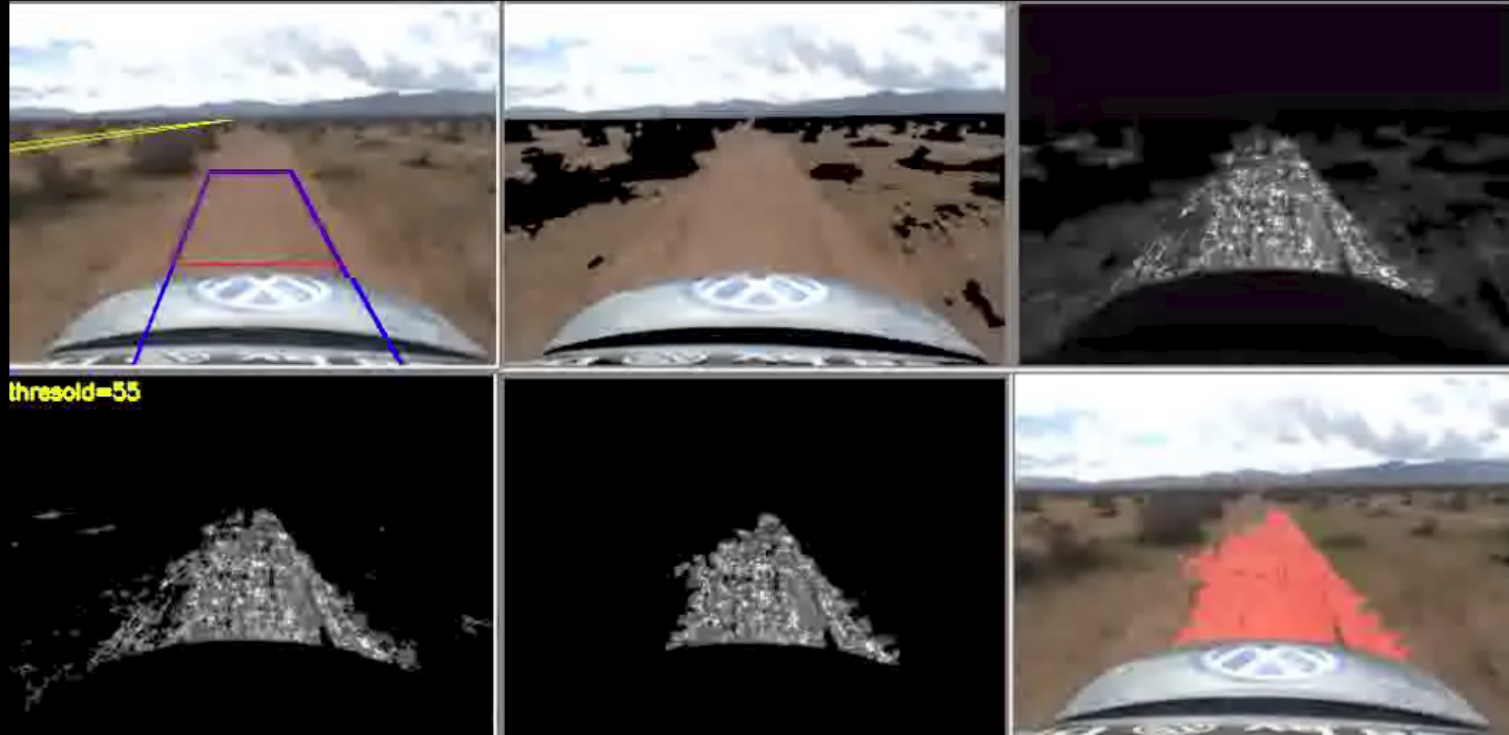




5 Finalistes



Reconnaissance de la route



Fast adaptation: Mean & covariance of Gaussian, exponential forgetting
Slow learning: memory of k past Gaussians

Apprendre à étiqueter des images: Reconnaissance de visages

B. Heisele et al. / Computer Vision and Image Understanding 91 (2003) 6–21

15

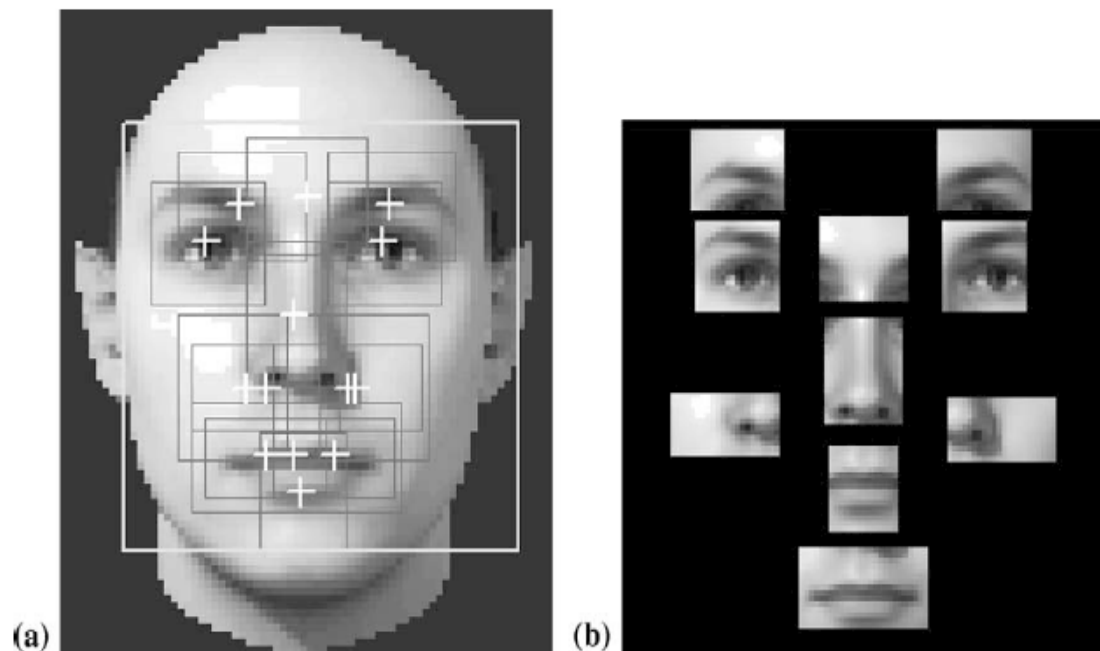


Fig. 5. (a) The 14 components of our face detector. The centers of the components are marked by a white cross. The 10 components that were used for face recognition are shown in (b).

