

# ML Primer

Amaru Cuba Gyllensten  
[amaru.cuba.gyllensten@ri.se](mailto:amaru.cuba.gyllensten@ri.se)

Ariel Ekgren  
[ariel.ekgren@ri.se](mailto:ariel.ekgren@ri.se)

# Data



# Det viktigaste: data

För att kunna göra något med maskininlärning krävs det data. Ju mer desto bättre. Detta är både en självklarhet men också något som i praktiken ofta underskattas.

Ju mer högkvalitativ data desto bättre. Men vad är högkvalitativ?

# Exempel på data

Bilder tillsammans med etiketter

Jättemycket fritext

Frågor och svar

E-mail tillsammans med etiketter

```
{  
  "id": 44,  
  "text": "Fiberoptik - Funktionsfordringar på anslutningsdon  
och passiva komponenter - Del 1: Allmänt och vägledning"  
}  
  
{  
  "id": 13,  
  "text": "Japp, då har tiden för den andra decembertävlingen  
passerat och det har kommit in en hel bunt med kreativa och  
fina bidrag!"  
}
```



Källa: <https://cs.stanford.edu/people/karpathy/cnnembed/>

# Hur mycket data?

Datamängder för övervakad inlärning: 1000 exempel

Datamängder för oövervakad inlärning:

KBBert: 22GB text

GPT-3: 570GB text

CLIP: 400 million (image, text) pairs

# Data-kvalité och tillgänglighet

Det är viktigt att datan har bra kvalité för att kunna använda den. Bra kvalite betyder många saker i det här sammanhanget.

- Att det finns tillräckligt många datapunkter
- Om man etiketterar datan, att de som gjort etiketterna har tydliga regler
- Att datan är sammanhängande

# Bias



**Vill vi visa världen som den är  
eller som vi vill att den skall vara?**

# Maskininläring (ML)



# Vad är maskininlärning?

Metoder som **lär** sig lösa problem från **data**.

Exempel:

- Bildigenkänning
- Rekommendationssystem
- Språkmodeller

# Vad är maskininlärning?

Inom matematiken pratar man om funktioner  $f(x)$ .

ML handlar om att lära sig en matematisk funktion mellan data och svar.

Ett svar kan vara till exempel vara en etikett eller ett likhetsmått.

# Vad är maskininlärning?

Matematiken som utgör modern ML är oftast linjär algebra och flervariabelanalys.

# Vad är maskininlärning?

Brukar delas upp i tre fält beroende på datan, problemet och hur dessa relaterar till varandra.

- Övervakad inlärning (Supervised Learning)
- Oövervakad inlärning (Self-supervised Learning)
- Förstärkningsinlärning (Reinforcement Learning)

# Övervakad inlärning

Om man har tillgång till indata och önskad utdata, kan man bygga en modell som lär sig mappningen indata - utdata.

Exempel:

- Bildigenkänning med indata (bilder) och utdata (etiketter), i.e. etiketterade bilder.

Tar ofta formen av klassificering eller regression.

# Övervakad inlärning

Klassificering:

Att givet data försöka mappa det till en av flera fördefinierade klasser. t.ex. sifferigenkänning: Mappa bild till symboler.

Regression:

Att givet data försöka mappa det till en skalär, eller vektor. t.ex. mappa lägenhetsannonser till säljpris.

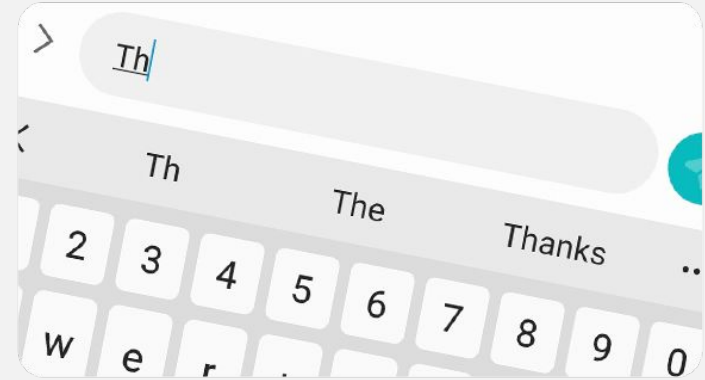
(Notera att klassificering ofta är enklare, då regression kräver antaganden om vad "närhet" är i den aktuella kontexten.)

# Oövervakad inlärning

Om man har tillgång till data och vill finna struktur i datan så som den är.

Exempel:

- Språkmodellering, där datan är text och modellen lär sig att predicera nästa ord.
- Lära sig känna igen egenskaper hos bilder.

