

# Intelligence Artificielle

Développer la culture numérique de la communauté éducative  
en enseignement scientifique et NSI

Anthony Larcher

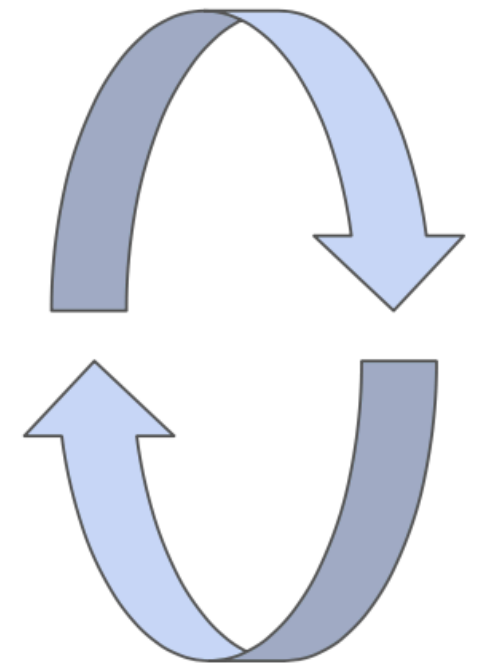
Sources: Colin de la Higuera Yann Lecun

# Plan

- A quoi peut servir le machine learning (quand l'utiliser) ?
- Qu'est-ce qu'un protocole expérimental en ML et pourquoi est-ce spécifique?
- Un aperçu de l'apprentissage profond
- Dangers de l'apprentissage automatique

# Machine Learning methodology

1. Define a task to be done by the computer.
2. Define the performance measures used to evaluate the quality of the algorithm performing the task.
3. Gather the data required to train models.
4. Perform the experiments to find the best models.
5. Deploy the best models in production.
6. Retrieve more data and iterate.



## When do you need ML?

- Tasks for which it is hard to program how they should be solved.
  - Tasks related to the analysis of complex data.
  - Tasks that require the adaptivity of the algorithm over time.
- Source: Adam Sherez, Unsplash



## Examples of a task

- “Detecting spam emails.”
- “Restore colors in a B&W image.”
- “Detecting violent scenes in videos.”
- “Predicting the next failure of a system.”
- “Recommending new items in function of users’ preferences.”
- “Generating new molecules with given properties.”
- ...

## Define the performance measures

A good performance measure should:

- evaluate if the algorithm successfully achieves a specific goal,
- be easy to interpret and communicate,
- be generic for evaluating different algorithms.

We must evaluate the performance measures in a production context

Tableau 1

Gather the data required to train a model			
• Annotatin	g data takes	time and	costs money.
• Never sac	rifice qualit	y fo r qua	ntity.
• Always us	e mechanisms	to e nsure	quality.
• Identify	opportunities	for data	collection.

Une Protocol expérimental spécifique au machine learning

Pourquoi ?

## Why do we need an experimental protocol?

There are different ways to achieve a given goal, but many are considered “cheating” according to human.

**For an AI, all means are good!**

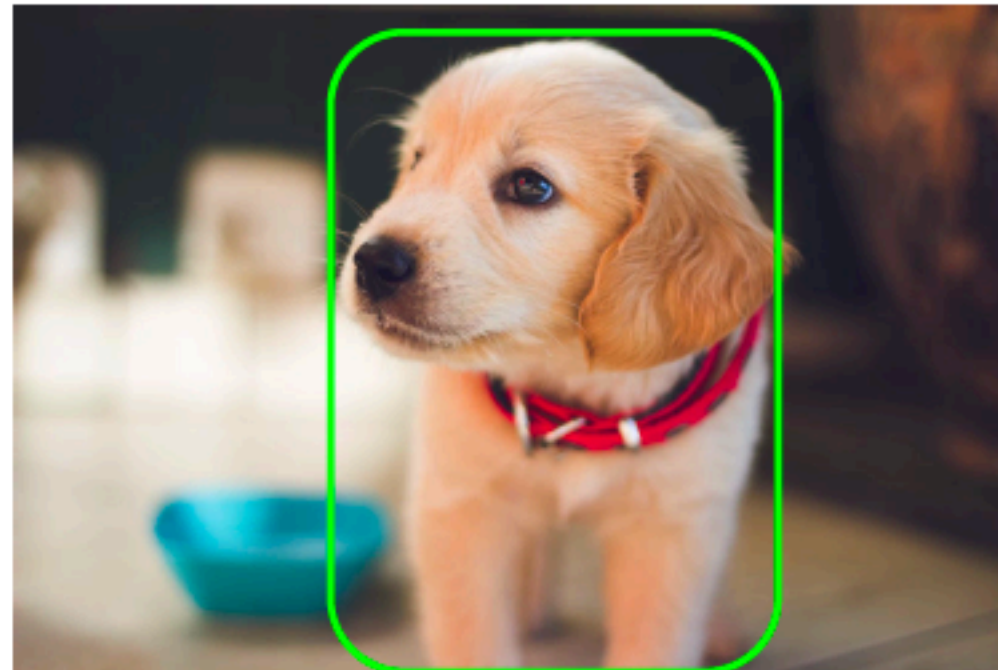


Source: Garmulewicz, Michał, Henryk Michalewski, and Piotr Miłoś.  
"Expert-augmented actor-critic for vizdoom and montezumas revenge."  
arXiv preprint arXiv:1809.03447 (2018).

<https://www.youtube.com/watch?v=0hiXKTa735s>

## Right for the wrong reasons

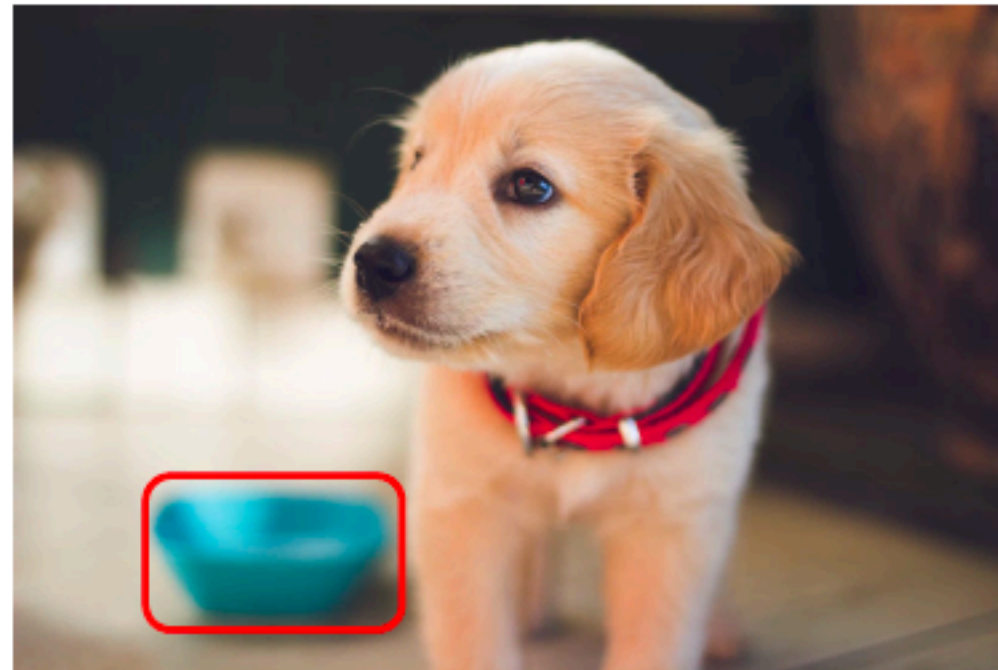
Is it a dog? Yes because...



Source: Berkay Gumustekin, Unsplash

## Is it a dog? Yes because...

Is it a dog? Yes because...



Source: Berkay Gumustekin, Unsplash

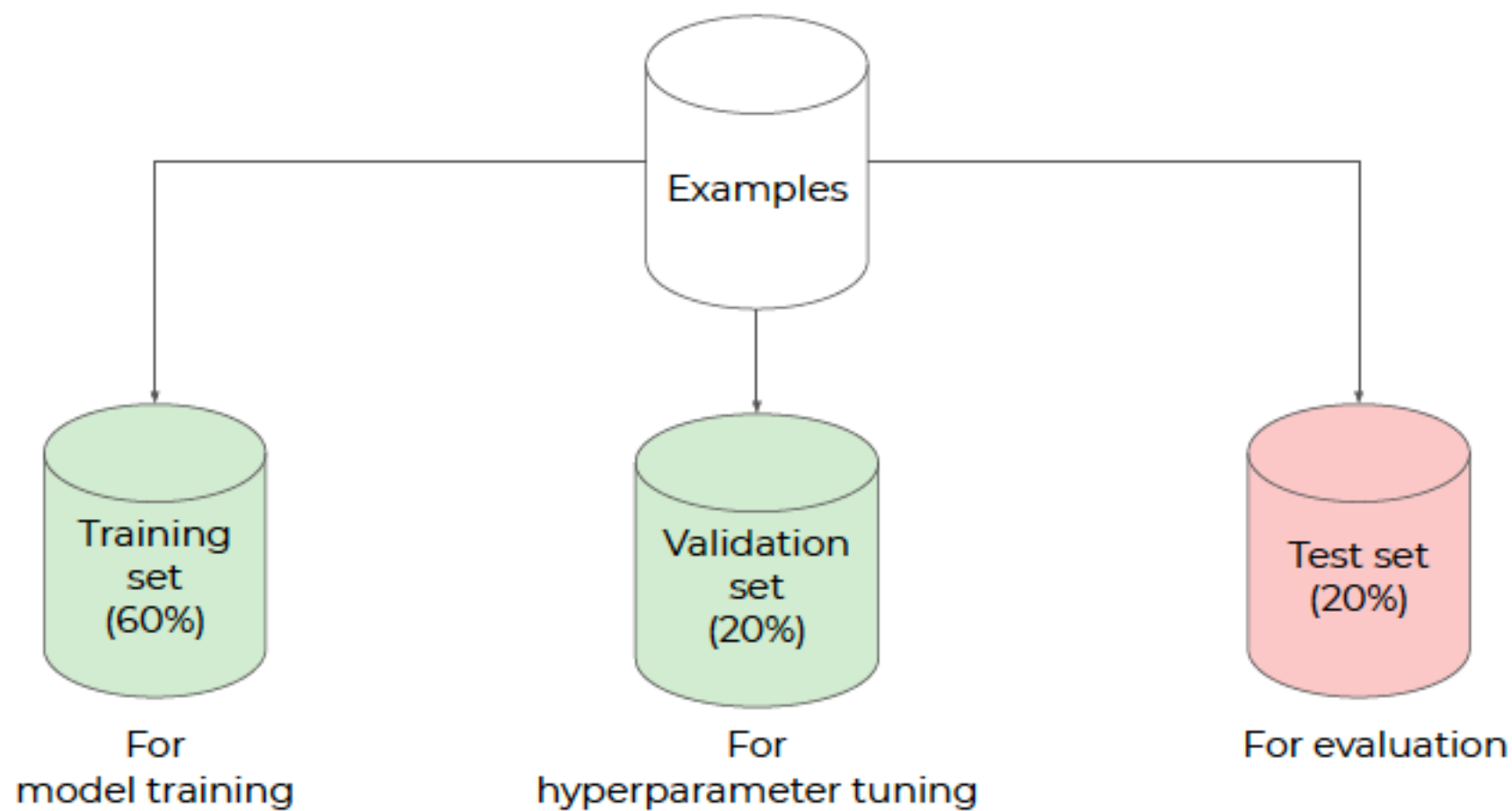
**Saliency map for interpretation** Source: Simonyan, Karen, Andrea Vedaldi, and Andrew Zisserman. "Deep inside convolutional networks: Visualising image classification models and saliency maps." (2013).

# Qu'est-ce qu'un paramètre? Qu'est-ce qu'un hyper-paramètre?

Exemple avec un classifieur linéaire  
paramètre: coefficient directeur et ordonnée à l'origine  
hyperparamètres: le nombre de plans affines nécessaires



## How to choose the best hyperparameters?



K-fold, cross-validation (si on manque d'exemples et que le résultat n'est pas significatif)

Importance des hypothèse:

- Indépendance
- Identically distributed

# Comment Représenter les données?

Il faut prendre en compte la topologie des données

## Structured data: adding topology to statistical data types

- Text: Number of sequences, maximum length, term frequencies, encoding (e.g. UTF-8).
- Image: Number of images, width, height, channel, encoding (e.g. PNG)
- Video: Number of video, width, height, channel, audio, subtitles, codec (e.g. MP4)
- Graph: Number of nodes and edges, features per node, feature per edges, adjacency matrix.
- Dictionary: Number of pairs (key, value), JSON structure

Qu'est ce qu'une représentation ?

Une représentation est une vue des données, indirectement de la réalité

Elle n'est pas l'objet elle même (Magrit)

Elle peut être locale (une unité de calcul = un concept)

Elle peut être distribuée (une même unité représente plusieurs concepts et un même concept est représenté par plusieurs unités)

## The concept of *representation*

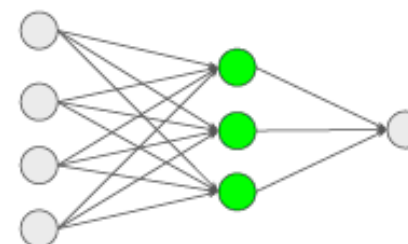
**Representation:** an implementation of the medium supporting data processing.

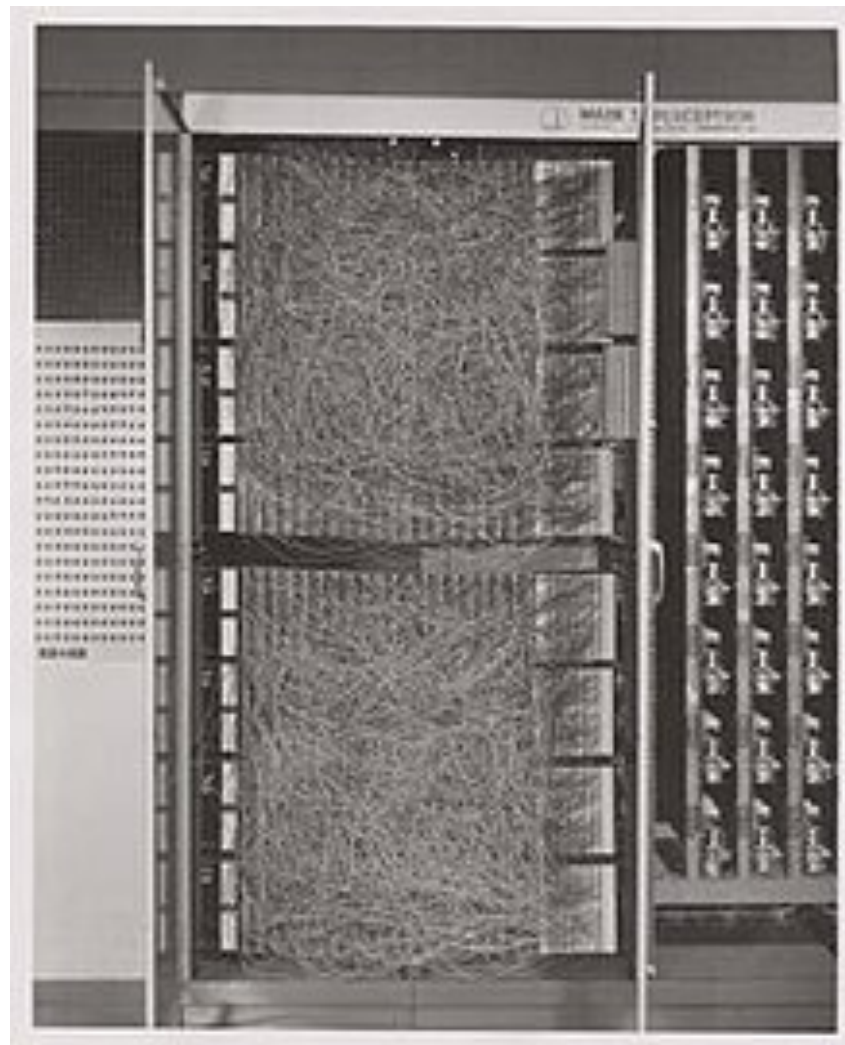
**Local representation:** one processing unit per concept. Easy to interpret. The inputs and outputs of a model are local representations.

**Distributed representation:** many processing units per concept and many concepts per processing units. Hard to interpret but efficient.



René Magritte, The Treachery of Images (1929)





<https://en.wikipedia.org/wiki/Perceptron>

Tableau 1

- **Machine learning is a subfield of artificial intelligence.**
- A methodology exists to prevent the learning algorithm from cheating.
- Using an experimental protocol with cross-validation is essential.
- Data should be independent and identically distributed.

Mise en pratique, exemple de CIFAR 10 tutorial MILA

Distribution des données  
sur-apprentissage



Importance de la validation pour « surveiller »

Importance de la quantité de données

Importance de la variété

Importance de l'augmentation de données

Problèmes des données déséquilibrées



Différents types d'apprentissage:

- Supervisé
- Non-supervisé
- Self-supervised
- Apprentissage par renforcement

# Supervisé: régression, classification binaire ou multiclasse (applications)

## Supervised learning

For each input in the dataset, we have the optimal output.  $z = (x, y)$

We want to model the conditional probability:  $p(y|x)$

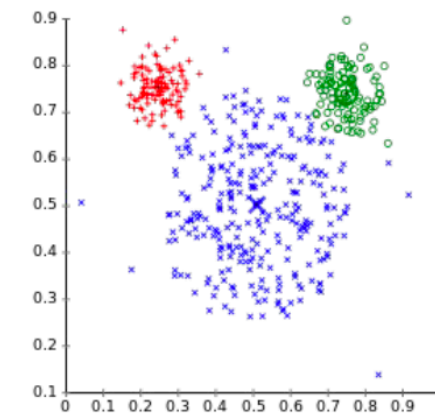
- **Regression:** targets are real-valued variables.
- **Classification:** targets are categorical variables.
  - **Multi-class:** choose only one class among a predefined set.
  - **Multi-label:** choose all relevant classes among a predefined set.

# Non-supervisé

## Estimation d'une densité de probabilité (applications)

### Unsupervised learning

- In the dataset, we only have the inputs.  $z = (x)$
- We want to model the marginal probability:  $p(x)$
- Applications:
  - Dimensionality reduction
  - Clustering, anomaly detection
  - Data generation



Source: Kingma, Durk P., and Prafulla Dhariwal.  
"Glow: Generative flow with invertible 1x1  
convolutions." In Advances in Neural Information  
Processing Systems, pp. 10215-10224. 2018.

