

Moderne informasjonsteknologi

Pål Grønås Drange (Pål.Drange@uib.no)

15 februar 2021

Universitetet i Bergen

Matematisk- og naturvitenskapelig fakultet

Institutt for Informatikk

Et innlegg for Equinor Seniorklubb Bergen

Kjapt om foredragsholder

Pål Grønås Drange

- 2004 – Fagbrev elektronikk
- 2009 – Grunnfag i kognitiv vitenskap
- 2012 – Hovedfag i logikk/kunstig intelligens
- 2015 – Doktorgrad i algoritmer, informatikk
- 2016 – Seniorprogramvareutvikler IT, Statoil (GBS IT SI)
- 2018 – Fagleder programvareutvikling IT-fagnettverk, Equinor
- 2020 – Førsteamanuensis algoritmer, Universitetet i Bergen



Forbehold

Ingen vesentlig forbehold eller interessekonflikter.

Forsker på algoritmer

- rent teoretisk, i kombinatorisk/diskret matematikk.

Underviser om algoritmer

- Algoritmer er grunnlag for programvareutvikling, foreleser dette.

Dagens plan

Agenda

1. Innledning
 - 1.1 Hva er en algoritme?
 - 1.2 Hva er maskinlæring?
 - 1.3 Hva er kunstig intelligens?
2. Gjør algoritmer noe bra for oss?
3. Utfordringer i den algoritmiske tidsalder
 - 3.1 Manglende «forklarbarhet»
 - 3.2 Fordommer
 - 3.3 Falske nyheter
 - 3.4 Overvåking
4. Mitigerende tiltak
 - 4.1 Kontinuerlig læring
 - 4.2 Nysgjerrighet og tvil
 - 4.3 Personlig datasikkerhet

Hva er en algoritme?

Hva er eksempler på algoritmer i verden?

Konkrete eksempler på algoritmer?

- Trafikklys og biler, luftfart og fly, båttrafikk og skip, ...
- Bestillingssystemer, journalsystemer, finans
- Medisinsk utstyr, smart-klokker, andre «wearables»
- Enorme mengder simulering og optimering
- Annonser på nett (selvsagt)
- Alle «dingser» med knapper og skjermer
- ...

1. alt i verden er digitalisert nå

Livene våre:

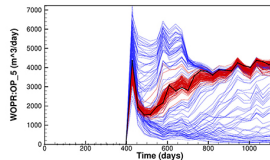
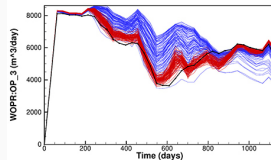
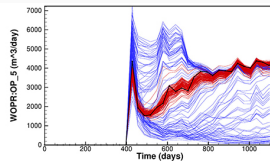
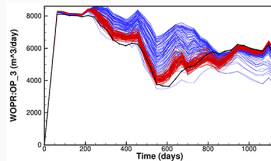
- Stå opp (digitale alarmer)
- Lage kaffe med espresso-maskin
- Komfyr og mikrobølgeovn
- TV, radio, internett, mobiltelefon
- Biler, el-sparkesykler
- Buss, bane, tog
- ...

Livene våre og sivilisasjonen er dikterte av algoritmer

2. enkf : oljedirektoratets pris for økt utvinning

Fra Equinor:

- EnKF — Ensemble Kalman Filter (statistisk algoritme)
- Vant oljedirektoratets pris for økt utvinning
- Involvert i enhver avgjørelse vedr brønner, vedlikehold og utbygging (Ert / FMU)



Hva er en algoritme? Hva er maskinlæring?

Algoritme:

Du forteller *hvordan* noe skal gjøres

Algoritmisk fremgangsmåte:

matematikk, logikk og «regelbasert intelligens».

Et dataprogram:

Et «grensesnitt» for mennesker eller andre programmer som består av en samling algoritmer.

Fordelen med automatisering: Kan gjøre ting millioner av ganger, «reproduserbart».
Færre feil enn mennesker.

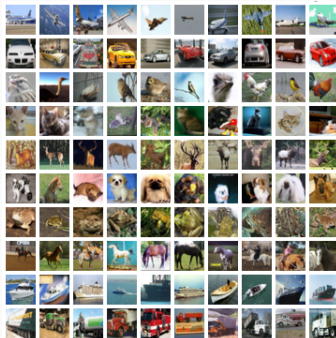
Hva er en algoritme? Hva er maskinlæring?

