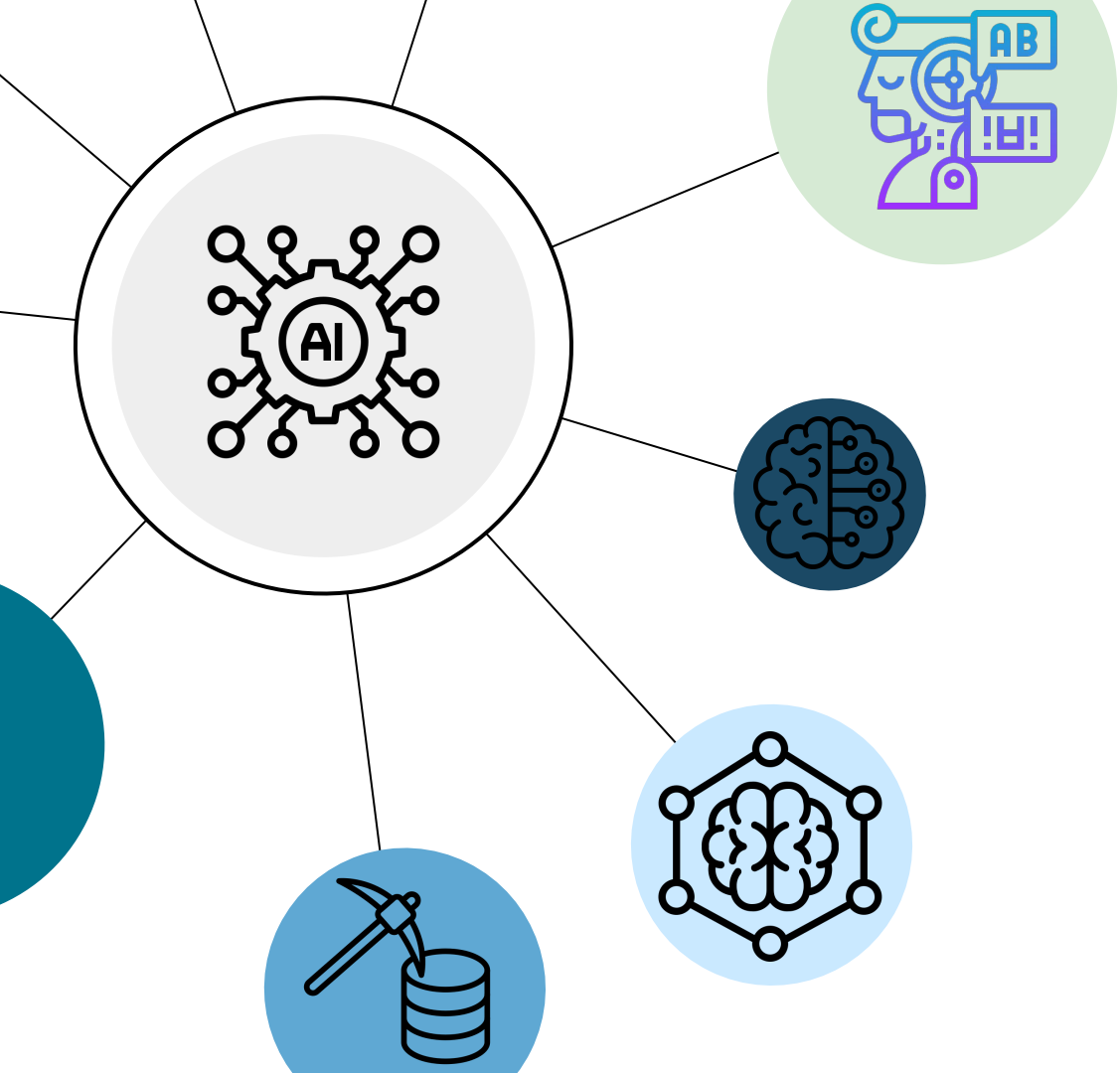


3iA Côte d'Azur
Institut interdisciplinaire d'intelligence artificielle

UNIVERSITÉ CÔTE D'AZUR

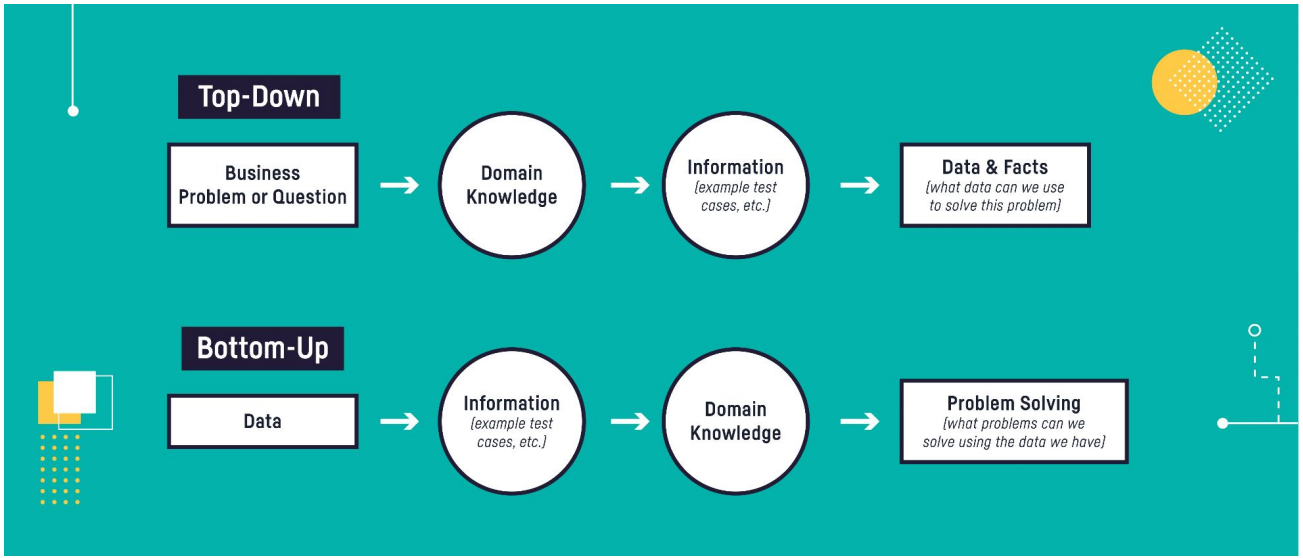
Introduction à l'Intelligence Artificielle

Anaïs Ollagnier
Université Côte d'Azur, CNRS, Inria, I3S

Data collection & Management

Data are the KEY !

AI systems, particularly machine learning models, require **data to learn and make predictions**. The more diverse and high-quality the data, the better the AI model's performance. Training data provides the model with the **patterns** and information it needs to make accurate decisions.



Structured vs Unstructured Data

Here are the key differences between structured data and unstructured data:

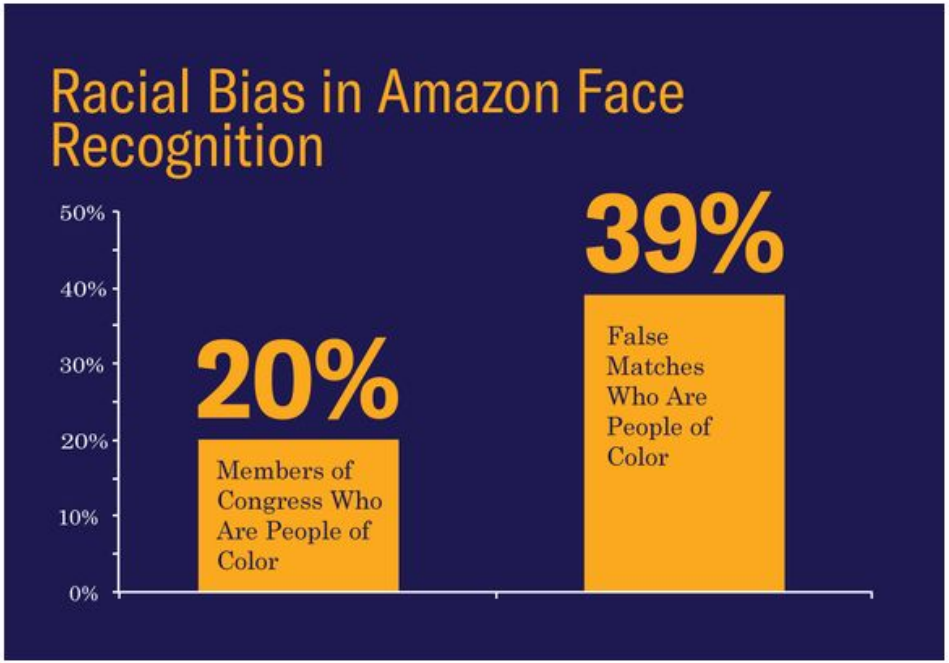
- Structured data is **standardized, clearly defined, and searchable data**, while unstructured data is usually **stored in its native format**.
- Structured data is **quantitative**, while unstructured data is **qualitative**.
- Structured data is **easy to search and analyze**, while unstructured data **requires more work to process and understand**.
- Structured data exists in **predefined formats**, while unstructured data is in a **variety of formats**.

UNSTRUCTURED DATA

STRUCTURED DATA

Data Collection Methods

Damageable failures



Source: ACLU

Damageable failures

Figure 1: Natural adversarial examples from IMAGENET-A. The red text is a ResNet-50 prediction with its confidence, and the black text is the actual class. Many natural adversarial examples are incorrectly classified with high confidence, despite having no adversarial modifications as they are examples which naturally occur in the physical world.

Source: *Berkeley*, *University of Chicago*, and *University of Washington*

https://www.immuniweb.com/blog/top-10-failures-of-ai.html
https://www.huffingtonpost.fr/actualites/article/photos-chihuahua-ou-muffin_73514.html

What could impact my system performance ?

Generalization:

- **High-Quality and Diverse Data**: The quality of training data directly impacts an AI system's generalization capabilities. Well-collected data, encompassing a wide range of scenarios and examples, enables the AI model to learn robust patterns. This, in turn, allows the model to adapt and make accurate predictions or classifications on new, unseen data.

- **Adaptability**: Generalization is vital for AI systems because it enables them to apply their acquired knowledge to real-world situations. If an AI model fails to generalize effectively, it may perform well on training data but poorly on new, unseen data, limiting its practical applicability.

What could impact my system performance ?

Quality of Data: AI learns from data, so the quality and quantity of data it receives are crucial. If the data it learns from is incomplete, biased, or inaccurate, it can lead to flawed learning outcomes.

