## SDU

## Supervised Learning and Clustering

Melih Kandemir<br>University of Southern Denmark<br>Department of Mathematics and Computer Science (IMADA)<br>kandemir@imada.sdu.dk

November 6, 2023

## What is machine learning?

Hint: Divide and conquer

- What is learning?
- What is a machine?
- Combine


## What is machine learning?

A computer program is said to learn
from experience E with respect to a task T and performance measure $\mathbf{P}$,
if its performance at task $T$, as measured in $P$, improves with experience $E$.

## What can machine learning do?



## What can machine learning do?



## What can machine learning do?

## M Tell me how ChatGPT works.

ChatGPT is a large language model that uses deep learning techniques to generate
human-like text. It is based on the GPT (Generative Pre-trained Transformer) architecture, which uses a transformer neural network to process and generate text. The model is pretrained on a massive dataset of text, such as books, articles, and websites, so it can understand the patterns and structure of natural language. When given a prompt or a starting point, the model uses this pre-trained knowledge to generate text that continues the given input in a coherent and natural way.

## Stock price prediction



We are given the following two observations:

- The stock price at day number 2 is 1 DKK.
- The stock price at day number 6 is 4 DKK.

How can we predict the price at an arbitrary day $x_{*}$ in the future?

## How far do we get with high school math?



- Find the equation of the line passing through the two points

$$
y-y_{1}=\frac{y_{2}-y_{1}}{x_{2}-x_{1}}\left(x-x_{1}\right) \rightarrow y-1=\frac{4-1}{6-2}(x-2) \rightarrow y=0.75 x-0.5
$$

- Treat the line as a predictor function: $f\left(x_{*}\right)=0.75 x_{*}-0.5$


## What if we have a third observation?



There is no line that can go through all the three data points!

## Which recipe did we follow?



- Collect a data set, i.e. a set of observations

$$
S=\{(2,1),(6,4)\}
$$

- Assume a model about how the system works: a line
- Fit the model to data, i.e. learn: Find the equation of the line passing through the two points
$y-y_{1}=\frac{y_{2}-y_{1}}{x_{2}-x_{1}}\left(x-x_{1}\right) \rightarrow y-1=\frac{4-1}{6-2}(x-2) \rightarrow y=0.75 x-0.5$
- Use $f\left(x_{*}, 0.75,0.5\right)=0.75 x_{*}-0.5$ to make new predictions, i.e. generalize.


## How about finding the best line $y=a x+b$ ?



- For each choice of $a, b$, we will have a different line. Which one is the best? Best in terms of what?
- Hint: Whichever line we choose, the model will make an error. Quantify it first, minimize it next.


## Error

Since it does not matter if our prediction $y_{*}$ was above or below the target value $y$, it is reasonable to define the error as:

$$
e\left(y, y_{*}\right)=(\underbrace{y_{*}}_{\text {predicted }}-\underbrace{y}_{\text {observed }})^{2}
$$

How does the error function look like?
Hint: Define $\delta=y_{*}-y$, then $\ldots$

## Loss

Each time our model makes a prediction, it will incur some error. The sum of these errors gives us the loss of our model (a line defined by a slope $a$ and an intercept $b$ ) on the data set $S^{1}$ :

$$
\begin{aligned}
L(a, b, S) & =\frac{1}{3} \sum_{i=1}^{3} e\left(f\left(x_{i}, a, b\right)-y_{i}\right) \\
& =\frac{1}{3} \sum_{i=1}^{3}\left(f\left(x_{i}, a, b\right)-y_{i}\right)^{2} \\
& =\frac{1}{3}(2 a+b-1)+\frac{1}{3}(6 a+b-4)+\frac{1}{3}(9 a+b-3) \\
& =\sum_{i=1}^{3} \frac{1}{3}\left(a x_{i}+b-y_{i}\right)^{2}
\end{aligned}
$$

${ }^{1}$ Remember: $S=\left\{\left(x_{1}, y_{1}\right)=(2,1),\left(x_{2}, y_{2}\right)=(6,4),\left(x_{3}, y_{3}\right)=(9,3)\right\}$

## Learning: Choosing the best of three lines

Let

$$
\mathcal{H}:=\left\{\left(a_{1}, b_{1}\right),\left(a_{2}, b_{2}\right), \ldots,\left(a_{K}, b_{K}\right)\right\}
$$

be all the options we have. How would you choose the best one?