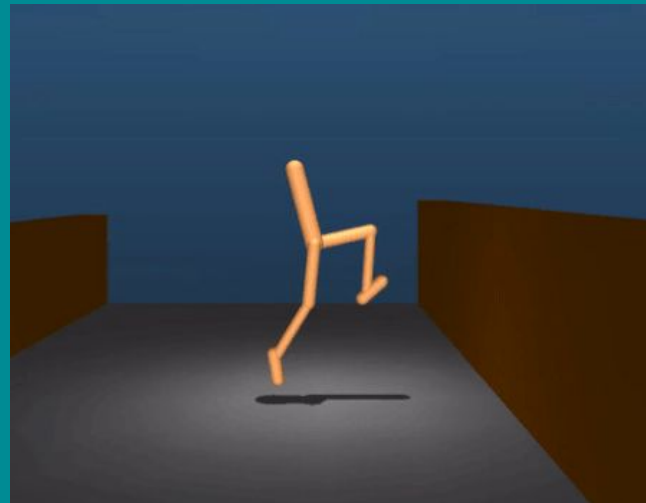


# Förstärkningsinlärning

Om man har svårt att definiera vad som är rätt i stunden men vet ett långsiktigt mål. Till exempel om man har en agent som ska lära sig utföra handlingar i en miljö.

Exempel:

- Spel-AI, där agenter lär sig vilka handlingar som ska utföras i vilka situationer för att vinna.



Källa: <https://deepmind.com/blog/article/producing-flexible-behaviours-simulated-environments>

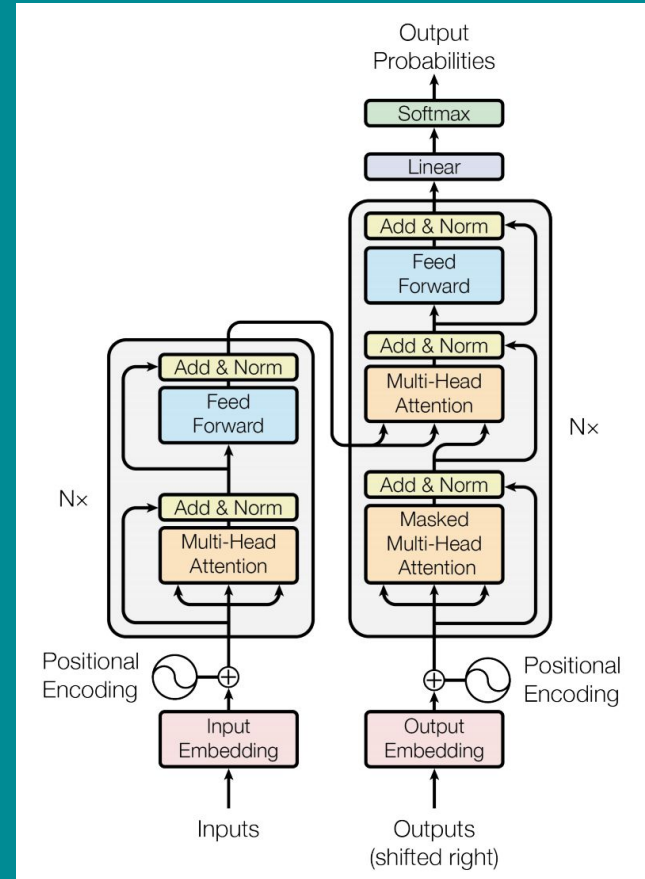


# Neurala Nätverk

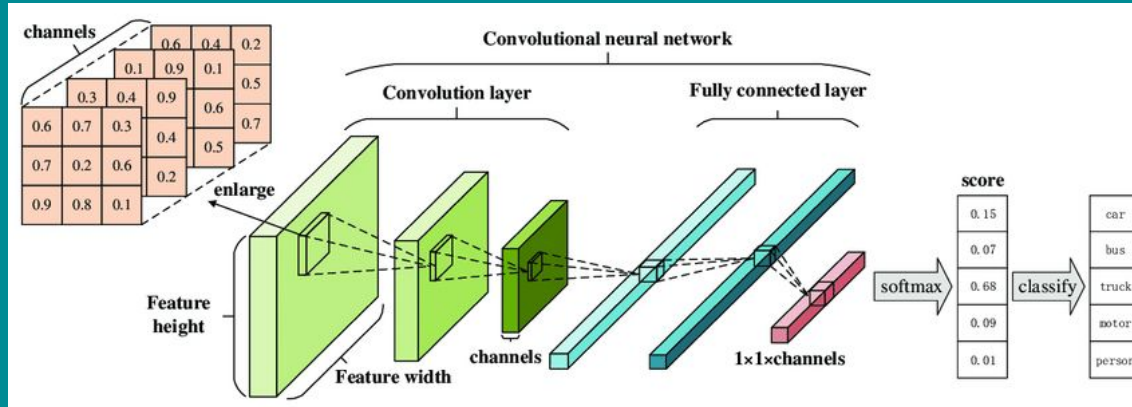
En typ av maskininlärning inspirerad av neuroner. Löser problemet som ett **optimeringsproblem**.