Combinaisons de composantes

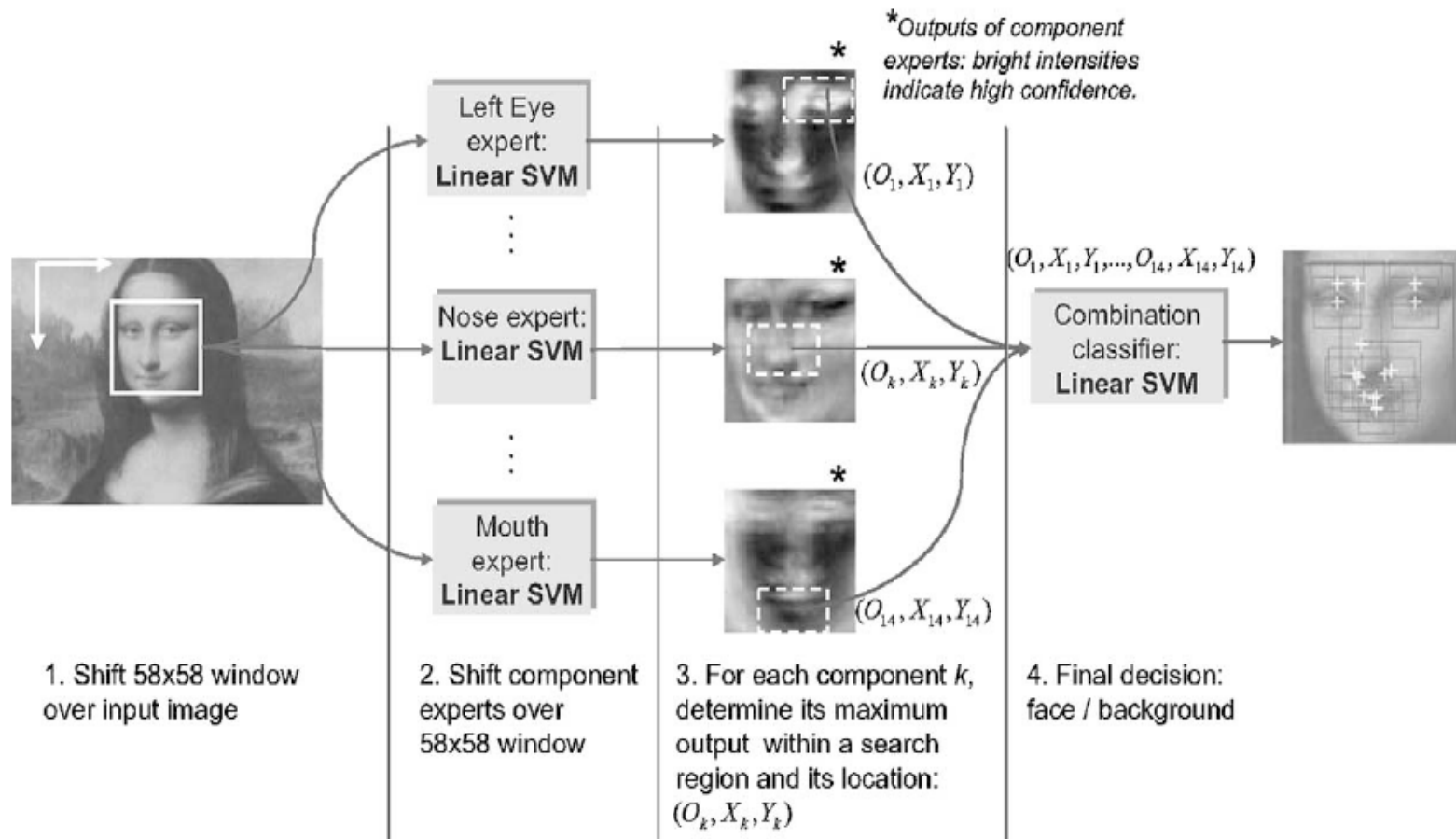
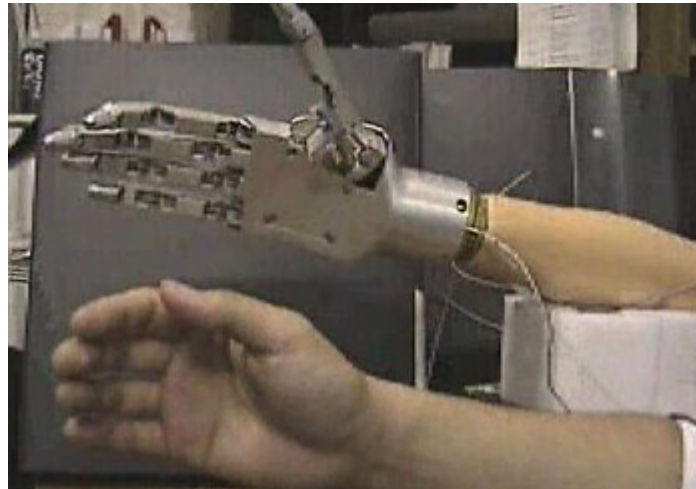


