IN1150 – Logiske metoder

Generelt

- To kapitler per uke
- Les boken
- Bruk nettkurset
- Bruk undervisningstilbudet
- Løs mange oppgaver
- Gjør innleveringer
- En innlevering i uka

https://logiskemetoder.no/nettkurs/

Eksamensøving

- Induksjon
- Gjøre om sammensatte utsagnslogiske formler til setninger
- Logisk konsekvens
- Logisk ekvivalens
- M|= p
- Ekvivalensklasse
- Partisjon
- P(mengde)
- Mengde^{noe}
- Potensmengde
    - Side 92
    - Hvis M er en mengde, er potensmengden til M mengden av alle delmengder av M. Vi skriver P(M) for potensmengden til M
    - Potensmengden til {Ø,{Ø}} er {Ø,{Ø},{Ø}}}
- Tillukninger
- Antall delmengder av en mengde
- Antall funksjoner mellom to mengder
    - Antall bijektive
        - antall valg for hver av elementene i første mengden ganger hverandre
- Antall forskjellige permutasjoner

– Hvis en endelig mengde har n elementer, har potensmengden alltid 2^n elementer.

- Bevis at noe er en tautologi eller en motsigelse
    - Vis at det finnes en sann og en usann valuasjon
- Hvilke formler er logiske konsekvenser av en mengde uttrykk
    - Sjekk om de er sanne samtidig som alle uttrykkene i mengden er sanne
- Vis at formelen er en tautologi
    - Vis at den er sann uansett

Definisjoner

- Innfører et begrep
- ... ved å fortelle hva det heter...
- ... og hva det betyr...
- ...ofte med notasjon.
- Mulig og nødvendig i matematikk
- Ofte mulig og ofte nødvendig i informatikk
- Starter alltid på et «fundament»
    - Om ikke annet, leserens samarbeidsvilje
    - Vi skal ikke bruke tid på fundamentene
- Vi bruker definisjoner:
    - I matematikk: til å bevise teoremer
    - I informatikk: for å vite hva vi skal implementere

Kapittel 1 – Grunnleggende mengdelære

Mengde

- Abstraksjon
    - Ved å se bort fra detaljene (biler eller bamser) kan vi forstå hva som er felles og trekke konsekvenser av det
    - Finne ut hva som gjelder for alle «samlinger»
- Masse ting
    - Datamaskiner kan jobbe med store mengde data
        - 400 oblig innleveringer
        - 10000 kunder
        - En halv million kattebilder
    - Må kunne:
        - Legge til flere
        - Fjerne noen
        - Finne de flinkeste/rikeste/søteste
    - Programmene blir veldig like
    - De typiske feilene er de samme
    - Nyttig å ha en Abstraksjon for samlinger
    - Arrays, Maps, Dictionaries, Sets osv.
- Definisjon mengde
    - En mengde er en endelig eller uendelig samling av objekter der innbyrdes rekkefølge og antall forekomster av hvert objekt ignoreres. Objektene i en mengde kalles elementer
- Mengdebygger

- En mengde kan defineres som mengde av alle elementer som en gitt egenskap
    - En slik konstruksjon kalles en mengdebygger
    - En definisjon på formen «mengden av alle elementer x slik/gitt at x har egenskapen P» skrives {x|x har egenskapen P}
    - Det som er til venstre for streken, kan også være et sammensatt uttrykk
- Mengder av mengder
    - a ∈ {a}, men a ∈ {{a}}
        - Ene objektet inneholder a
        - Andre objektet inneholder en mengde som inneholder a
    - Mengden {1,2,3,4,{1,2,3},{1,2,{3}}} er en hybrid
- Notasjon for mengde
    - ∩ - snittet inneholder en mengde der elementene finnes i begge mengdene på vs av likhetstegnet. {1,2} ∩ {2,3} = {2}
    - ∪ -union inneholder et samlet set av to mengder. {1,2} ∪ {2,3} = {1,2,3}
    - ⊆ - delmengde. {1} ⊆ {1,2,3}. {{1}} ⊆ {1,2,3{1}}
    - \ - mengdedifferansen er litt likt subtraksjon. {a,b}\{a} = {b}. {a,b}\{c,d} = {a,b}
    - {1,2}
    - ⟨1,2⟩
        - Et tuppel med n elementer, et n-tuppel, er en samling med n objekter der både innbyrdes rekkefølge og antall forekomster av hvert objekt teller.
        - Et 2-tuppel med to elementer x og y kalles et ordnet par, eller bare et par, og skrives ⟨x,y⟩
    - x – kartesisk produkt, også kalt kryssproduktet. {a} x {1,2} = {⟨a,1⟩, ⟨a,2⟩}
    - [1,2]
        - En multimengde er en samling objekter er rekkefølgen, men ikke antall forekomster av hvert element ignoreres
        - [1,2,3] = [3,2,1]
        - [1,1,2,3]≠ [1,2,3]
    - Tre forskjellige abstraksjoner, forskjellige operasjoner
    - Tupler er ikke «en slags mengde,» eller omvendt
        - Altså ikke sånn som at alle naturlige tall også er reelle tall!
- Endringer
    - I programmering(Spesielt OO) endrer vi ofte objekter
    - catPics.add(cutestEverCatPick);
    - endrer mengden av bilder som er representert i datastrukturen
    - Dette gjør vi aldri i matematikk
    - Digresjon: mutable og immutable datastrukturer
- Likhet
    - Hvis A = {1,2} og B = {2,1} vil A=B, fordi A ⊆ B og B ⊆ A
- Mulige delmengder av en mengde er generelt $2^{\text{lengden av mengden}}$