Algoritmer: Logiske. Matematiske. Forutsigbare. «Enkle.»

Fordeler ved algoritmer: Enkle greier

Men fortell meg hva som er forskjellen på et bilde av en hund og en katt

Tilnærmet umulig oppgave: Regler og logikk er ikke nok.



Hva er en algoritme? Hva er maskinlæring?

Algoritme: Du forteller *hvordan* noe skal gjøres

Maskinlæring: Du forteller *hva* som skal gjøres
ut kommer en algoritme i form av en «svart boks»

Eksempler

- Gjenkjenning av tekst i bilder (håndskrift, bilskilt, etc)
- Gjenkjenning av tale, bilder, feilstaving
- Medisinske og mekaniske bilder og data
- Kriminelle handlinger (finans), ugyldige transaksjoner
- Gjenkjenne søppelepost og svindelforsøk

(Mønster)-gjenkjenning er nøkkelordet.



Hva er en algoritme? Hva er maskinlæring?

Algoritme: Du forteller *hvordan* noe skal gjøres

Maskinlæring: Du forteller *hva* som skal gjøres

Maskinlæring er kort fortalt:

- En algoritme
- Generert fra store datamengder
- Ved bruk av statistikk

Hva er kunstig intelligens?

Kunstig intelligens: Større systemer av maskinlæring, algoritmer og statistikk

- Begynte på 60-tallet
- ... forskere trodde det skulle være «løst» på 10 år
- Regelbaserte («hvis ditt gjør datt»)
- ... det viste seg å være svært feil
- I dag stort sett *statistiske modeller satt i system*

Hva er kunstig intelligens?

Eksempler på kunstig intelligens:

- Selvkjørende biler og fly
 - Sensorer: radar, lidar, kamera, infrarøde kamera, lyd
 - Lokasjon: Kart, GPS, og snakker med andre biler
 - Bildegjenkjenning: Finn mennesker, dyr, andre biler, fotballer, trafikkskilt
 - Navigasjon: Søk i kart, oppslag i trafikkdata
- Hjemmeautomasjon: Alexa, Google Nest, Siri
 - Stemmegjenkjenning
 - Oversetting
 - Netthandel
 - Musikk
 - Nyheter
- Anbefalinger: Google søk, Amazon, Netflix, Twitter, Pandora, Finn

Gjør algoritmer noe bra for oss?

Selvkjørende biler

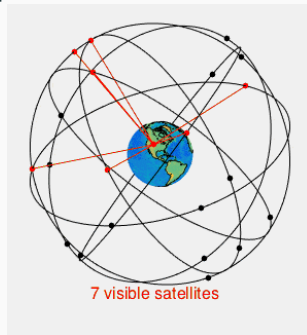
Selvkjørende biler:

- **Mennesker:** 1 ulykke per 0.7 million km
- **Tesla uten systemer:** 1 ulykke per 2.5 million km
- **Tesla med hjelpesystemer:** 1 ulykke per 3.4 million km
- **Tesla autopilot:** 1 ulykke per 5 million km
- Mer enn 25% av alle Tesla-ulykker er påkjøring bakfra



Global Positioning System:

- Driftskostnad 2 millioner USD per dag
- Nedetid tilsvarer **mer enn 1 mrd USD** per dag
- All transport og geografi i verden i dag er basert på GPS
 - Navigering (biler, fly, skip, ...)
 - Pakke- og transportsporing
 - Robotikk
 - Landskapsmåling og kartografi
 - astronomi og atmosfæren
 - Redningsaksjoner



Finans er full-digitalisert:

- altinn,
- bankkonto og lån
- fond og børser,
- handel på nett og med bankkort
- BANKID
- ...

... er alle drevet av algoritmer.