Algorithm Selection: Different algorithms are used for different tasks in AI. Choosing the right algorithm for a specific task is important. Some algorithms might be more suitable for certain types of data or learning objectives than others.

Computational Resources: The computational power available to the AI system can impact its performance. More powerful hardware can process larger amounts of data and perform complex computations faster, which can lead to better learning outcomes.

What could impact my system performance ?

- **Model Complexity**: The complexity of the AI model being used can also affect performance. More complex models can potentially learn more intricate patterns in the data, but they may also require more computational resources and data to train effectively.
- **Training Process**: The process used to train the AI model, including the selection of training data, the optimization of parameters, and the duration of training, can influence performance. Proper training techniques need to be applied to ensure effective learning.
- **Feedback Mechanism**: Providing accurate and timely feedback to the AI system during the learning process is important for course correction and improvement. Without proper feedback mechanisms, the AI may continue to make the same mistakes or fail to adapt to changing conditions.

What could impact my system performance ?

- Domain Specificity: AI systems are often designed for specific domains or tasks. A system trained for one task may not perform well in a different domain. It's important to consider the applicability of the AI system to the specific learning task or subject matter.

E.g.:

Model:

- In mathematics, a model is a simplified representation of a system or process used to make predictions or understand phenomena.
- In fashion, a model refers to a person who poses for photographs or walks the runway to display clothing or accessories.

Branch:

- In botany, a branch is a woody extension of a tree or plant.
- In version control systems like Git, a branch is a parallel version of a repository, allowing developers to work on different features or fixes simultaneously.

Advantages of Data-driven Approach

1. **Objective Decision-Making**: Data-driven decisions are less influenced by personal biases, emotions, or subjective opinions. They rely on empirical evidence and objective analysis, making them more reliable.
2. **Accurate Predictions**: AI models trained on data can make accurate predictions and recommendations. They learn from historical data patterns, which can lead to improved decision-making and outcomes.
3. **Optimized Processes**: Data-driven insights can help optimize processes, reducing inefficiencies and costs. This is particularly valuable in industries like manufacturing and logistics.
4. **Quick Adaptation**: Data-driven organizations can quickly adapt to changing conditions and customer preferences, making them more competitive in dynamic markets.
5. **Scientific Research**: In scientific research, data-driven approaches can lead to discoveries and advancements in various fields, including healthcare, environmental science, and physics.

Disadvantages of Data-driven Approach

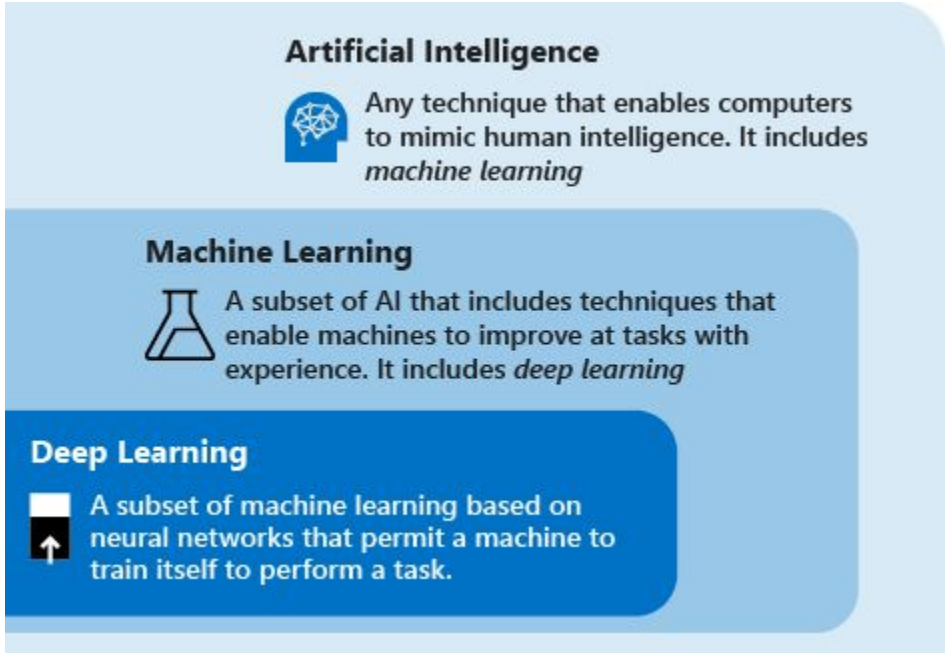
1. **Data Quality**: The accuracy and quality of data are crucial. Poor-quality data can lead to incorrect conclusions and flawed decision-making.
2. **Bias**: Data can inherit biases present in the collection process. Biased data can perpetuate discrimination and unfair practices when used in AI models.
3. **Privacy Concerns**: Collecting and using personal data for data-driven decisions can raise privacy concerns. Striking a balance between data utility and privacy is a challenge.
4. **Overreliance on Data**: An overreliance on data can lead to a lack of human judgment and intuition. Some decisions require a human touch and contextual understanding.
5. **Data Collection Costs**: Collecting, storing, and managing large volumes of data can be costly. Small organizations may face financial challenges in implementing data-driven approaches.
6. **Interpretability**: Complex AI models may lack interpretability. Understanding why a model makes a particular decision can be challenging, especially in deep learning.
7. **Data Security**: Protecting data from breaches and unauthorized access is a critical concern. Data-driven systems can be vulnerable to cyberattacks.

Your first artificial neural network (ANN)

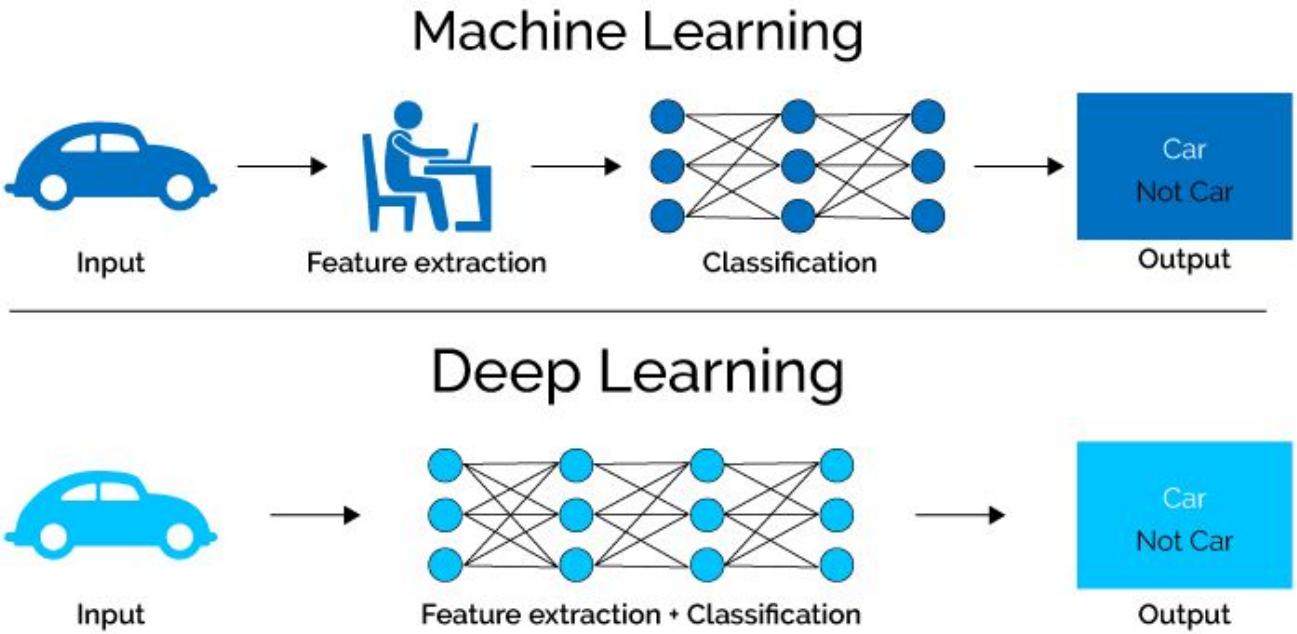
Resources of this course

- The content of the following part (MLP) is entirely borrowed from:
  - https://www.3blue1brown.com/
  - https://www.3blue1brown.com/lessons/neural-networks
  - https://www.3blue1brown.com/lessons/gradient-descent

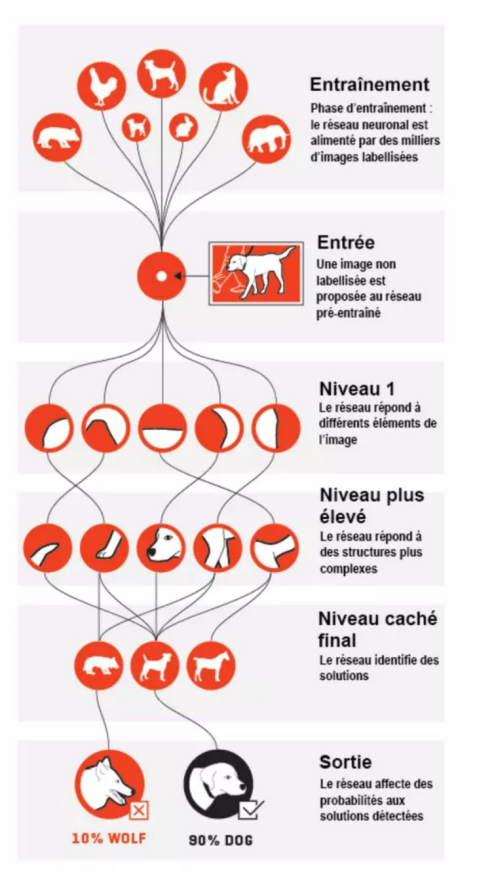
IA VS Machine Learning VS Deep Learning



“Deep Learning”



“Deep Learning”

