atheneum Dendermonde

AI dankzij machine learning en neurale netwerken

Kennis- versus datagebaseerde systemen

Om AI in te zetten voor een bepaald probleem, wordt informatie over dat probleem aan de computer gegeven. Vervolgens verwerkt het AI-systeem deze informatie en komt er een *output*.

Er zijn twee types AI-systemen:

- **Kennisgebaseerde** (of regelgebaseerde) AI systemen, die met regels worden geprogrammeerd. Dit houdt in dat men de kennis van menselijke experts zoveel mogelijk in regels probeert te gieten.
- **Datagebaseerde** (of lerende) AI systemen, die met lerende algoritmes worden geprogrammeerd en ook ***machine learning*-systemen** worden genoemd. Met statistische methodes worden patronen in relevante data opgespoord en dan gebruikt om nieuwe problemen op te lossen.

Wat is een machine learning model?

Bij *Machine Learning* (ML) gaat men vooral proefondervindelijk te werk, maar op een wiskundig onderbouwde manier, en gebruikmakend van principes uit de wiskundige statistiek (Chollet, 2018). (zie ook What is Machine Learning?)

Een mens ontwikkelt het AI-systeem. In dat systeem verwerkt hij parameters waarvan de waarden nog niet vastliggen. Gedurende de **training** leert het **systeem**, d.w.z. dat het systeem a.d.h.v. **een lerend algoritme** op zoek gaat naar de optimale waarden voor die parameters. Na de training zijn deze waarden bepaald en beschikt men over **een machine learning-model**: een machine learning-systeem dat klaar is voor gebruik.

Een machine learning-systeem verwerft met lerende algoritmes kennis uit data met de bedoeling uitkomsten te kunnen voorspellen betreffende nieuwe data.

- De nieuwe data moeten wel gelijkaardig zijn aan de aangeboden data.
- Deze voorspellingen worden gedaan met een bepaalde zekerheid. Zulke machine learning-modellen zullen dus nooit honderd procent accuraat zijn.

Lerende algoritmes zijn algoritmes waarbij het machine learning-systeem zelf gaandeweg aanpassingen doet aan de aanwezige parameters tijdens het leerproces, om geleidelijk aan te komen tot betere prestaties.

Een machine learning-model neemt zijn beslissingen dus niet op basis van vooraf in detail geprogrammeerde instructies. De beslissingen van een machine learning-model

worden **voorspellingen** genoemd. Voorspellen betekent bijvoorbeeld dat er uit voorbije tendensen cijfers voor de toekomst gegenereerd worden (**regressie**) of dat een object bij een bepaalde categorie (klasse genoemd) wordt ingedeeld (**classificatie**).

Hoe wordt een Machine Learning-model getraind?

Voorbeeld:

Stel dat men een spamfilter wilt trainen. Een spamfilter moet e-mails die spam zijn, leren onderscheiden van e-mails die geen spam zijn. Zo'n machine learning-systeem wordt getraind aan de hand van een zogenaamde gelabelde trainingset: een groot aantal e-mails waarbij vermeld wordt of ze spam zijn of niet. Na de training heeft men een model ter beschikking om nieuwe e-mails te beoordelen als zijnde spam of geen spam. Dit model zal niet perfect zijn. Er zullen nog steeds spam e-mails door de mazen van het net glippen en sommige e-mails zullen onjuist in het spampostvak terechtkomen.

Hoe verloopt zo'n training?

Bij het begin van de training kiest het algoritme willekeurige waarden voor de parameters van het systeem. Het is dus niet verwonderlijk dat het netwerk initieel niet goed presteert. Gedurende de training past het algoritme de waarden van de parameters aan, gebaseerd op de gelabelde voorbeelden, en verbeteren de resultaten.

De wiskundige algoritmes die gebruikt worden voor de training van machine learning systemen, worden samen gebracht in deep learning-modellen voor taken zoals regressie en classificatie. De **convolutionele diepe neurale netwerken** zijn uitermate geschikt om objecten te herkennen. (zie ook EDUbox Artificiële Intelligentie: Hoe werken neutrale netweren?)

Model voor objectherkenning vs generatief model

- Een **model voor objectherkenning**, een classificatiemodel dus, zal aan een bepaalde afbeelding een label toekennen, bv. hond. Een classificatiemodel dat een label voorspelt, zal kijken van welk label het het meest zeker is voor een gegeven afbeelding.
- Een model dat afbeeldingen genereert, een **generatief model** dus, zal een afbeelding genereren die beantwoordt aan een gegeven label. Als zo'n model geleerd heeft wat de kenmerken zijn van een hond, dan kan het een afbeelding van een hond genereren die niet in de trainingset zit. Een generatief model zal kijken van welke afbeelding het het meest zeker is voor het gegeven label.

Wie meer wil weten en zelf een neuraal netwerk wil trainen, verwijzen we buiten deze lescontext door naar deze website: learning-path | Dwengo: supporting teachers worldwide!

Gebaseerd op de bron: https://dwengo.org/kiks/ - leerpad artificiële intelligentie