Kapittel 2 - Utsagnslogikk

Viktigste spørsmålet

- Hva er som følger hva?
- Hva er et utsagn
    - Et utsagn er noe som kan være sant eller usant. Dette noe kan være en setning, ytring eller meningsinnholdet til slike.
    - Eksempel
        - $2+2 = 8$
        - $1 \in \{1,2\}$
        - Det finnes uendelig mange tall
    - Ikke utsagn
        - Når er eksamen?
        - Hurra!
- Atomære og sammensatte utsagn
    - Utsagn kan analyseres og deles opp i mindre og mindre biter, helt til vi kommer til såkalte atomære utsagn. Noen atomære utsagn kan være
        - Oslo er hovedstaden i Sverige
        - Alle partall er delelige med to
    - Den interne strukturen til atomære utsagn blir ikke analysert, og hva som er våre atomære utsagn, kan vi velge fritt
    - Fra atomære utsagn kan vi bygge opp sammensatte utsagn ved hjelp av logiske bindeord, som og, eller, ikke, og, hvis, så
        - Oslo er hovedstaden i Sverige, og $5+6 = 7$
        - Hvis $5+6 = 7$, så er alle partall delelige med 2
    - Hvilke utsagn er sanne uavhengig av sannhetsverdiene til de atomære utsagnene? Slike utsagn kalles tautologier
- Atomære og sammensatte formler
    - En utsagnsvariabel er en variabel, P, Q, R,.. eller liknende. En utsagnsvariabel er en atomær formel.
    - Sammensatte formler
        - For å fange inn og representere sammensatte utsagn
            - Hvis man trener, så blir man sterk.
                - T = man trener
                - S = man blir ster
            - Det sammensatte utsagnet kan nå representeres ved hjelp av formelen $(T \to S)$
- Konnektiver
    - Intuisjonen bak konnektivene er at de representerer de logiske bindeordene:
        - $\neg$ betyr ikke
        - $\wedge$ betyr og
        - $\vee$ betyr eller
        - $\to$ betyr impliserer eller hvis, så
    - Konnektivene er en del av symbolspråket; de er symbolene vi skal bruke for å sette mindre formler sammen til større
- Utsagnslogiske formler
    - Enhver atomær formel er en utsagnslogisk formel. Hvis F og G er utsagnslogiske formler, har vi at følgende også er utsagnslogiske formler:
        - $\neg F$ er en utsagnslogisk formel; vi kaller denne **negasjonen** til F.

        - $(F \land G)$ er en utsagnslogisk formel; vi kaller denne **konjunksjonen** av F og G. Formlene F og G kalles **konjunktene**.
        - $(F \lor G)$ er en utsagnslogisk formel; vi kaller denne **diskusjonen** av F og G. Denne representerer «F eller G». Formlene F og G kalles **disjunktene.**
        - $(F \rightarrow G)$ er en utsagnslogisk formel; vi kaller denne **implikasjonen** mellom F og G.

- Nødvendige og tilstrekkelige begreper
    - Hvis $(A \rightarrow B)$ uttrykker «hvis A, så B»
    - At A er sann, er en **tilstrekkelig** betingelse for at B er sann.
        - Dette betyr at det er nok at A er sann for at B også skal være sann
        - Formelen B kan være usann uten at A er sann, men hvis A er sann, så må B være sann
    - At B er sann er en **nødvendig** betingelse for at A er sann.
        - Dette betyr at A ikke kan være sann uten at B også er sann.
        - Formelen A er sann bare hvis B er sann.
- Hvis og bare hvis
    - Jeg spiser det hvis det er godt
        - Jeg spiser det «$\leftarrow$» det er godt
        - Det er godt «$\rightarrow$» jeg spiser det
          (Med andre ord er jeg glupsk)
    - Jeg spiser det bare hvis det er godt
        - Jeg spiser det «$\rightarrow$» det er godt
          (med andre ord er jeg kresen)
    - Jeg spiser det hvis og bare hvis det er godt
        - Jeg spiser det «$\leftrightarrow$» det er godt
          (Med andre ord, jeg er glupsk, men kresen)
        - Det er ganske vanlig å bruke ordet «hviss» som en forkortelse for «hvis og bare hvis»: Jeg spiser det **hviss** det er godt.
- Parenteser, presedensregler og praktiske forkortelse
    - Vi gir konnektivene ulike presedens i forhold til hverandre
        - $\neg$ binder sterkest
        - $\land$ binder svakere enn $\neg$
        - $\lor$ binder svakere enn både $\neg$ og $\land$
        - $\rightarrow$ binder svakest
    - Det at $\bullet$ binder sterkere enn $\circ$ betyr at $P \bullet Q \circ R$ står for $((P \bullet Q) \circ R)$ og ikke $(P \bullet (Q \circ R))$.