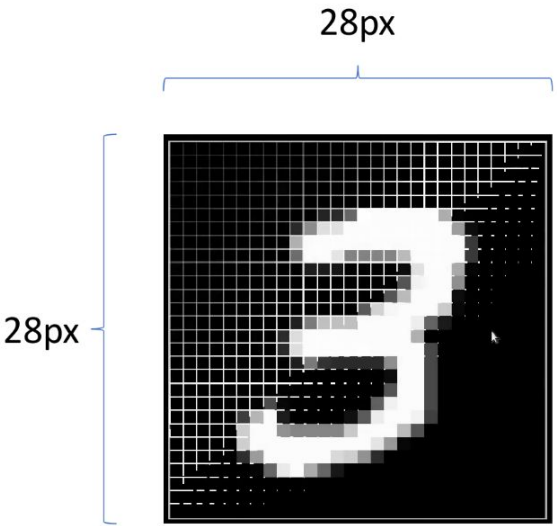


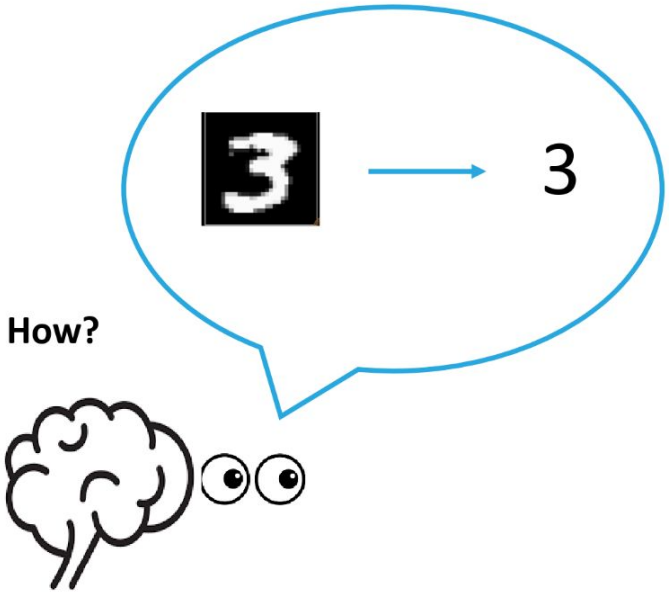
- “deep learning” is a set of methods that leverages the advancements in neural networks to recognize objects, images, images within images, donations, phrases in a phone call, and more.

- It always involves two phases: a training or education phase, which is carried out on labeled data, and a discovery phase, which uses unlabeled data.

AI for vision: how to recognize a digit?

- Our brain has no difficulty recognizing the number 3 here.

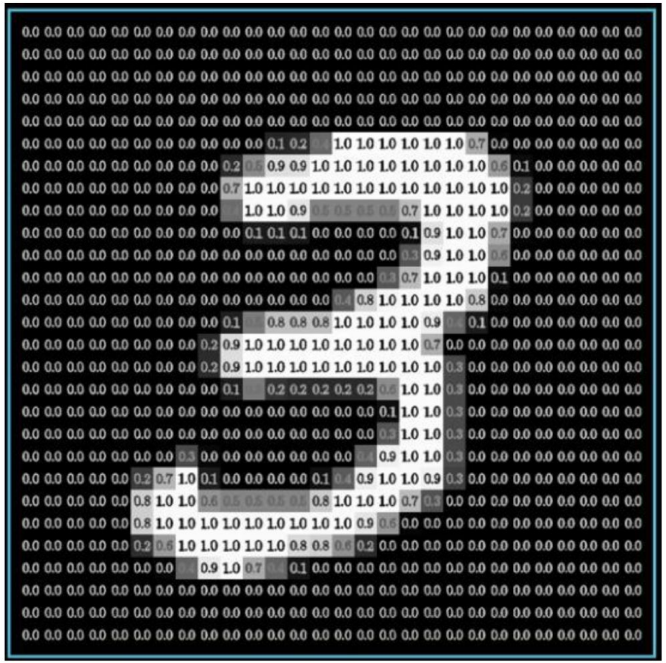


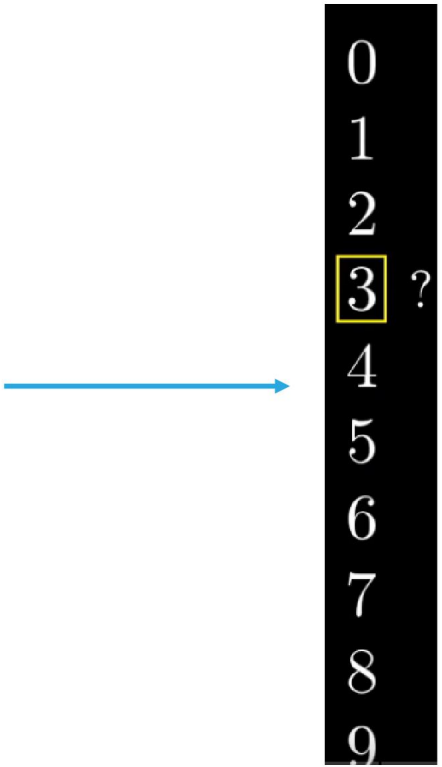


How can we make a decision?

- It is not possible to list all the patterns corresponding to a single digit (thickness, curves, etc.).

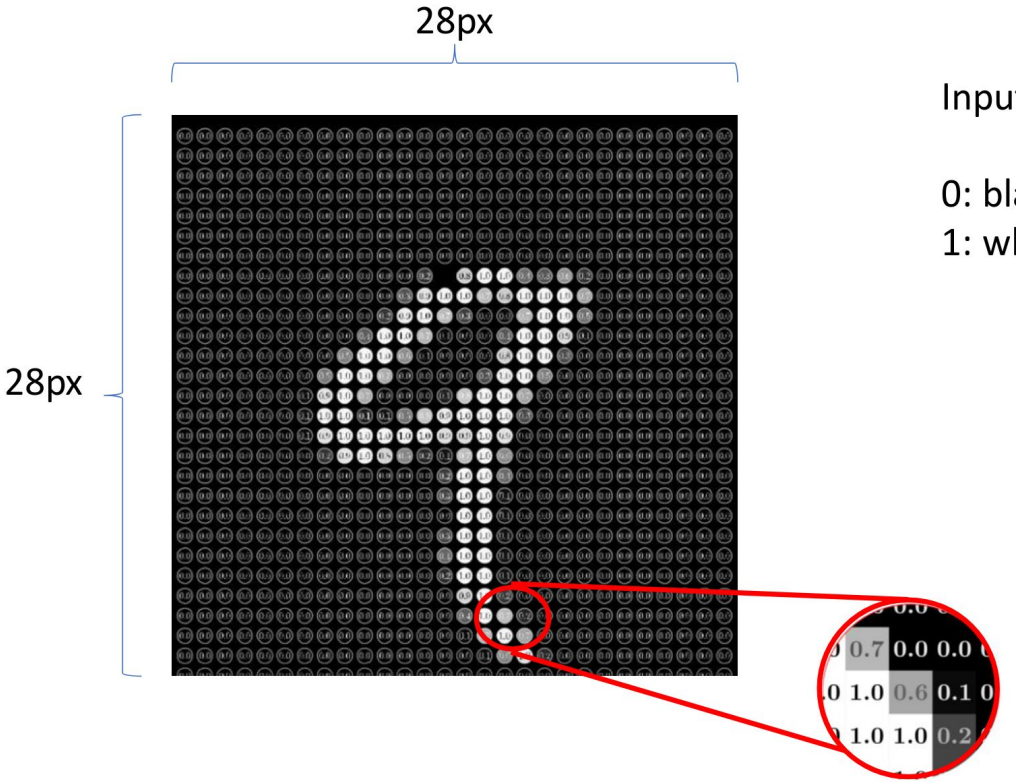
➔ AI, and more specifically ML, allows for the accomplishment of these targeted tasks.





How to do it? Build a neural network! (v0.1)

- Let's consider the following input:

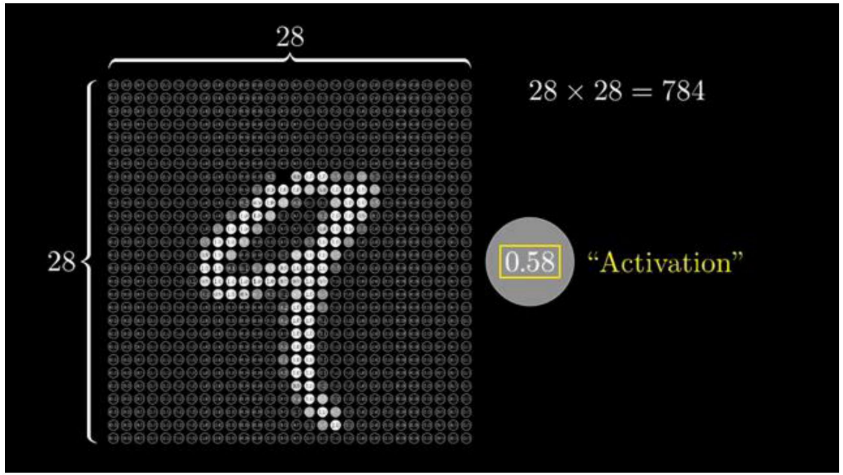


Input size: 28 x 28 = 784

0: black
1: white

Objective: Build a neural network.

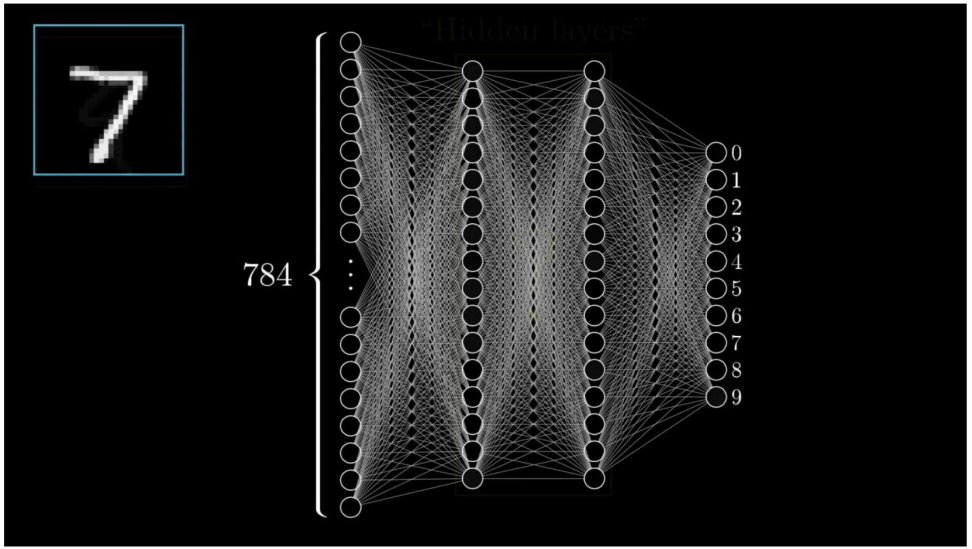
- Which one:
  - takes an input of dimension 784
  - produces 10 score values for how well the image corresponds to each digit



➔ This is a **Multi-Layer Perceptron** (MLP)

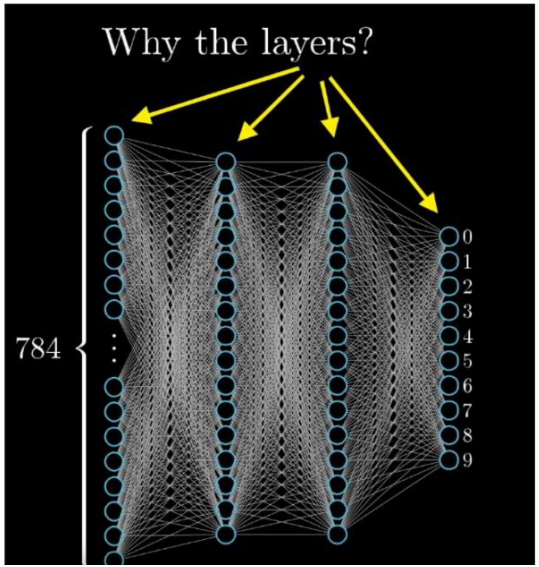
How to build an artificial neural network?