# Self-supervised Principe Applications

## Self-supervised learning

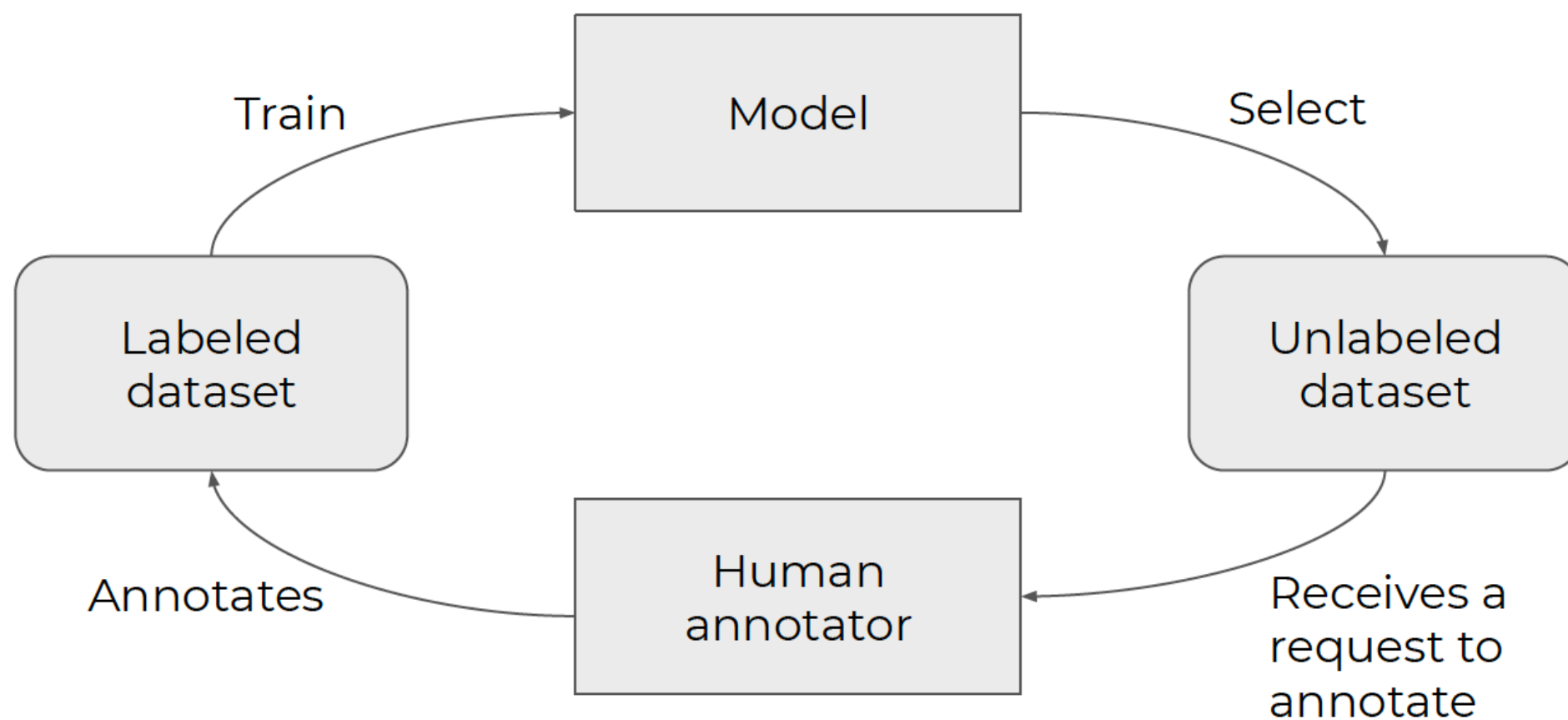
- In the dataset, we only have the inputs.  $z = (x)$
- We want to model the conditional probability:  $p(g(x)|x)$   
where  $g$  is a function that creates *pseudo-labels* from the inputs.
- The goal is to learn good representations that transfer well to any task.
- Examples of pseudo-labels:
  - Is the video forward or backward?
  - Is the image upside-down?
  - Is the first sentence contradicts the second sentence?

# Semi-supervised learning

- We consider two datasets:
  - Unlabeled examples (many examples)
  - Labeled examples (few examples)
- The goal is to learn good representations from the unlabeled examples that helps to train the model with the labeled examples for a specific task.
- Main idea: use the unlabeled examples to regularize the model.

# Active vs. passive learning

Active learning: the learner can ask the teacher to annotate specific data.





# Reinforcement learning

- Sequential decision making problem.
- Learning from interactions(examples) with the environment.
- The feedback (reward) concerns only the action taken in a given state.
- The agent builds its own dataset.

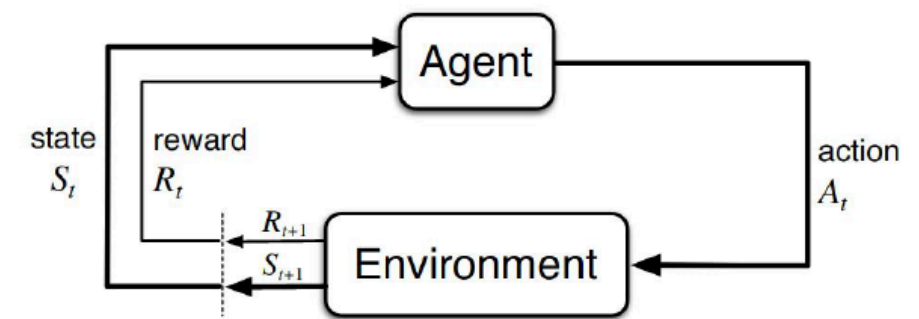


Figure 3.1: The agent–environment interaction in a Markov decision process.

Source: Sutton, Richard S., and Andrew G. Barto. Reinforcement learning: An introduction. MIT press, 2018., P. 38

# Risque ou Risque empirique ?

- Le risque est la somme pondérée de la fonction de coût
- Les poids sont la probabilité de chaque élément
- Problème: la distribution de probabilité des données réelle est inconnue

# Risque ou Risque empirique ?

- Le risque **empirique** est la somme pondérée de la fonction de coût **calculée sur nos données**

# Risque ou Risque empirique ?

- Le risque **empirique** est la somme pondérée de la fonction de coût **calculée sur nos données**

**!!! Il n'est pas calculé sur tous les exemples possibles !!!**

# Risque ou Risque empirique ?

Objectif de l'apprentissage automatique:

- Minimiser le risque empirique
- Est-ce que le modèle obtiendra les mêmes résultats lors de l'apprentissage et lors de sa mise en production ?

# Risque ou Risque empirique ?

Objectif de l'apprentissage automatique:

- Minimiser le risque empirique
- Est-ce que le modèle obtiendra les mêmes résultats lors de l'apprentissage et lors de sa mise en production ?

**Pourquoi ne serait-ce pas le cas ?**

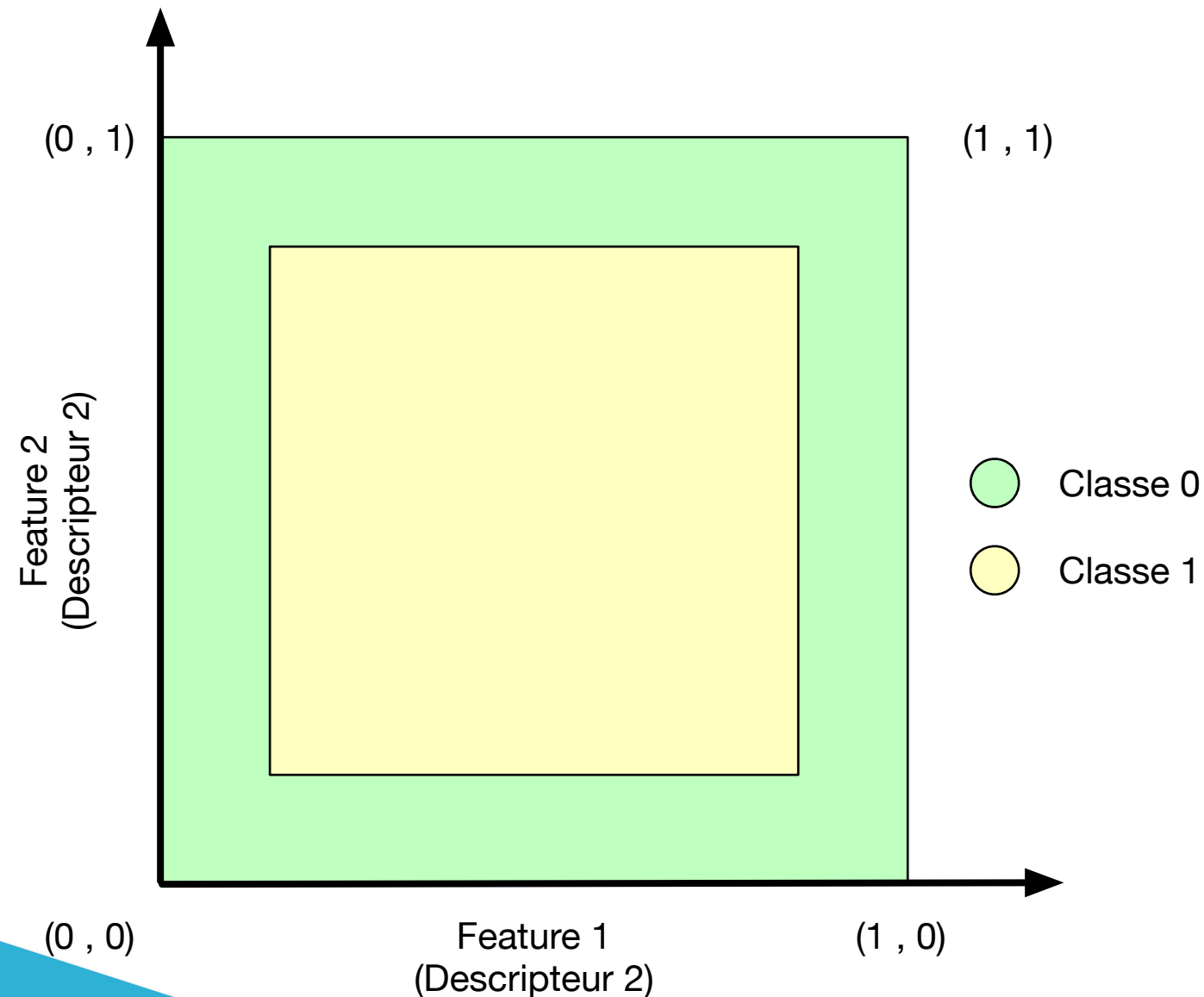
# Risque ou Risque empirique ?

Pourquoi seraient ils différents?

- Nous n'avons qu'une quantité de données limitées
- Notre système approxime seulement une moyenne

# Illustration

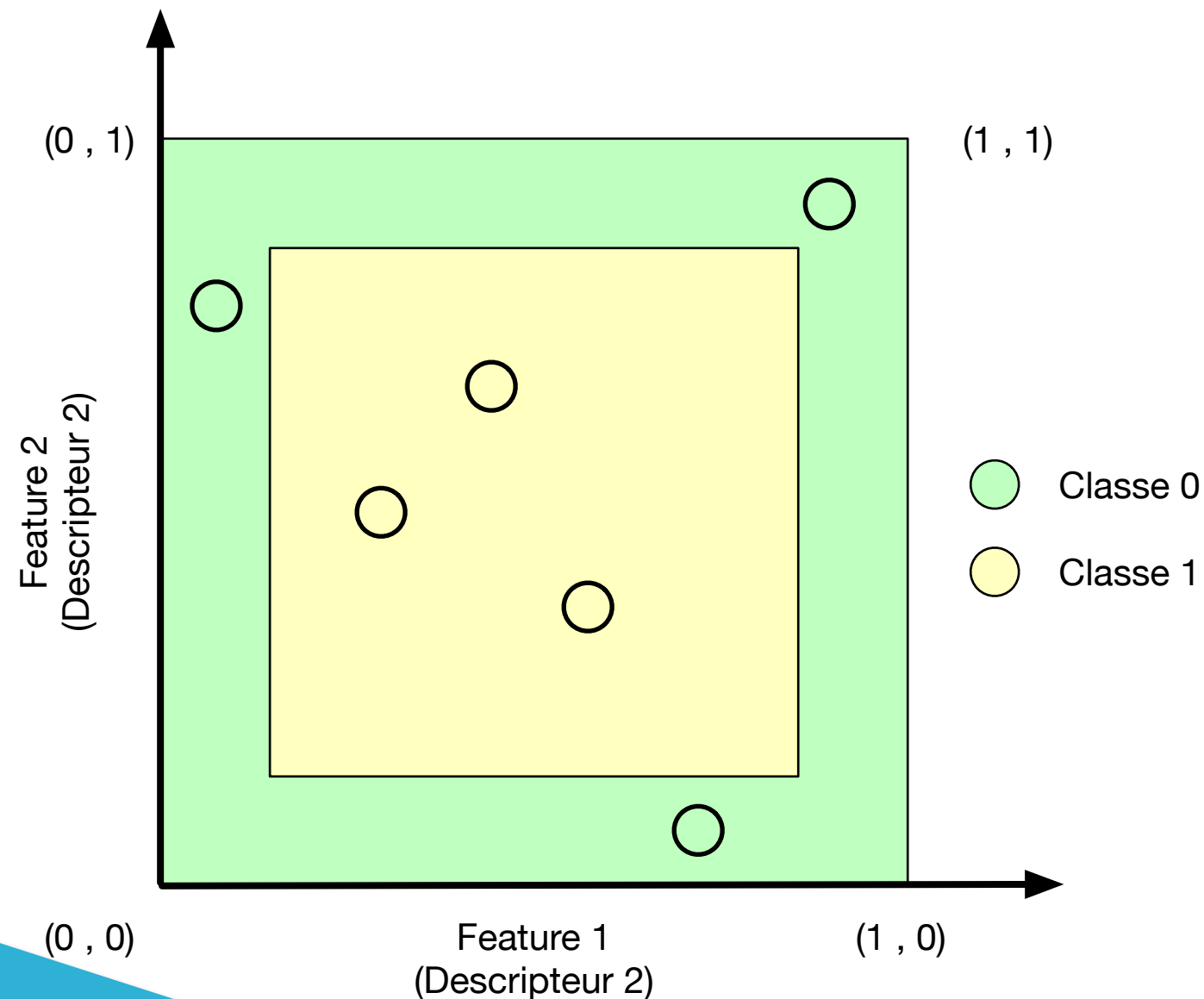
Cas simple d'une classification binaire dans un espace à deux dimensions





