

HTX Opgaver

Karl Meisner-Jensen

March 21, 2024

Ikke for at flekse, men dokumentet er skrevet i \LaTeX (◡ ◡)

1 Kort Intro

Jeg har lavet disse opgaver lidt ad-hoc. De består af en smule programmering, hvor I skal ind og kigge i den kode jeg har inkluderet i dette repo. Ellers er der også nogle regneopgaver og nogle lidt mere... filosofiske nogle.

Det er som sådan helt op til jer hvilke I bruger, jeg skal ikke være jeres mor eller slavedriver der. I må hjertens gerne springe lidt rundt i dem, det er kun godt! Hvis I har brug for hjælp eller I sidder lidt fast, så endelig hiv en hånd i vejret. Jeg judgeer ikke hvis der var ting man ikke lige fangede eller 100% forstod under fremlæggelsen... det **er** et pisse svært emne at blive smidt nøgen ind i.

Med det sagt, så er rigtigt meget af det af at lære programmering (det kender I vel) og machine learning, at prøve sig frem. Så kig i koden, fuck lidt rundt i den, lav nogle fejl og søg lidt på nettet. Der er næsten **altid** en person klogere end en selv der har siddet med samme problem og løst det eller fået hjælp af en anden til at løse det. Chat-GPT, StackOverflow, Google, jeres sidemakker, jeres lærer, og vinden der blæser er alle værdifulde værktøjer I kan (og virkelig burde!!!) lytte til hver chance I får.

2 Matematik-delen

Dette består primært af regneopgaver der følger op på noget af matematikken jeg introducerede under fremlæggelsen

2.1 Tilbage til Entropi

2.1.1 Entropien af et møntkast

Givet en (uvægtet) mønt som vi slår plat eller krone med, hvordan kan det være entropien af udfaldet er lige præcis 1 bit?

2.1.2 Entropien af en D8

En D8 er en ottesidet terning blandt andet brugt i *Dungeons and Dragons*. Forklar med naturligt sprog hvad entropien er at kaste med sådan en terning.

2.1.3 Den præcise entropi af en terning

En seksidet terning har en meget mærkelig og måske uintuitiv entropi ift. den traditionelle ja/nej spørgsmål beskrivelse. Udregn denne entropi præcist ved hjælp af formlen for entropi i bits givet nedenunder:

$$H(X) = \sum_{i=1}^N p(X = x_i) \log_2(p(X = x_i))$$

HINT: Husk alle er lige sandsynlige når vi slår med en sekssidet terning, dvs. $p(X = 1) = p(X = 2) = p(X = 3) = p(X = 4) = p(X = 5) = p(X = 6) = \frac{1}{6}$

2.1.4 At måle i 'trits', 'dits', eller 'p-bits'

Som det står er der faktisk flere måder at måle information i end bare bits (og, nej jeg snakker ikke om bytes). Heriblandt findes bl.a. *trits* og *dits* som måler det forventet antal spørgsmål med henholdsvis tre forskellige svar eller 10 forskellige svar (husk, en bit som bruger ja/nej spørgsmål har kun 2 svar!).

Med dette i mente, kom med et forslag på en formel for entropien af et udfald målt i trits og dits. Når du har gjort dette, så find et generelt udtryk som gælder for en "p-bit" hvor at p kan være hvilket som helst heltal.

HINT: I skal pille ved logaritmen.

2.2 Udregning af fejl

2.2.1 Manuel udregning af fejl

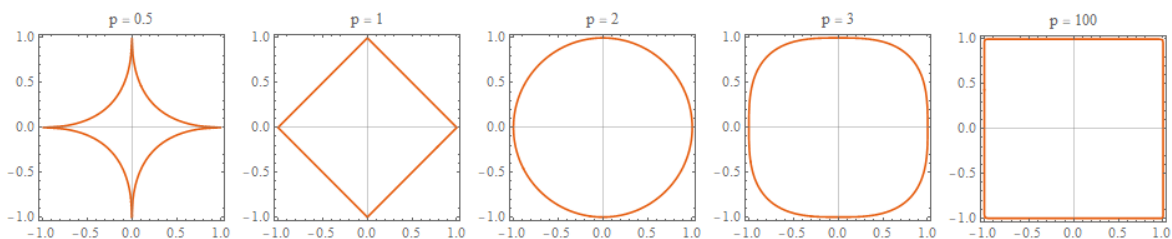
Givet de følgende sande y værdier og estimeret y værdier \hat{y} , udregn fejlen imellem dem som **summen af kvadreret fejl**, som:

$$\mathcal{L}(y, \hat{y}) = \sum_{i=1}^N (y - \hat{y})^2$$

Herefter gør det samme, men find nu den så eftertragtede *Mean squared error*, eller gennemsnitlige kvadreret fejl (her skal I selv finde på, eller grave formelen op)

$$\mathbf{y} = \begin{pmatrix} -3 \\ 7 \\ 12 \\ -5 \\ 0 \\ -15 \end{pmatrix}, \quad \hat{\mathbf{y}} = \begin{pmatrix} -9 \\ -4 \\ 1 \\ 14 \\ -15 \\ 5 \end{pmatrix}$$

2.2.2 "P-normen"



Ok, hold nu fast, for nu bliver det potentielt lidt funky. Basically når vi udregner den kvadreret fejl bruger vi en slags 'bastardized' version af hvad man i matematik kalder en **norm**. Normer er måder at udregne afstanden mellem punkter, vektorer, osv. på. Dette er ufatteligt brugbart i ML, hvor man hele tiden gerne vil måle similaritet mellem forskellige observationer for at komme frem til bedre predictions, lavere loss, osv.

Normalt når vi skal måle afstand, bruger vi den Euklidiske afstand altså en lige linje fra punkt til punkt, givet således:

$$\|x_1, x_2\|_2 = \sqrt{\sum_{i=1}^N |x_{1i} - x_{2i}|^2} = \left(\sum_{i=1}^N |x_{1i} - x_{2i}|^2 \right)^{\frac{1}{2}}$$

Altså, vi trækker hver koordinat fra hinanden, kvadrerer resultatet, og så summer over hvert koordinat. Til sidst tager vi kvadratroden. Omskrivningen vi laver til aller højre, bruger at $\sqrt{x} = x^{\frac{1}{2}}$. Værd at vide, er at denne euklidiske afstand er også hvad vi kalder **L2-normen**, eller sommetider bare **2-normen**

Nu til opgaven: Kig på de plots der er givet i toppen af denne opgave og forklar hvad de viser ift. den euklidiske afstand. Bagefter skal I komme op med en formel for den norm der bruges på hver af disse plots.

HINT: Husk at L2-Normen bruger summen af kvadrater og KVADRATroden, til dens udregning.

Bagefter I har fundet dette, kan I prøve at svare på følgende spørgsmål:

1. Hvordan bliver outliers (punkter med større end normal fejl) behandlet forskelligt af de forskellige normer?
2. Hvornår kan det være smart at bruge noget andet end L2 normen?
3. Hvad sker der med normen når vi lader $p \rightarrow 0$? HINT: Overvej hvordan en L0-norm ville se ud
4. Hvad ville der ske med normen når vi lader $p \rightarrow \infty$?
5. Det viser sig, at der faktisk er nogle meget specifikke krav for hvornår noget er en "sand norm", bl.a. skal det altid være større end 0 (man kan ikke måle "negative" afstande"). Men det skal også overholde **trekantsuligheden**. Find ud af hvad denne er, og sig så noget om hvilke I tror der *ikke* overholder trekantsuligheden.

2.3 Neurale netværk og optimering

3 Programmeringsdelen

Her skal I ind og grave i den kode jeg forhasteligt skrev 4 uger og dagen før jeg kom herind. God fornøjelse. HUSK: Det vigtigste er bare at I skal prøve at forstå noget af hvad der foregår. Jeg forventer ikke at alt sammen bare giver mening

Før I kan køre programmerne, skal I lige igennem disse steps (jeg antager I bruger windows fordi I er nogle plebs, hvis ikke, så undskyld min presumptuousness).

Først, åben en kommandoprompt og skriv følgende:

```
curl https://repo.anaconda.com/miniconda/Miniconda3-latest-Windows-x86_64.exe -o mini
start /wait "" miniconda.exe /S
del miniconda.exe
```

Så burde du gerne have fået et nyt program, søg efter "miniconda prompt" i stifinderen, og åben sådan en, kør følgende kommandoer (i samme folder som du har snuppet fra github):

```
conda create --name htx-torch
conda activate htx-torch
conda install pip
pip install -r requirements.txt
```

Og efter en længere (men ikke den værste) download process, er du flyvende.