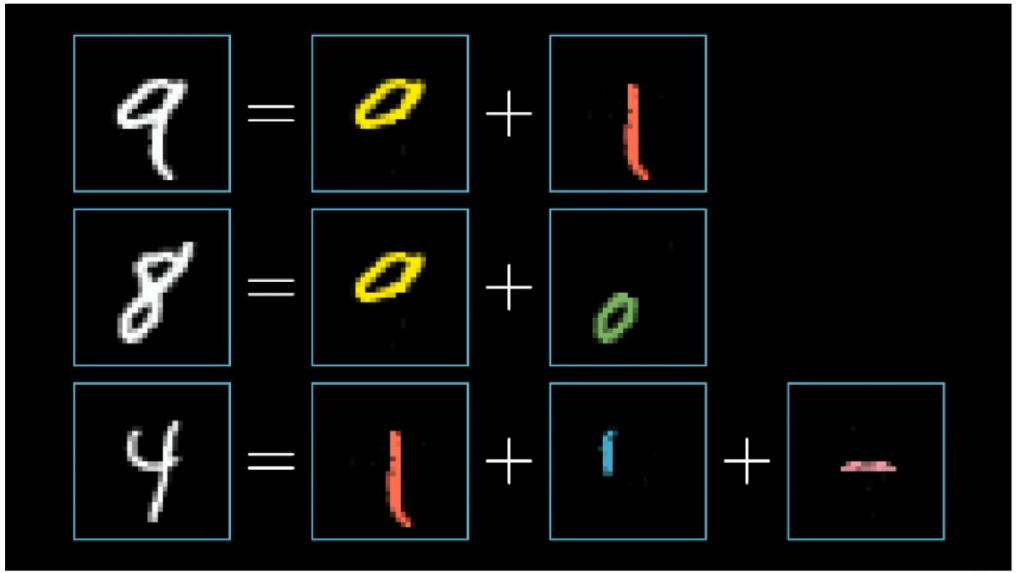
- Architecture: arbitrary (2 hidden layers and 16 neurons here)
- Information processing: the activation of one layer is established from the activations of the previous one.



What is the rationale behind the 'layers' of neurons?

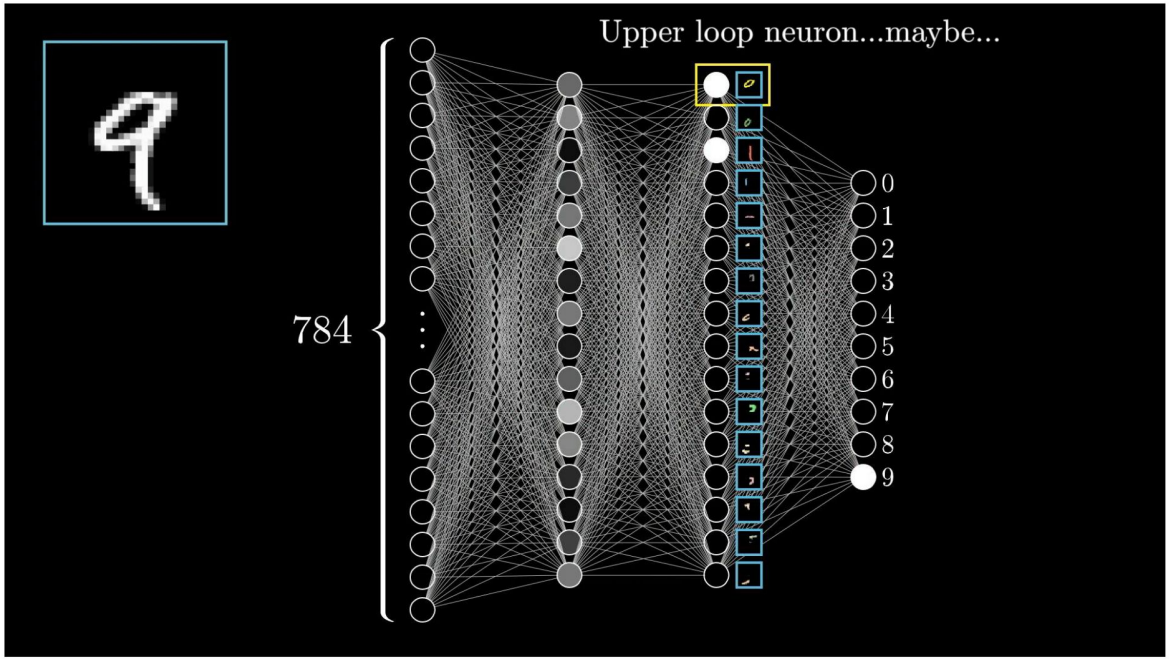
- We can hope that the hidden layers detect basic patterns just as humans break them down in their visual reasoning:





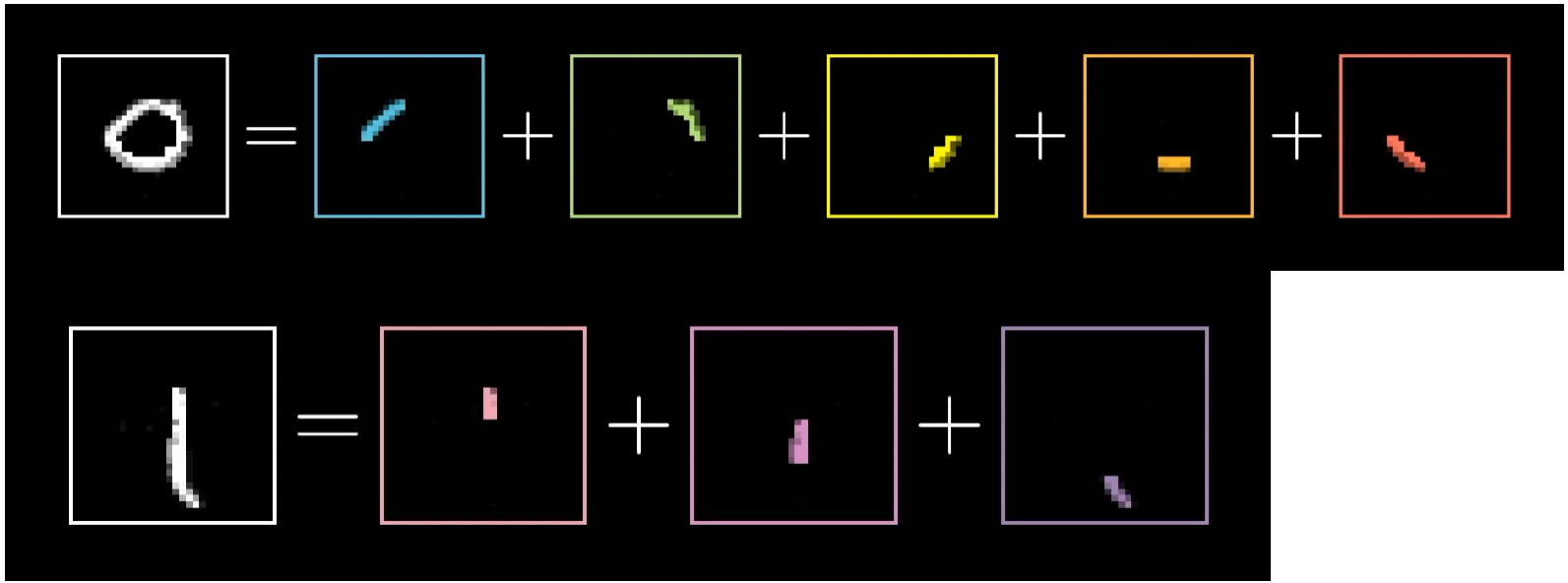
What is the rationale behind the 'layers' of neurons?

- From the last layer to the output layer: what combination of which patterns represents which digit?



But how are these patterns recognized?