Kapittel 3 – Semantikk for utsagnlogiske formler

- Sannhetsverdier
    - Vi lar 1 og 0 stå for sannhetsverdiene sann og usann
    - Hvis F og G er itt er sannhetsverdien til $\neg F$, $(F \land G)$, $(F \lor G)$ og $(F \rightarrow G)$ som gitt i følgende tabeller som viser hvordan konnektivene skal tolkes.

F	¬F
1	0
0	1

F	G	(F ∧ G)
1	1	1
1	0	0
0	1	0
0	0	0

F	G	(F ∨ G)
1	1	1
1	0	1
0	1	1
0	0	0

F	G	(F → G)
1	1	1
1	0	0
0	1	1
0	0	1

- Valuasjoner
    - Vi snakker ofte om en tilordning av sannhetsverdier til utsagnsvariabler. Det betyr at for enhver utsagnsvariabel har vi valgt en spesifikk verdi, enten 1 eller 0. Når en slik tilordning er valgt, er det nøyaktig en måte å gi alle utsagnslogiske formler en verdi på, gitt at vi tolker konnektivene.
    - Definisjon Valuasjon
        - En tilordning av sannhetsverdier til alle utsagnslogiske formler som er slik at tabellene overholdes, valuasjon.
        - F.eks.
            - Se på formelen (P∧¬Q)
            - Anta at vi har en valuasjon som gjør P sann og Q usann.
            - Denne valuasjonen må gjøre ¬Q sanne
            - Det er fordi det er slik¬- formler tolkes
            - Da har vi både P og ¬Q sanne
            - Da kan vi konludere med at (P∧¬Q) er sann.
            - Det er fordi det slik ∧-formler tolkes
    - Sannhetsverditabeller
        - En praktisk måte å regne ut valuasjoner på
        - En sannhetsverditabell er en tabell som forteller hva sannhetsverdien til en sammensatt utsagnslogisk formel er på bakgrunn av hvilke sannhetsverdier som er tilordnet utsagnsvariablene
- Egenskaper ved implikasjon
  «Hvis du betaler, så får du komme inn»

  Dette kan representeres ved den utsagnslogiske formelen (B→K), hvor B representerer «du betaler» og K representerer «du får komme inn». Tenk på hva det vil si at dette utsagnet er henholdsvis sant og usant.
    - Hva vet du hvis du vet at utsagnet er sant?
        - Da må K være sann- at du får komme inn – gitt at B er sann – at du betaler. Det er en slags garanti som forteller hva som må være tilfellet hvis B er sann. Hva skjer når B er usann – at du ikke betaler – spiller ingen rolle for sannhetsverdien til hele utsagnet; da kan K – at du får komme inn – være sann eller usann
    - Hva vet du hvis utsagnet er usant?
        - Da må B være sann – at du betaler – og K være usann – at du ikke får komme inn. Dette er den eneste måten hele utsagnet kan være usant på
- Logisk ekvivalens
- https://www.uio.no/studier/emner/matnat/ifi/IN1150/h17/ressurser/notat-fra-gruppetime-2.pdf

- To formler F og G er logisk ekvivalente, eller bare ekvivalente, hvis de har samme sannhetsverdi for enhver tilordning av sannhetsverdier til utsagnsvariablene. Vi skriver $F \Leftrightarrow G$ når F og G er logisk ekvivalente.
- Hvis to formler er ekvivalente, har de samme meningsinnhold
- Hvis to formler ikke er ekvivalente, kav vi finne en valuasjon som gjør den ene formelen sann og den andre formelen usann
  - Formlene P og $\neg\neg P$ er ekvivalente.
  - Hvis en valuasjon gjør P sann, må den også gjøre $\neg\neg P$ sann, og omvendt
  - De har alltid samme sannhetsverdi.
- Ikke-ekvivalente formler
  - Formlene $P \vee Q$ og $P \wedge Q$ er ikke ekvivalente
  - En valuasjon som gjør P sann og Q usann, vil gjøre $P \vee Q$, men $P \wedge Q$ usann.
  - De har ikke alltid samme sannhetsverdi og er derfor ikke ekvivalente.

- Ekvivalente formler vist ved sannhetsverditabell
  - Ekvivalente formler
    - De utsagnslogiske formlene $(P \rightarrow Q)$ og $(\neg P \vee Q)$

P	Q	(P	$\rightarrow$	Q)	($\neg$P	$\vee$	Q)
1	1	1	1	1	0	1	1
1	0	1	0	0	0	0	0
0	1	0	1	1	1	1	1
0	0	0	1	0	1	1	0

    - VI ser at formlene har samme sannhetsverdi uansett tilordning av sannhetsverdier til utsagnsvariablene.

