Kunskapskontroll – Teoretiska Frågor

1. Hur är AI, Maskininlärning och Deep Learning relaterat?

AI, Maskininlärning och Deep Learning är relaterade begrepp inom datavetenskap och artificiell intelligens. AI är den övergripande disciplinen som syftar till att skapa intelligenta system, maskininlärning är en gren av AI som fokuserar på att utveckla modeller som kan lära sig från data, och Deep Learning är djupa neurala nätverk för att lära sig abstrakta representationer av data likt hur vår egen hjärna fungerar med neuroner.

1. Hur är Tensorflow och Keras relaterat?

Keras till en del av TensorFlow biblioteket och det standard API för att bygga och träna neurala nätverk. Vi kan tänka på Tensorflow som motorn och Keras som ratten på en bil.

1. Vad är en parameter? Vad är en hyperparameter?

En parameter i sammanhanget med maskininlärning är en variabel som modellen justerar under träningen för att anpassa sig till datan. Å andra sidan är en hyperparameter en inställning som används för att styra inlärningsprocessen eller modellens arkitektur. Dessa värden väljs ofta av användaren före träningen och påverkar hur modellen tränas och generaliserar till nya data.

1. När man skall göra modellval och modellutvärdering så kan man använda ett tränings, validerings och test data. Förklara hur de olika delarna kan användas.

När man skall göra modellval och modellutvärdering så kan man dela upp datamängden i tre delar för att ha en tydlig struktur för modellträning och utvärdering. Träningsdatan används för att träna modellen genom att anpassa dess viktningar och biaser baserat på förekomsten av olika mönster i data. Valideringsdatan används för att finjustera modellens arkitektur och hyperparametrar för att förbättra dess prestanda. Till slut testas modellen på testdatan för att bedöma dess prestanda på oberoende data och säkerställa att den kan generalisera väl.

1. Förklara vad nedanstående kod gör:

En bild som visar text, Teckensnitt, skärmbild

Automatiskt genererad beskrivning

Beräknar antalet kolumner (funktioner) i träningsdatan X\_train. Skapar en sekventiell modell, vilket innebär att lagren är ordnade i en linjär sekvens. Lägger till ett Dense-lager med 100 noder och ReLU-aktiveringsfunktion. Input-shapen specificeras baserat på antalet kolumner i data. Den ReLU-aktiverade funktionen hjälper till att undvika "vanishing gradient" och ökar modellens träningseffektivitet. Lägger till ett Dropout-lager med en dropout-frekvens på 20%. Detta hjälper till att förhindra överanpassning genom att slumpmässigt inaktivera noder under träningen. Lägger till ett ytterligare Dense-lager med 50 noder och ReLU-aktiveringsfunktion. Lägger till ett output-lager med en nod och sigmoid-aktiveringsfunktion. Sigmoid-aktiveringsfunktionen används för att generera sannolikheter för binär klassificering, där resultatet ligger mellan 0 och 1. Kompilerar modellen med Adam-optimeraren och binär korsentropi som förlustfunktion. Målet med optimeringen är att minska förlusten under träningen, medan noggrannhetsmetriken används för att utvärdera modellens prestanda.

Skapar en tidig stoppning monitor som avbryter träningen om valideringsförlusten inte minskar efter 5 på varandra följande epoker. Tränar modellen på träningsdatan med 20% av data som valideringsdata. Träningen utförs under högst 100 epoker, med tidig stoppning för att förhindra överanpassning och optimera modellens prestanda.

1. Vad är syftet med att regularisera en modell?

Syftet med att regularisera en modell är att förbättra dess generaliseringsförmåga och förhindra överanpassning (overfitting). Man kan tillämpa olika regulariseringstekniker gör modellen bättre på att hantera nya, osedda data. Dessa tekniker hjälper till att skapa mer effektiva modeller som presterar bra både på träningsdata och på nya data.

1. ”Dropout” är en regulariseringsteknik, vad är det för något?

Dropout används för att förhindra överanpassning. Detta leder till att neuronerna tvingas till att ”lära sig själva” och inte ”samarbeta” (co-adaptations).

1. ”Early stopping” är en regulariseringsteknik, vad är det för något?

Vi kan kolla på en modells valideringsfel för att tillämpa regularisering. När valideringsfelet slutar minska i ett visst antal epoker så med patience kan vi stoppa träningen.

1. Din kollega frågar dig vilken typ av neuralt nätverk som är populärt för bildanalys, vad svarar du?

Convolutional Neural Networks (CNN).

1. Förklara översiktligt hur ett ”Convolutional Neural Network” fungerar.

Först identifieras ”low-level features” såsom enklare former och färger. Dessa enkla egenskaper kombineras därefter för att skapa ”high level features” såsom delar av ögon, mun och dylikt. Egenskaperna modellen hittar påverkar slutligen vår prediktion om det. Modellen använder ”convolutional layers” ofta i kombination med ”pooling layers”.

1. Din vän har ett album med 100 olika bilder som innehåller t.ex. tennisbollar och zebror. Hur hade han/hon kunnat klassificera de bilderna trots att han/hon inte har någon mer data att träna en modell på?

Att använda data augmentation är ett bra steg när man har ett begränsat antal bilder, som de 100 bilderna i detta fall. Man kan generera "ny" träningsdata genom att ta den befintliga träningsdatan och förändra den på olika sätt, såsom rotering, spegling, zoomning och skjuvning (Tensorflow, n.d.). Det är ett effektivt sätt att öka datamängden och förbättra modellens prestanda. Men det är bäst att ha tillgång till så mycket varierande data som möjligt för bästa resultat.

1. Vad gör nedanstående kod?

En bild som visar text, Teckensnitt, skärmbild, linje

Automatiskt genererad beskrivning

Denna kod sparar en Keras-modell till en HDF5-fil med namnet 'model\_file.h5' på hårddisken. Sedan laddar den samma modell från filen 'model\_file.h5' och lagrar den i minnet under variabeln my\_model.

1. Deep Learning modeller kan ta lång tid att träna, då kan GPU via t.ex. Google Colab skynda på träningen avsevärt. Läs följande artikel: <https://blog.purestorage.com/purely-informational/cpu-vs-gpu-for-machine-learning/> och skriv mycket kortfattat vad CPU och GPU är.

CPU (Central Processing Unit) är datorns huvudprocessor som hanterar sekventiella beräkningar och allmänna datorprogram. GPU (Graphics Processing Unit) är specialiserad på parallella beräkningar och används främst för grafikrendering, men den har även blivit viktig för maskininlärning och djupinlärning tack vare sin förmåga att bearbeta stora datamängder parallellt.