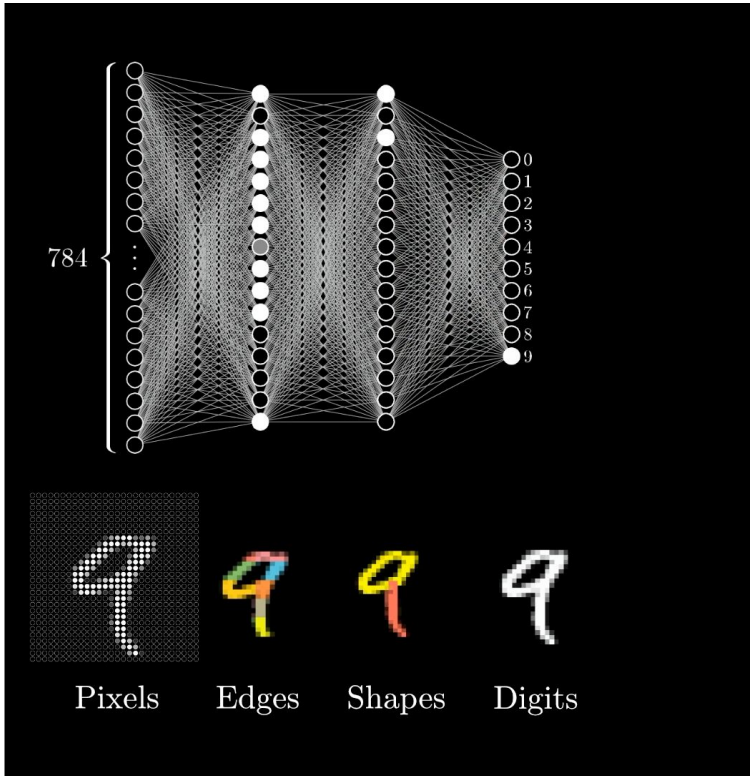
- These patterns (bars, loops, etc.) are further broken down into smaller patterns:



So, we hope that the layers will recognize and reconstruct the patterns:

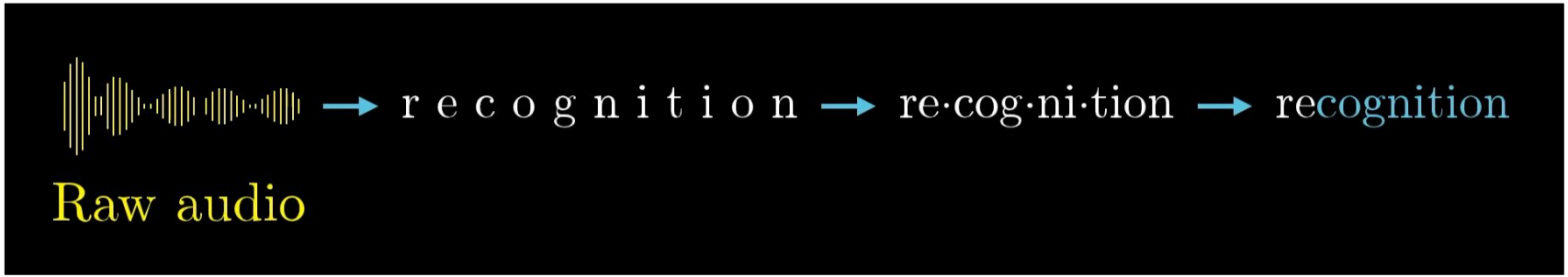
- From the image/input activations, each layer should recognize more complex patterns by combining the activations/patterns from the previous layer, ultimately activating the scores for the digits based on the activated patterns:

- ... but are we capable of doing that with this type of ANN (MLP)?"



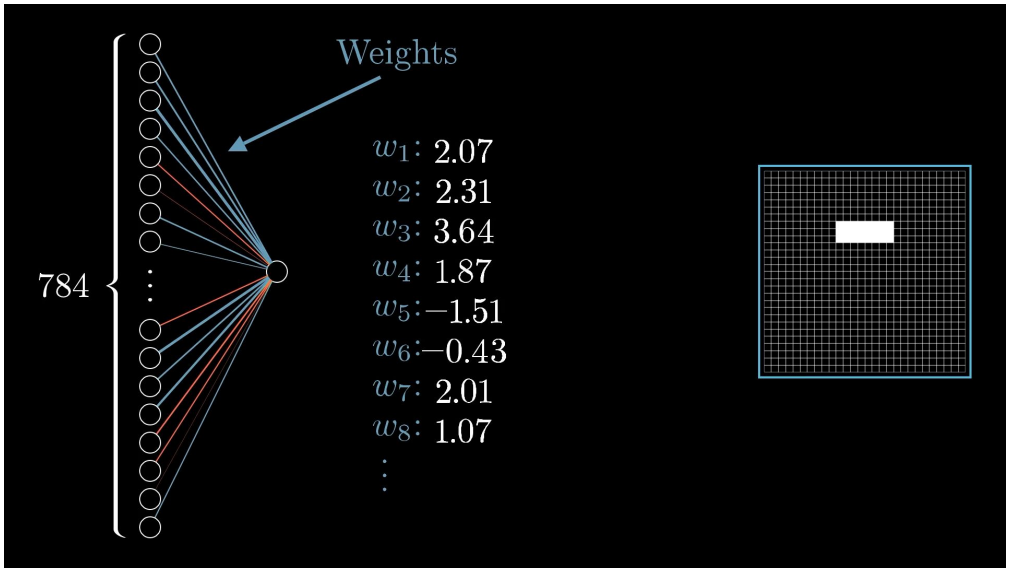
Not just the images.

- The same principle of decomposing the signal into simple patterns for detection and assembly can also be applied to audio:



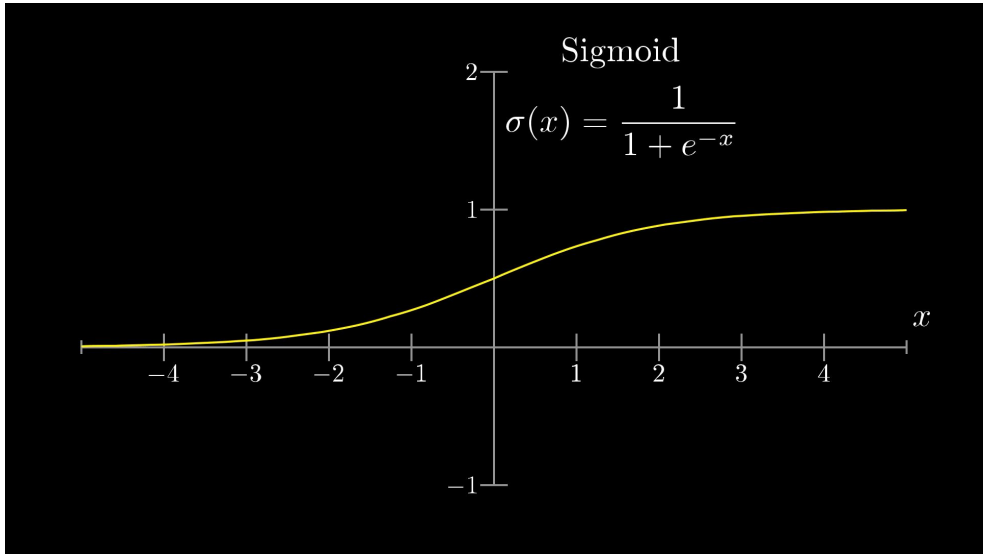
What do the connections do?

- Let's suppose we want to choose the weight to detect a horizontal edge in this area:



A non-linearity for more flexibility.

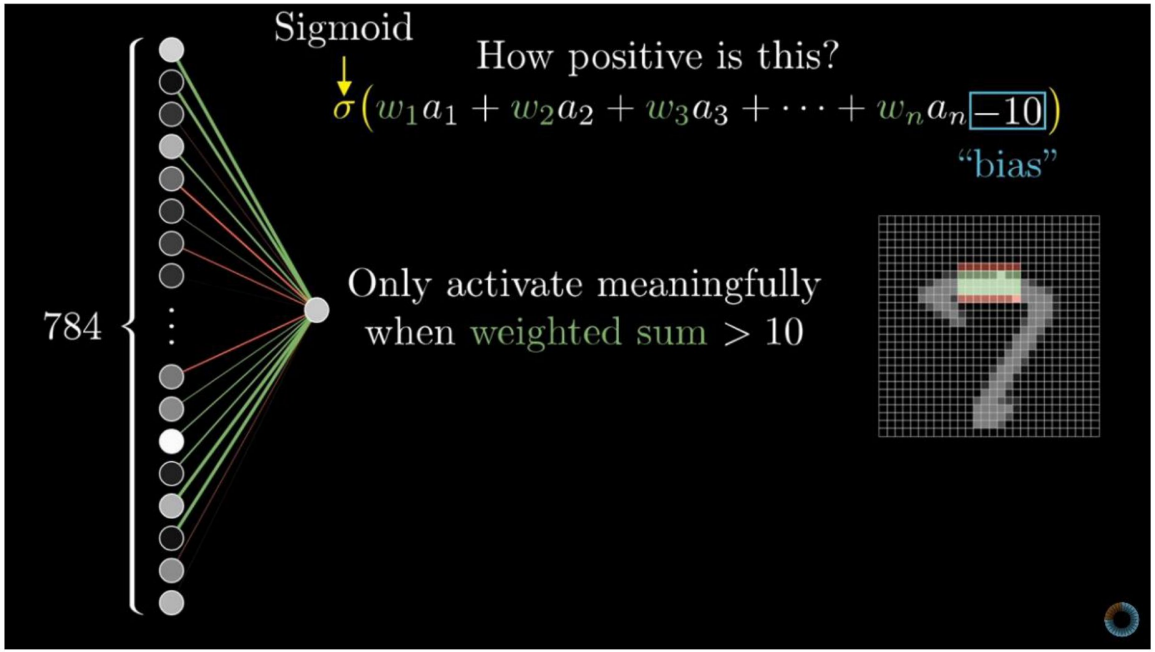
- We keep the activations in [0,1] by using the sigmoid function applied to the weighted sum:



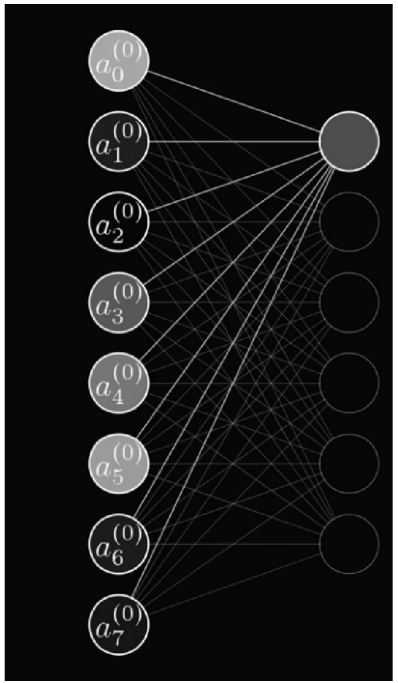
Une introduction douce à la fonction sigmoïde :
https://neuroconnection.eu/une-introduction-douce-a-la-fonction-sigmoide/

And finally, a bias for each neuron

- The bias/polarity activates only when the edge/contour is significant enough:



So, the activation of a neuron is formulated as follows:

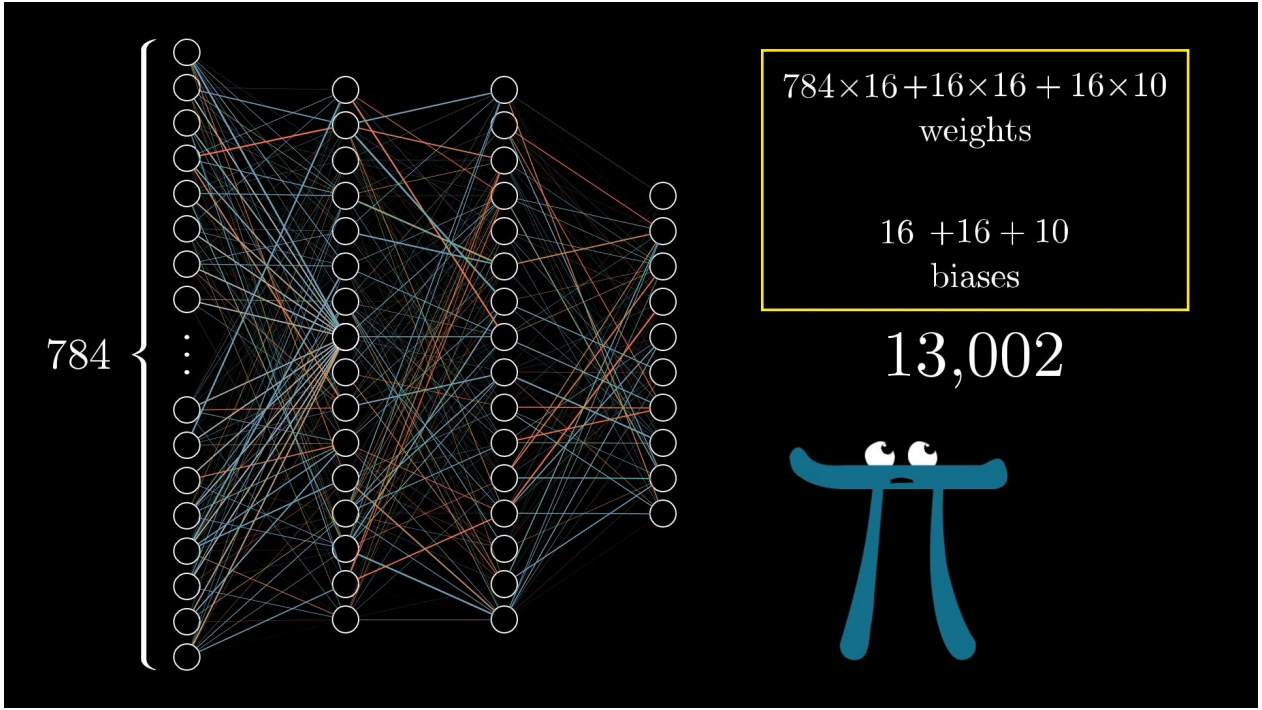


Superscript corresponds to the layer

$$a_0^{(1)} = \sigma\left(w_{0,0}a_0^{(0)} + w_{0,1}a_1^{(0)} + \cdots + w_{0,n}a_n^{(0)} + b_0\right)$$

Subscript corresponds to a neuron in the layer

Now what to do? Choose the parameter values!



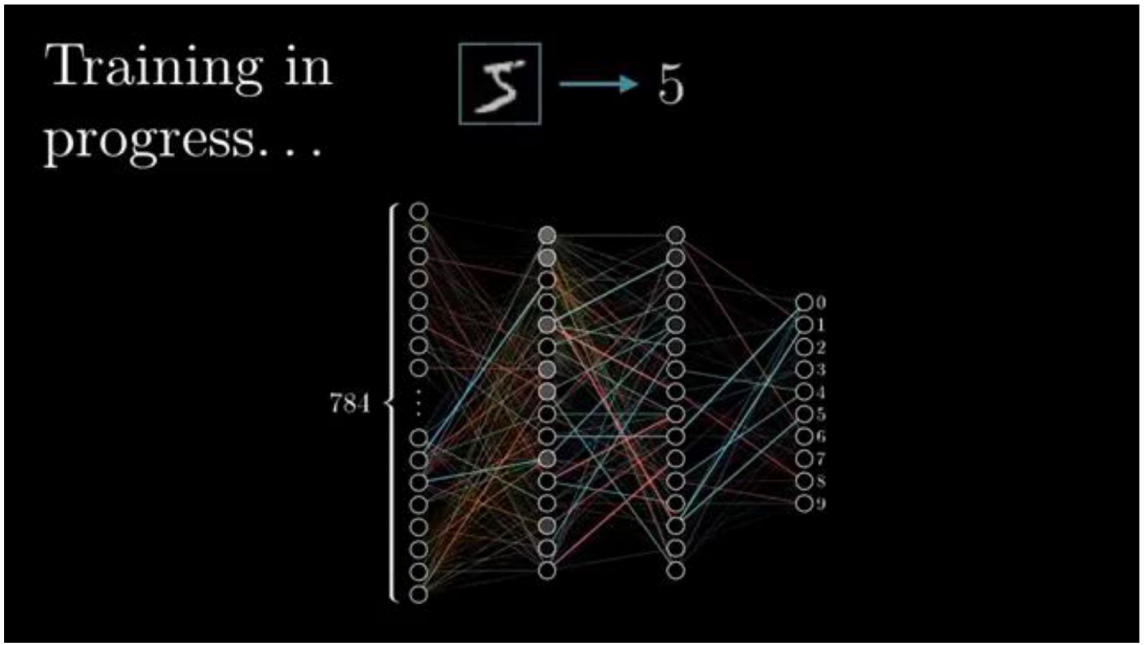
- **Learning** := Finding the weights and biases for each neuron in the chosen architecture.

Your first ANN: a MLP

Learning

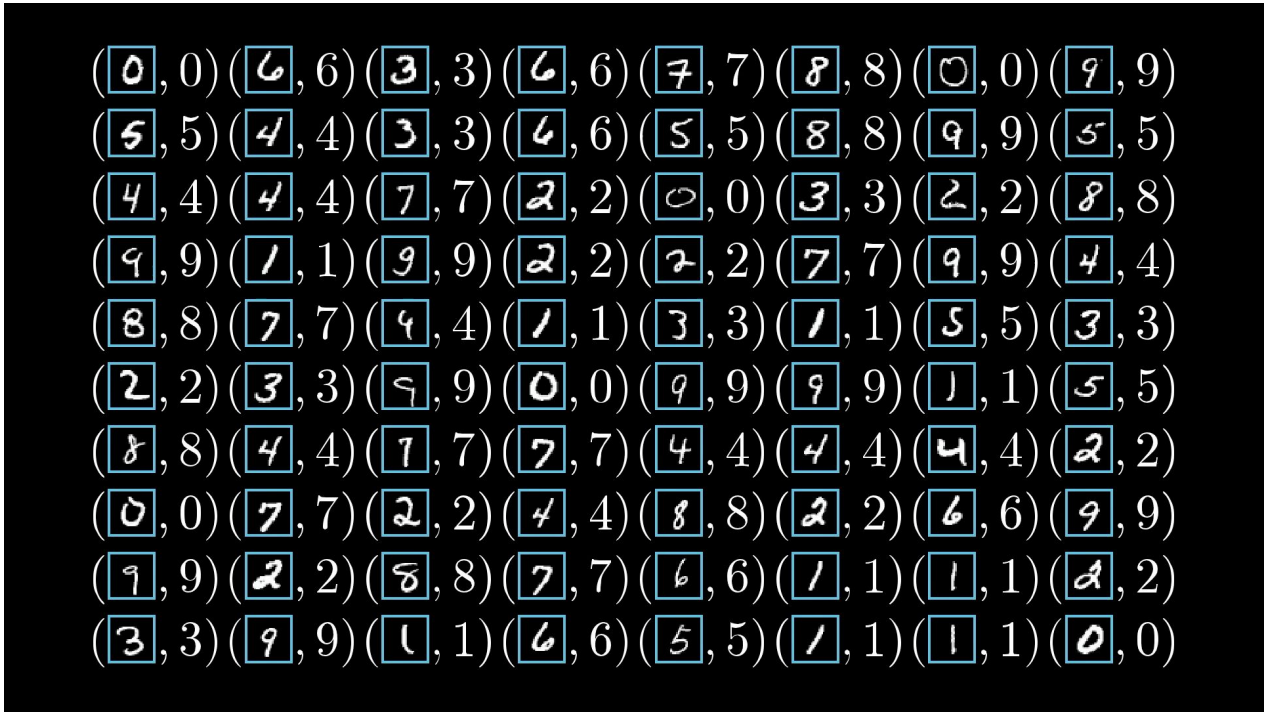
Learning

- Learning consists of adjusting the parameter values to maximize the accuracy of recognition.

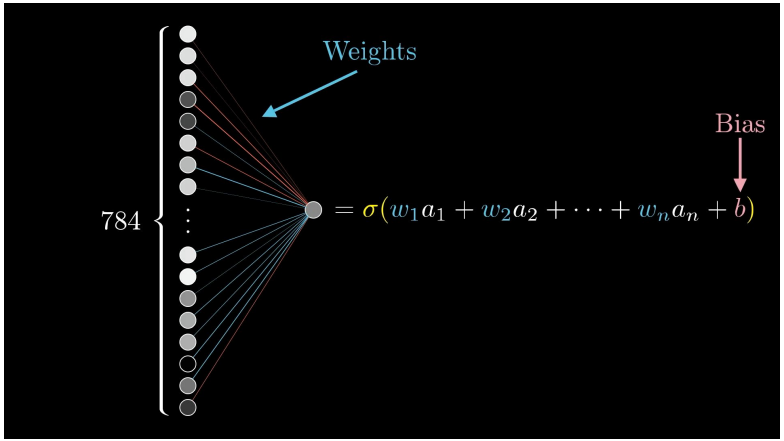


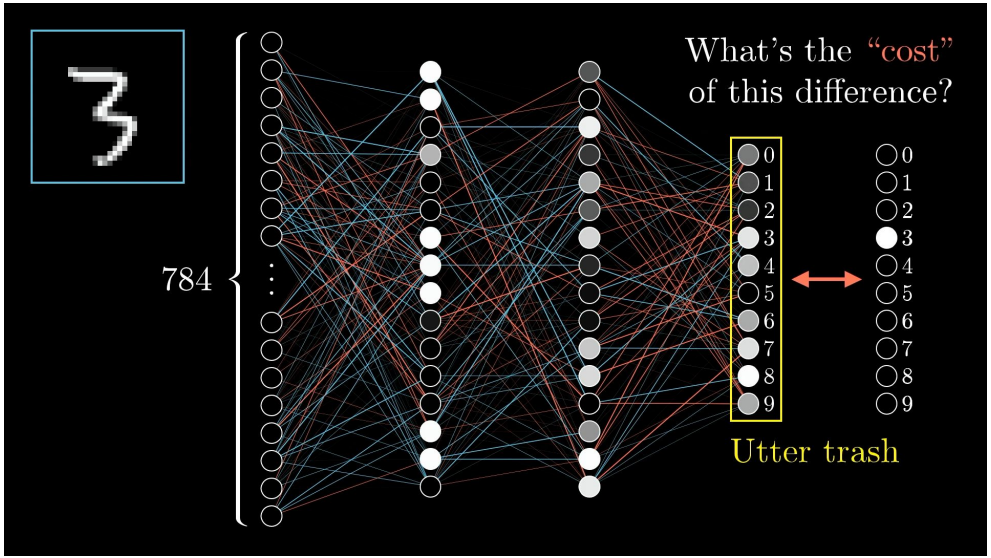
Training on the dataset: MNIST

- A dataset is composed of images and their labels (the corresponding digit).