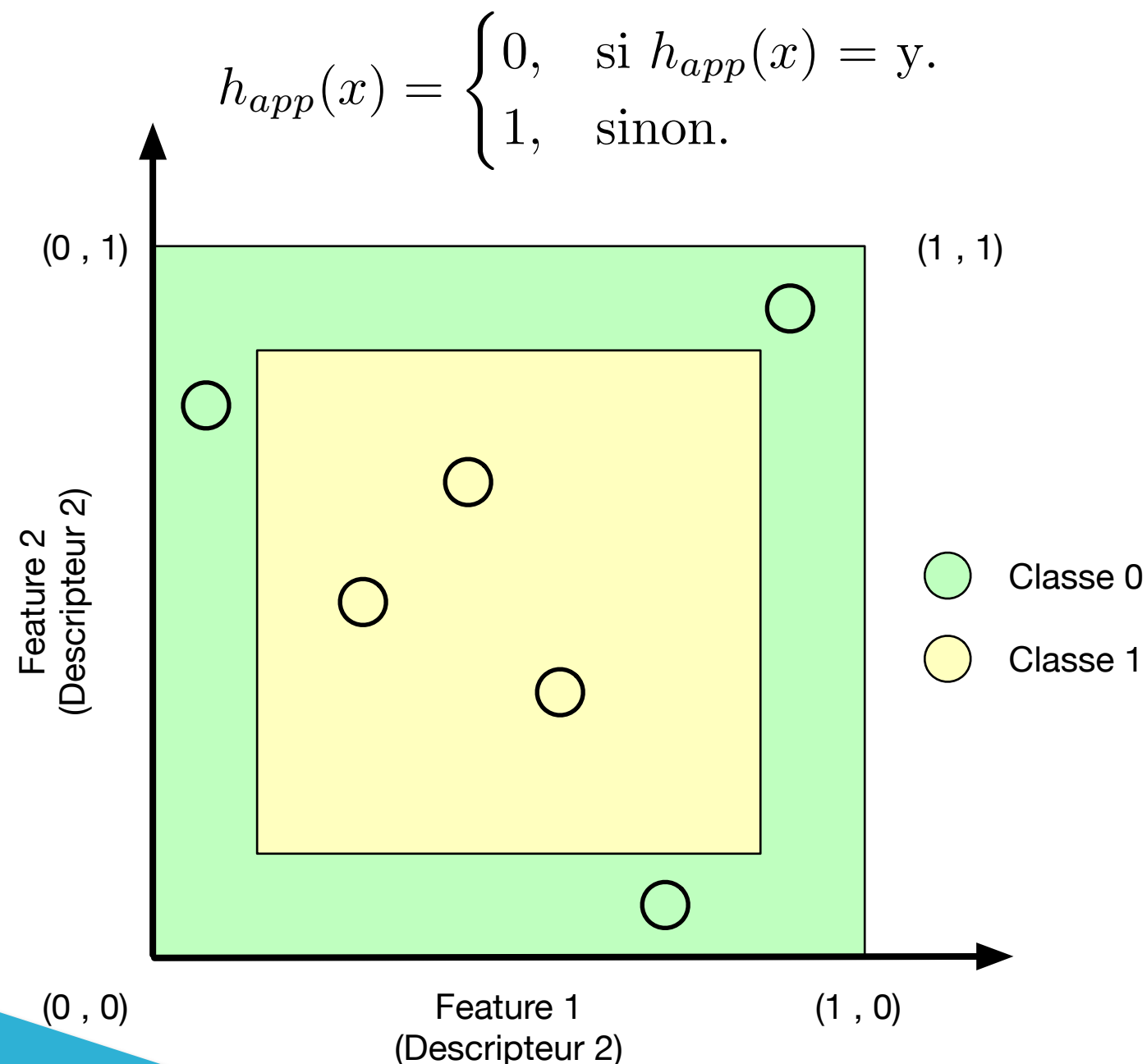
# Illustration

Nos données d'apprentissage



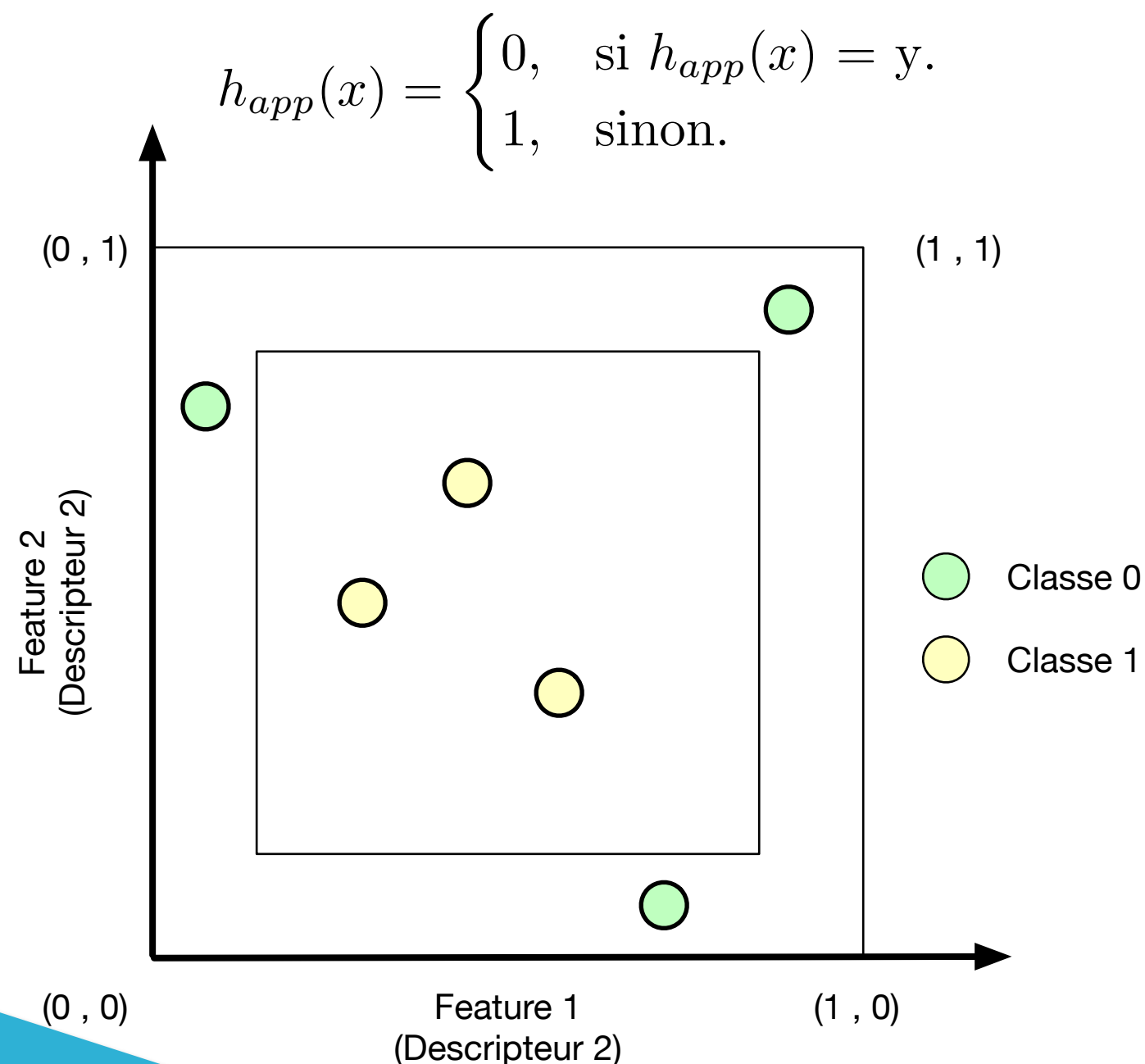
# Illustration

Classifieur idéal: la table de correspondance



# Illustration

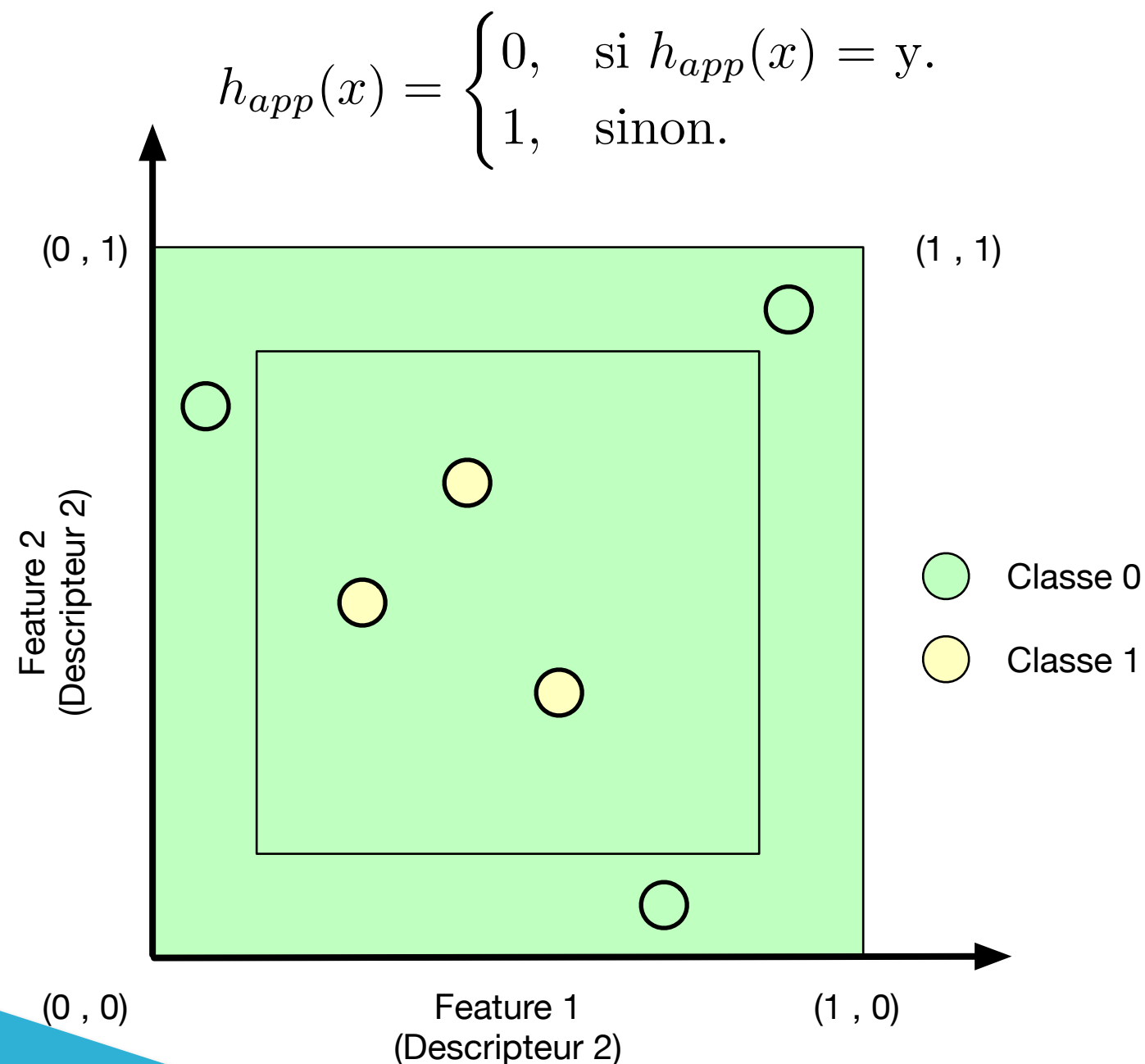
Calcul du risque empirique:  $\mathcal{L}_{\text{empirique}} = 0$



# Illustration

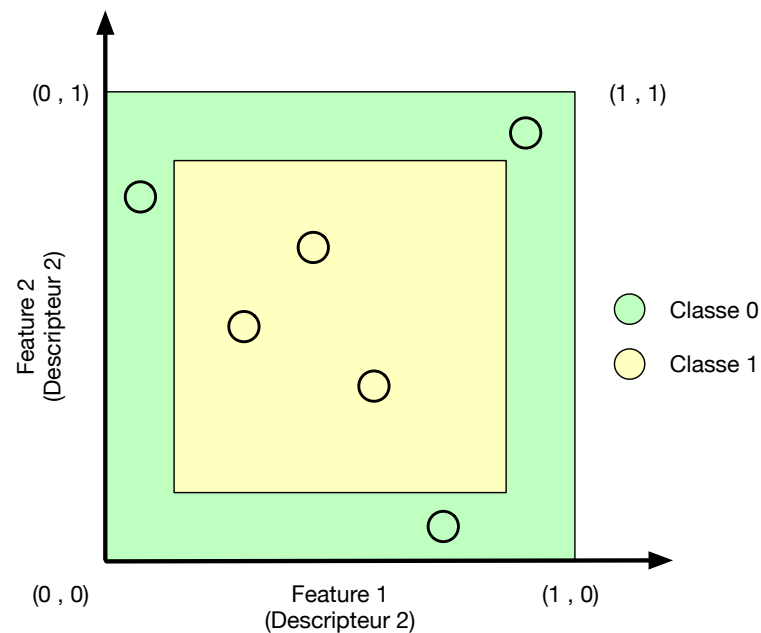
Calcul du risque réel:

$$\mathcal{L}_{reel} \sim 0,5$$



# Illustration

Quel est le problème?



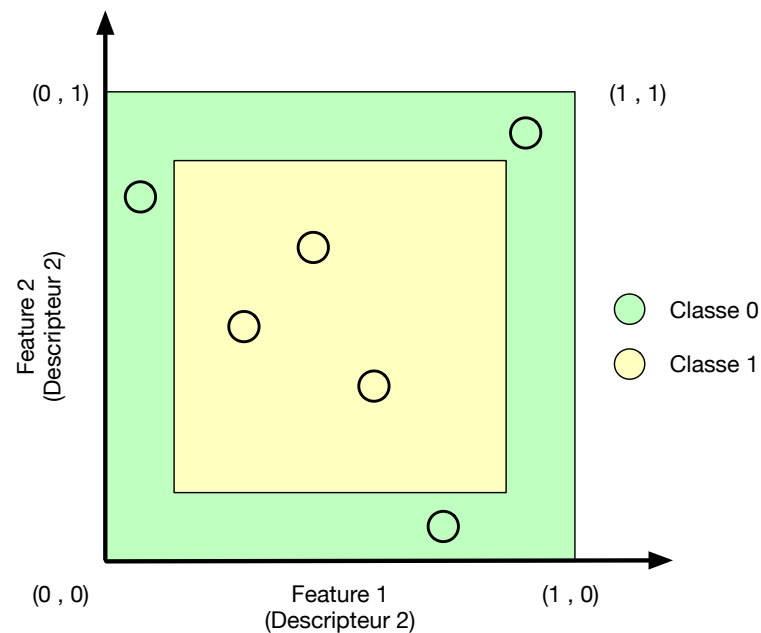
$$h_{app}(x) = \begin{cases} 0, & \text{si } h_{app}(x) = y. \\ 1, & \text{sinon.} \end{cases}$$

$$\mathcal{L}_{reel} \sim 0,5$$

$$\mathcal{L}_{empirique} = 0$$

# Illustration

Quel est le problème?



$$h_{app}(x) = \begin{cases} 0, & \text{si } h_{app}(x) = y. \\ 1, & \text{sinon.} \end{cases}$$

$$\mathcal{L}_{reel} \sim 0,5$$

$$\mathcal{L}_{empirique} = 0$$

## Le sur-apprentissage

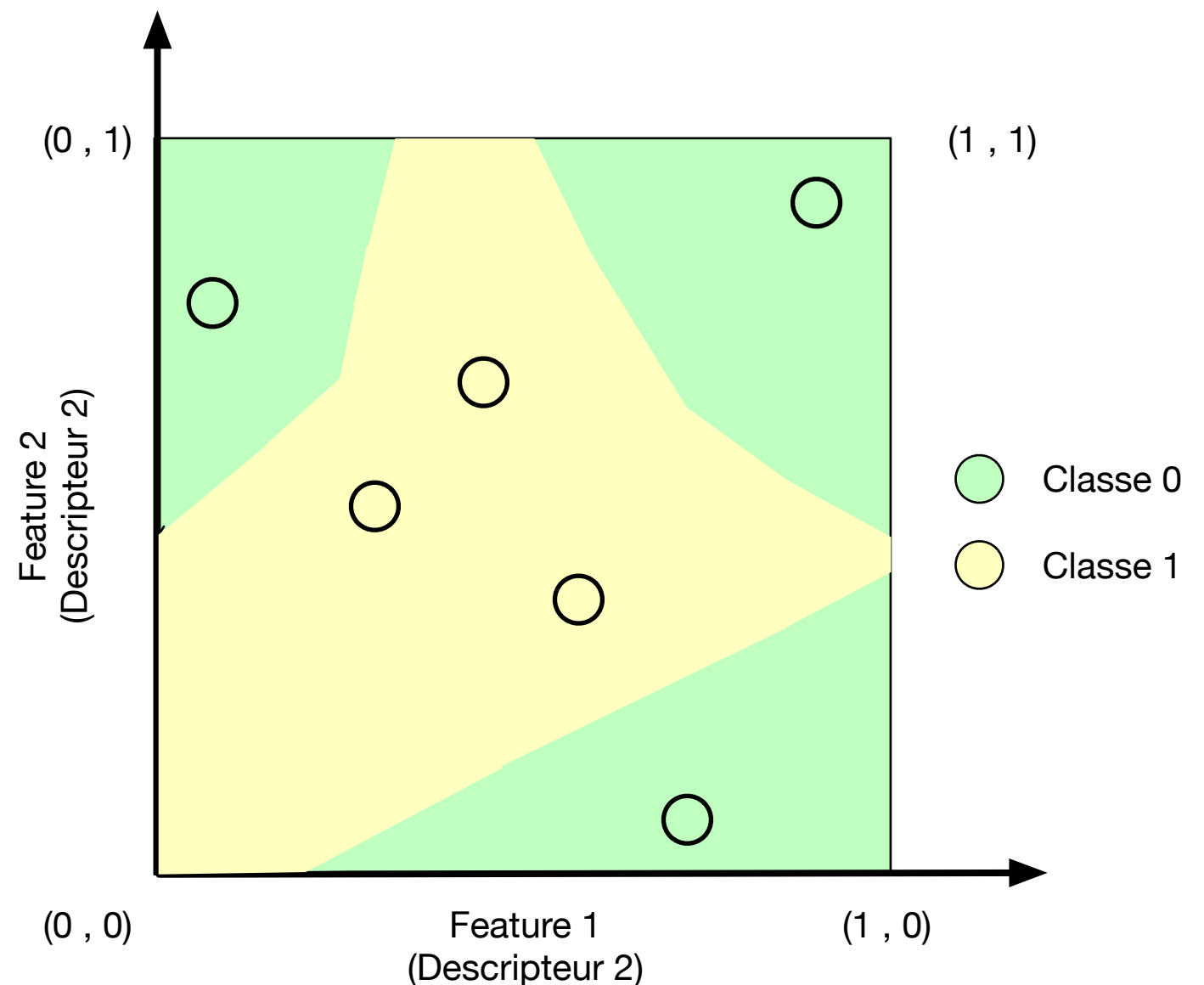
# Comment faire mieux?