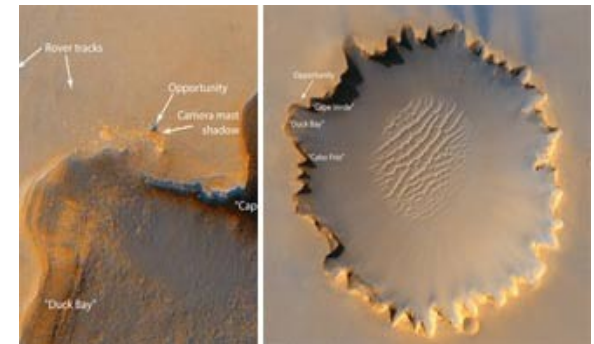
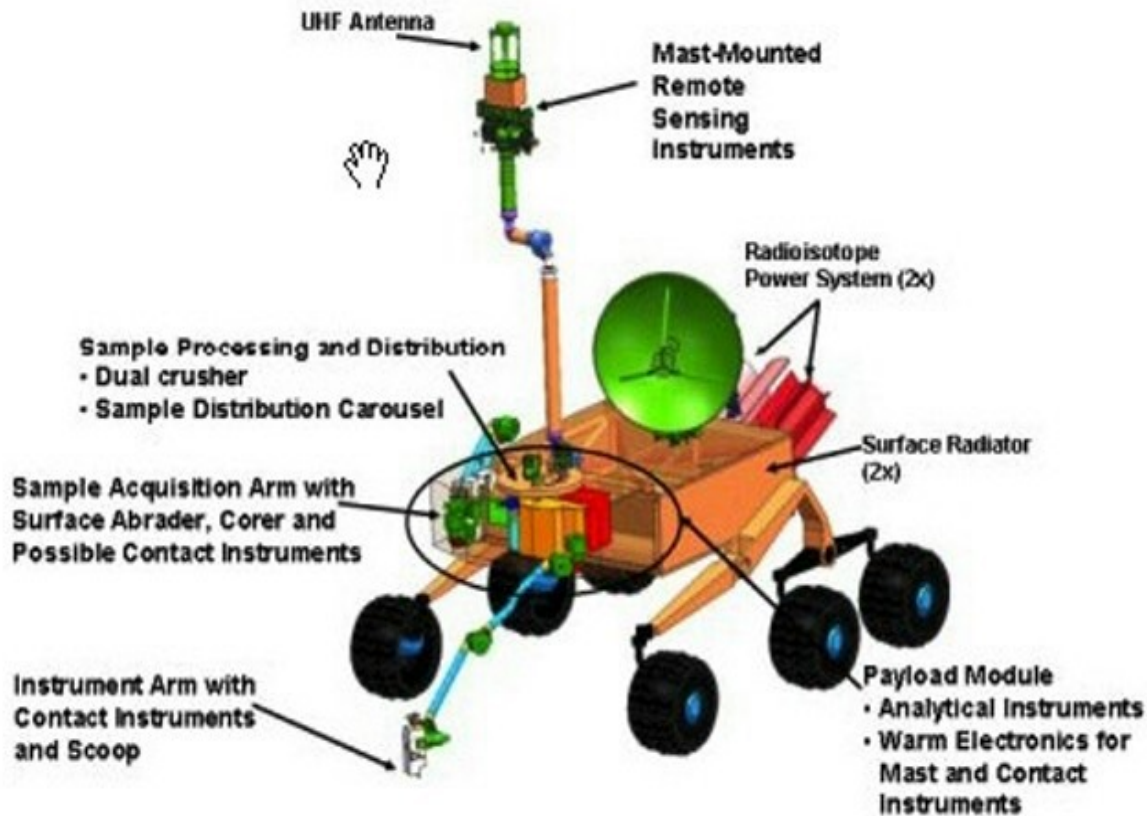
Fig. 4. System overview of the component-based face detector using four components.

Prothèse de main



- Reconnaissance des signaux pronateurs et supinateurs
 - ❑ capteurs imparfaits
 - ❑ bruit des signaux
 - ❑ incertitude

Robot autonome sur Mars



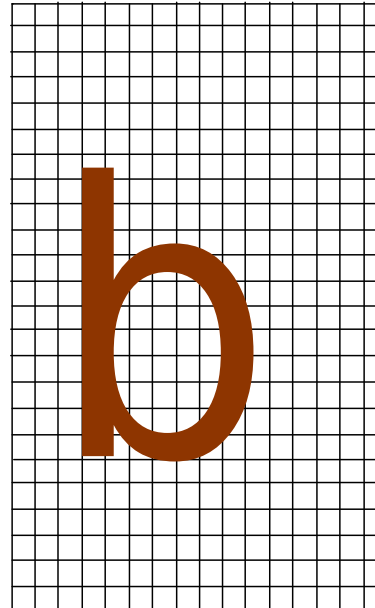
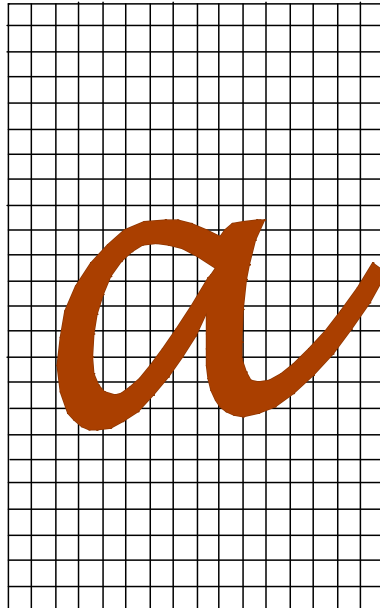
1. 1- Des scénarios

Apprendre par coeur ? **INEXPLOITABLE**

→ **Généraliser**

Apprentissage supervisé

Comment coder les formes ?



Typologie de l'apprentissage

« Capacité d'un système à améliorer ses performances via des interactions avec son environnement »

- **Quel « système » ?**
 - types de modèle (Ad hoc ? Issu d'une famille particulière de fonctions mathématiques [tq splines, arbre de décision, réseau de neurones, arbre d'expression, machine à noyau...] ?)
- **Quelles « interactions avec l'environnement » ?**
 - apprentissage « hors-ligne » v.s. « en-ligne »
 - apprentissage « supervisé » ou non, « par renforcement »
- **Quelles « performances » ?**
 - fonction de coût, objectif, critère implicite, ...
- ***Comment* améliorer ?**
 - type d'algorithme (gradient, résolution exacte problème quadratique, heuristique, ...)

Paradigme d'apprentissage

Chaque paradigme se caractérise par :

Un modèle, le plus souvent paramétrique

+

Une façon d'interagir avec l'environnement

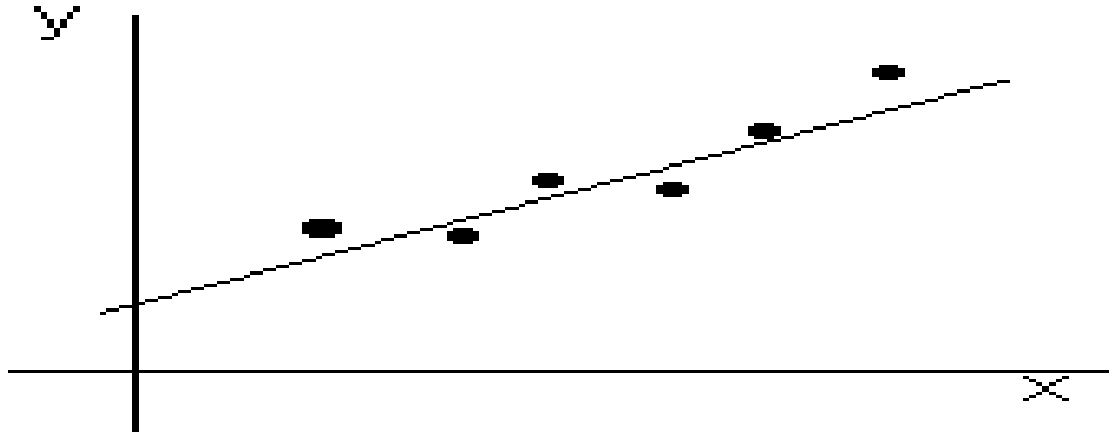
+

Une « fonction de coût » à minimiser (sauf exceptions)