How to train: Operate the ANN





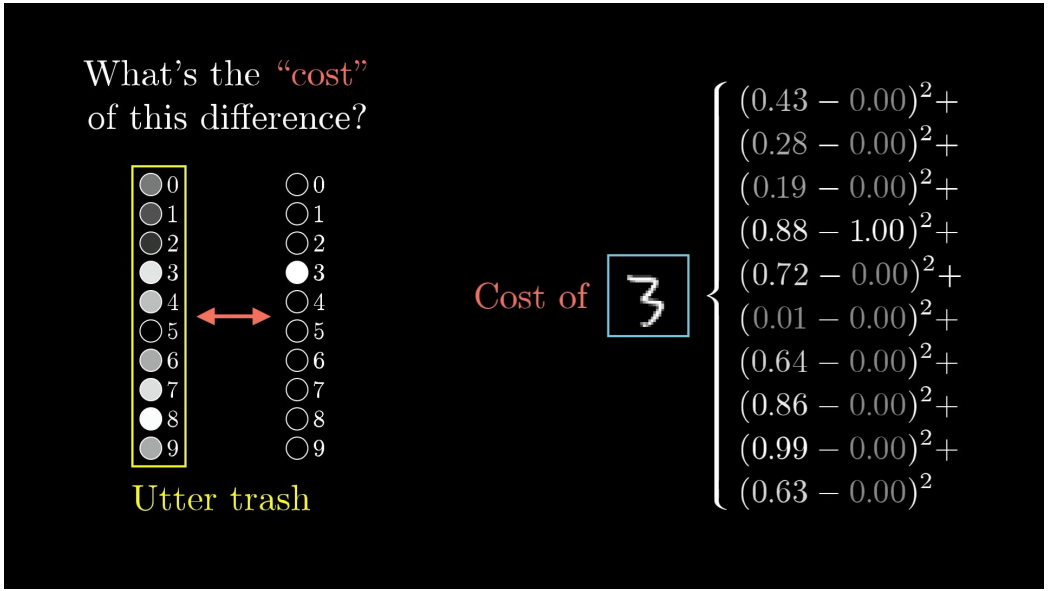
- We need to choose all the values of weights and biases
- First: Initialize the parameters randomly and obtain results

How to train: Compare the results of the ANN to the truth

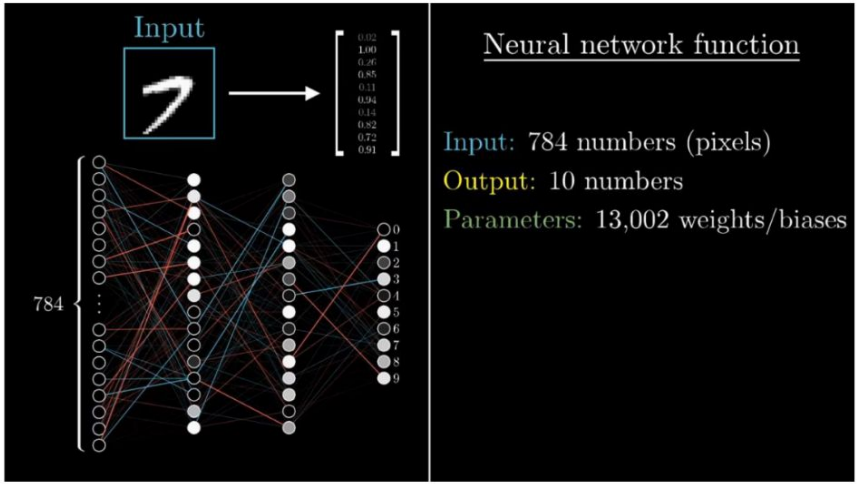
- with ground truth labels

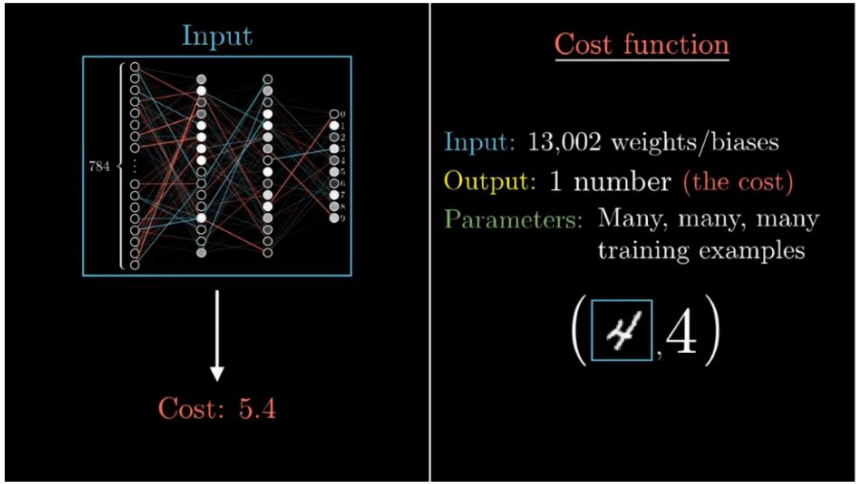
➔ calculate the cost for each training example

- then average the costs for all training examples



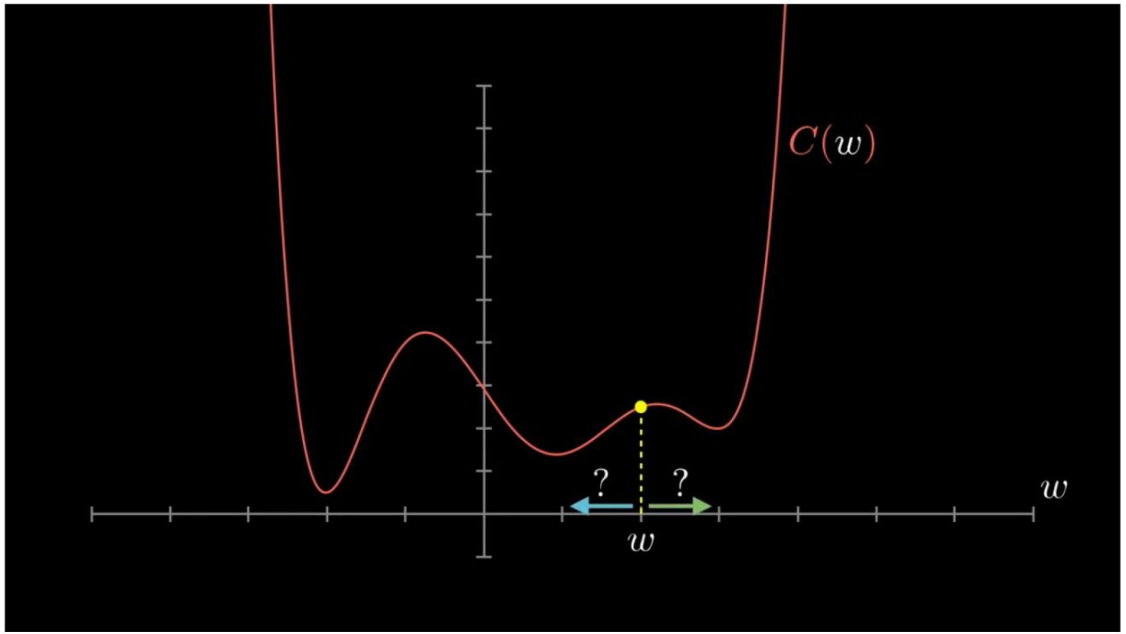
ANN and the cost function



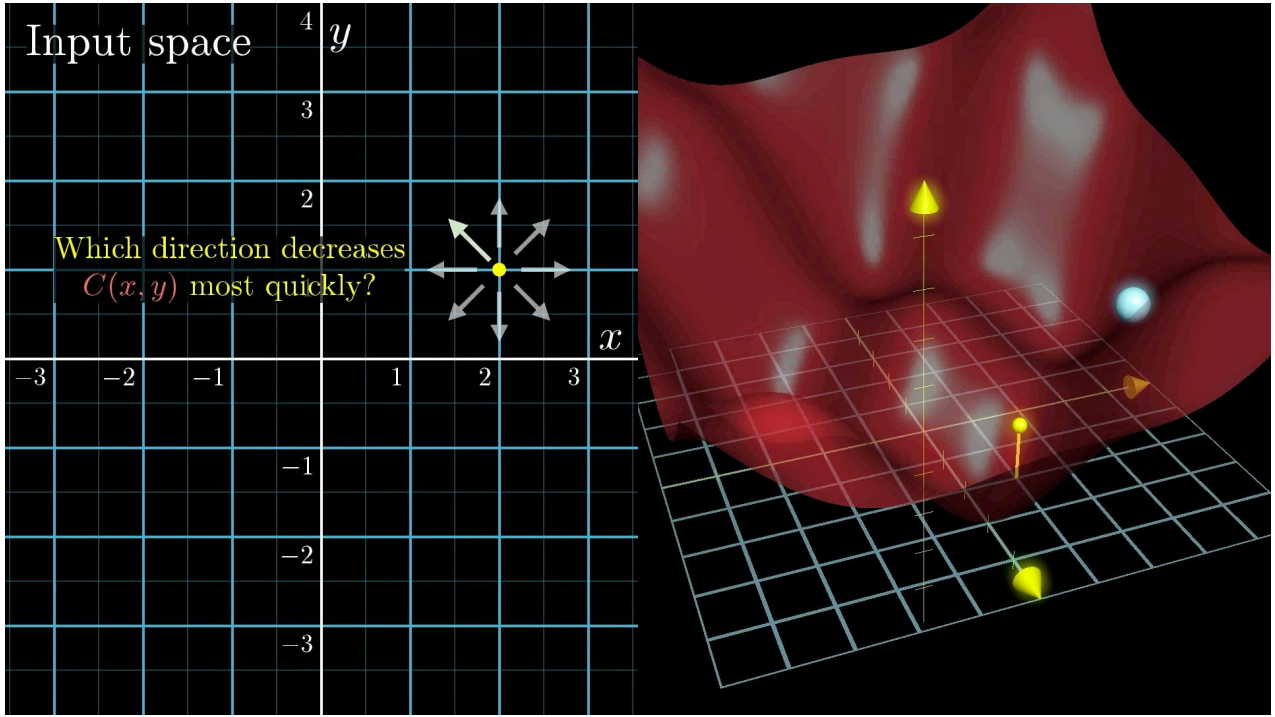


Learning for an ANN is...