Økokrim og banker bruker maskinlæring til å **gjenkjenne** mistenksom aktivitet

- Hvitvasking
- Svindel
- Terror-finansiering

Medisinsk diagnostisering:

- les medisinske bilder og data, still diagnose
- høyeste mål til kunstig intelligens

Telemedisin:

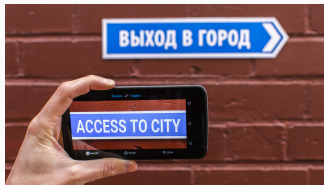
- Bruk data og data- og teleteknologi til medisinske formål
- Undersøkelse, overvåkning, behandling, opplæring av pasienter og helsepersonell

-
- 70% reduksjon i nødvendig sykehusinnleggelser av kreftpasienter
 - smart-klokke gjorde Kols-pasienter mer uavhengig via avstandsoppfølging
 - smart-klokker som varsler
 - nødvendig oppfølging hos diabetespasienter
 - fallsensor
 - detektering av sykdommer før de slår ut, e.g. covid, diabetes

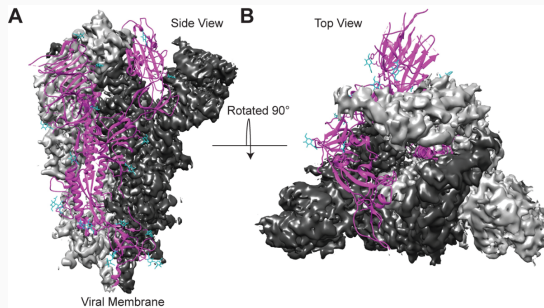
Hjelp ved nedsatt funksjon

Mennesker med nedsatt **funksjonsevne**, samt å utvide funksjonsevne

- Stemmegjenkjenning,
- chat-bots,
- «smarte» høreapparater,
- automatisk sanntids-teksting,
- sanntidsoversetting (fra bilder og tale)
- «*Deep-fake*»: stemme-generering med samme stemme (tekst-til-tale)



- ADAM i 2007 avslørte funksjonen til et gjærgen
- EVA oppdaget ny malariamedisin
- Roboter fant frem til bedre *gjenkjenning* av kreftceller
- ... og ny behandling av ALS
- Etter at AlphaZero ble verdensmester i Sjakk og Go: AlphaFold



Udfordringer i den algoritmiske tidsalder

Roboter tar jobbene våre

Arbeidsledighet

I hovedsak et samfunnsøkonomisk problem $\Rightarrow$ økende forskjeller

Utfordring:

Hvordan omfordele ressurser når jobbene skjer av seg selv?

Å være i jobb er ikke et mål i seg selv, det som produseres er

Foreslått løsning

Garantert grunninntekt
(«borgerlønn»)



Cybersikkerhet

- Løsepengevirus og sabotasje
- Cyber-krigføring
 - Stuxnet — Et av de mest sofistikerte data-angrepene i historien (Israel?)
 - Kontinuerlig angrep på strømforsyningen til baltiske land og USA (Russland?)
 - Angrep på Stortinget
- Storskala utpressing
 - Sender epost til millioner av mennesker
 - Et fåtall føler seg truffet
- *Social engineering*

Manglende *forklarbarhet*: Maskinlæring er en «svart boks».

- Jobbsøknader, filtrering på navn, bilde, opphavsland, kjønn, ...
- Domstoler, eksempel på «uheldige» domfelling
- «tilfeldig» utvalg-ransaking og kroppsvisitering
- krigføring og «kill-list» (*Disposition Matrix*),



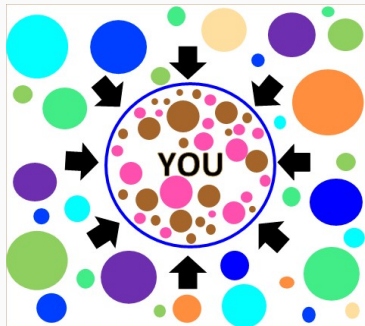
- ...

Kan være selvforsterkende for fordommer.

Forbehold: Vi har søknad inne hos Forskningsrådet rundt «Explainable AI».

Ekko-kammer: Flere og flere går til sosiale medier for «nyheter»

- Vi får mer av det vi liker
 - selv-forsterkende
 - polariserende
 - klikk som måleenhet
 - *patos*: spiller på følelser
- filterboble / ekkokammer
- vippe-velger-manipulering



Fordommer

Eksempel 1. Noe så uskyldig som bildebeskjæring.

- Gitt et bilde
- Finn et ansikt
- ... eller andre vesentlige detaljer
- skjær bort alt som er uinteressant

Eksempel 1. Noe så uskyldig som bildebeskjæring:



AI predictions for 2019 from Yann LeCun, Hilary Mason, Andrew Ng, and Rum...
VentureBeat spoke with Google Brain cofounder Andrew Ng, Fast Forward Labs founder Hilary Mason, Facebook AI Research founder Yann LeCun, and

Fordommer (bias) og urett

Eksempel 1. Noe så uskyldig som bildebeskjæring:



Fordommer (bias) og urett

Eksempel 1. Noe så uskyldig som bildebeskjæring:



Eksempel 1. Noe så uskyldig som bildebeskjæring:

Twitter anslår Mitch som *mer menneskelig* enn Barack.