## Learning: Choosing the best of three lines

## Evaluate the loss with each option

$$
\begin{aligned}
& L\left(a_{1}, b_{1}, S\right):=\frac{1}{3}\left(2 a_{1}+b_{1}-1\right)+\frac{1}{3}\left(6 a_{1}+b_{1}-4\right)+\frac{1}{3}\left(9 a_{1}+b_{1}-3\right) \\
& L\left(a_{2}, b_{2}, S\right):=\frac{1}{3}\left(2 a_{2}+b_{2}-1\right)+\frac{1}{3}\left(6 a_{2}+b_{2}-4\right)+\frac{1}{3}\left(9 a_{3}+b_{3}-3\right) \\
& L\left(a_{3}, b_{3}, S\right):=\frac{1}{3}\left(2 a_{3}+b_{3}-1\right)+\frac{1}{3}\left(6 a_{2}+b_{2}-4\right)+\frac{1}{3}\left(9 a_{3}+b_{3}-3\right)
\end{aligned}
$$

and choose the line that gives the smallest loss. In formal terms, choose $a_{\text {best }}, b_{\text {best }}$ that satisfies

$$
L\left(a_{\text {best }}, b_{\text {best }}, S\right)=\min \left\{L\left(a_{1}, b_{1}, S\right), L\left(a_{2}, b_{2}, S\right), L\left(a_{3}, b_{3}, S\right)\right\}
$$

Choosing the argument that minimizes a function can be expressed shortly via the arg min operation:

$$
a_{\text {best }}, b_{\text {best }}=\arg \min _{(a, b) \in \mathcal{H}} L(a, b, S)
$$

## Learning: Choosing the best of infinitely many lines

- In fact $a, b$ can be any real number. So we have infinite number of options. How shall we find out the best one?
- Best: $a, b$ that minimizes the loss:

$$
a_{\text {best }}, b_{\text {best }}=\arg \min _{a, b \in \mathbb{R}} L(a, b, S)
$$

- What is special with the point $L\left(a_{\text {best }}, b_{\text {best }}, S\right)$ ?

Hint: How does the function value change?

- If there is upward slope, turn back and go down.
- If there is downward slope, go further ahead.
- If there is no slope, here it is!

How can we express change in mathematical terms?

## The derivative!

We are looking for values $a_{\text {best }}, b_{\text {best }}$ that satisfy:

$$
\begin{aligned}
& \left.\frac{d L(a, b, S)}{d a}\right|_{a=a_{b e s t}}=0 \\
& \left.\frac{d L(a, b, S)}{d b}\right|_{b=b_{b e s t}}=0 .
\end{aligned}
$$

## Let us solve it for $a$

$$
\begin{aligned}
& \frac{d L(a, b, S)}{d a}=\frac{d \frac{1}{3} \sum_{i=1}^{3}\left(a x_{i}+b-y_{i}\right)^{2}}{d a} \\
& =\frac{1}{3} \sum_{i=1}^{3} \frac{d\left(a x_{i}+b-y_{i}\right)^{2}}{d a} \quad \text { because } \frac{d(f+g)}{d x}=\frac{d f}{d x}+\frac{d g}{d x} \\
& =\frac{1}{3} \sum_{i=1}^{3} 2\left(a x_{i}+b-y_{i}\right) \frac{d a x_{i}}{d a} \quad \text { because } \frac{d(f \circ g)}{d x}=\frac{d f}{d g} \frac{d g}{d x} \\
& =\frac{2}{3} \sum_{i=1}^{3}\left(a x_{i}+b-y_{i}\right) x_{i} \\
& =0
\end{aligned}
$$

## Let us solve it for $a$

$$
\begin{aligned}
& \frac{3}{2} \frac{2}{3} \sum_{i=1}^{3}\left(a x_{i}+b-y_{i}\right) x_{i}=\frac{3}{2} 0 \\
& \Rightarrow \sum_{i=1}^{3}\left(a x_{i}+b-y_{i}\right) x_{i}=0 \\
& \Rightarrow a \sum_{i=1}^{3} x_{i}^{2}+\sum_{i=1}^{3}\left(b-y_{i}\right) x_{i}=0 \\
& \Rightarrow a_{\text {best }}=\frac{\sum_{i=1}^{3}\left(y_{i}-b\right) x_{i}}{\sum_{i=1}^{3} x_{i}^{2}}
\end{aligned}
$$