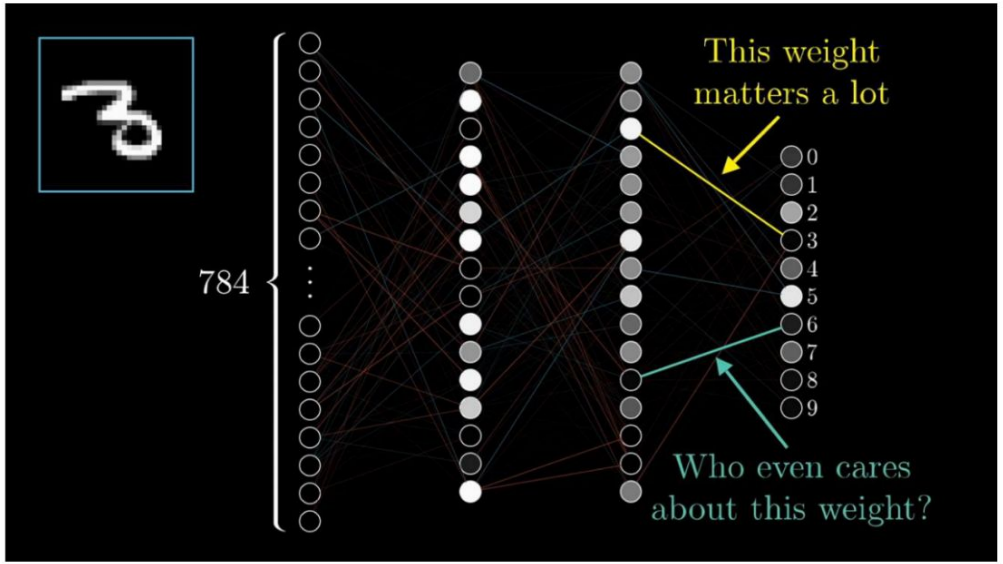
- ...nothing but derivative calculations to minimize a function! (no magic...)



Gradient descent



Weight adaptation



$$\vec{\mathbf{W}} = \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ \vdots \\ w_{13,000} \\ w_{13,001} \\ w_{13,002} \end{bmatrix}$$

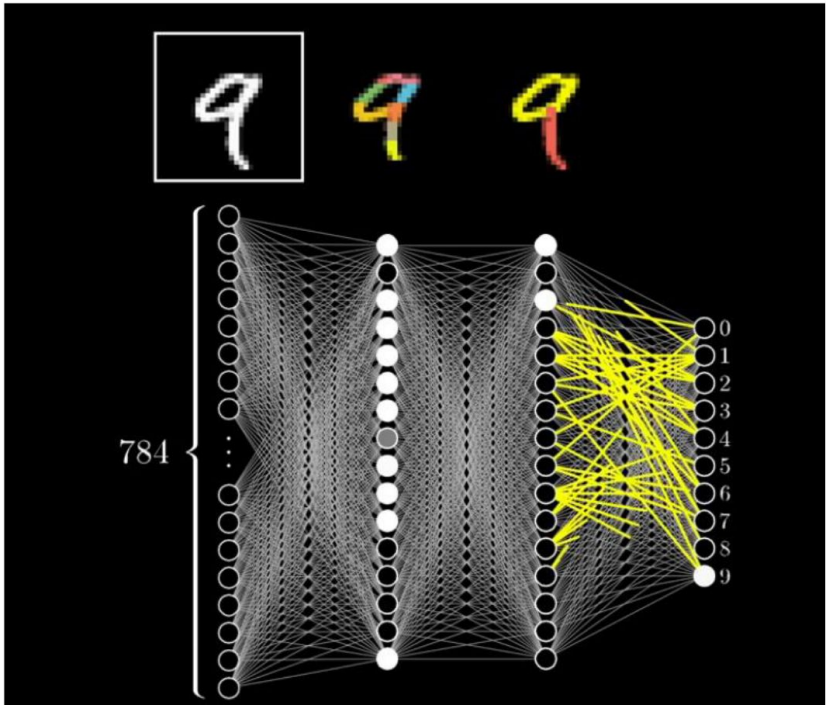
$$-\nabla C(\vec{\mathbf{W}}) = \begin{bmatrix} 0.31 \\ 0.03 \\ -1.25 \\ \vdots \\ 0.78 \\ -0.37 \\ 0.16 \end{bmatrix}$$

w_0 should increase somewhat
w_1 should increase a little
w_2 should decrease a lot

$w_{13,000}$ should increase a lot
$w_{13,001}$ should decrease somewhat
$w_{13,002}$ should increase a little

What do the formed layers do?

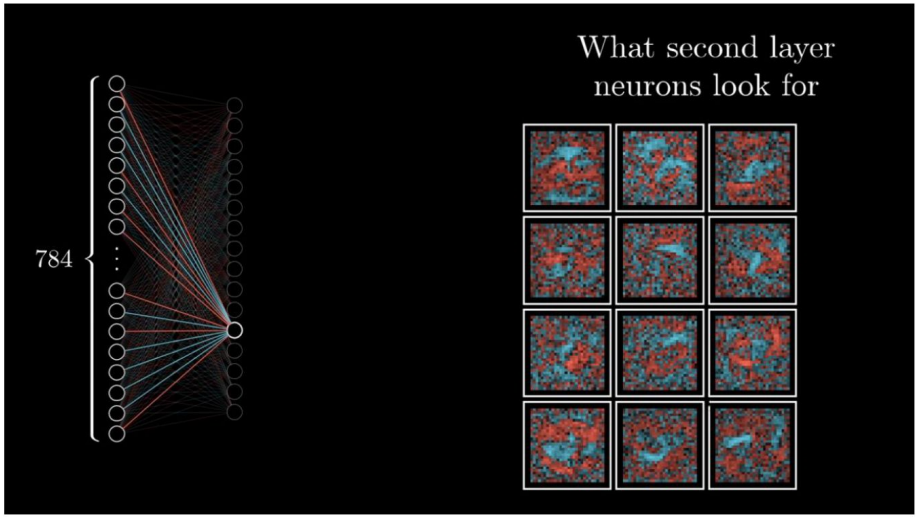
- Does the trained network extract the edges of the pixels, subpatterns of the edges, and patterns of subpatterns to recognize the combinations of patterns for each digit?



What do the formed layers do?

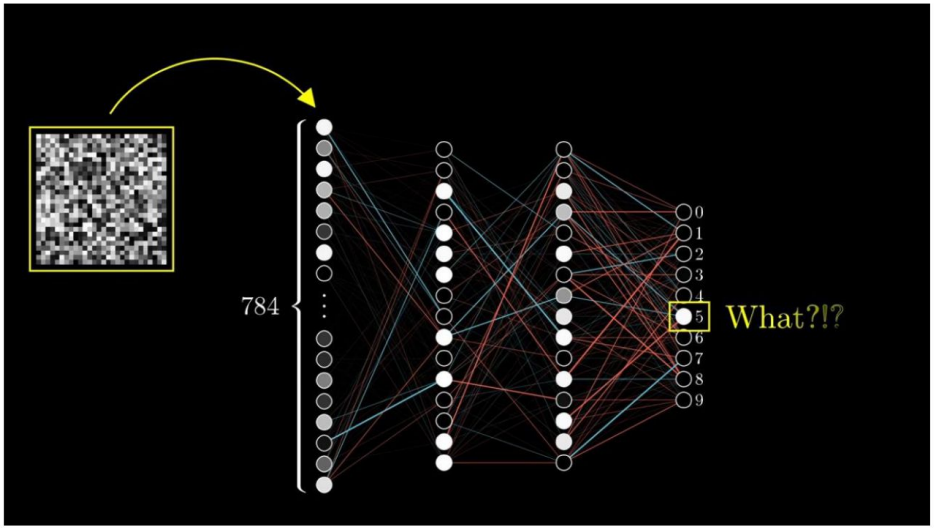
- This type of ANN (MLP) achieves a recognition accuracy of ~96%...

- ...but it doesn't learn as we had expected:



Not what we expected!

- And indeed, it provides a very certain answer when it's completely wrong:



Beyond the MLP: CNN!

- The MLP is an old technology (from the 90s) – it's not deep learning.
- Modern ANN: Convolutional Neural Networks (CNNs are deep).

RNs Advantages

- **Self-learning:** Based on a basic algorithm and a few examples, the algorithm itself decides how to achieve the desired objective.

- **Effective noise filtering in data:** Neural networks can isolate only the information they need from a massive stream of data, ignoring any unwanted noise.

- **Adaptation to change:** The ability to adapt to changes in input data. After a short period of adaptation to changes, they continue to work with the same efficiency.

- **Work speed:** Their work speed is determined by the computing power available to them.

- **Exciting opportunities:** Neural networks operate like the human brain, meaning that once trained, they can perform various tasks in different domains. The key is having a sufficient amount of real or synthetic training data.

RNs Disadvantages

- **The problem of the black box:** Neural networks are often considered "black boxes," making it challenging to understand how and why they arrive at a specific result.
- **Probabilistic nature of responses:** Even a well-trained neural network may not produce definitive results.
- **Development time:** While there are many libraries that can save time and effort when developing artificial neural networks, they are not always applicable.
- **Data quantity:** Training neural networks typically requires much more data than traditional machine learning algorithms.
- **Computationally expensive:** Modern deep learning algorithms based on artificial neural networks can take weeks or even years to learn from scratch.

Your turn !

- Image classification with a MLP !

https://colab.research.google.com/drive/1LJGkhp3ObmT8xq7xEo4kp8BKsQqySyks?usp=sharing