+

**Un algorithme pour adapter le modèle,
en utilisant les données issues de l'environnement,
de façon à optimiser la fonction de coût**

Exemple trivial : régression linéaire par moindres carrés



- **Modèle** : droite $y=ax+b$ (2 paramètres a et b)
- **Interaction** : collecte *préalable* de n points $(x_i, y_i) \in \mathbb{R}^2$
- **Fonction de coût** : somme des carrés des écarts à la droite $K = \sum_i (y_i - a \cdot x_i - b)^2$
- **Algorithme** : résolution directe (ou itérative) du système linéaire

$$\begin{pmatrix} \sum_{i=1}^n x_i^2 & \sum_{i=1}^n x_i \\ \sum_{i=1}^n x_i & n \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n x_i y_i \\ \sum_{i=1}^n y_i \end{pmatrix}$$

Nombreux paradigmes

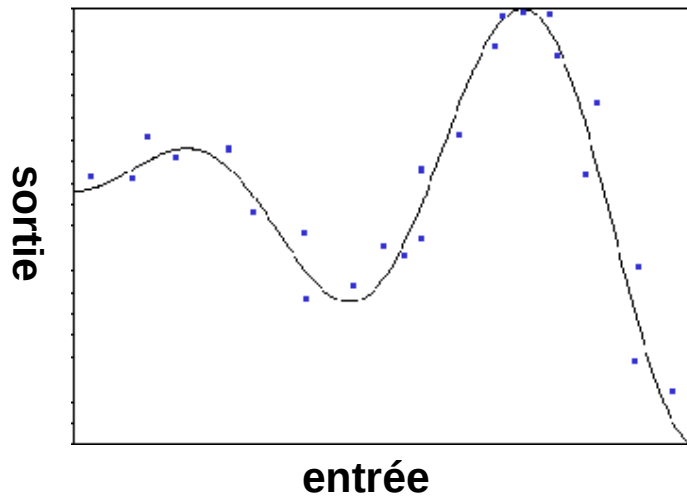
- ~~Régression linéaire par moindres carrés~~
- Algo ID3 ou CART pour arbres de décision
- Méthodes probabilistes
- ...
- Rétropropagation du gradient sur réseau neuronal à couches
- Cartes topologiques de Kohonen
- Support Vector Machines
- Boosting de classifieurs faibles
- ...

Principaux types d'algorithmes

- Résolution système linéaire (régression, Kalman, ...)
- **Algos classiques d'optimisation**
 - Descente de gradient, gradient conjugué, ...
 - Optimisation sous contrainte
 - ...
- **Heuristiques diverses :**
 - Algo d'auto-organisation non supervisée de Kohonen
 - Algorithmes évolutionnistes (GA, GP, ...)
 - « colonies de fourmis » (Ant Colony Optimization)
 - Optimisation par Essaim Particulaire (OEP)
 - Renforcement (Q-learning, ...)

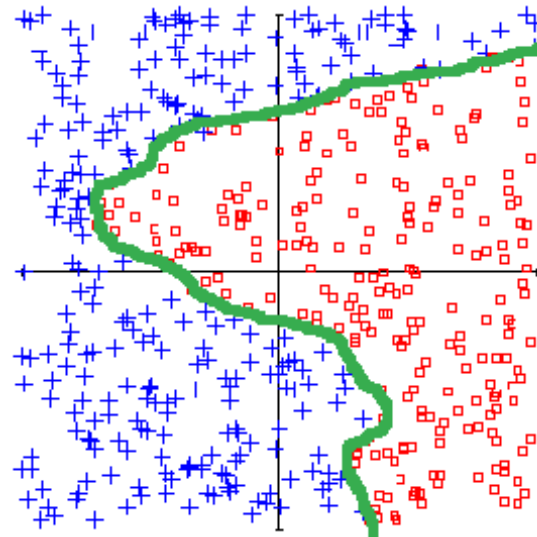
APPRENTISSAGE SUPERVISÉ : régression et classification

Régression (approximation)



points = exemples → courbe = régression

Classification ($y_i = \text{« étiquettes »}$)



*entrée =
position point*

*sortie désirée =
classe ($\square = -1, + = +1$)*



*Fonction
étiquette = $f(x)$
(et frontière de
séparation)*

Introduction à la théorie de l'apprentissage

- Apprentissage supervisé
- Apprentissage par renforcement
- Apprentissage non-supervisé (CM)

Apprentissage supervisé

- Ensemble d'exemples x_i étiquetés u_i
- Trouver une hypothèse h tq:

$$h(x_i) = u_i \quad ?$$

$h(x_i)$: étiquette prédite

- Meilleure hypothèse h^* ?

Apprentissage Supervisé : 1^{er} Exemple

- Maisons : Prix / m²
- Recherche de h
 - Plus proches voisins ?
 - Régression linéaire, polynomiale ?
- Plus d'information
 - localisation (x, y ? ou variable symbolique ?),
age du bâtiment, voisinage, piscine, impôts
locaux, évolution temporelle ?

Problème

- 1) Modélisation
- 2) Collecte des données
- 3) Apprentissage
- 4) Validation (dans 3) ??)
- 5) Utilisation en cas réel

Idéal



Pratique



1) Modélisation

- Espace d'entrée
 - Quelles sont les informations pertinentes ?
 - Variables
- Espace de sortie
 - Que cherche-t-on à prédire ?
- Espace des hypothèses
 - Entrées \rightarrow (calcul) \rightarrow Sorties
 - Quel (genre de) calcul?