Exempel:

- Bildigenkänning



# Bildigenkänning med Neurala Nätverk



# Loss eller Felfunktion

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i)^2$$

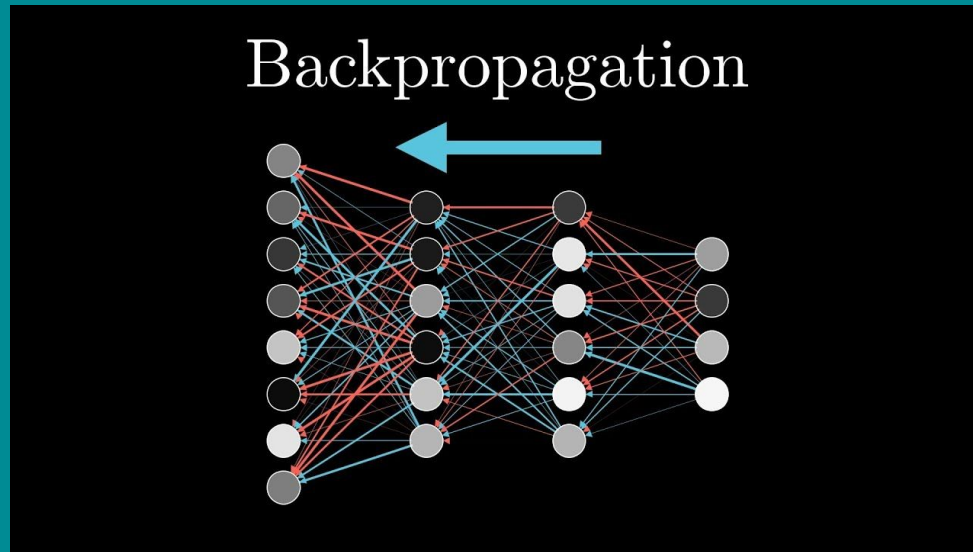
I korthet tränas neurala nätverk genom att hitta en parameterisering som minimerar en "loss", eller felfunktion.

I fallet klassificering ges lossen ofta av cross entropy: ett mått på hur en prediktion (i form av en sannolikhetsdistribution) överensstämmer med verkligheten.

I fallet regression ges lossen ofta av ett avståndsmått mellan det predicerade värdet och verkligheten.

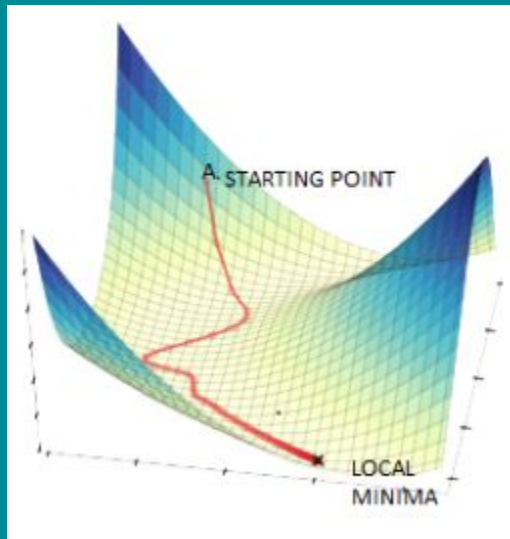
# Backprop

Neurala nätverk är parameteriserade och differentierbara med avseende på dess parametrar. Detta innebär att när man beräknat lossen, kan beräkna gradienten.



# Optimering

Man kan finna parametrar som minimerar lossen genom att uppdatera parametrarna med gradienten.



# Modeller

Det finns väldigt många olika typer av maskininlärningsmodeller. Som alla har olika arkitekturer.

- Multi Layer Perceptrons
- Convolutions nät
- Transformers

# Domäner

Det finns lika många domäner för ML som man kan komma på att applicera ML på.

Text, Ljud, Bild, Tidsserier, Finansiell data, med mera

**Amaru Cuba Gyllensten**

**amaru.cuba.gyllensten@ri.se**

**Ariel Ekgren**

**ariel.ekgren@ri.se**