- Ekvivalente formler vist ved resonnement
  - Vis at formlene $\neg (P \rightarrow Q)$ og $(P \wedge \neg Q)$ er ekvivalente
  - For å bevise dette er det nok å vise at $\neg (P \rightarrow Q)$ er sann hvis og bare hvis $(P \wedge \neg Q)$ er sann
  - Anta først at $\neg (P \rightarrow Q)$ er sann.
    - Da må $(P \rightarrow Q)$ være usann. (Det er slik $\neg$ -formler tolkes)
    - Da må P være sann og Q være usann.
    - Da må $\neg Q$ være sann
    - Da må og $(P \wedge \neg Q)$ være sann. Når P og $\neg Q$ må være sanne.
  - Anta da at $(P \wedge \neg Q)$ er sann
    - Da må P og $\neg Q$ være sann
    - Da må Q være usann
    - Da må $(P \rightarrow Q)$ være usann
    - Da må $\neg (P \rightarrow Q)$ være sann

- Noen viktige ekvivalenser
  - Distribusjon – likt som å ta ut av parentes
    - $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

        - A∨ (B∧C) ⇔ (A∨B) ∧ (A∨C)
    - De Morgan
        - ¬ (A∧ B) ⇔ (¬A ∨ ¬B)
        - ¬ (A∨B) ⇔ (¬A ∧ ¬B)
    - Assosiativitet
        - A∧(B∧C) ⇔ (A∧B) ∧C
        - A∨(B∨C) ⇔ (A∨B) ∨C
    - Kommutativitet
        - A ∧ B ⇔ B ∧ A
        - A ∨ B ⇔ B ∨A
    - Dobbel negasjon
        - P ⇔ ¬¬P
    - Implikasjon
        - A→B ⇔ ¬ A ∨ B

Hvilken av disse formlene er ekvivalente med $\neg A \wedge (B \vee \neg C)$?

- ○ $(A \wedge B) \vee (A \wedge \neg C)$
- ○ $(A \wedge \neg B) \vee (A \wedge C)$
- ● $(\neg A \wedge B) \vee (\neg A \wedge \neg C)$ ✓

Konjunksjon distribuerer over disjunksjon.

Test deg selv

Hvilke av disse formlene er ekvivalente med $(A \wedge \neg B)$? Resten av formlene er ekvivalente med hverandre.

- [x] $\neg(\neg A \vee B)$ ✓
- [ ] $\neg(A \vee \neg B)$
- [x] $\neg(A \rightarrow B)$ ✓
- [ ] $\neg(\neg A \rightarrow \neg B)$
- [ ] $(\neg A \wedge B)$

Helt riktig! ✓ Vis løsning og forklaringer

- Logisk konsekvens
    - La M være en mengde av utsagnslogisk formler, og la F være en utsagnslogisk formel. Hvis D er sann for alle valuasjoner som gjør alle formlene i M sanne samtidig, er F en logisk konsekvens, eller bare en konsekvens av, av formlene i M. VI skriver M|= F når F er en logisk konsekvens av M
    - For å sjekke om F er en logisk konsekvens av en mengde M, må vi med andre ord se på valuasjoner som gjør alle formlene i M sanne samtidig, og sjekke om

disse også gjør F sann. Hvis det er slik, er F en logisk konsekvens av M. Hvis ikke, kan vi finne en valuasjon som gjør alle formlene i M sanne, men som gjør F usann.

- Eksempel
    - VI har at Q er en logisk konsekvens av mengden som består av P→ Q fordi alle valuasjoner som gjør både P og (P→ Q) sanne, også må gjøre Q sann.

P	Q	P	(P → Q)	Q
1	1	1	1	1
1	0	1	0	0
0	1	0	1	1
0	0	0	1	0

      Dermed kan vi skrive {P, P→Q} |=Q
    - Er (P→(Q∨ R)) en logisk konsekvens av (P→Q)
      La oss sjekke i en sannhetsverditabell

P	Q	R	(P → Q)	(P	→	(Q ∨ R))
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	0	1	1	1
1	0	0	0	1	0	0
0	1	1	1	0	1	1
0	1	0	1	0	1	1
0	0	1	1	0	1	1
0	0	0	1	0	1	0

      Denne formelen må være logisk konsekvens av mengden P→Q, fordi den er sann hver gang P→Q er sann
      Altså fordi alle valuasjoner som gjør P→Q sann, som er alle radene utenom 3 og 4, også gjør (P→(Q∨ R)) sann.

- Gyldige argumenter
    - Et resonnement eller argument er gyldig eler holdbart hvis konklusjonen er en logisk konsekvens av mengden av premisser

Hvis solen skinner, så er jeg glad.	$(S \to G)$
Jeg er ikke glad.	$\neg G$
Solen skinner ikke.	$\neg S$

– Dette er også et eksempel på et *gyldig* argument. En sannhetsverditabell kan brukes til å analysere argumentet.