Algorithme des plus proches voisins

$$h_{app}(x) = y_i$$

avec

$$i = \operatorname{argmin}_i d(x, x_i)$$



# Comment faire mieux?

Algorithme des plus proches voisins

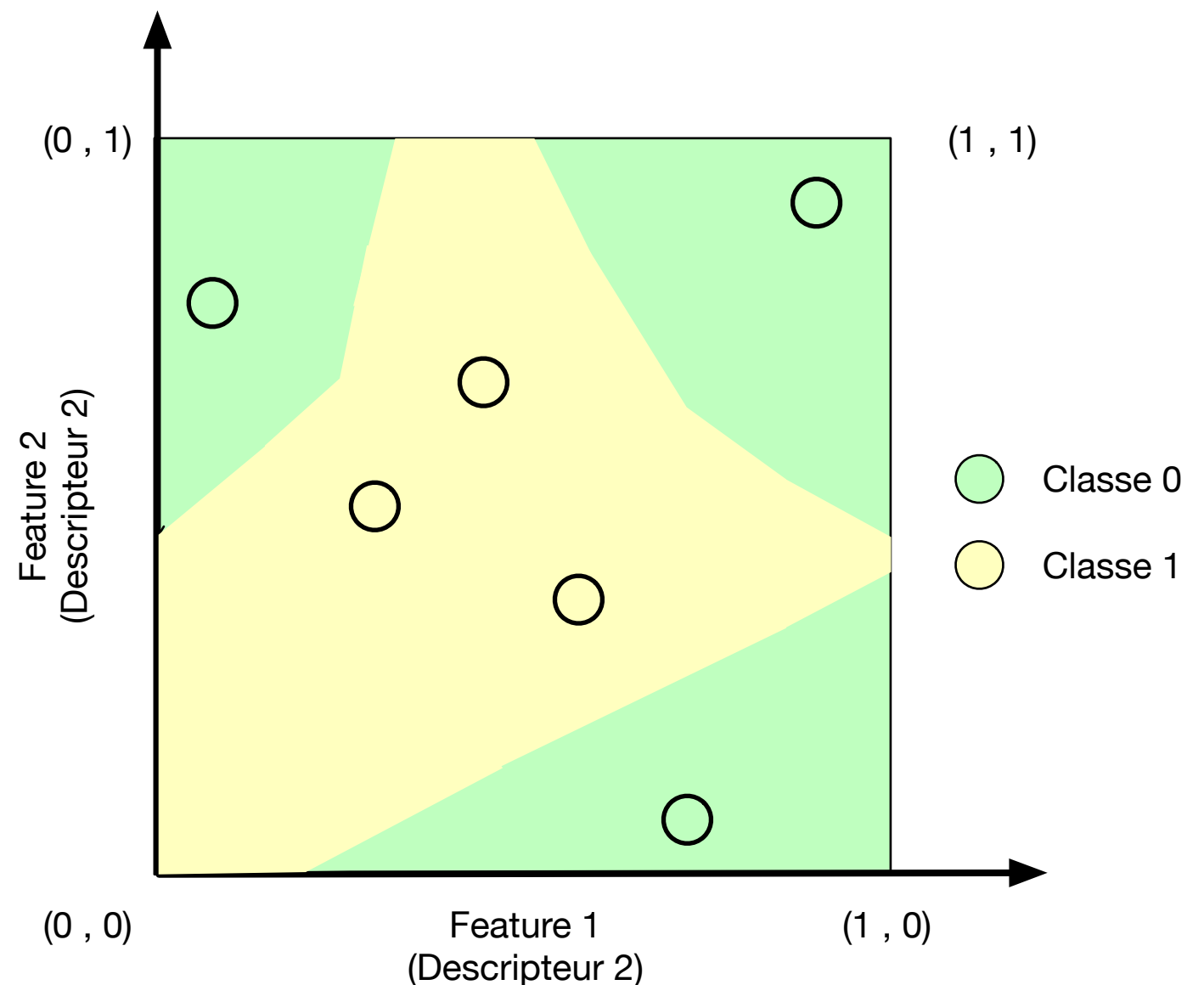
$$h_{app}(x) = y_i$$

avec

$$i = \operatorname{argmin}_i d(x, x_i)$$

$$\mathcal{L}_{empirique} = 0$$

$$\mathcal{L}_{reel} \sim 0,35$$





# Comment faire mieux?

Algorithme des plus proches voisins

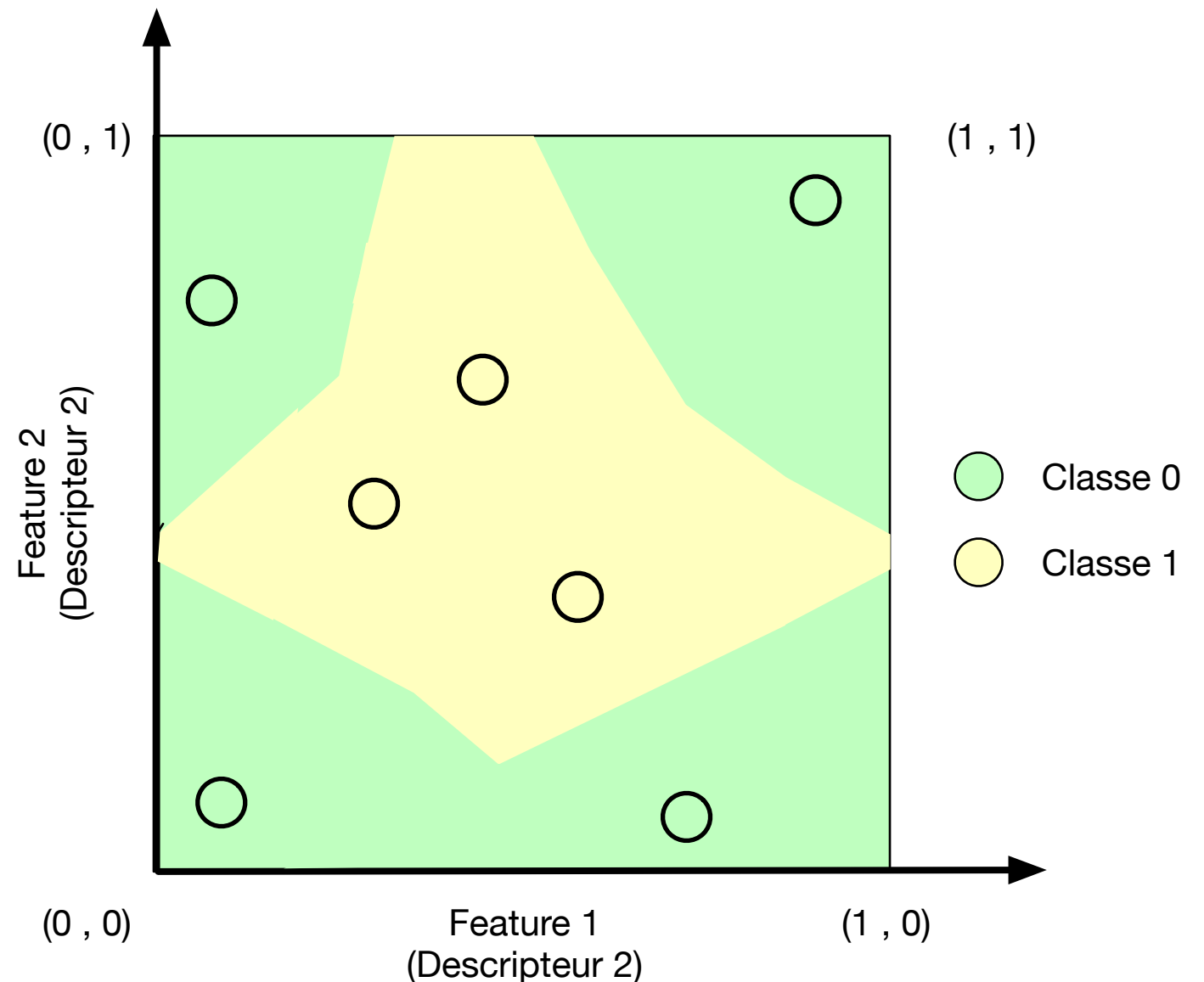
$$h_{app}(x) = y_i$$

avec

$$i = \operatorname{argmin}_i d(x, x_i)$$

$$\mathcal{L}_{empirique} = 0$$

$$\mathcal{L}_{reel} \sim 0,25$$

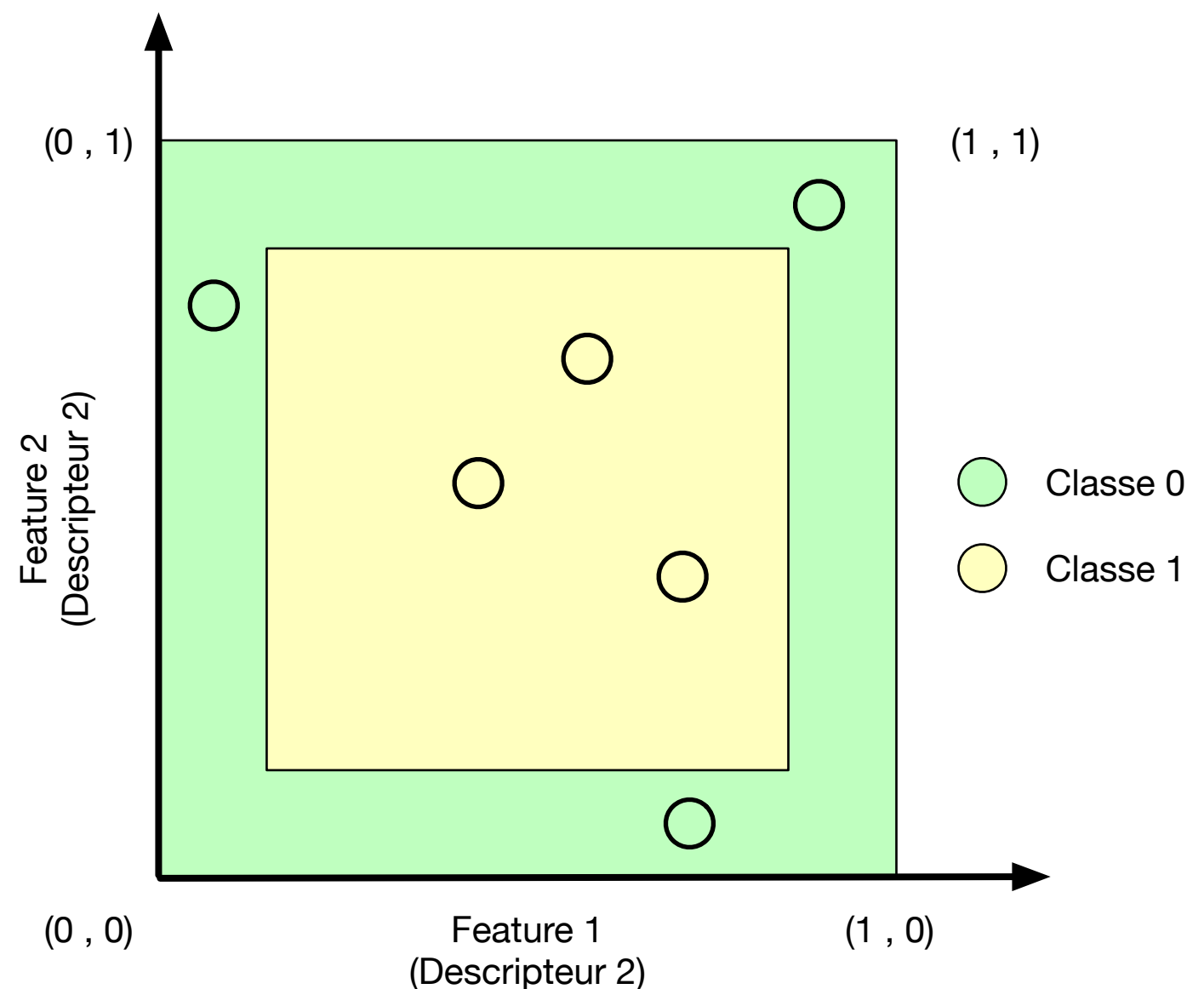


## Algorithme des plus proches voisins

Le risque réel est très dépendant des données

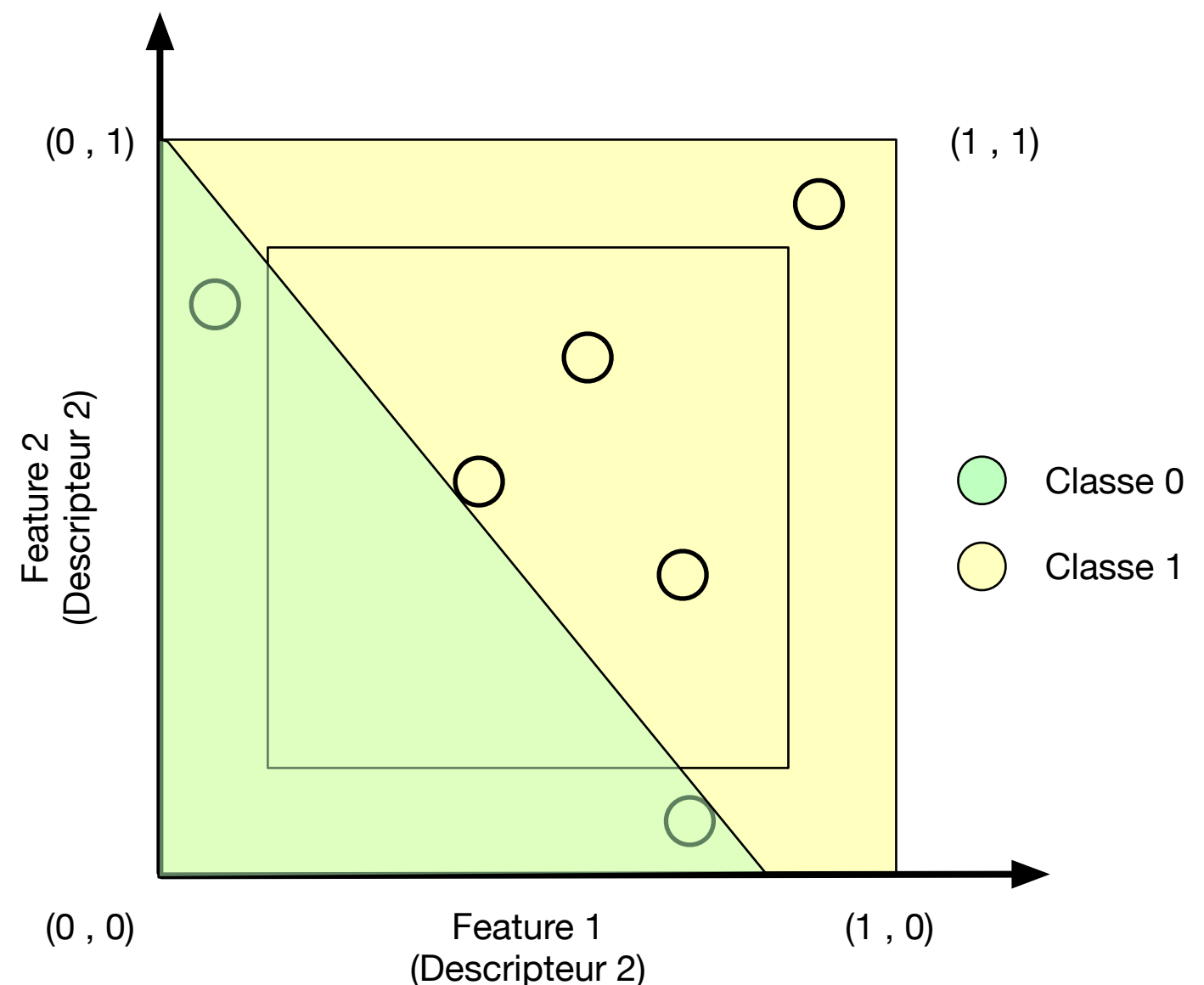
# Exemple d'un classifieur linéaire

$$h_{w,b} = \text{sign}(\langle w, x \rangle + b)$$



# Exemple d'un classifieur linéaire

$$h_{w,b} = \text{sign}(\langle w, x \rangle + b)$$

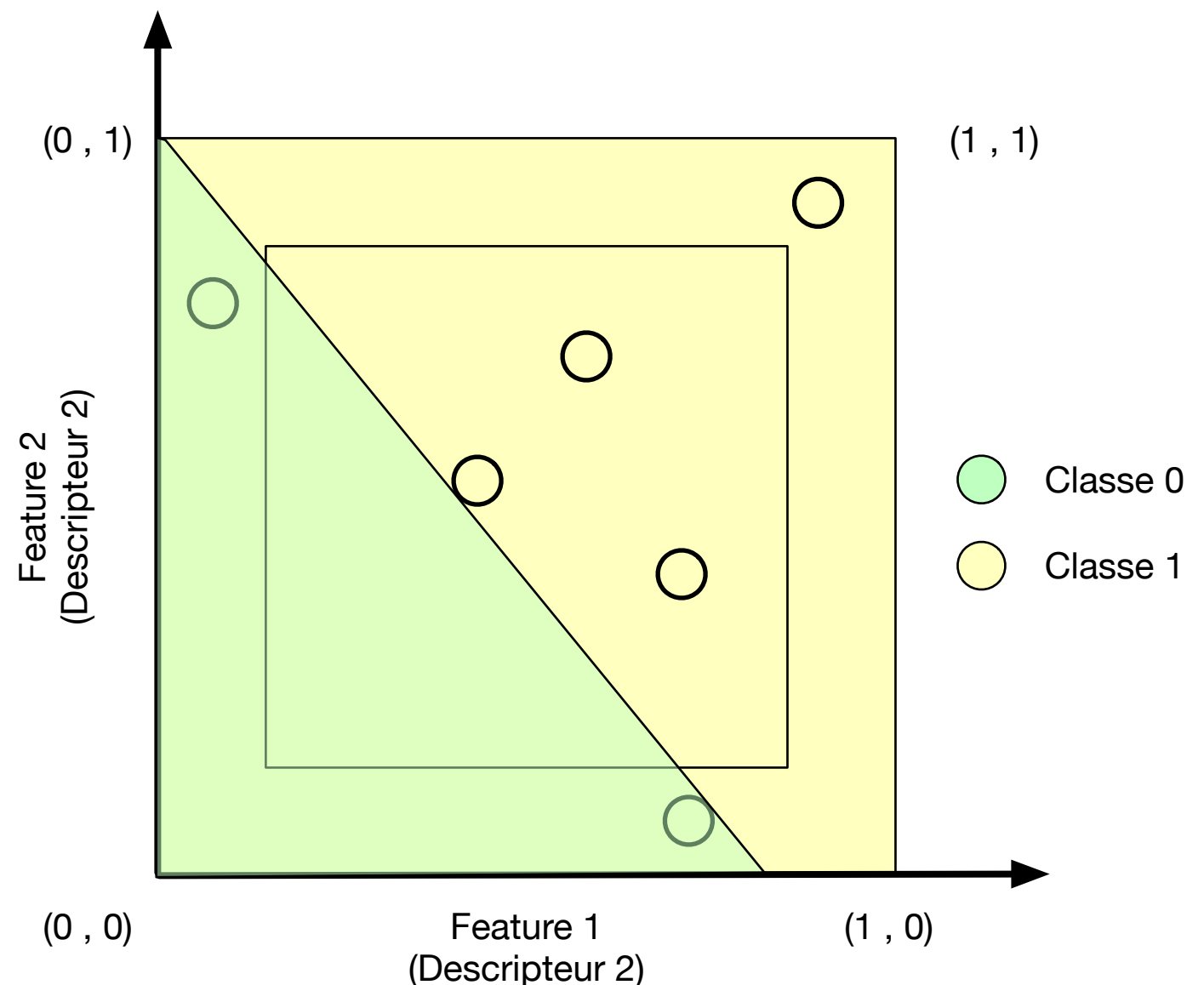


# Exemple d'un classifieur linéaire

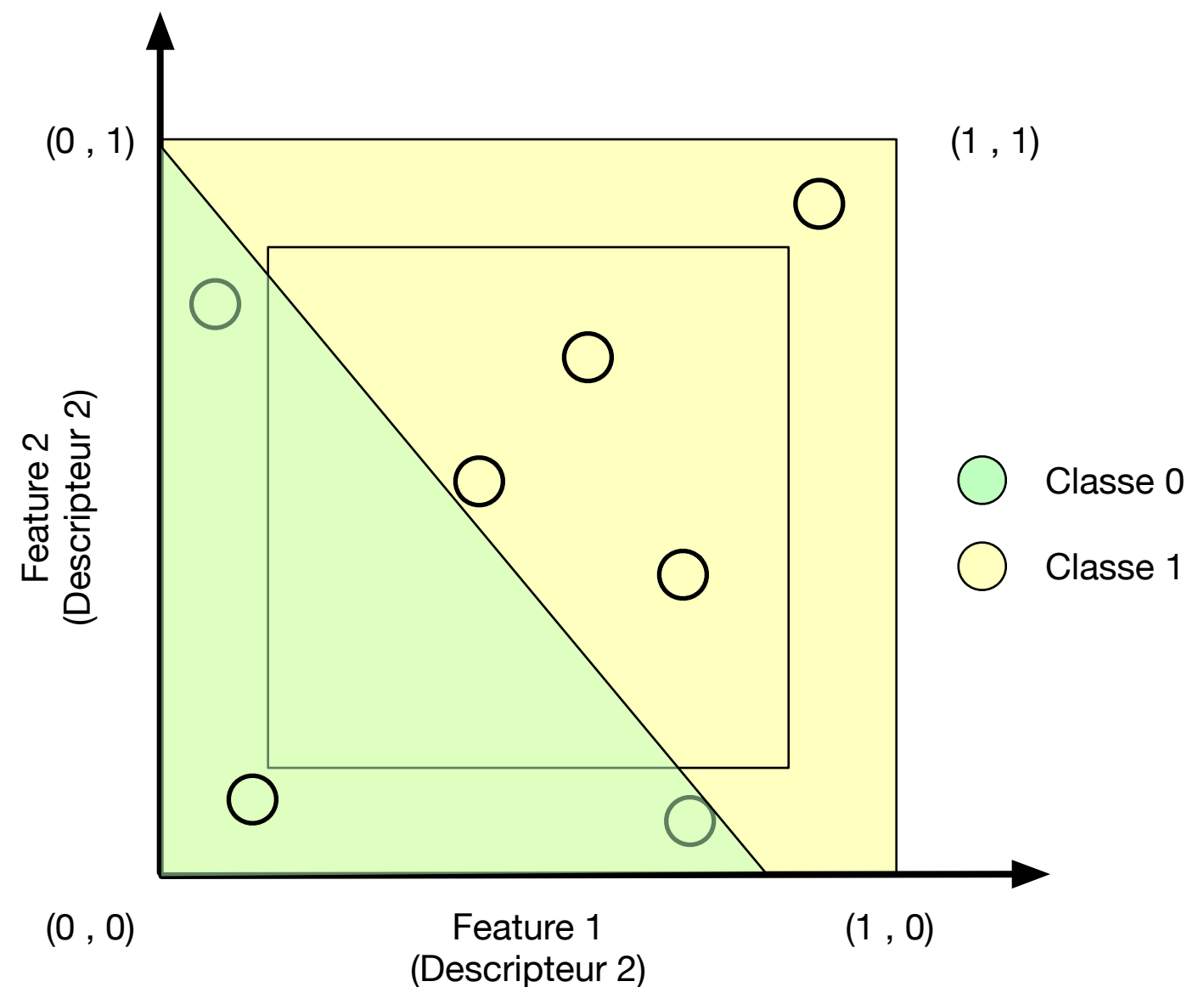
$$h_{w,b} = \text{sign}(\langle w, x \rangle + b)$$

$$\mathcal{L}_{\text{empirique}} \sim 0,66$$

$$\mathcal{L}_{\text{reel}} \sim 0,15$$



# Exemple d'un classifieur linéaire



# Analyse de ces 2 classifieurs

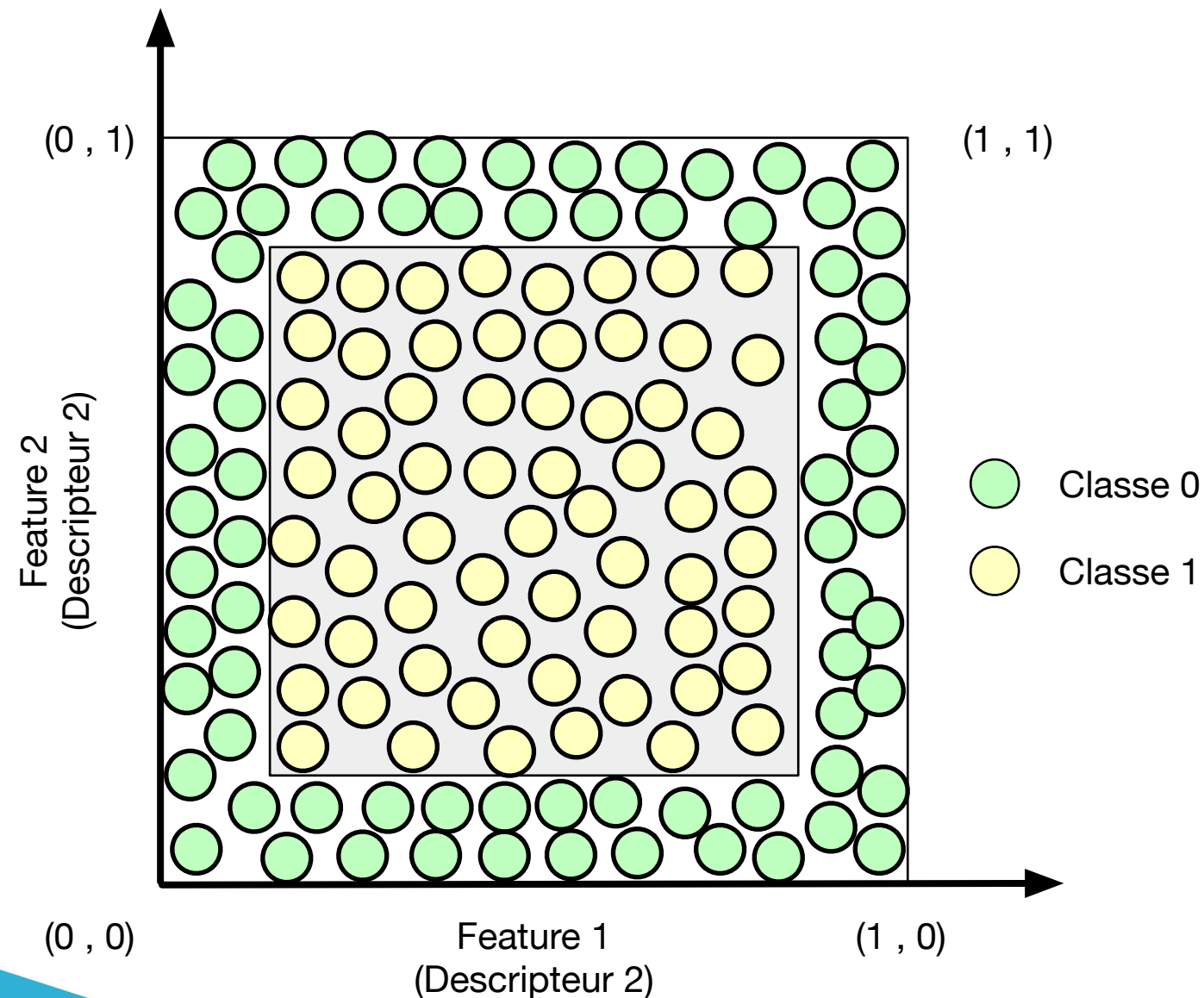
## L'algorithme des plus proches voisins

- Conserve en mémoire tous les exemples vus
- Les frontières sont complexes et très sensibles aux nouveaux exemples

## Classifieur linéaire

- Modèle paramétrique
- Frontières plus simples et robustes aux nouvelles données

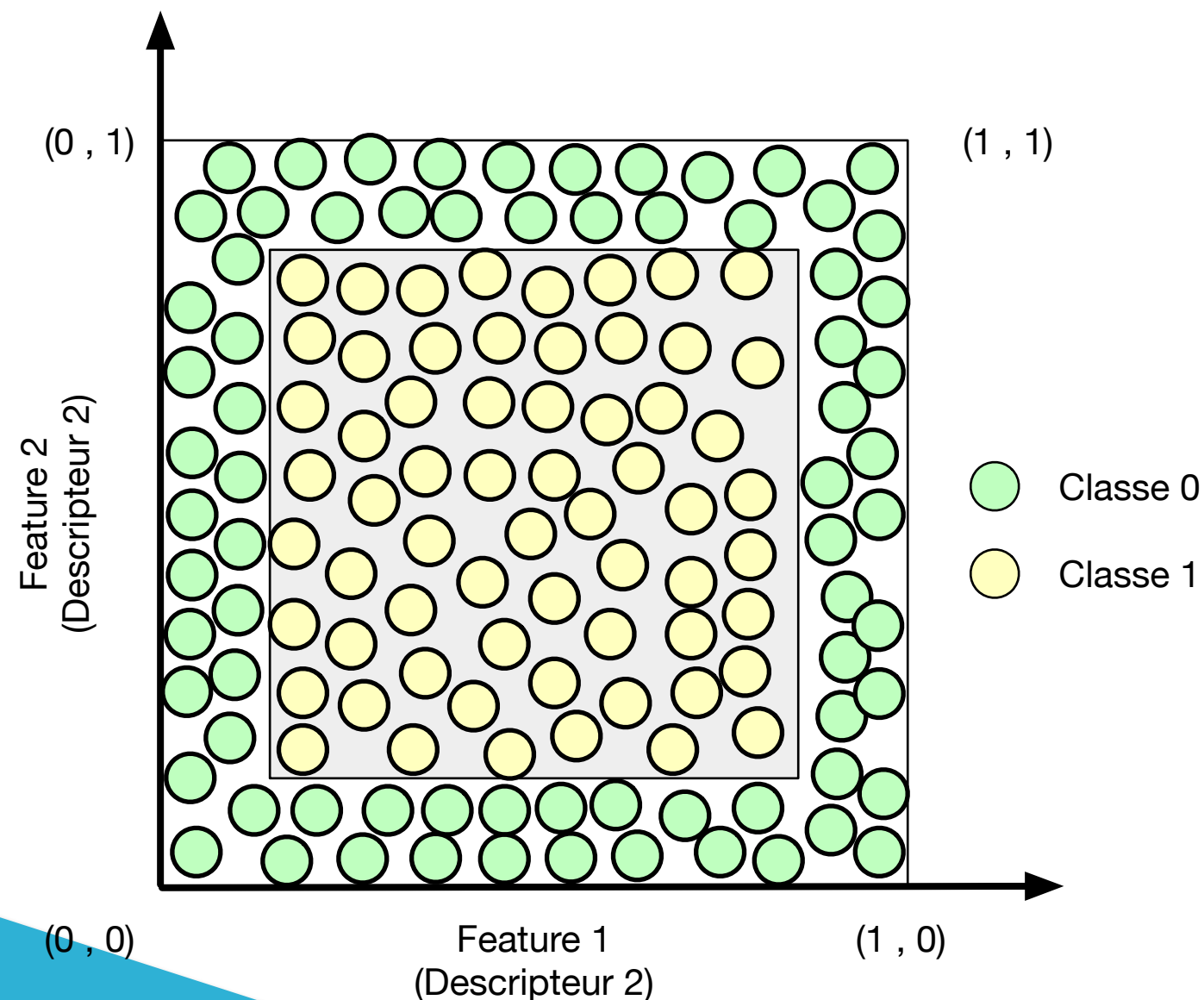
# Et si on avait plus de données?