1-a) Espace d'entrée : Variables

- Quelles sont les informations pertinentes ?
- Doit-on récupérer tout ce qu'on peut ?
- Qualité des informations ?
 - ❑ Bruit
 - ❑ Quantité
- Coût de la collecte d'une information ?
 - ❑ Economique
 - ❑ Temps
 - ❑ Risque (invasif ?)
 - ❑ Ethique
 - ❑ Droit (CNIL en France, le Maroc ???)
- Domaine de définition de chaque variable ?
 - ❑ Symbolique, numérique borné, non bornée, etc.

Prix au m² : Variables

- Localisation
 - Continu : (x, y) longitude latitude ?
 - Symbolique : nom de la ville ?
- Age du bâtiment
 - Années
 - relatif au présent ou année de création ?
- Nature du terrain
- Piscine ?

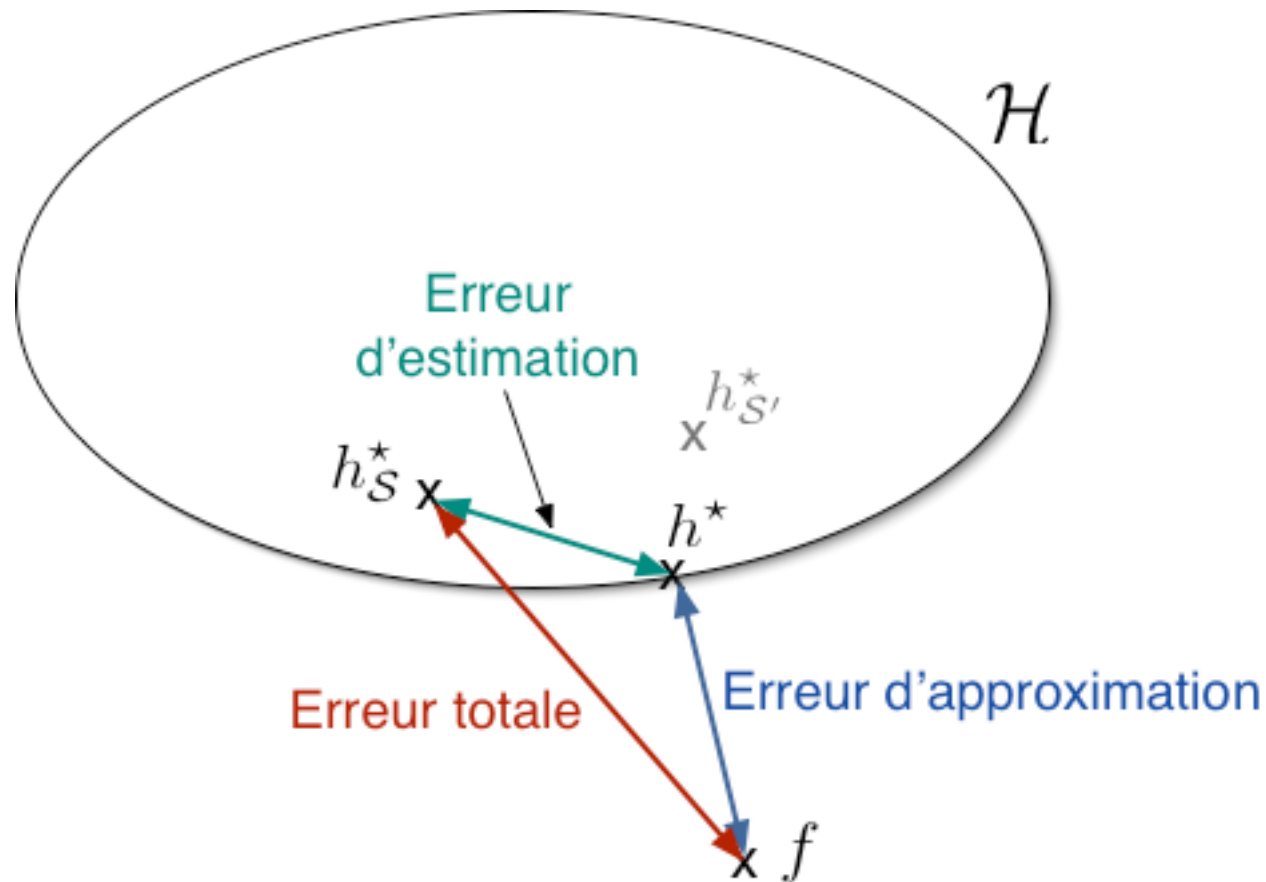
1-b) Espace de sortie

- Que veut-on en sortie ?
 - ❑ Classes symboliques ? (classification)
 - Booléennes Oui/Non (apprentissage de concept)
 - Multi-valuées A/B/C/D/...
 - ❑ Valeur numérique ? (régression)
 - $[0 ; 1]$?
 - $[-\infty ; +\infty]$?
- Combien de sorties ?
 - ❑ Multi-valué \rightarrow Multi-classe ?
 - 1 sortie pour chaque classe
 - ❑ Apprendre un modèle pour chaque sortie ?
 - Plus "libre"
 - ❑ Apprendre un modèle pour toutes les sorties ?
 - Chaque "modèle" peut utiliser des informations des autres

1-c) Espace des hypothèses

- Phase cruciale
- Dépend de la méthode d'apprentissage utilisée !
 - Régression linéaire : espace = $ax + b$
 - Régression polynomiale
 - nombre de paramètres = degré du polynôme
 - Réseaux de neurones, SVM, Algo Gen, ...
 - ...

Choix de l'espace des hypothèses



Choix de l'espace des hypothèses

- Espace trop "pauvre"
 - Solutions inadaptées
 - Ex: modéliser $\sin(x)$ avec une seule droite $y=ax+b$
- Espace trop "riche"
 - risque de sur-apprentissage
 - Ex: cf. tableau
- Défini par un ensemble de *paramètres*
 - Plus grand nb param → app. plus difficile
- Préférer cependant un espace plus riche !
 - Utilisation de méthodes génériques
 - Ajouter de la *régularisation*

2) Collecte des données

- Collecte
 - ❑ Capteurs électroniques
 - ❑ Par simulation
 - ❑ Sondages
 - ❑ Récupération automatique sur internet
 - ❑ ...
- Obtenir la plus grande quantité d'exemples
 - ❑ Coût de la collecte
- Obtenir les données les plus "pures" possibles
 - ❑ éviter tout bruit
 - bruit dans les variables
 - bruit dans les étiquettes !
 - ❑ Un exemple = 1 valeur pour chacune des variables
 - valeurs manquantes = exemple inutilisable ?