S	G	$(S \to G)$	$\neg G$	$\neg S$
1	1	1	0	0
1	0	0	1	0
0	1	1	0	1
0	0	1	1	1

– Det er den nederste raden som er relevant, for det er kun her både $(S \to G)$ og $\neg G$ sanne. Vi ser at også $\neg S$ er sann da.

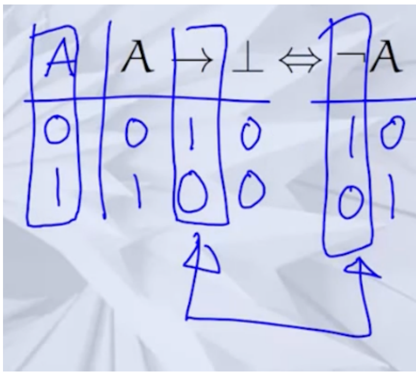
Hvis solen skinner, så er jeg glad.	$(S \to G)$
Solen skinner ikke.	$\neg S$
Jeg er ikke glad.	$\neg G$

– Dette er *ikke* et gyldig argument.
– Det er fordi $(S \to G)$ og $\neg S$ kan begge være *sanne* uten at $\neg G$ er det. (Jeg kan være glad selv om solen ikke skinner.)
– Med andre ord, $\neg G$ er *ikke* en *logisk konsekvens* av $(S \to G)$ og $\neg S$.
– Vi kan også se dette via (en rad i) en sannhetsverditabell.

S	G	$(S \to G)$	$\neg S$	$\neg G$
0	1	1	1	0

- Oppfyllbarhet
  - Hvis en valuasjon v gjør en utsagnslogisk formel F sann, så sier vi at valuasjonen oppfyller formelen og skriver $v \models F$.
  - Eksempler
    - Formelen $P \to Q$ er oppfyllbar; den oppfylles av enhver valuasjon som gjør P usann eller Q sann.
    - Formelen $(P \wedge \neg P)$ er ikke oppfyllbar; det finnes ingen valuasjon som gjør både P og $\neg P$ sanne samtidig.
- Falsifiserbarhet
  - Hvis en valuasjon v gjør en utsgangslogisk formel F usann, sier vi at valuasjonen falsifiserer formelen og skriver $v \not\models F$
  - En utsagnslogisk formel er falsifiserbar hvis det finnes en valuasjon som falsifiserer den.
  - Eksempler
    - Formelen $P \to Q$ er falsifiserbar; den falsifiseres av enhver valuasjon som gjør P sann og Q usann
    - Formelen $(P \vee \neg P)$ er ikke falsifiserbar; det finnes ingen valuasjon som gjør både P og $\neg P$ usanne samtidig.
- Tautologi/gyldighet

-
  - Hvis en utsagnsformel F er sann for alle valuasjoner, sier vi at formelen er en tautologi, eller er gyldig, og skriver |=7
  - F.eks.
    - $(P \lor \neg P)$
  - Formelen P er ikke en tautologi fordi det finnes en valuasjon som gjør P usann.
- Motsigelse/kontradiksjon
  - Hvis en utsagnslogisk formel F er usann for alle valuasjoner, sier vi at formelen er kontradiktorisk , eller en kontradiksjon, eller en motsigelse.
  - F.eks.
    - Formelen $(P \land \neg P)$ er kontradiktorisk fordi ingen valuasjon gjør både P og $\neg P$ sanne samtidig; enhver valuasjon vil enten gjøre P usann eller $\neg P$ usann, og dermed $(P \land \neg P)$ usann.
- Symboler for sannhetsverdiene
  - Det er ofte nyttig å ha symbolske representasjoner for sannhetsverdiene 1 og 0.
  - Vi lar T og $\perp$ regnes som utsagnslogiske formler i tillegg til de vi har fra før av
  - Det er vanlig å lese T som «topp» eller sann og $\perp$ som «bunn» eller usann
  - Enhver valuasjon må gjøre T sann og $\perp$ usann
  - $T \rightarrow A$. Her vil elementene ha sannhetsverdiene 1 1 og 1. Og vi kan derfor si at $T \rightarrow A \Leftrightarrow A$
  - $A \rightarrow \perp$. Se figur til høyre for forklaring for hvorfor $A \rightarrow \perp \Leftrightarrow \neg A$



- Sammenhenger mellom begreper
  - $F \Leftrightarrow G$. Hvis og bare hvis $\models F \Leftrightarrow G$
  - $\{F\} \models G$ hvis og bare hvis $\models F \rightarrow G$
  - $F \Rightarrow G$ hvis og bare hvis
- Uavhengighet av formler
  - En formel F er uavhengig av en mengde formler M hvis hverken F eller $\neg F$ er en logisk konsekvens av M.
  - En mengde av formler er uavhengig hvis enhver formel er uavhengig av mengden av de andre formlene
  - Eksempel
    - Formel P er uavhengig av mengden $\{P \lor Q, R\}$, fordi hverken P eller $\neg P$ er en logisk konsekvens av den
    - Men P er ikke uavhengig av mengden $\{P \land Q, R\}$, fordi P er en logisk konsekvens av den.