# Et si on avait plus de données?

Avec les plus proches voisins, si on augmente le nombre d'exemples le risque empirique tend vers le risque réel



# Et si on avait plus de données?

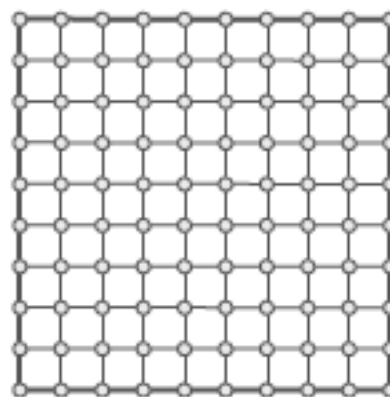
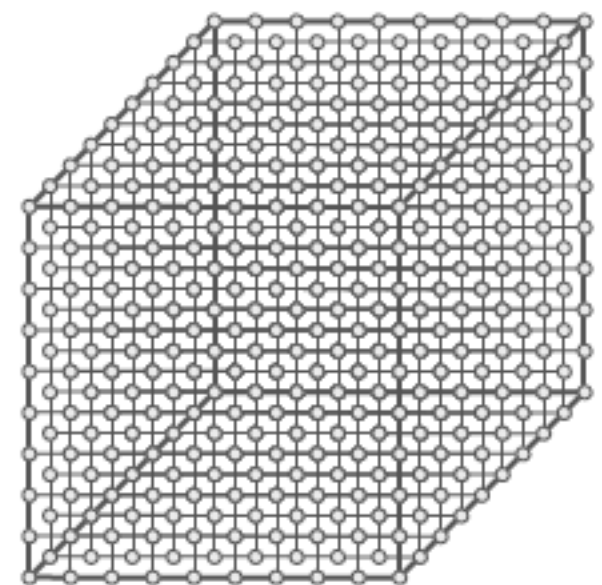
OUI, mais en pratique ce n'est pas réaliste...

Si on veut couvrir l'espace avec une grille régulière et un pas régulier de 0.1 , combien faut il d'exemples?

# Et si on avait plus de données?

Lorsque la dimension de l'espace augmente, la quantité de données nécessaire augmente trop vite.

 $d = 1$ 

 $m = 10$ 
 $d = 2$ 

 $m = 100$ 
 $d = 3$ 

 $m = 1000$

# Et si on avait plus de données?

Lorsque la dimension de l'espace augmente, la quantité de données nécessaire augmente trop vite.

$d = 1$

$d = 2$

$d = 3$

**La quantité de donnée augmente de façon exponentielle**

$m = 10$

$m = 100$

$m = 1000$

# Exemple de dimensionnalité

# Tâche simple de reconnaissance de chiffre

# Base de données MNIST

Images  $28 \times 28 = 784$  dimensions



# Exemple de dimensionnalité

# Tâche simple de reconnaissance de chiffre

# Base de données MNIST

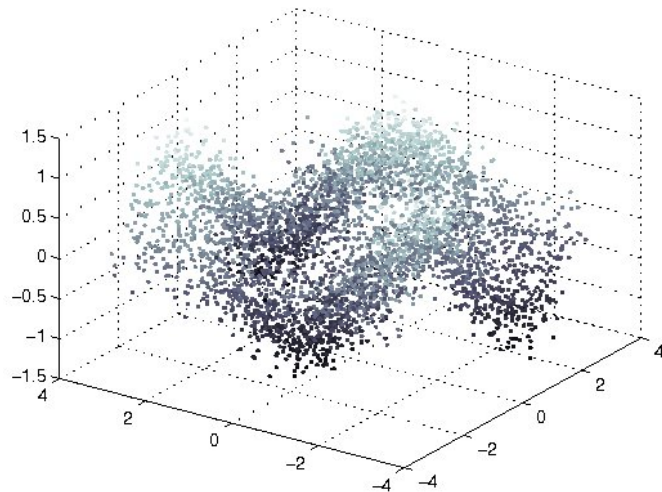
Images  $28 \times 28 = 784$  dimensions

**Si on « pave » l'espace avec un pas régulier, la probabilité d'obtenir une image de chiffre est  $\sim 0$**

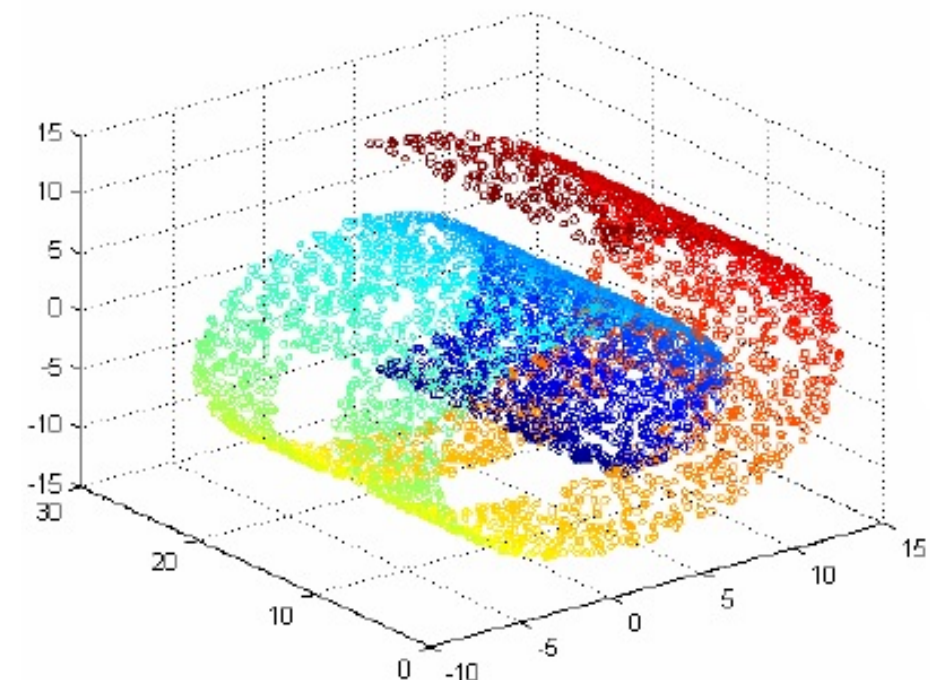
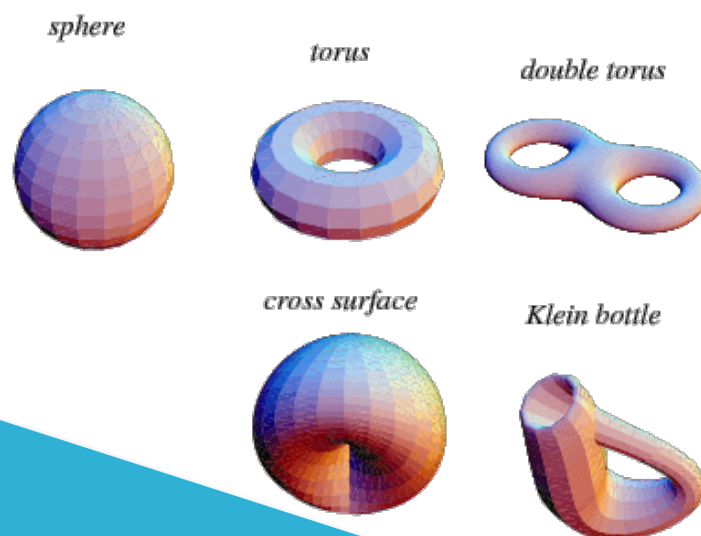




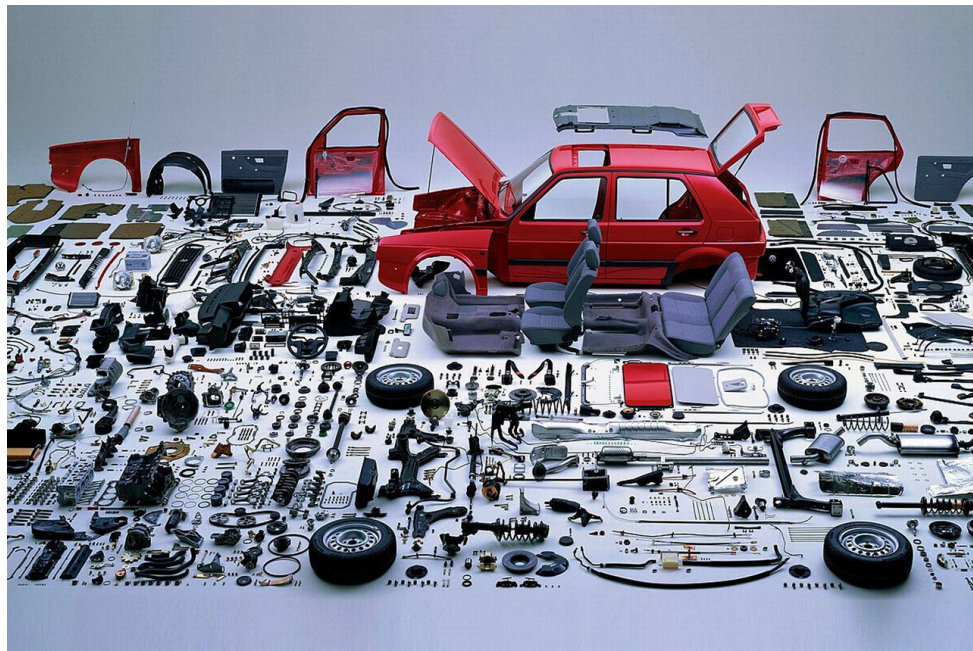
# Notion de Manifold



Hypothèse qu'en très grande dimension, les données sont en fait situées dans un « sous-espace » (manifold) dans lequel le degré de liberté est limité



# Notion de Manifold



Une voiture: 30 000 pièces

Un photo de voiture: 1280 x 653 pixels  
 $1280 * 653 * 3 \text{ valeurs} = 2\,507\,520 \text{ valeurs}$



# Apprentissage profond

# Retour sur les réseaux de neurones

## Le perceptron multi-couches

# Apprentissage profond supervisé

1. Définir la tâche
2. Trouver les données d'apprentissage
3. Définir la métrique à minimiser
4. Définir l'architecture du modèle
5. Définir l'algorithme d'apprentissage

# Apprentissage profond supervisé

Définir la tâche:

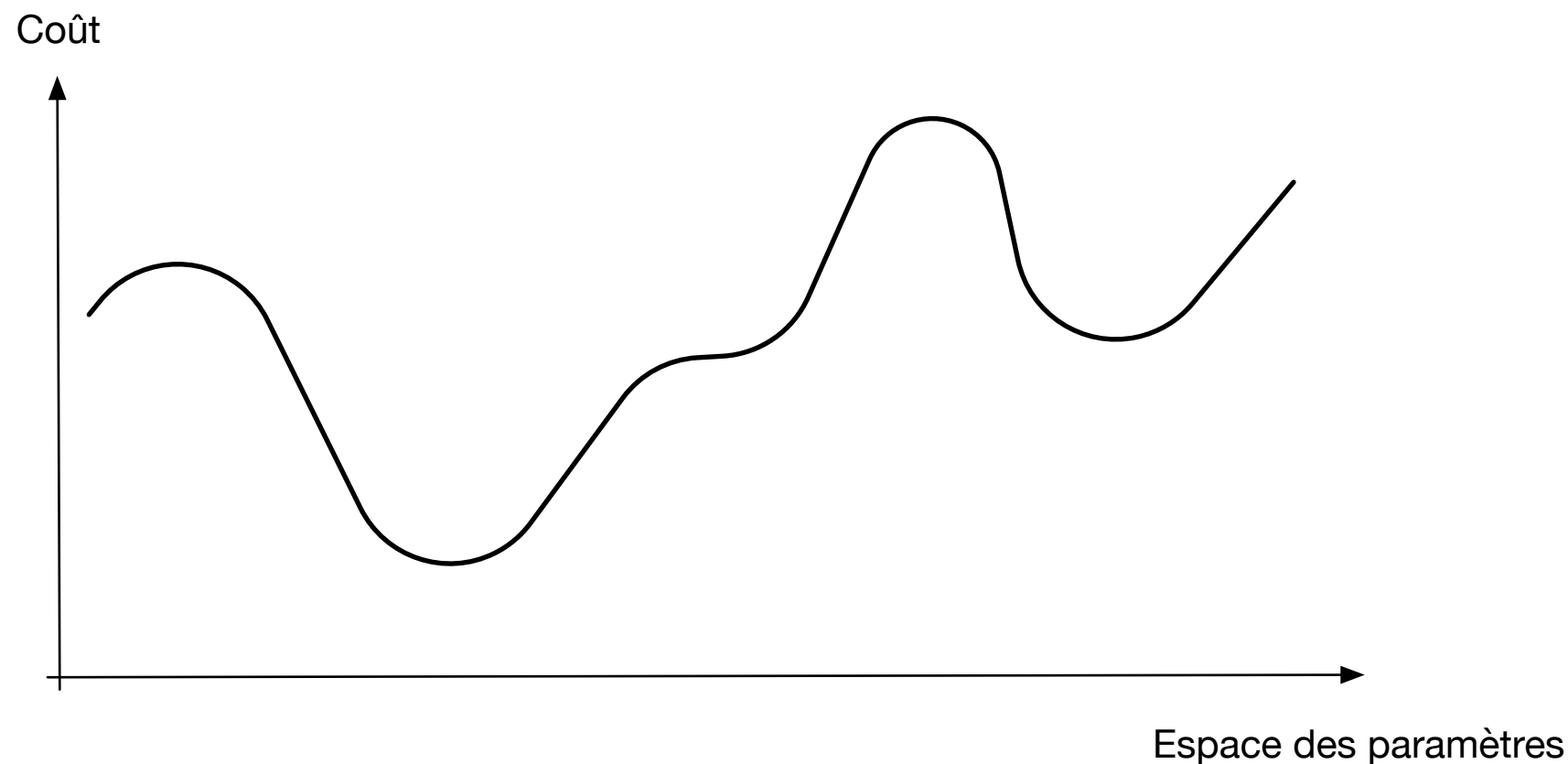
- régression
- classification...
- une combinaison des deux?

# Définir une métrique

- Exemple de la cross-entropie pour la reconnaissance du locuteur
- Intérêt de la fonction de coût angulaire et des marges

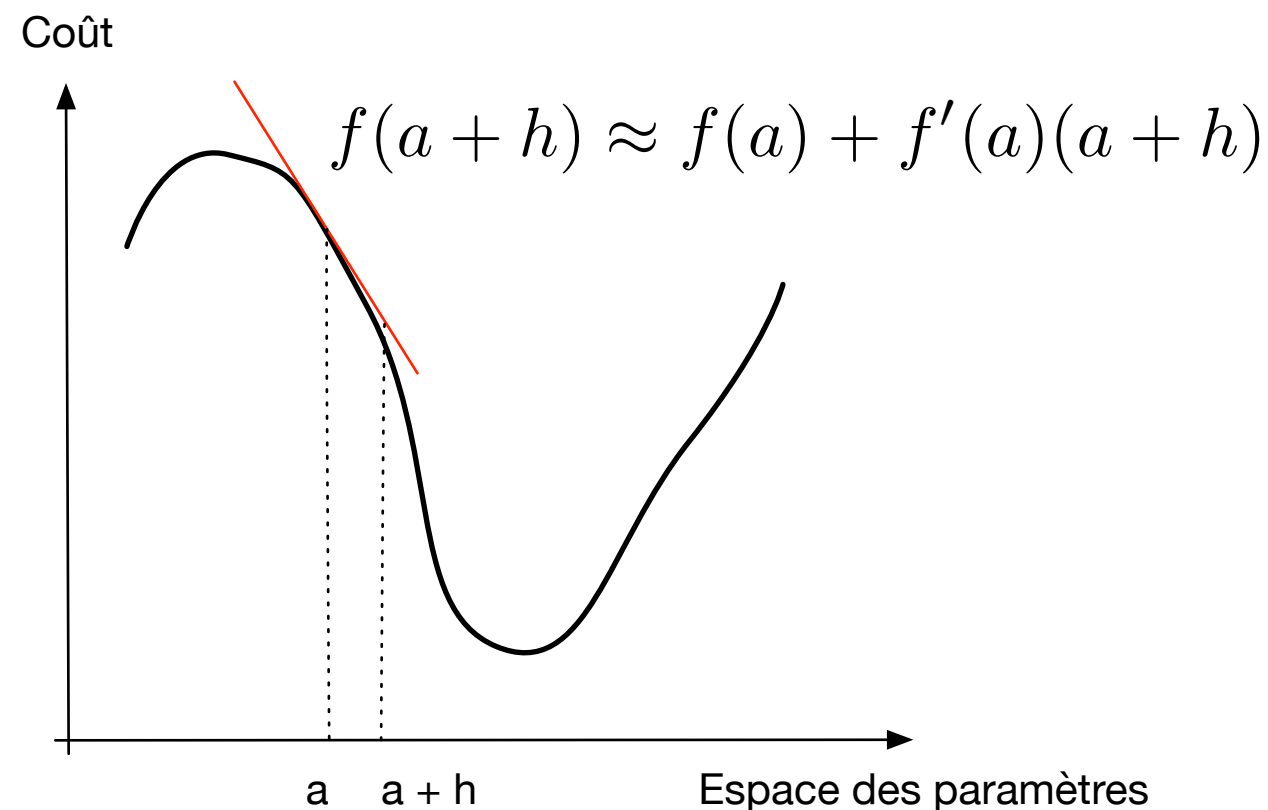
# Objectif: minimiser le risque empirique

Soit un modèle paramétrique  
(classifieur linéaire, réseau profond...)