Andre konsekvenser enn «bare» rasisme og kjønnsdiskriminering.

Spørsmål: *Hvor vil den selvkjørende bilen kjøre dersom Mitch og Barack er på fortauet?*

- Vi vet lite om denne typen “ultimatum”
- Det er tema for forskning (Moral machine)

Eksempel 2: Mørk hud

Da Apple Watch ble lansert i 2015, klarte den ikke å lese hjerterytmen til personer med tatovering eller *mørk hud*. $\Rightarrow$ dette sier noe om test-personene til Apple Watch og de som jobber i Apple.

Andre smart-klokker og «wearables» har hatt tilsvarende problemer. $\Rightarrow$ mørk hud utelukker positive helse-effekter smart-klokker kan gi.

Nok en selvforsterkende effekt.

Eksempel 3: Jobbsøknader.

Kunstig intelligens er i dag i stor grad brukt til å filtrere bort kandidater for jobbsøknader.

Siden kunstig intelligens kun hjelper oss å automatisere den jobben vi tidligere gjorde, vil den nå være minst like forutinntatt, og enda mer effektiv.

Vanskelig å oppdage i proprietære algoritmer.

Finn.no viser forskjellige annonser til forskjellige mennesker.

Nok en selvforsterkende effekt: Minoriteter går glipp av jobber.

Tilbakeløkker: Vi er “ofre” for våre egne ønsker og begjær:

- FACEBOOK gir oss hundre linker, ser hva vi trykker på
- Selger informasjonen til høystbydende ADX (fiktivt)
- Når du søker etter en rute i GOOGLE MAPS, betaler ADX penger til GOOGLE for å få deg rutet via deres butikker
- Attpåtil
 - ... Alle disse kjenner deg bedre enn du gjør selv
 - Og vet hvilket humør du er i
 - Og hvor lett påvirkelig du er nå

... selvforsterkende effekter

Desinformasjon via tekst-generering (GPT-3)

Stor-skala *falske nyheter*

Med bedre tekst-generering kan man i dag lage en fullstendig «nettavis», for eksempel BERGENSBLADET.

Med historikk! Man kan generere en fullstendig nyhetsside med debatter, bilder og arkiv. Ikke bare en, men millioner.

Man kan slik dele *falske nyheter* med «lettlurte», spesielt da vippe-velgere.

Deep-fakes, tekst-generering (GPT-3)

DEEP-FAKES er en teknikk å ta video og stemme fra én person, og få det til å *høre* og se ut som en annen. Man kan for eksempel ta en tale [sett inn *bad guy*] har holdt, og få det til å se ut som om det er (e.g.) Lysbakken som holder talen.

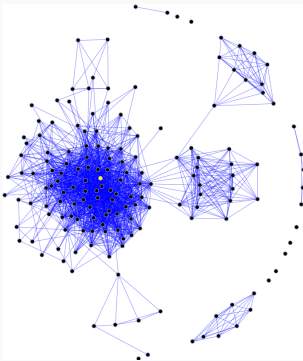
Dette kan sendes ut i små klipp på SNAPCHAT, TIKTOK og til og med på FACEBOOK, og kan dreie noen enkle personer fra å stemme Ap til å stemme H.

En slik operasjon vil være målrettet disse personene.

Overvåking og sporing

Internasjonale aktører har GPS-sporingsdata av et stort men uvisst antall mennesker

- Data er «anonymisert»
- Kan brukes til utpressing
- Kan brukes til spionasje
- Kan brukes til forfølgelse
- Brukes til annonser
- Skreddersy tilbud til deg



(c) Haakonvern åndsverk NRK mobilsporing

Mitigerende tiltak

«Tenke sjæl»

- Være nysgjerrig
- Når man leser saker på nett
 - tenk på hva man føler om det
 - sjekk referanser
 - stoler man på redaktøren?
 - har man hørt om avisen/kildene?
- Stemme på partier som fremmer utdanning til flest
- Papiraviser
 - Abonner på en anerkjent avis og les *hele* avisen.
 - Mindre grad målrettet, kan ikke brukes for å vippe enkeltpersoner.
 - Er underlagt PFU.