Kapittel 5 – bevis formodninger og moteksempler

- Bevis
  - Et bevis for en påstand fra en mengde gitte antakelser er en rekk logiske slutninger som viser hvordan vi kommer fra antakelsene til påstanden
  - For hvert steg må konklusjonen være en logisk konsekvens av antakelsene
- Tenke ut fra antakelser
  - Du kan anta hva som helst, men du må ta konsekvensen av det
- Formodninger

- En formodning er en påstand som vi tror, eller har god grunn til å tro, er sann, men som vi ikke har bevist eller motbevist
- Goldbachs formodning
  - Ethvert partall større enn to kan uttrykkes som summen av to primtall
  - F.eks. 12 = 5+7, 100 = 97+3
  - Ingen vet hvorvidt dette er sant eller ikke; ingen har klart hverken bevise eller motbevise motstanden.

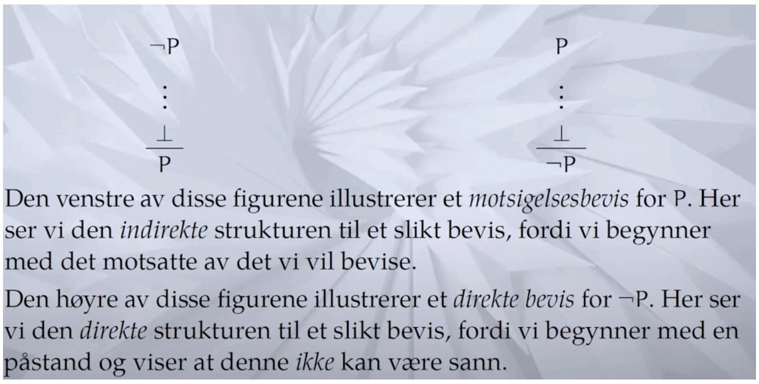
- Bevismetoder
  - Ikke-lovlige bevismetoder
    - Bevis ved overtalelse: «Det er trvilielt!»
    - Bevis ved utelatelse: «Leseren kan gjøre resten.»
    - Bevis ved autoritet: «Foreleseren sa det.»
    - Bevis ved konsensus: «Alle vet at det er slik.»
    - Bevis ved bilde: «Se her»
    - Bevis ved kosmologi: «Det er umulig å forestille seg det motsatte.»
  - Direkte bevis
    - Et direkte bevis for en påstand på formen «hvis F, så G», er et logisk gyldig resonnement som begynner med antakelsen om at F er sann og som ender med konklusjonen om at G er sann.
    - Et direkte bevis begynner typisk med «anta at F er sann» og slutter med «det følger derfor at G er sann»
    - Eksempel
      - Anta at en valuasjon er gitt. Bevis påstanden «hvis valuasjonen gjør $(P \wedge Q)$ sann, så gjør valuasjonen P sann»
        - Anta at valuasjonen gjør $(P \wedge Q)$ sann
        - Da må valuasjonen gjøre både P og Q sanne, fordi det er slik $\wedge$-formler tolkes
        - Da må valuasjonen gjøre P sann.
        - Det følger derfor at hvis $(P \wedge Q)$ er sann, så er P sann.
      - Anta at vi har en valuasjon gjør $(P \rightarrow Q)$ sann. Bevis påstanden «Hvis P er sann, så er $(Q \vee R)$ sann »
        - Vi vet (1) at valuasjonen gjør $(P \rightarrow Q)$ sann
        - For å bevise påstanden, antar vi (2) at valuasjonen gjør P sann
        - Målet vårt er å vise at valuasjoen gjør $(Q \vee R)$ sann.
        - Fra (1) og (2) følger det at Q er sann
        - Da må også $(Q \vee R)$ være sann
        - Antakelsen om at P, leder konklusjonen om at $(Q \vee R)$
        - Vi kan konkludere med at påstanden holder
      - Bevis påstanden «hvis P er usann så er $P \vee (P \wedge Q)$ sann»
        - Vi antar at P er usann
        - Hvis P er usann er også $(P \wedge Q)$ usann
        - Da er også $P \vee (P \wedge Q)$ usann
        - Da har vi vist at hvis P er usann så er $P \vee (P \wedge Q)$ usann.
    - Legg merke til at bevisene i de to første eksemplene ikke inneholder noen forkomster av ordene «ikke» eller «usann» eller konnektivet $\neg$.