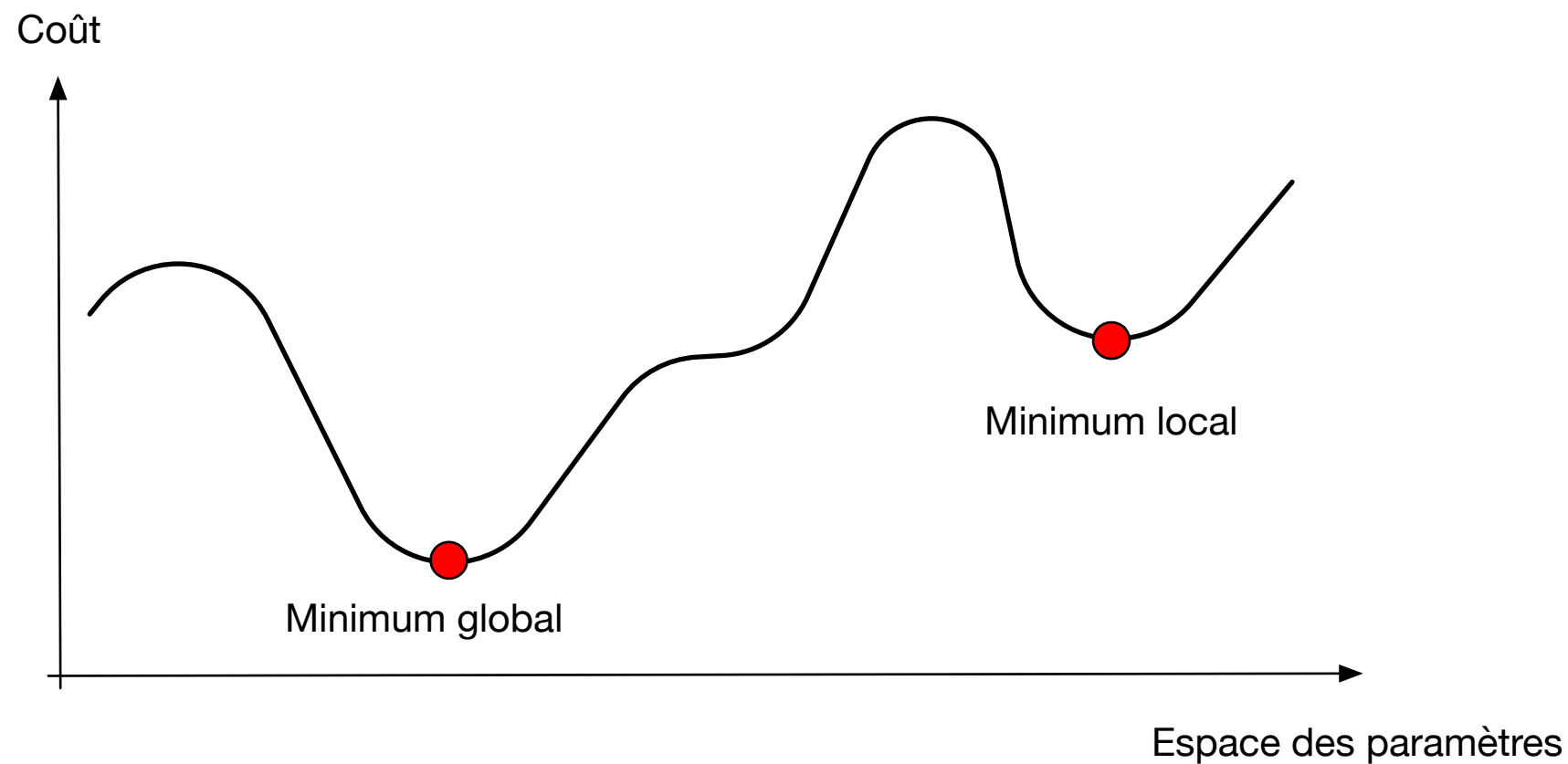
Le risque empirique dépend de la valeur des paramètres du modèle

# Objectif: minimiser le risque empirique



Utilisation d'une approximation linéaire.

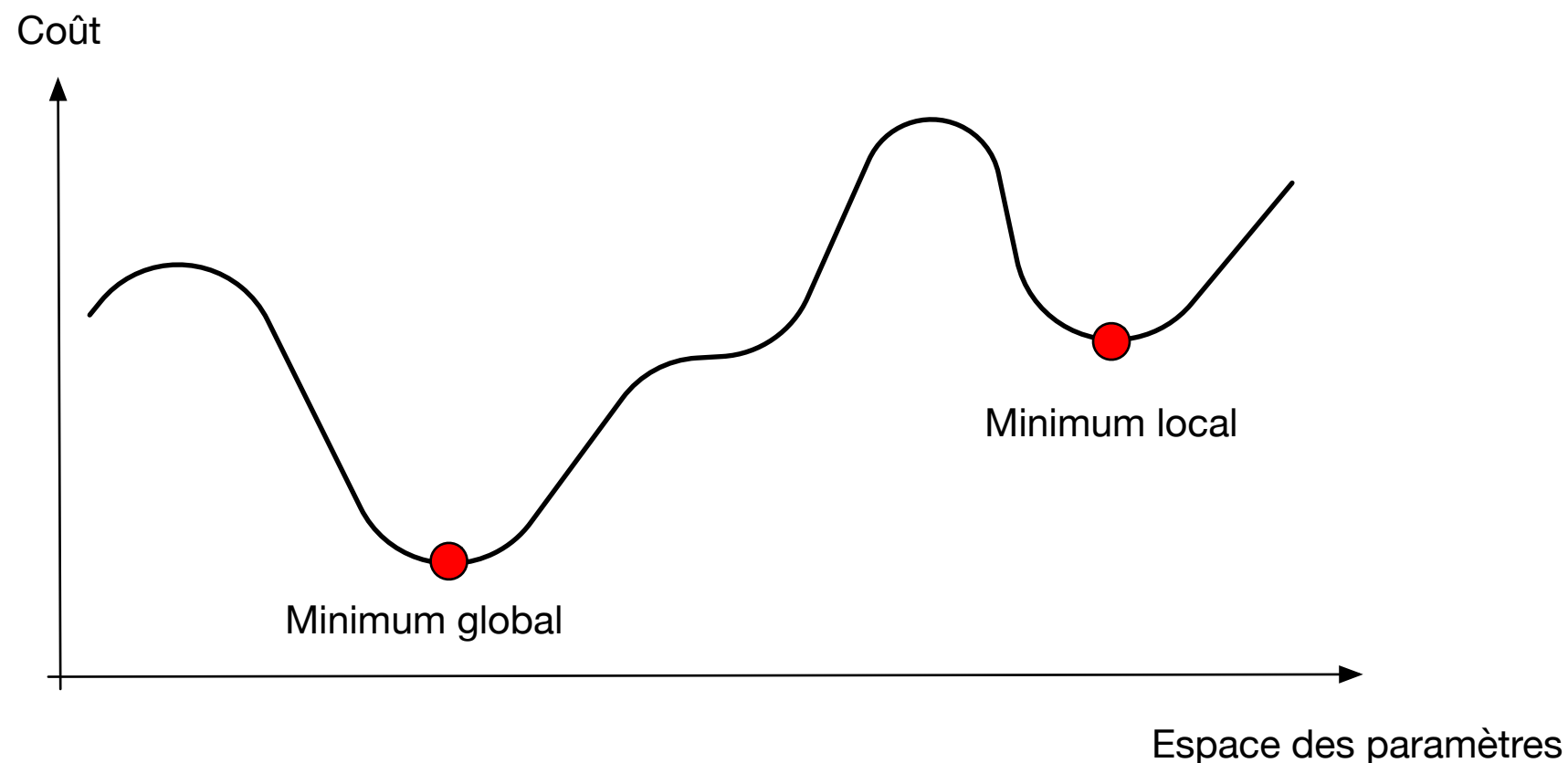
# Objectif: minimiser le risque empirique



Tout minimum n'est pas bon

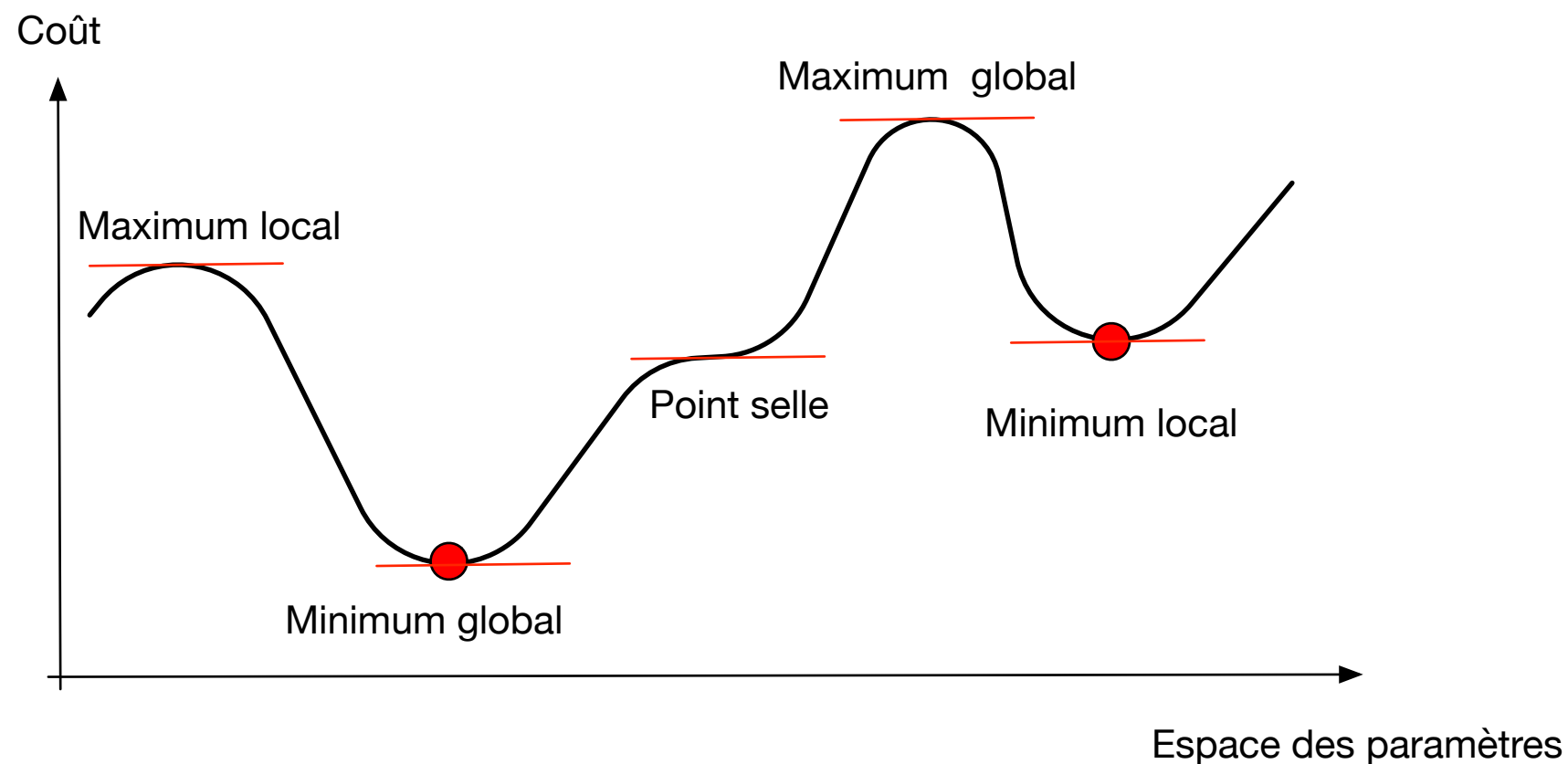


# Objectif: minimiser le risque empirique



Comment chercher les extrema ?

# Objectif: minimiser le risque empirique

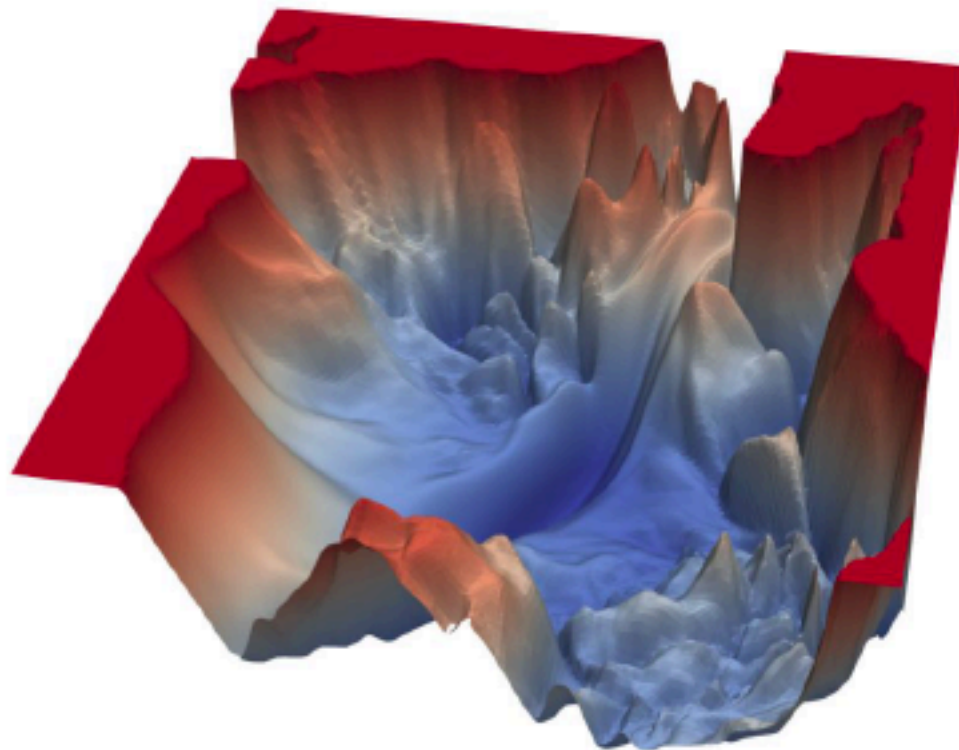


Toute valeur qui annule la dérivée n'est pas satisfaisante

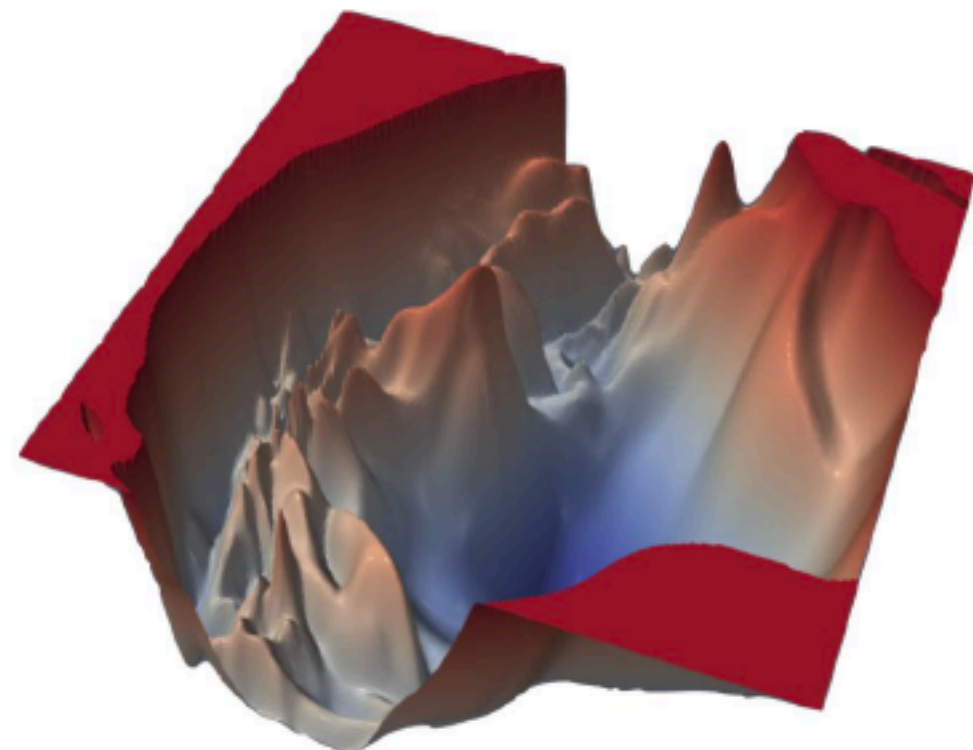
# Objectif: minimiser le risque empirique

Dans la réalité...