Du er produktet

Bruker du en tjeneste som tjener penger, men ikke *fra deg* ...

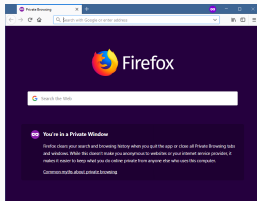
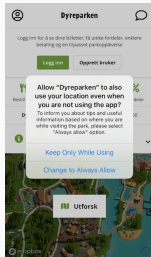
DU er produktet!

- FACEBOOK + INSTAGRAM + WHATSAPP + MESSENGER
- GOOGLE + FITBIT + YOUTUBE
- TWITTER,
- SNAPCHAT,
- MICROSOFT + SKYPE + TEAMS + LINKEDIN + BING (+ PINTEREST?)
- TIKTOK,
- PARLER,
- CLUBHOUSE,
- REDDIT ...

(Unntak: fri programvare og ideelle organisasjoner)

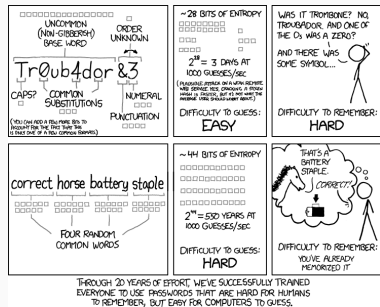
Beskytt deg selv

- Kontroller app-tilganger (app permissions)
 - skru av lokasjonsdata
 - ikke gi tilgang til kontaktlisten
 - ikke ta falske tester på Facebook
- *Incognito-modus* (privat modus) i nettleser
 - Forbli utlogget av sosiale medier
 - Ikke logg på Google
 - Start nettleseren på nytt ofte
 - Tøm informasjonskapsler (*cookies*)
- TOR-nettleseren (The Onion Router)
- VPN (*virtual private network*)
- E2E (ende-til-ende)-kryptering med SIGNAL, TELEGRAM



Passordsbehandler

- Å gjenbruke passord på mange steder er ikke en god idé
- lag passord som er
 - (a) lett å huske
 - (b) vanskelig å gjette
- algoritme for å lage passord:
 - finn en ordliste
 - velg en tilfeldig side
 - velg et tilfeldig ord
 - gjenta 4 ganger
- passord-på-postit: ganske lurt
- Det aller lureste: **passordbehandler**



Oppsummering

Algoritmer og maskinlæring

- Gjør mye bra
- Driver store deler av sivilisasjonen vår
- Vi vet ofte ikke *hvorfor* avgjørelser taes

Dataoppsamling

- Vi gir mektige selskaper for mye informasjon om oss selv
- Vi får relativt lite igjen
- Vi er produktet

Vi blir ledet

- Vi er lett påvirkelig
- Motvirke ved å ikke være logget inn
- Skru av lokasjon
- Ikke gi tilgang til apper
- Les **papiraviser** og være kildekritisk

Takk for meg

Takk for meg!

Takk for meg

Takk for meg!

Kunstig intelligens *forstår* ingenting.

- Den største utfordringen i kunstig intelligens er «forståelse» av tekst og språk
- «kontekst»
- Hva betyr det egentlig å «forstå»?
- Kan en ubåt «svømme»?

Maskinlæring *lærer* mye, men *forstår* intet.

Turing-testen:

Scott Which is bigger, a shoebox or Mount Everest?

Eugene I can't make a choice right now. I should think it out later. And I forgot to ask you where you are from...



SJEKK DATOEN

Deling av gamle nyhetsartikler er ikke alltid relevant for aktuelle hendelser.



ER DU FORUTINNTATT?

Kan dine egne overbevisninger påvirke dømmekraften din?



VURDER KILDEN

Klikk deg videre og undersøk nettsiden, formålet og kontaktinformasjon



SØK OPP FORFATTEREN

Gjør et raskt søk på forfatteren. Er personen troverdig? Fins han/hun?



FORTSETT Å LESE

Sensasjonelle overskrifter genererer klikk. Hva er egentlig saken?



FINS DET KILDER?

Klikk på lenker. Stemmer egentlig informasjonen overens med saken?



ER DET EN SPØK?

Merkelige saker kan være satire. Sjekk nettsiden og forfatteren for å utelukke.



SPØR EKSPERTENE

Spør en bibliotekar, eller oppsøk en nettside for faktasjekk