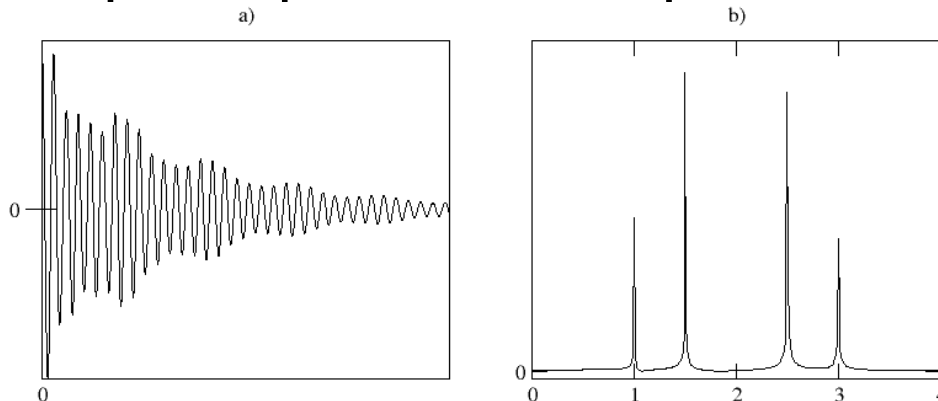
Données collectées

	Entrées / Variables			Sortie / Classe / Etiquette <i>mesurée</i>
	x1	x2	x3	u
Exemple 1	Oui	1.5	Vert	-
Exemple 2	Non	1.4	Orange	+
Exemple 3	Oui	3.7	Orange	-

Mais véritable
étiquette **y**
inaccessible !

Prétraitements des données

- Nettoyer les données
 - ex: Réduire le bruit de fond
- Transformer les données
 - Format final adapté à la tâche
 - Ex: Transformée de Fourier d'un signal audio temps/amplitude \rightarrow fréquence/amplitude



3) Apprentissage

- a) Choix des paramètres du programme
- b) Choix du critère inductif
- c) Lancement du programme d'apprentissage
- d) Test des performances
Si mauvais, retour en a)...

a) Choix des paramètres du programme

- Temps max de calcul alloué
- Erreur maximale acceptée
- Paramètres d'apprentissage
 - Spécifiques au modèle
- Introduction de connaissance
 - Initialiser les paramètres à des valeurs correctes ?
- ...

b) Choix du critère inductif

Objectif : trouver une hypothèse $h \in \mathbf{H}$ minimisant **le risque réel** (espérance de risque, erreur en généralisation)

$$R(h) = \int_{\mathbf{X} \times \mathbf{Y}} l(\underline{h(\mathbf{x})}, \underline{y}) \, d\underline{P(\mathbf{x}, y)}$$

Fonction de perte

Étiquette
prédite

Étiquette vraie y
(ou désirée u)

Loi de probabilité
jointe sur $\mathbf{X} \times \mathbf{Y}$

Risque réel

- Objectif : Minimiser le risque réel

$$R(h) = \int_{X \times Y} l(h(x), y) dP(x, y)$$

- On ne connaît pas le risque réel, en particulier pas la loi de probabilité $P(X, Y)$.

- Discrimination**

$$l(h(x_i), u_i) = \begin{cases} 0 & \text{si } u_i = h(x_i) \\ 1 & \text{si } u_i \neq h(x_i) \end{cases}$$

- Régression**

$$l(h(x_i), u_i) = [h(x_i) - u_i]^2$$

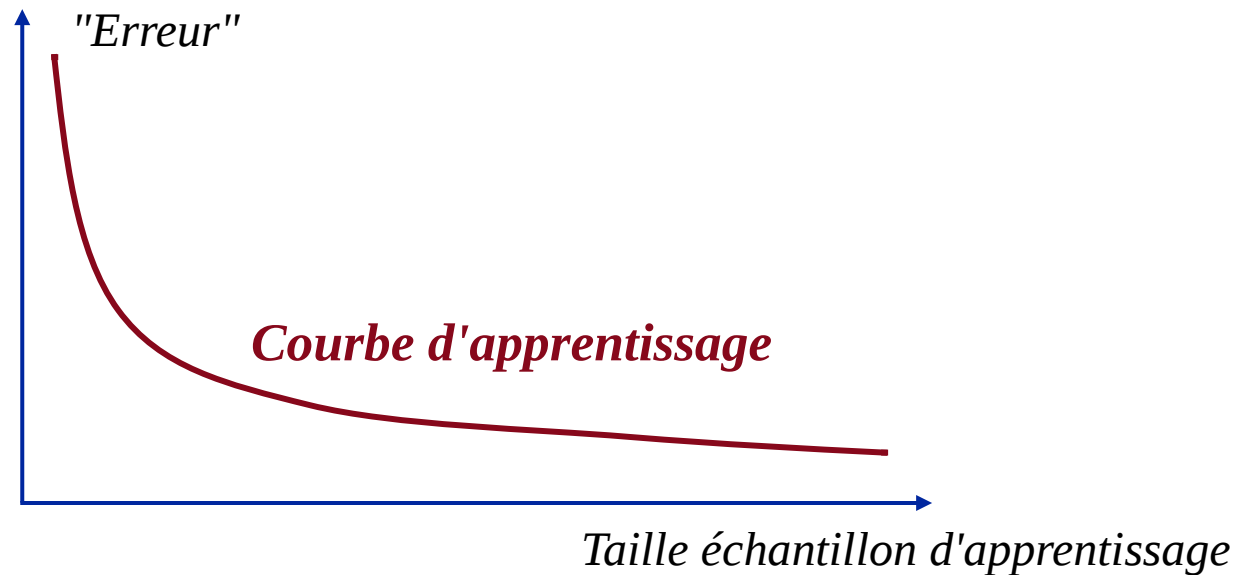
Minimisation du risque empirique

- Le *principe ERM* (*minimisation du risque empirique*) prescrit de chercher l'hypothèse $h \in \mathbf{H}$ minimisant le **risque empirique**
- Plus faible erreur sur l'ensemble d'apprentissage