3.1 "Whats that clothing??" Starring Neurale netværk

Dette består af to filer ment til at introducere jer til hvordan neurale netværk rent faktisk er programmeret. Det er vigtigt at pointere, at I **ikke forventes at forstå det hele**. Der er meget ved begge scripts der er "black boxet", hvilket er et tema som går meget igen når man arbejder med neurale netværk, simpelthen fordi de er så pokkers svære at få til at fungere effektivt.

3.1.1 'Fashion Mnist' med PyTorch.

Som det første, så så undersøg filen der hedder **mnist_network.py**. Det er en implementation af et *Feedforward Neural Network* (den som jeg nævnte i præsentationen, som er ment til at kunne klassificere forskellige billeder af tøj som den slags tøj de er. Python pakken som bruges hedder *PyTorch* og er nok den mest udbredte måde at definere neurale netværk på nu om dage. Hvis nogen siger I skal bruge *TensorFlow*, så ring til plejehjemmet, da de nok så savner sikkert en undsluppet pensionist.

Anyways, undervejs er der kommentarer som burde forklare det vigtigste. Prøv at svare på følgende spørgsmål:

1. Hvilke funktioner synes PyTorch umiddelbart at filøje til det hele?
2. PyTorch plejer at arbejde med 'tensors' i stedet for matricer - hvorfor tror I at de gør dette?
3. Kan I komme på en funktion til at plotte resultaterne af de predictions der bliver lavet?

3.1.2 Nu med LIGHTNING

Den anden fil, **lightning_mnist_network.py** bruger en pakke der bygger som PyTorch: Lightning. Dette er en måde at undgå at skrive så meget "Boilerplate" (ting man skal skrive hver gang som ikke ændrer sig særligt meget). Her er der som sådan mest kun én opgave: **Hvordan ændrer koden sig fra den normale PyTorch fil?**

4 Cases og filosofi

Dette er spørgsmål af en mere filosofisk/tænkemæssig art hvor det rigtige svar måske bare er ét af mange forskellige. Snak med jeres sidemakre og kom frem til forskellige ting, jeg forventer ikke at I alle bliver helt enige. Jeg har selvfølgelig en løsning jeg synes passer bedst, men fuck det, jeg er bare another guy.

4.1 Karl's højdestudie - En case om statistik



4.1.1 Karl's første forsøg

I denne opgave følger vi Karl (en totalt hypotetisk person) som er en kæmpe kontrol-freak. Udover at være lidt speciel på det punkt, så elsker han også statistik.

Han elsker det så meget, at han faktisk har sat sig for at kende højden af ALLE gymnasieelever i Danmark.

Dog så er Karls kærlighed til statistik kun matched af hans dovenskab... og han gider ikke rigtig måle ALLE gymnasieelever i Danmark. I stedet måler han højden af eleverne i én klasse fra AATG, en med meget programmering fordi det kan han så godt lide. Han udregner så gennemsnitshøjden som følgende:

$$\mu_h = \frac{1}{N} \sum_{i=1}^N h_i$$

Hvor N er mængden af elever i klassen, og h_i er højden af den i 'te elev. Han bruger dette gennemsnit til at sige noget om højden af alle andre gymnasieelever i Danmark.

Nu stiller vi så følgende spørgsmål til Karls metode:

1. Sagt i dagligdagstale, hvordan udregner Karl gennemsnitshøjden af elever i Danmark?
2. Når Karl bruger dette gennemsnit til at sige noget om højden af elever i resten af landet, hvad antager Karl så implicit?
3. Er der noget galt med det estimat Karl får fra gymnasieklassen på AATG?
4. Hvordan kan Karl forbedre det estimat han får?

4.1.2 Karl's Andet forsøg

"Ok, det var faktisk ikke så slemt at måle højden af nogle gymnasieelever" tænker Karl. Så nu måler han **alle gymnasieelever** i **alle gymnasieklasser** i Danmark, og udregner gennemsnitshøjden μ_h som før.

Men det er for et være ærlig, lidt weird, synes Kong Frederik og Mette Frederiksen, så efter at Karl bliver færdig med sin sidste måling, gør de det nu ulovligt at måle højden af gymnasieelever i fremtiden. "Lev Mette, kammerat prut" siger de.

Karl står nu med en gennemsnitshøjde for gymnasieelever i Danmark anno 2024 og har følgende spørgsmål:

1. Når nu en ny årgang af gymnasieelever starter næste år, hvordan kan Karl så sige noget om deres højde?
2. Hvis nu at der viser sig at starte udvekslingsstuderende fra rundt omkring i verden, er Karls forrige målinger stadig relevante for at bestemme deres højde?
3. Mette og Kong F. har jo kun gjort det ulovligt at måle **højden** af gymnasieelever. Er der andre fysiske træk ved dem der kan måles for at finde deres højde?