## Let us solve it for $b$

$$
\begin{aligned}
& \frac{d L(a, b, S)}{d b}=\frac{1}{3} \sum_{i=1}^{3} \frac{d\left(a x_{i}+b-y_{i}\right)^{2}}{d b} \\
& =\frac{1}{3} \sum_{i=1}^{3} 2\left(a x_{i}+b-y_{i}\right) \underbrace{\frac{d b}{d b}}_{=1} \\
& =\frac{2}{3} \sum_{i=1}^{3}\left(a x_{i}+b-y_{i}\right)=0 \\
& \Rightarrow \sum_{i=1}^{3} b+\sum_{i=1}^{3}\left(a x_{i}-y_{i}\right)=0 \\
& \Rightarrow 3 b=-\sum_{i=1}^{3}\left(a x_{i}-y_{i}\right) \Rightarrow b_{\text {best }}=\frac{\sum_{i=1}^{3}\left(y_{i}-a x_{i}\right)}{3}
\end{aligned}
$$

## The best fitting line to data set $S$ is then

$$
f(x)=\underbrace{\frac{\sum_{i=1}^{3}\left(y_{i}-b\right) x_{i}}{\sum_{i=1}^{3} x_{i}^{2}}}_{a_{\text {best }}} x+\underbrace{\frac{\sum_{i=1}^{3}\left(y_{i}-a x_{i}\right)}{3}}_{b_{\text {best }}}
$$

We can use this function to predict the output of any $x$ we want.

## What if?

- The input-output relationship is nonlinear, i.e. no line-shaped predictor evaluated on the input can even approximate the output.
- We can evaluate the derivatives for arbitrary $a, b$, but, cannot find $a, b$ values that make the derivatives zero?



## Re-express the derivative in a more generic way

$$
\frac{d L(a, b, S)}{d a}=\frac{2}{3} \sum_{i=1}^{3} \underbrace{\left(a x_{i}+b-y_{i}\right)}_{f\left(x_{i} ; a, b\right)-y_{i}} \underbrace{x_{i}}_{\frac{d a x_{i}}{d a}}
$$

The solution template would be the same if:

- we had not 3 but $m$ data points, i.e. $S=\left(x_{1}, y_{1}\right), \ldots,\left(x_{m}, y_{m}\right)$
- our model were not a line but an arbitrary function $f(x ; \theta)$
- we computed the derivative of an arbitrary parameter $\theta$ of this function

$$
\frac{d L(\theta, S)}{d \theta}=\frac{2}{m} \sum_{i=1}^{m}\left(f\left(x_{i} ; \theta\right)-y_{i}\right) \frac{d f\left(x_{i} ; \theta\right)}{d \theta}
$$

## The Gradient Descent Algorithm

- Choose a learning rate $\alpha>0$.
- Initialize $\theta$ to an arbitrary value
- repeat
- $\theta \leftarrow \theta-\alpha \frac{d L(\theta, S)}{d \theta}$
- until $\theta$ no longer changes


## Making sense of gradient descent

Placing the generic loss derivative calculated in the previous slide into the update rule:

$$
\theta \leftarrow \theta-\frac{2 \alpha}{m} \sum_{i=1}^{m}\left(f\left(x_{i} ; \theta\right)-y_{i}\right) \frac{d f\left(x_{i}\right)}{d \theta}
$$

In natural language, change parameter $\theta$ proportionally to

- The signed prediction error of the current model $f\left(x_{i} ; \theta\right)-y_{i}$
- The rate the predictions of the model changes $\frac{d f\left(x_{i}\right)}{d \theta}$

This means,

- Make big changes when predictions are bad
- Stop changing when predictions are good


## Perceptron: The atom of intelligence

## North-West: Biological neuron <br> South-East: Artificial neuron (perceptron)



## The computational graph of a perceptron

Computational graph: block diagram of mathematical operations.


The neuron has weights assigned to each input channel:

- $w_{1}$ for $x_{1}, w_{2}$ for $x_{2}, w_{3}$ for $x_{3}$, and a bias term $b$ to model the intercept just as in the line fitting example above.
It processes the given input in two steps:
- Linear mapping: $f=\sum_{i_{1}}^{3} w_{i} x_{i}+b$
- Nonlinear activation, for example: $h=\max (0, f)$


## Neural net: A group of connected perceptrons



This neural net will make the following prediction for the input observations $\left(x_{1}, x_{2}\right)$ :

$$
\begin{aligned}
f\left(x_{1}, x_{2}\right) & =w_{5}\left(\max \left(w_{1} x_{1}+w_{2} x_{2}+b_{1}, 0\right)\right) \\
& +w_{6}\left(\max \left(w_{3} x_{1}+w_{4} x_{2}+b_{2}, 0\right)\right)+b_{3}
\end{aligned}
$$

## The Multi-Layer Perceptron (MLP)



## Large Language Models

- The predictor is not a line but a neural network

- The input is not a single value but a long sequence of words:

$$
f(\text { her mother would like })=\text { to }
$$

## Large Language Models

- The neural net learns to pay more attention to important information in the input sequence:

$$
f(\underbrace{\text { her mother }}_{\text {ignore }} \underbrace{\text { would like }}_{\text {attend }})=\text { to }
$$

Attended words influence the output, unattended words are ignored.