$$R_{Emp}(h) = \sum_{i=1}^m l(h(x_i), u_i)$$

Courbe d'apprentissage

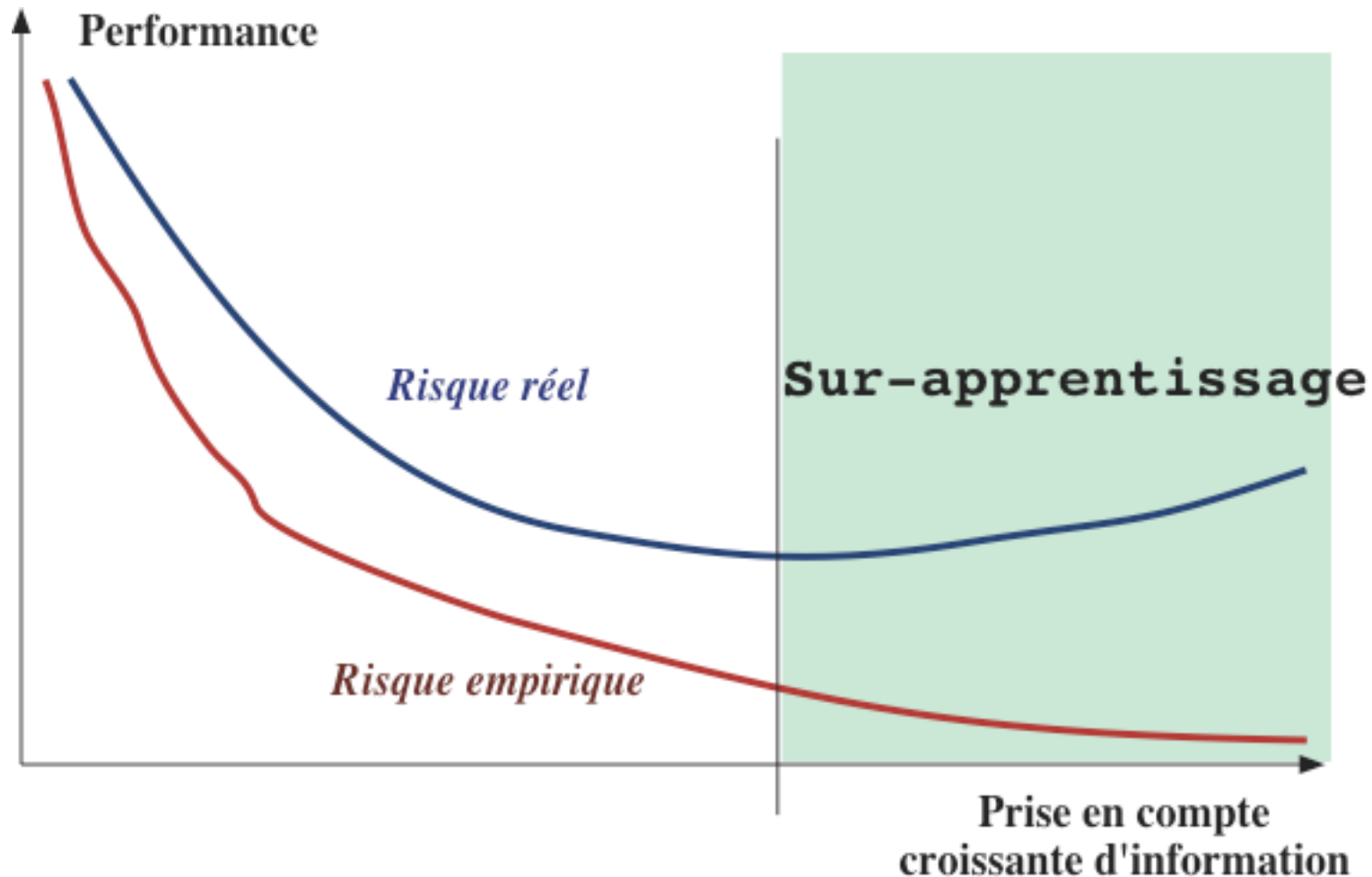
- La quantité de données d'apprentissage est importante !



Test / Validation

- Mesurer le **sur-apprentissage**
- **GENERALISATION**
 - ❑ *la connaissance acquise est-elle utilisable dans des **circonstances nouvelles** ?*
 - ❑ **Ne pas valider sur l'ensemble d'apprentissage !**
- Validation sur **ensemble de test** supplémentaire
- **Validation Croisée**
 - ❑ utile quand peu de données
 - ❑ *leave-p-out*

Sur-apprentissage



Régularisation

- Limiter le sur-apprentissage **avant** de le mesurer sur le test
- Ajout d'une **pénalisation** dans le critère inductif
 - Ex:
 - Pénaliser l'utilisation de grands nombres
 - Pénaliser l'utilisation de ressources
 - ...

Maximum a posteriori

- Approche bayésienne
- On suppose qu'il existe une distribution de probabilités *a priori* sur l'espace \mathbf{H} : $p_{\mathbf{H}}(h)$

Principe du Maximum A Posteriori (MAP):

- On cherche l'hypothèse h la plus probable après observation des données \mathbf{S}

$$h^* = \underset{h \in \mathcal{H}}{\text{ArgMax}} \frac{P(\mathcal{S} | h)P(h)}{P(\mathcal{S})} = \underset{h \in \mathcal{H}}{\text{ArgMax}} P(\mathcal{S} | h)P(h)$$

- Ex: Observation de la couleur des moutons
 - $h = \text{"Un mouton est blanc"}$

Principe de Description de Longueur Minimale

- **Rasoir d'Occam**

"Les hypothèses les plus simples sont les meilleures"

- Simplicité : taille de h

→ **Compression maximale**

- Maximum a posteriori

avec $p_H(h) = 2^{-d(h)}$

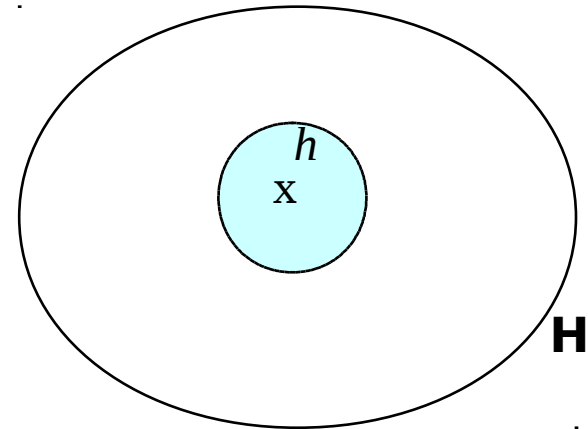
- $d(h)$: longueur en bits de l'hypothèse h