4.1.3 Karl's tredje forsøg

Det viser sig faktisk at Karls højdestudie var så sejt, at hele staten faktisk vil have ham til at fortsætte... Nu skal han **forudsige** højden af ALLE gymnasieelever, men uden at måle den?? Han er lidt på bar bund, men han har hørt at machine learning er "the shit" så han hyrer nogle top-of-the-line machine learning eksperter (jer) til at hjælpe ham med denne astronomiske opgave.

Fra statens side er I givet lov til at indsamle informationer efter følgende regler:

- I må 50000 datapunkter fra gymnasieelever rundt omkring i landet
- Hver oplysning om en gymnasieelev tæller som ét datapunkt brugt (f.eks. højde og vægt fra én elev ville være to datapunkter)
- ALLE **tilgængelige** oplysninger må tilgås, dvs. CPR-nummer er til rådighed, men ikke nødvendigvis hele det menneskelige genom (det har sundhedsvæsenet i Danmark nok ikke)
- I skal indsamle de samme "features" fra hver unik elev. Dvs. hvis I vælger at indsamle 1000 features fra hver elev, kan I kun have 50 elever...
- Efter studiet skal I forudsige højden af fremtidige elever, her får I alle datapunkter I tidligere har indsamlet om den, **pånær** deres højde (at måle højden på elever bliver ulovligt efter dette studie!!)

Med dette i mente, skal I svare følgende:

1. Hvilke oplysninger vil I indsamle og hvorfor? Husk målet er at bestemme højden af fremtidige elever så langt ud i fremtiden som muligt
2. Hvilket sammenhæng tror I der er mellem jeres valgte oplysninger og elevers højde? Er det lineært, eksponentielt eller noget helt tredje?
3. Hvilke af jeres valgte oplysninger tror I indeholder mest *information*? Dvs. med hvilke oplysninger kan man sige *mest muligt* om alle andre ting om eleven?
4. Hvilken statistisk/machine learning model vil I bruge for at forudsige denne højde? Hvorfor?
5. Ville det i den virkelige verden være etisk forsvarligt at udføre dette studie? Specielt set i lyset af de oplysninger I indsamler?

4.2 Lovgivning om AI og ML



Among eu

Det er ingen hemmelighed at både EU og alle andre lande og stater lige nu, famler efter at lave lovgivning om alt slags ny teknologi. Antag nu, at I er tekniske konsulenter, ansat til at komme med lovforslag ift. regulering af AI og ML til EU-parlamentet.

EU har i dette tilfælde udvist speciel interesse i at løse følgende problemstillinger:

- At scammers kan bruge stemmerne af andre mennesker til at lave opkald for at scam folk
- At begynder ML bliver brugt i diverse krigsværktøjer
- At mange ML modeller ikke har transparens (dvs. man ikke kan bestemme *hvorfor* de kom frem til en given beslutning)
- At der bruges så meget strøm på at træne store sprogmodeller
- At mange kunstnere føler deres værker bliver brugt for at træne store ML modeller der genererer billeder (de mener dette er brud på ophavsretten).
- Mange menneskers job er potentielt i fare for at blive ersattet af ML modeller

Vær ikke bange for at udbrede jeres lovforeslag til andet hvis I føler der er andre problemer der har overset. Husk dog, at hver lovforeslag I kommer med, har potentielt negative konsekvenser for udvikling af teknologi, konkurrenceevne med resten af verdenen, osv. Tænk dette ind i jeres beslutninger.

4.3 Tidsmaskinen lavet af statistikeren



Du er nu givet en tidsmaskine lavet af en gal statistiker. De forklarer du skal bruge den til at ændre noget der skete i verdenshistorien der havde betydning for udviklingen af statistik, machine learning og/eller kunstig intelligens. Det er **lige meget** om du gør det **værre** eller **bedre**, bare at du ændrer noget.

Ydermere præciserer de, at hvis det du gør ikke har relevans for statistik, machine learning og/eller kunstig intelligens, vil du øjeblikkeligt blive desintegreret af tidsmaskinen, så vælg nøje.

Hvad vælger du at bruge denne tidsmaskine til? (De siger for øvrigt at du bliver desintegreret hvis du **ikke** bruger den)