- The model generates text progressively by taking its own predictions as input, i.e. autoregression:
$f($ her mother would like $)=$ to
$f($ her mother would like to $)=$ buy
$f($ her mother would like to buy $)=$ an
$f$ (her mother would like to buy an $)=$ icecream


## Purpose of Clustering

- identify a finite number of categories (classes, groups: clusters) in a given dataset
- similar objects shall be grouped in the same cluster, dissimilar objects in different clusters
- similarity is highly subjective, depending on the application scenario


## A Dataset can be Clustered in Different Meaningful Ways


(a) Original points.


(c) Four clusters.

(b) Two clusters.


$\square$
(d) Six clusters.

Figure 8.1. Different ways of clustering the same set of points.

## Criteria of Quality: Cohesion and Separation

- cohesion: how strong are the cluster objects connected (how similar, pairwise, to each other)?
- separation: how well is a cluster separated from other clusters?

small within cluster distances

large between cluster distances


## Optimization of Cohesion

Partitional clustering algorithms partition a dataset into $k$ clusters, typically minimizing some cost function (compactness criterion), i.e., optimizing cohesion.

## Assumptions for Partitioning Clustering

Central assumptions for approaches in this family are typically:

- number $k$ of clusters known (i.e., given as input)
- clusters are characterized by their compactness
- compactness measured by some distance function (e.g., distance of all objects in a cluster from some cluster representative is minimal)
- criterion of compactness typically leads to convex or even spherically shaped clusters



## Construction of Central Points: Basics

- data points (objects) are $d$-dimensional real-valued vectors $x=\left(x_{1}, \ldots, x_{d}\right) \in \mathbb{R}^{d}$
- and we measure distances between data point pairs by

$$
\|x-y\|_{2}=\sqrt{\sum_{i=1}^{d}\left(x_{i}-y_{i}\right)^{2}}
$$

- centroid $\mu_{C}$ : mean vector of all points in cluster $C$


$$
\mu_{C_{i}}=\frac{1}{\left|C_{i}\right|} \cdot \sum_{o \in C_{i}} o
$$

## Construction of Central Points: Basics

- data points (objects) are $d$-dimensional real-valued vectors $x=\left(x_{1}, \ldots, x_{d}\right) \in \mathbb{R}^{d}$
- and we measure distances between data point pairs by

$$
\|x-y\|_{2}=\sqrt{\sum_{i=1}^{d}\left(x_{i}-y_{i}\right)^{2}}
$$

- centroid $\mu_{C}$ : mean vector of all points in cluster $C$


$$
\mu_{C_{i}}=\frac{1}{\left|C_{i}\right|} \cdot \sum_{o \in C_{i}} o
$$

## Construction of Central Points: Basics

- measure of compactness for a cluster $C$ :

$$
T D^{2}(C)=\sum_{p \in C}\left\|p-\mu_{C}\right\|_{2}^{2}
$$

(a.k.a. SSQ: sum of squares)

- measure of compactness for a clustering
$T D^{2}\left(C_{1}, C_{2}, \ldots, C_{k}\right)=\sum_{i=1}^{k} T D^{2}\left(C_{i}\right)$



## Construction of Central Points: Basics

- measure of compactness for a cluster $C$ :

$$
T D^{2}(C)=\sum_{p \in C}\left\|p-\mu_{C}\right\|_{2}^{2}
$$

(a.k.a. SSQ: sum of squares)

- measure of compactness for a clustering
$T D^{2}\left(C_{1}, C_{2}, \ldots, C_{k}\right)=\sum_{i=1}^{k} T D^{2}\left(C_{i}\right)$



## Basic Algorithm

Clustering by Minimization of Variance

- start with $k$ (e.g., randomly selected) points as cluster representatives (or with a random partition into $k$ "clusters")
- repeat:
- assign each point to the closest representative
- compute new representatives based on the given partitions (centroid of the assigned points)
- until there is no change in assignment
(a) Initialization

(b) First Iteration

(c) Convergence



## $k$-means

$k$-means is a variant of the basic algorithm:

- a centroid is immediately updated when some point changes its assignment
- $k$-means has very similar properties, but the result now depends on the order of data points in the input file
The name " $k$-means" is often used indifferently for any variant of the basic algorithm.


## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm



## $k$-means Clustering - Lloyd/Forgy Algorithm


reassign points no change convergence!

## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm


reassign more points possibly more iterations

## $k$-means Clustering - MacQueen Algorithm



## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - MacQueen Algorithm

 Alternative Run - Different Order

## $k$-means Clustering - Quality



First solution: $T D^{2}=61 \frac{1}{2}$

Note: $S S Q(\mu, p)=\|\mu-p\|_{2}^{2}$.

## $k$-means Clustering - Quality



$$
\begin{aligned}
& S S Q\left(\mu_{1}, p_{1}\right)=|10-10|^{2}+|1-1|^{2}=0 \\
& T D^{2}\left(C_{1}\right)=0 \\
& S S Q\left(\mu_{2}, p_{2}\right) \approx|4.7-2|^{2}+|6.3-3|^{2} \approx 18.2 \\
& S S Q\left(\mu_{2}, p_{3}\right) \approx|4.7-3|^{2}+|6.3-4|^{2} \approx 8.2 \\
& S S Q\left(\mu_{2}, p_{4}\right) \approx|4.7-1|^{2}+|6.3-5|^{2} \approx 15.4 \\
& S S Q\left(\mu_{2}, p_{5}\right) \approx|4.7-7|^{2}+|6.3-7|^{2} \approx 5.7 \\
& S S Q\left(\mu_{2}, p_{6}\right) \approx|4.7-6|^{2}+|6.3-8|^{2} \approx 4.6 \\
& S S Q\left(\mu_{2}, p_{7}\right) \approx|4.7-7|^{2}+|6.3-8|^{2} \approx 8.2 \\
& S S Q\left(\mu_{2}, p_{7}\right) \approx|4.7-7|^{2}+|6.3-9|^{2} \approx 12.6 \\
& T D^{2}\left(C_{2}\right) \approx 72.86
\end{aligned}
$$

First solution: $T D^{2}=61 \frac{1}{2}$
Second solution: $T D^{2} \approx 72.68$

Note: $S S Q(\mu, p)=\|\mu-p\|_{2}^{2}$.

## $k$-means Clustering - Quality



$$
\begin{aligned}
& S S Q\left(\mu_{1}, p_{2}\right)=|2-2|^{2}+|4-3|^{2}=0+1=1 \\
& S S Q\left(\mu_{1}, p_{3}\right)=|2-3|^{2}+|4-4|^{2}=1+0=1 \\
& S S Q\left(\mu_{1}, p_{4}\right)=|2-1|^{2}+|4-5|^{2}=1+1=2 \\
& T D^{2}\left(C_{1}\right)=4 \\
& S S Q\left(\mu_{2}, p_{1}\right)=|7.4-10|^{2}+|6.6-1|^{2}=6 \frac{19}{25}+31 \frac{9}{25}=38 \frac{3}{25} \\
& S S Q\left(\mu_{2}, p_{5}\right)=|7.4-7|^{2}+|6.6-7|^{2}=\frac{4}{25}+\frac{4}{25}=\frac{8}{25} \\
& S S Q\left(\mu_{2}, p_{6}\right)=|7.4-6|^{2}+|6.6-8|^{2}=1 \frac{24}{25}+1 \frac{24}{25}=3 \frac{23}{25} \\
& S S Q\left(\mu_{2}, p_{7}\right)=|7.4-7|^{2}+|6.6-8|^{2}=\frac{4}{25}+1 \frac{24}{25}=2 \frac{3}{25} \\
& S S Q\left(\mu_{2}, p_{8}\right)=|7.4-7|^{2}+|6.6-9|^{2}=\frac{4}{25}+5 \frac{19}{25}=5 \frac{23}{25} \\
& T D^{2}\left(C_{2}\right)=50 \frac{2}{5}
\end{aligned}
$$

First solution: $T D^{2}=61 \frac{1}{2}$
Second solution: $T D^{2} \approx 72.68$
Optimal solution: $T D^{2}=54 \frac{2}{5}$

Note: $S S Q(\mu, p)=\|\mu-p\|_{2}^{2}$.

## Discussion

pros

- efficient: $\mathcal{O}(k \cdot n)$ per iteration, number of iterations is usually in the order of 10.
- easy to implement, thus very popular
cons
- $k$-means converges towards a local minimum
- $k$-means (MacQueen-variant) is order-dependent
- deteriorates with noise and outliers (all points are used to compute centroids)
- clusters need to be convex and of (more or less) equal extension
- number $k$ of clusters is hard to determine
- strong dependency on initial partition (in result quality as well as runtime)