        - Hvis vi skal bevise at Y er en logisk konsekvens av X, kan vi anta at X er sann og ut fra denne antakelsen alene vise at Y også er sann
        - Når vi ønsker å vise at en påstand på formen «hvis F, så G» er sann, begynner vi med å anta at F er sann, og fra det viser vi at G også må være sann.
        - Hvorfor må vi ikke også se på tilfellet hvor F er usann?
            - Fordi vi ikke trenger det. Det er kun ett tilfelle hvor en påstand på formen «hvis F, så G» blir usann, og det er når F er sann og G er usann. Et direkte bevis ekskluderer denne muligheten
    - Eksistensbevis
        - En eksistenspåstand er en påstand som sier at noe eksisterer
        - VI beviser eksistenspåstander ved å helt enkelt finne objektet som gjør påstanden sann. Slike bevis kalles eksistensbevis
            - Eksempel
                - «Det finnes et naturlig tall x slik at x + x = 4»
                    - Bevis: La x være tallet 4. Da må x +x være lik 8
                - «Det finnes en valuasjon som gjør $P \rightarrow \neg P$»
                    - Bevis: Velg en valuasjon som gjør P usann. Denne gjør $P \rightarrow \neg P$ sann.
    - Bevis ved tilfeller
        - En annen, vanlig bevismetode er bevis med tilfeller eller bevis ved uttømmelse
        - Her deles et bevis opp i mindre deler, som til sammen dekker det vi skal bevise, og hver enkelt del blir bevist hver for seg.
            - La A = {1,2} og la B = {1,2,3,4}. Vis at $A \subseteq B$
            - Bevis:
                - La x være et element i A
                - Vi må fra denne antakelsen vise at x er et element i B
                - Enten vil x =1 eller x = 2
                - I begge tilfeller er x et element i B
                - Vi kan konkludere med at x er et element i B, og dermed med at $A \subseteq B$
    - Bevis for universelle påstander
        - Universelle påstander er påstander som sier noe om alle objekter av en bestemt type
        - For eksempel «alle partall er delelige med 2» eller «enhver valuasjon som gjør P sann, må gjøre $(P \vee Q)$ sann»
        - En vanlig måte å beise universelle påstander, er ved å velge et vilkårlig objekt og vise at dette objektet har den ønskede egenskapen
        - Ordet «vilkårlig» betyr at det ikke ligger noen føringer på hvilket objekt vi velger; det kunne like gjerne ha vært et annet objekt.
        - Med andre ord skal vi ikke anta noe som helst om objektet.
        - Hvis vi skal være presise, sier vi gjerne til slutt «fordi objektet vilkårlig valgt, holder påstanden for alle objekter.»
        - Eksempel
            - Vis at enhver valuasjon som gjør P sann, må gjøre $P \vee Q$ sann
            - Velg en vilkårlig valuasjon, og anta at denne gjør P sann.

        - Ved definisjonen av sannhetsverditabellen for $\vee$-formler må den gjøre (P$\vee$Q) sann
        - Fordi valuasjonen var vilkårlig valgt, følger det at enhver valuasjon som gjør P sann, må gjøre (P$\vee$Q) sann
    - Hvorfor er det slik at dette alltid fungerer?
    - Grunnen er at nå vi velger et vilkårlig element, kan det være et hvilket som helst element
    - Dette elementet blir en plassholder for et hvilket som helst av de andre elementene.
    - Hvis argumentet fungerer for dette elementet, må det også fungere for alle de andre elementene. Derfor må argumentet golde for alle elementene.
- Moteksempler
    - Hvis en påstand ikke er sann, er det umulig å bevise den
    - Hvis påstanden er universell, er det i prinsippet mulig å finne et moteksempel til den.
    - Et moteksempel er en for form eksistensbevis; det er bevis for at det finnes et tilfelle som gjør den usann.
    - Et moteksempel til Goldbachs formodning vil, for eksempel, være et partall større enn to som ikke kan skrives som summen av to primtall
    - Eksempel
        - Påstanden «P er en logisk konsekvens av (P$\vee$Q)» er ikke sann
        - Valuasjonen som gjør P usann og Q sann er et moteksempel
        - Denne gjør (P$\vee$Q) sann, men P usann, og derfor er ikke P en logisk konsekvens av (P$\vee$Q).
- Kontrapositive bevis
    - Et kontrapositivt bevis for en påstand på formen «hvis F, så G», er et logisk gyldig resonnement som begynner med antakelsen om at G er usann, og som konkluderer med at F er usann
    - Den kontrapositive av formelen (F$\rightarrow$G) er formelen ($\neg$G $\rightarrow\neg$F)
    - En $\rightarrow$ - formel og den kontrapositive formelen er ekvivalente med hverandre
    - God praksis: å si at man har bevist noe kontrapositivt, hvis det er det man gjør
    - Noen ganger er det enklere å bevise påstander kontrapositivt, men et direkte bevis er som oftest å foretrekke.
    - Eksempel
        - Bevis påstanden «hvis 3n + 2 er et oddetall, så er n et oddetall».
        - Vi beviser den kontrapositive påstande, som er ekvivalent
        - «hvis n ikke er et oddetall, så er ikke 3n +2 et oddetall»
        - Herfra er strukturen på beviset identisk med et direkte bevis.
        - Anta at n ikke er et oddetall, altså at n er et partall.
        - Da er n på formen 2x for et heltall x
        - Da er 3n + 2 lik 3(2x) + 2 som er lik 6x + 2.
        - Siden dette tallet er lik 2(3x+1) er det et partall