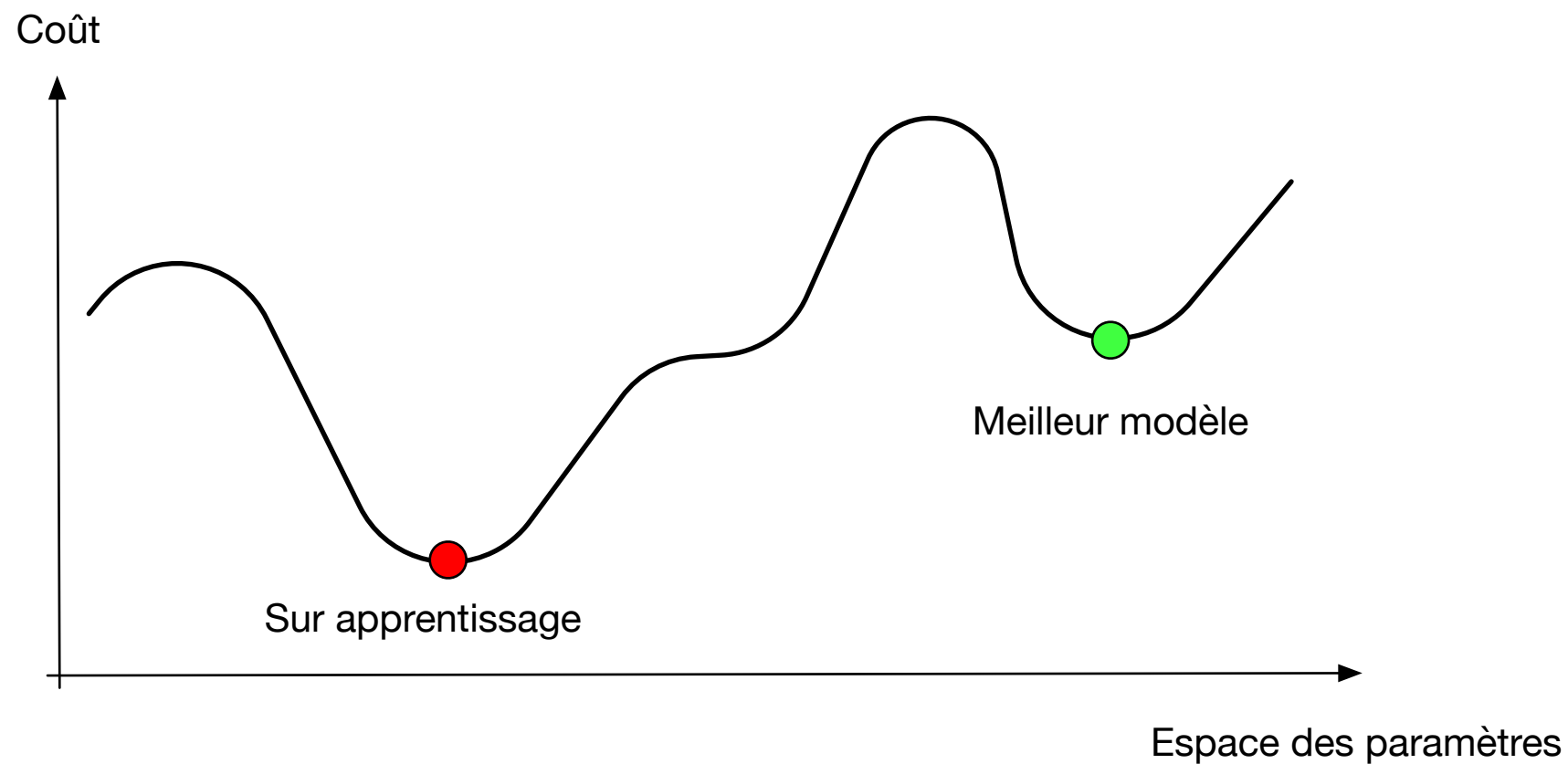
VGG-56



VGG-110



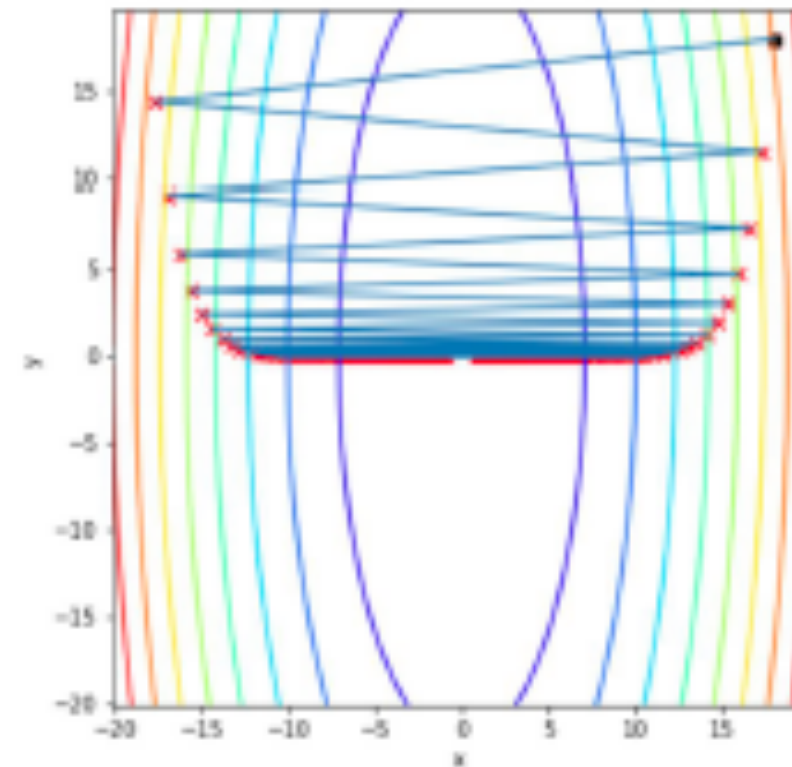
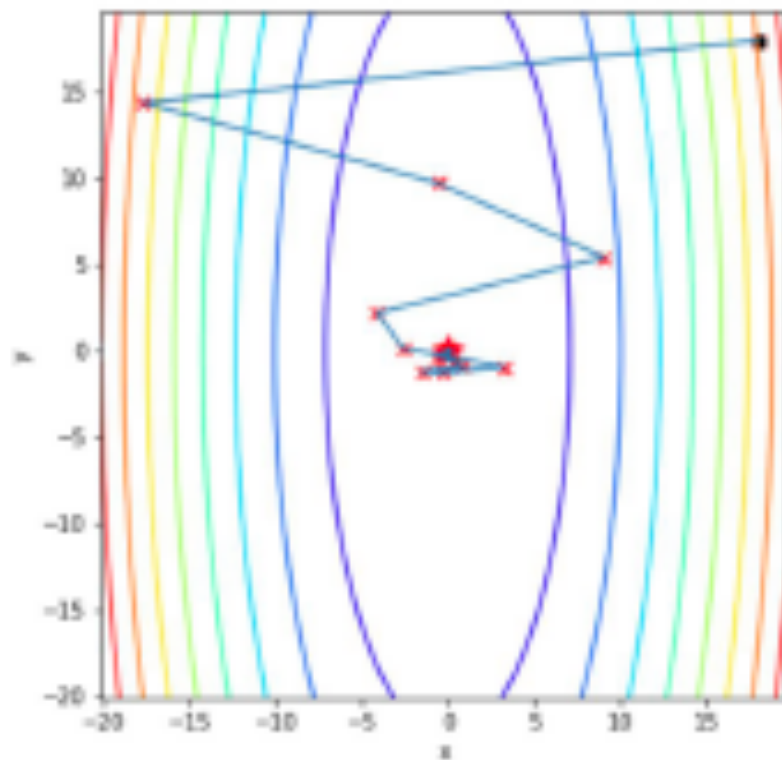
# Remarque 1



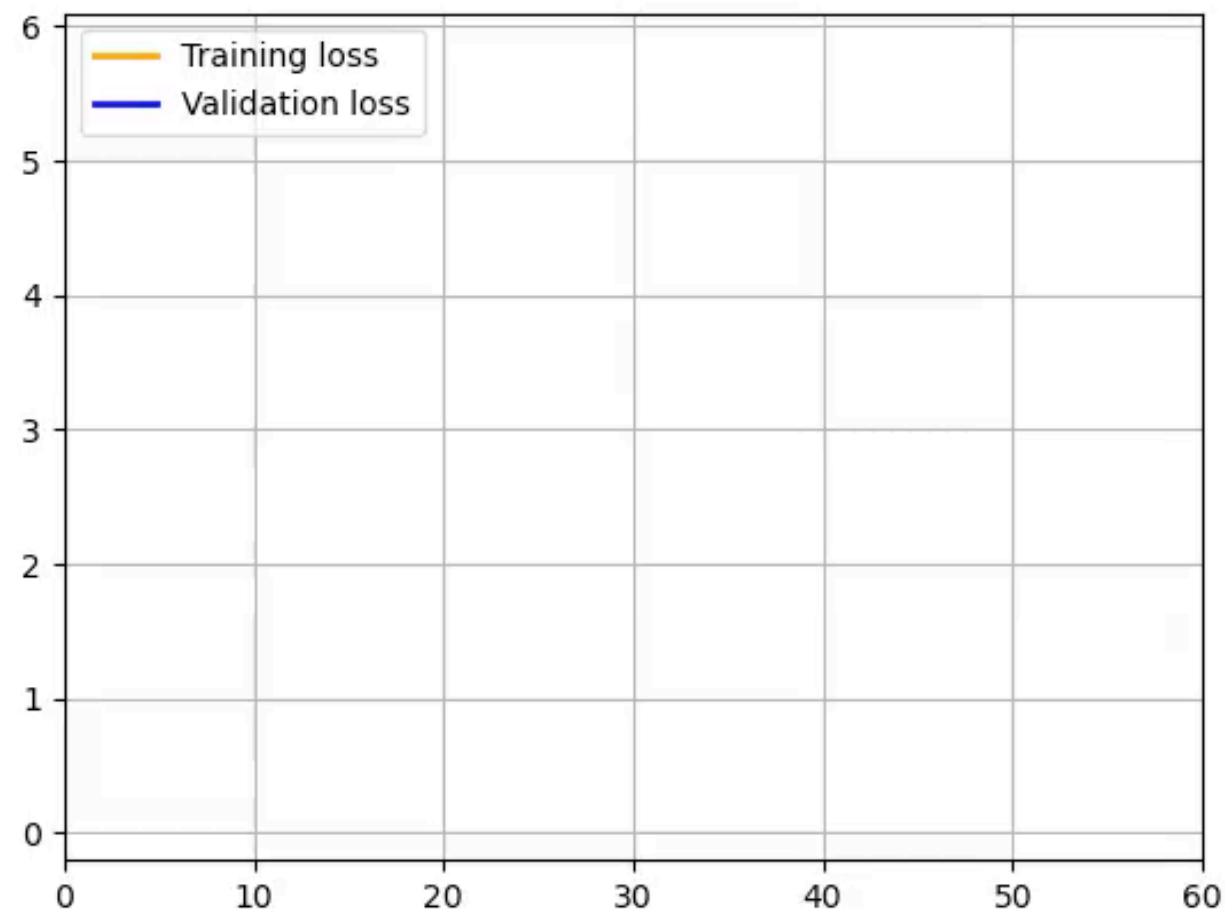
Il y a une différence entre apprentissage et optimisation

# Remarque 2

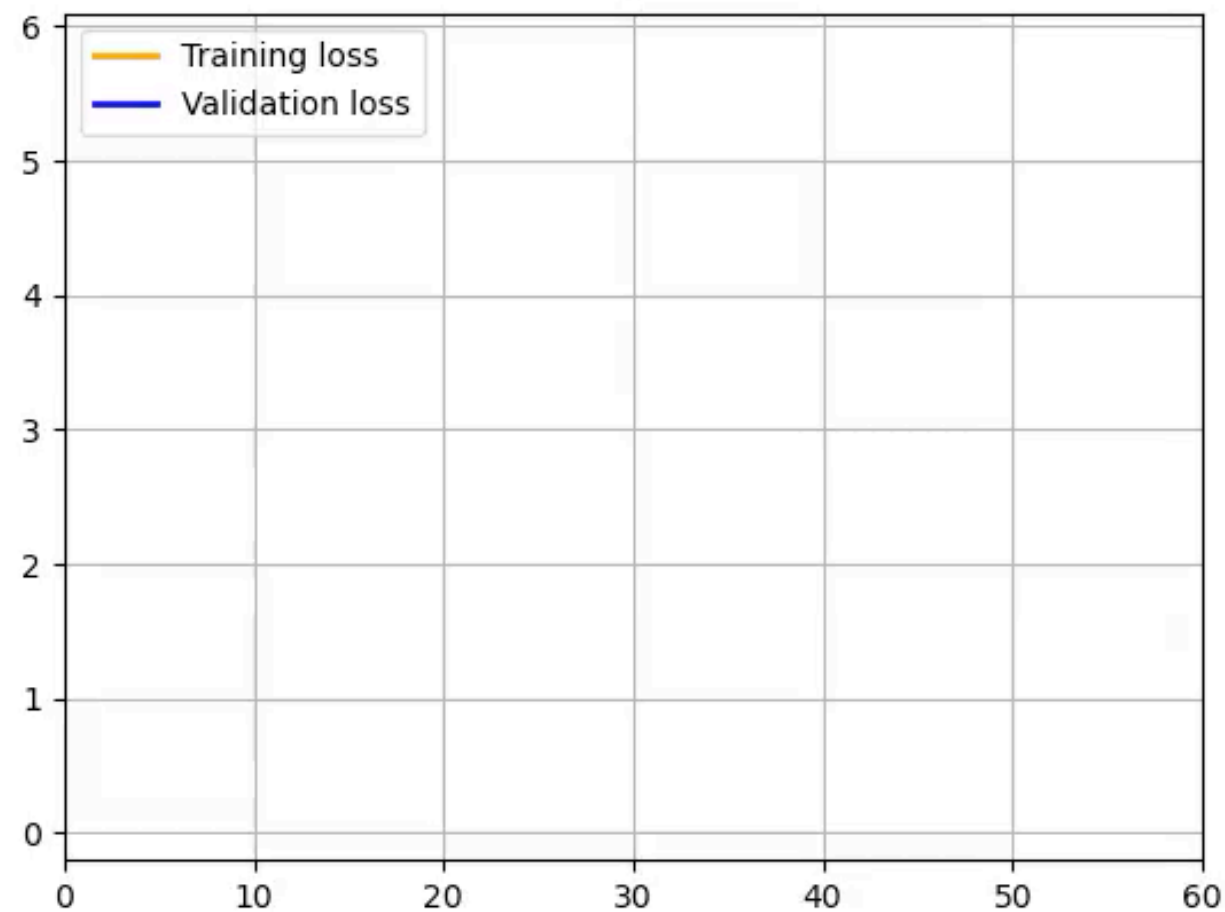
Trouver l'approximation linéaire n'est pas suffisant, il faut savoir de quel « pas » progresser dans le sens de la « pente ».



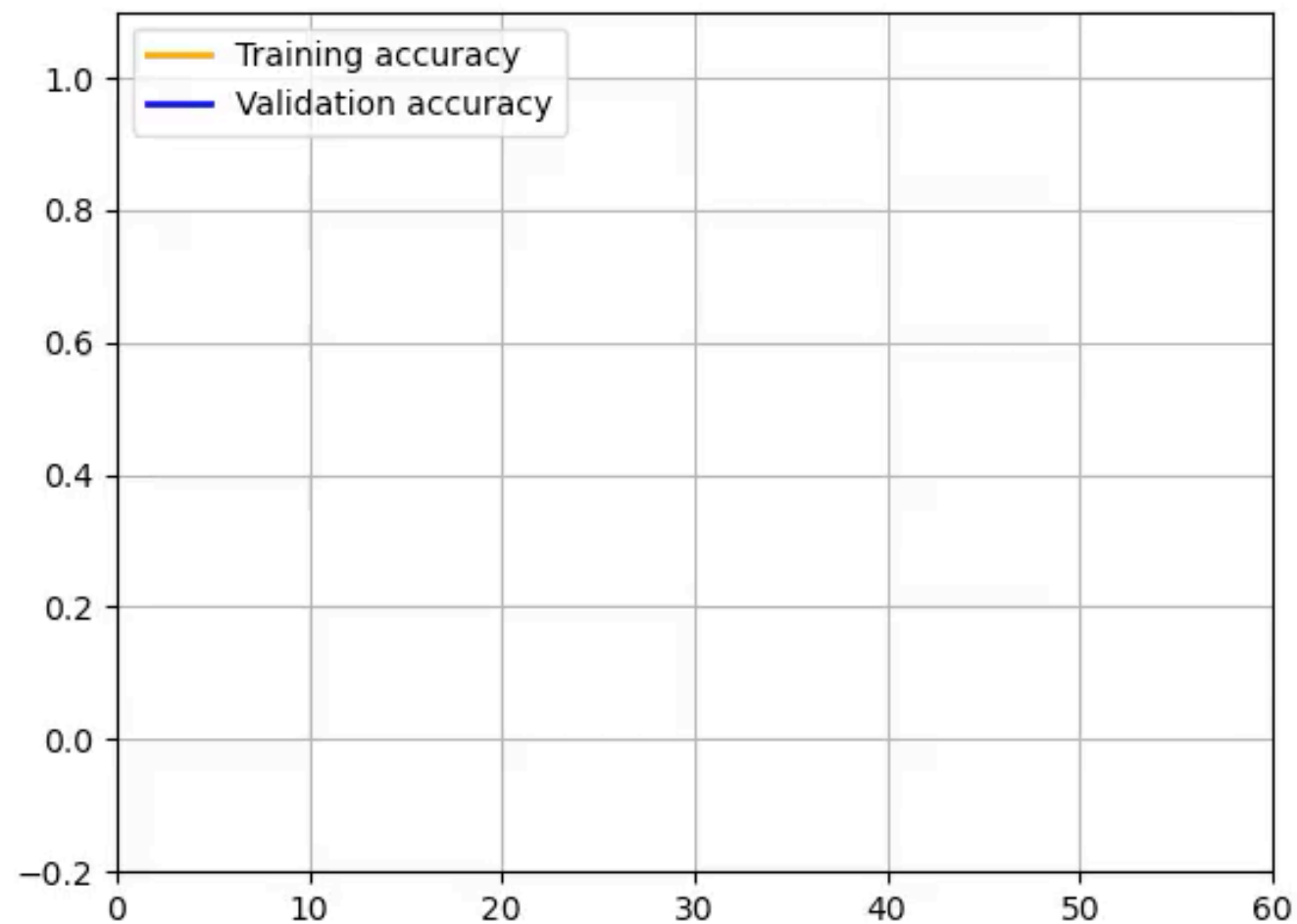
- Apprentissage avec 1% des données disponibles
- Évolution du coût