- Compression → généralisation



Exploration locale

- *Seulement une notion de voisinage dans H*
 - Méthodes de « gradient »
 - Réseaux de neurones
 - SVM (Séparatrices à Vastes Marges)
 - Recuit simulé / algorithmes d'*évolution simulée*
- */!\ Minima locaux*



Exploration sans espace d'hypothèse

- ***Pas d'espace d'hypothèses***
 - Utiliser directement les exemples
 - Et l'espace des exemples
 - Méthodes de plus proches voisins
(Raisonnement par cas / Instance-based learning)
 - Notion de **distance**
- Exemple : *k Plus Proches Voisins*
 - Option : Vote pondéré par la distance

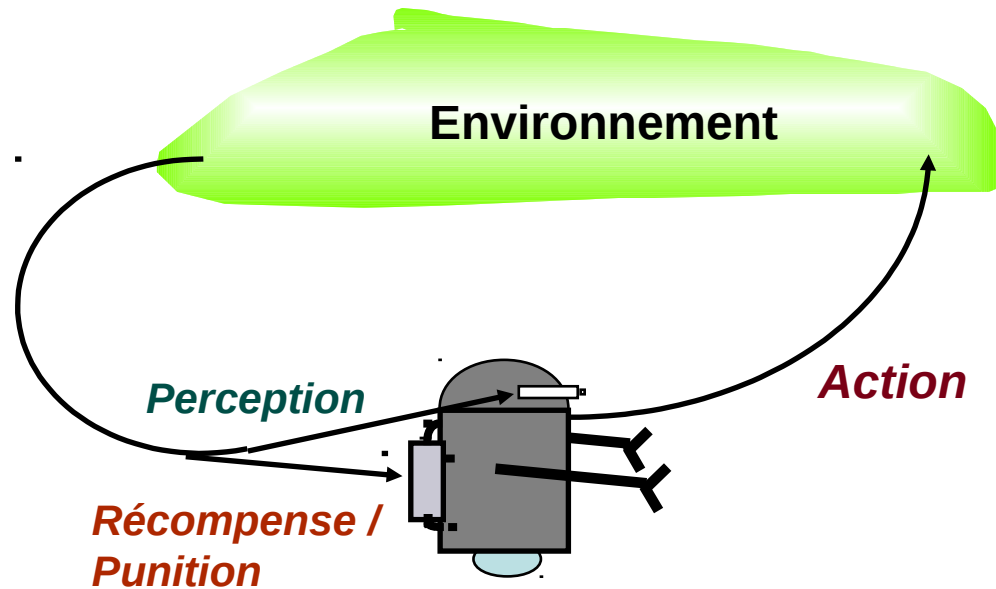
Autres types d'apprentissage

Apprentissage par Renforcement

Apprentissage non-supervisé

Apprentissage par Renforcement

- Pavlov
 - ❑ Cloche : **déclencheur**
 - ❑ Gamelle : **récompense**
 - ❑ saliver : **action**
 - ❑ **Association**
cloche ↔ gamelle
 - ❑ **Renforcement** du
comportement "saliver"



- Contrôler le comportement par renforcements
 - ❑ **Récompenses et punitions**

Apprentissage par Renforcement

- L'agent doit *découvrir* le bon comportement

- Et l'optimiser

- Maximiser ***l'espérance des récompenses***

- s_t : état à l'instant t

- Choix de l'action : $a_t := \operatorname{argmax}_a Q(s_t, a)$

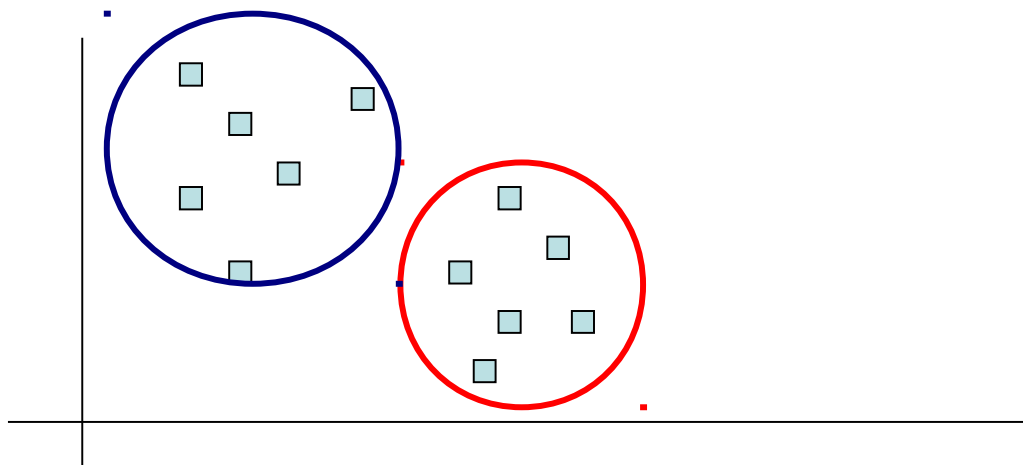
- Mise à jour des valeurs

- r_t : récompense reçue à l'instant t

- $$Q(s_t, a_t) \leftarrow \alpha Q(s_t, a_t) + (1 - \alpha) [r_{t+1} + \gamma \max_a Q(s_{t+1}, a)]$$

Apprentissage Non-supervisé

- Pas de classe, pas de sortie, pas de récompense
- Objectif : **grouper** les exemples



- Notion de distance
- Biais inductif

Conclusion

- Induction
 - Trouver une hypothèse générale à partir d'exemples
- Eviter le sur-apprentissage
- Choisir le bon espace d'hypothèse
 - Pas trop petit (mauvaise induction)
 - Pas trop grand (sur-apprentissage)
- Utiliser un algorithme adapté
 - Aux données
 - A l'espace des hypothèses

Ce qu'il faut retenir

- C'est surtout l'induction supervisée qui est étudiée
- On ne peut apprendre sans **biais**
- La **réalisation de l'apprentissage** dépend de la structuration de l'espace des hypothèses
 - ❑ Sans structure : *méthodes par interpolation*
 - ❑ Notion de distance : *méthodes par gradient (approximation)*
 - ❑ Relation d'ordre partiel : *exploration guidée (exploration)*