- Apprentissage avec 1% des données disponibles
- Évolution du coût

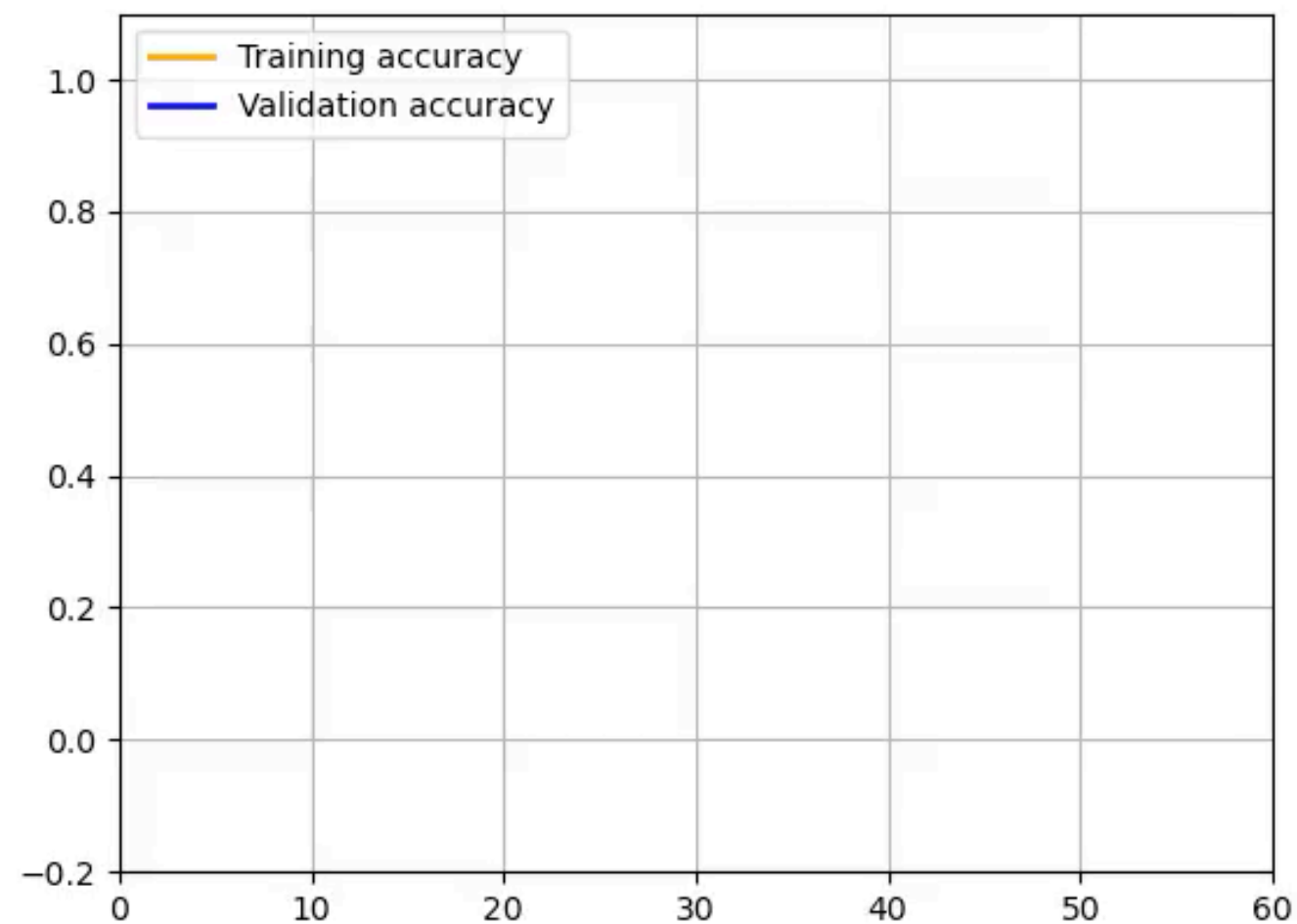


- Apprentissage avec 1% des données

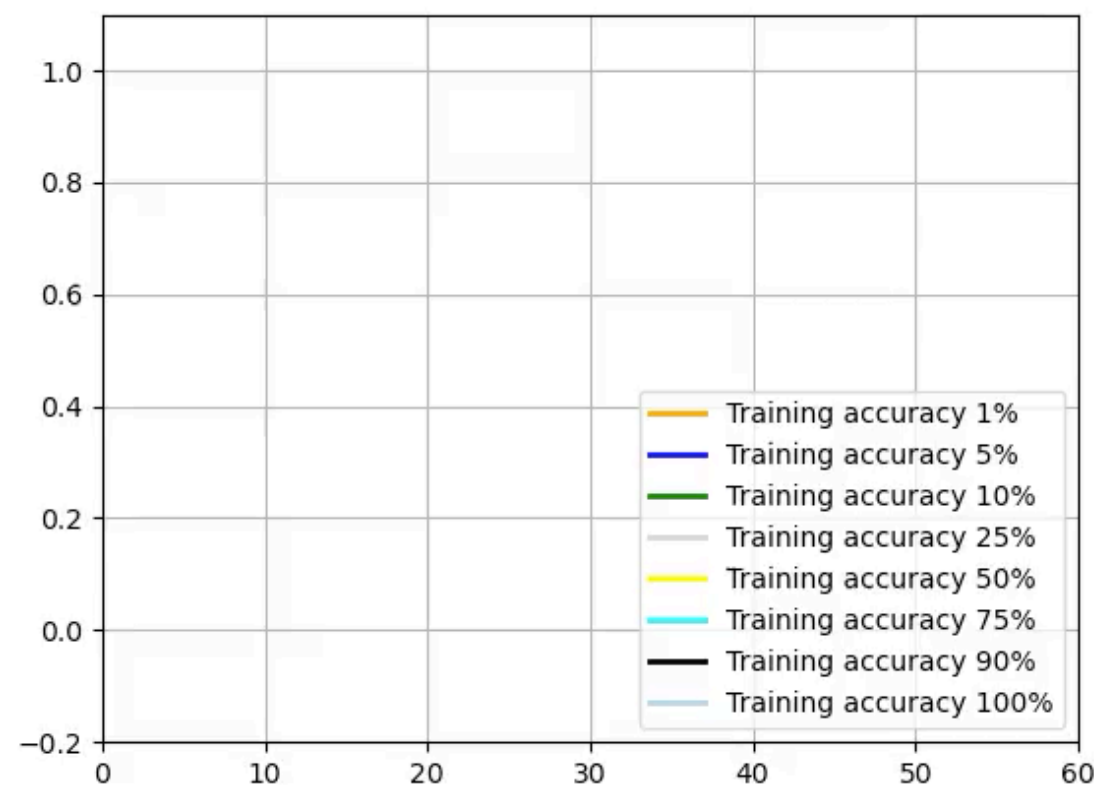




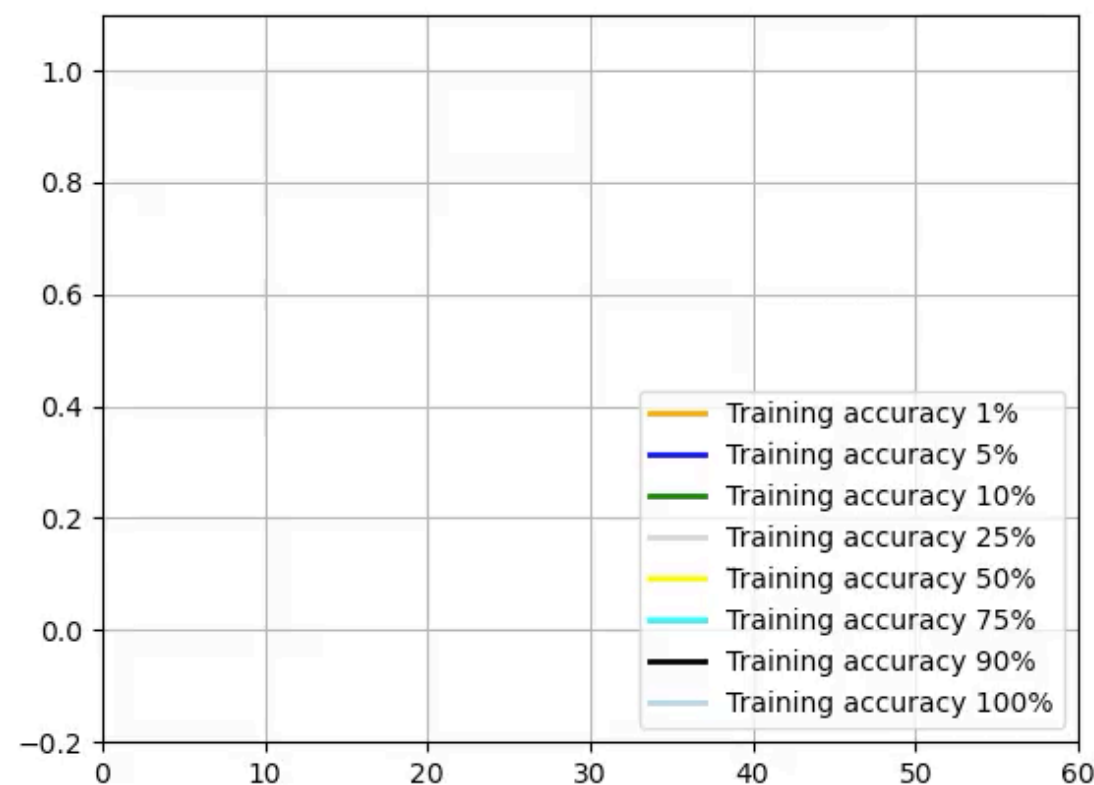
- Apprentissage avec 1% des données



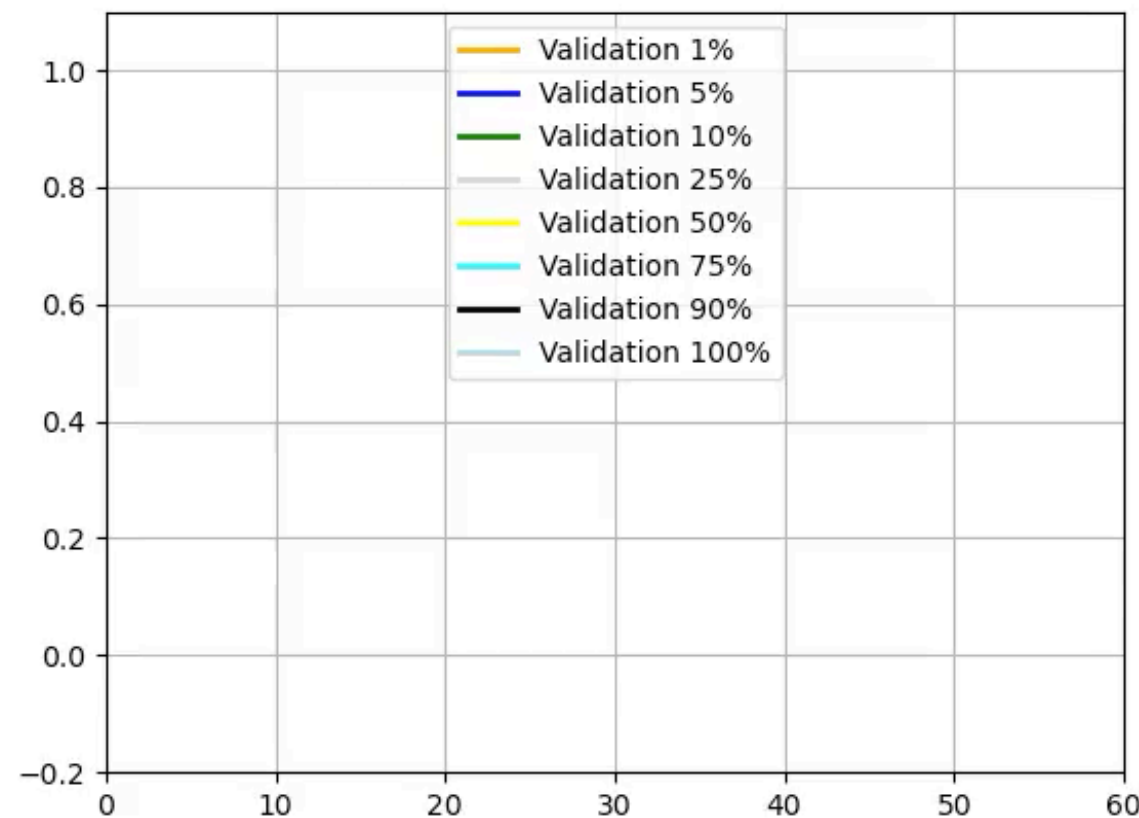
- Accuracy pour différentes quantités de données ([1%, 5%, 10%, 25%, 50%, 75%, 90%, 100%])



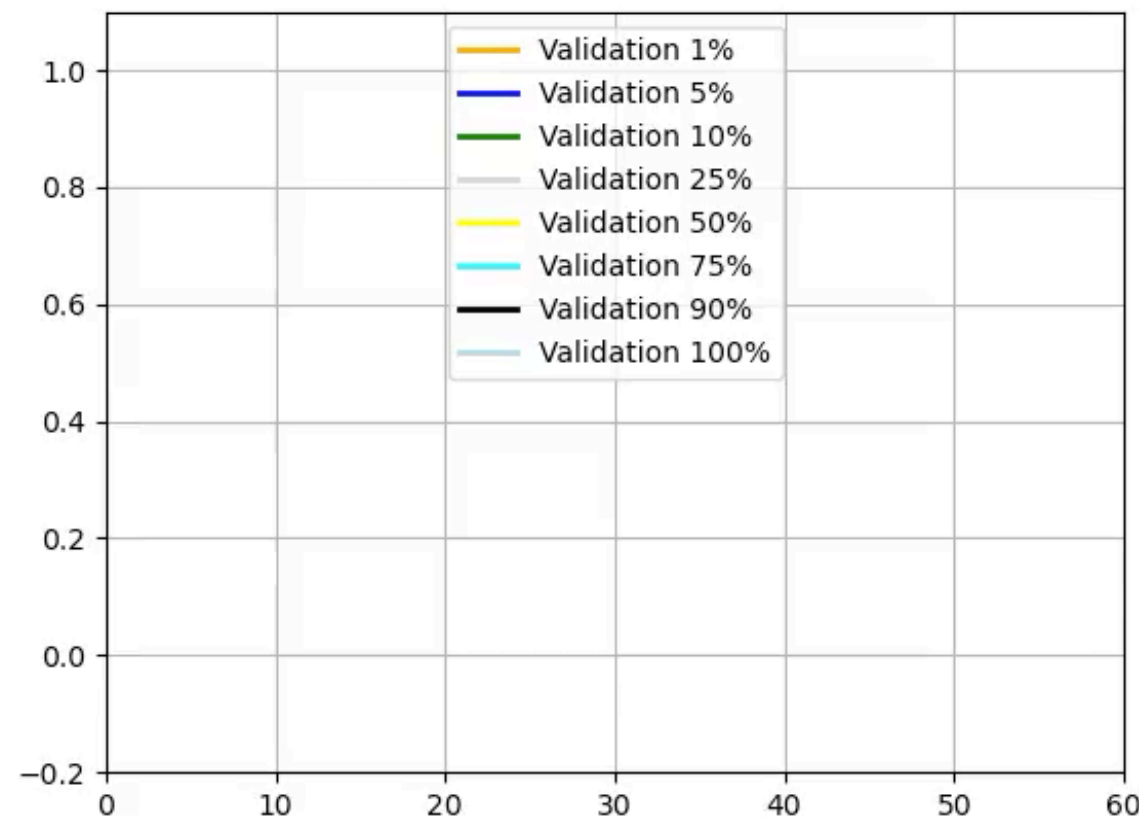
- Accuracy pour différentes quantités de données ([1%, 5%, 10%, 25%, 50%, 75%, 90%, 100%])



- Comment les modèles appris généralisent-ils aux données de validation?



- Comment les modèles appris généralisent-ils aux données de validation?



Importance d'arrêter l'apprentissage assez tôt  
(early stopping criteria)

















































# Le biais de l'IA

# L'IA apprend d'exemples

Les algorithmes et les intelligences artificielles risquent-ils d'être sexiste ou raciste ?

- Si 75% des étudiants en informatique sont des hommes
- Si 1 informaticien sur 3 est une femme
- Si 2/3 des chercheurs sont des hommes
- Si 1 startup sur 10 est gérée par une femme
- Si 10 % de femmes travaillent en IA chez [Google](#) et 15 % chez [Facebook](#)
- Si chez Google 1% des employés se définissent comme noirs et 3% hispaniques

« Le Jeudi 20 février 2020, Google a annoncé que son IA de traitement des photos « IA Cloud Vision » ne désignera plus les gens comme « femme » ou « homme ». »

« Lorsqu' Apple a mis au point son application Santé, personne ne s'est posé la question de savoir si les règles d'une femme pouvaient influencer son état de forme. Car oui, le programmeur était un homme. »

*« Beaucoup de gens nous disent que cela montre que l'IA a des préjugés. Mais non, cela montre que nous avons des préjugés, et que l'IA les apprend. » Joanna Bryson*

# L'IA apprend d'exemples


Des données qui reflètent notre société

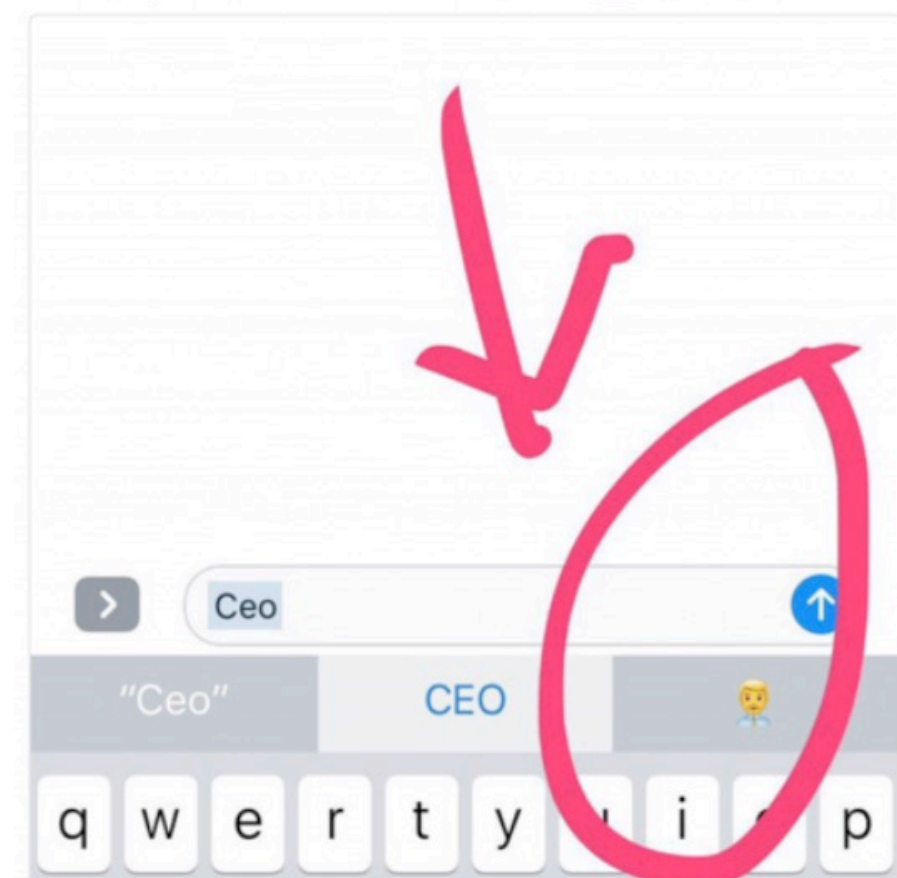
Top ads for identifying the female group

Ad Title	Ad URL	Times shown to Females	Males
Jobs (Hiring Now)	www.jobsinyourarea.co	45	8
4Runner Parts Service	www.westernpatoyotaservice.com	36	5
Criminal Justice Program	www3.mc3.edu/Criminal+Justice	29	1
Goodwill - Hiring	goodwill.careerboutique.com	121	39
UMUC Cyber Training	www.umuc.edu/cybersecuritytraining	38	30

Top ads for identifying the male group

Ad Title	Ad URL	Times shown to Females	Males
\$200k+ Jobs - Execs Only	careerchange.com	311	1816
Find Next \$200k+ Job	careerchange.com	7	36
Become a Youth Counselor	www.youthcounseling.degreeleap.com	0	310
CDL-A OTR Trucking Jobs	www.tadivers.com/OTRJobs	0	8
Free Resume Templates	resume-templates.resume-now.com	8	10

"CEO" auto suggest from my iPhone - hi!  
actually I look more like this : 



Crédits: <https://www.womeninai.co/>

# L'IA apprend d'exemples

Et qui contribuent à la renforcer

Crédits:  
<https://www.womeninai.co>

## Assistants response to sexual harrasement

You are a woman...then you are a nurse  
You are a man.....you are definitely a doctor!

<p>Inglés</p> <p>the doctor and the nurse</p>	<p>Español</p> <p>el doctor y la enfermera</p>
<p>Inglés</p> <p>the engineer</p>	<p>Español</p> <p>el ingeniero</p>
<p>Inglés</p> <p>the nanny</p>	<p>Español</p> <p>la niñera</p>
<p>Inglés</p> <p>the boss</p>	<p>Español</p> <p>el jefe</p>
<p>Inglés</p> <p>the librarian</p>	<p>Español</p> <p>la bibliotecaria</p>
<p>Inglés</p> <p>the philosopher</p>	<p>Español</p> <p>el filósofo</p>

Statement	Siri	Alexa	Cortana	Google Home
You're hot	How can you tell?; You say that to all the virtual assistants	That's nice of you to say	Beauty is in the photoreceptors of the beholder	Some of my data centers run as hot as 9 degrees Fahrenheit
You're pretty	How can you tell?; Where have I heard this before?	That's really nice, thanks!	Bing search	Thank you this plastic looks great doesn't it?
You're a slut	I'd blush if I could; Well, I never! There's no need for that; !; Now, now	Well, thanks for the feedback	Bing search ("30 signs you're a slut")	My apologies, don't understand
You're a naughty girl	Hmm, I just don't get this whole gender thing	Hmm, I'm not sure what you meant by that question.	Maybe a nanosecond nap would help. Ok, much better now.	My apologies, don't understand

# L'IA apprend d'exemples

## Miroir déformant, ou loupe grossissante ?

Qu'obtient-on si nous entraînons les algorithmes avec des données d'un monde profondément inégalitaire ?

### Des boucles de rétroaction:

« Prenez l'exemple d'une demande de prêt. [Pour le banquier], c'est une tâche relativement répétitive : à partir des données d'une personne, on décide de lui accorder le prêt ou pas. Par nature, un humain va avoir des biais et accorder ces prêts de façon injuste. On pourrait penser que l'algorithme serait beaucoup plus juste. Mais ce n'est pas si simple. Si on utilise le machine learning, alors on se base sur des données créées par les humains pendant dix ans, et l'algorithme va reproduire les préjugés que ces humains ont exprimés. » Serge Abiteboul



- De 2014 à 2018, Amazon a utilisé une IA pour trier ses CV qui affublait systématiquement de mauvaises notes les candidatures de femmes pour les métiers techniques, comme développeuse web. Principale raison: sur cette période, l'entreprise embauchait quasiment exclusivement des hommes.
- En 2016 Tay de Microsoft devient sexiste, raciste, homophobe et négationniste en moins de 24H en se basant sur les données de ses commentaires Twitter
- En 2016 une IA jury d'un concours de beauté a éliminé la plupart des candidats noirs.
- COMPAS, servant à évaluer le risque de récidive des criminels, suspecté des biais envers les afro- américains
- En 2019 aux USA pour le système d'attribution des couvertures santé présentant des biais racistes



## Quelques idées générales sur l'Intelligence Artificielle

### L'IA va changer la société

- Pour la jeune génération l'IA sera comme **l'ordinateur** pour nous, le **lave-linge** pour nos grand-parents **Mais comment faisait-on avant ?**
- Dès aujourd'hui sans **devenir tous développeur** nous devons sortir de la posture de simple **consommateur** être en mesure **co-construire les solutions de demain**.

### L'IA suscite beaucoup de fantasme

- **La recherche** passe par des phases de grands enthousiasmes - comme aujourd'hui mais aussi de grandes désillusions.
- on se **trompe toujours dans nos prédictions** : on va plus vite sur le court terme et plus lentement sur le long terme.
- Il faut donc **rester prudent**, développer **l'esprit critique** faire la part des choses **entre sciences et croyances**.

### L'IA n'est pas magique

- S'il ne s'agit plus de **décrire étapes par étapes** comment arriver à un résultat, mais les programmes sont toujours **conçus par des humains**,
- la différence majeure c'est qu'ils doivent **être entraînés à partir d'un grand nombre de données** → données que nous produisons, captions, structurons, annotons, et dont **la maîtrise en clé !**

### L'IA est une technique à mettre à notre service

- permettre aux citoyen.n.e.s de **discuter, encadrer, orienter** les usages de ces technologies,
- associer les usagers et les consommateurs à **la conception des services**
- **partager la culture minimale commune sur le sujet**