    - Da er 3n+2 ikke et oddetall
    - Dermed har vi bevist den opprinnelige påstanden.
- Motsigelsesbevis
  - Et motsigelsesbevis for en påstand er et bevis som begynner med antakelsen om at påstanden er usann og som viser hvordan denne antakelsen fører til en motsigelse. Beviset konkluderer med at påstanden må være sann
  - Hvis vi antar at en påstand ikke er sann, og dette fører til en motsigelse, konkluderer vi med at påstanden må være sann
  - Legg merke til at konklusjonen er positiv; den sier at påstanden er sann
  - I et motsigelsesbevis antar vi at det motsatte av hva vi vil bevise, og hvis dette fører til en motsigelse, er det ikke mulig, og da har vi bevist det vi ønsker
  - Eksempel
    - Bevis at formelen $(P \to Q) \vee (Q \to P)$
    - Anta for motsigelse at påstanden ikke holder
    - Da må det finnes en valuasjon som gjør formelen usann.
    - Den eneste måten å gjøre en diskusjon usann på, er ved å gjøre begge disjunktene usanne
    - Da må denne valuasjonen gjøre både $(P \to Q)$ og $(Q \to P)$ usanne
    - Siden valuasjonen gjør $(P \to Q)$ usann, må den gjøre P sann og Q usann.
    - Siden valuasjonen gjør $(Q \to P)$ usann, må den gjøre Q sann og P usann.
    - Det er ikke mulig at en valuasjon gjør både P sann og usann, og vi har en motsigelse
    - Vi kan konkludere med at $(P \to Q) \vee (Q \to P)$ er sann for alle valuasjoner.
  - I et motsigelsesbevis viser vi at noe er sant ved å vise at det ikke er mulig at det er usant
  - Dette forutsetter riktignok at en påstand er sann hvis og bare hvis den ikke er usann, men slik er det i utsagnslogikk
  - Slike bevis begynner som oftest med «anta for motsigelse at påstanden ikke holder»
  - Det kan noen ganger være enklere å bevise noe ved et motsigelsesbevis, men som oftest er det mer enn vi behøver
  - Motsigelsesbevis er heller ikke konstruktive i samme forstand som eksistensbevis og direkte bevis.
- Konstruktive bevise versus ikke-konstruktive bevis
  - Et motsigelsesbevs er et eksempel på et ikke-konstruktivt bevis
  - Et motsigelsesbevis for en påstand om at noe finnes trenger ikke å vise frem objektet som gjør påstanden sann
  - Det er det som gjør det til et ikke-konstruktivt bevis
  - Hvis beviset viser fem eller gir en metode for å finne objektet, er det konstruktivt

        - Anta for eksempel at vi ønsker å bevise påstanden «det finnes liv på Mars»
        - Et motsigelsesbevis vil begynne med antakelsen om at det ikke finnes liv på Mars og ende med en motsigelse, for så å konkludere med at det faktisk finnes liv på Mars.
        - Mange mener at et slikt bevis ikke er godt nok. Et konstruktivt bevis er et hvor vi faktisk finner og påviser at det er liv på Mars.
- Bevis for at noe ikke er sant
    - Hvis vi vil bevise at en påstand ikke er sann, kan vi begynne med å anta påstanden er sann, og vise hvordan det leder til en motsigelse
    - Dette er ikke det samme som et motsigelsesbevis, men et drekte bevis for at noe er usant
    - Dette er en subtil, men viktig, forskjell, som vi kan illustrere med utsagnslogikk. Et motsigelsesbevis for at en påstand P er sann, er et bevis for at $\neg$ P leder til en motsigelse
    - Et bevis for at en påstand P ikke er sann, er et bevis for antakelsen om at P er sann leder til en motsigelse.
    - Vi kan illustrere det på følgende måte.



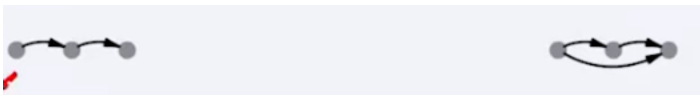
        - Bevis at formlene P og (P$\rightarrow\neg$P) ikke kan være sann samtidig
            - Anta at P og (P$\rightarrow\neg$P) er sanne samtidig
            - Da finnes det en valuasjon som gjør P sann og (P$\rightarrow\neg$P) sann
            - Ved tolkningen av $\rightarrow$ - må valuasjonen gjære $\neg$P sann
            - Ved tolkningen av $\neg$ - formler følger det at P er usann
            - Men det er umulig fordi vi har antatt at valuasjonen gjør P sann
            - Vi kan konkludere med at formlene ikke kan være sanne samtidig.

Kapittel 6 – relasjoner

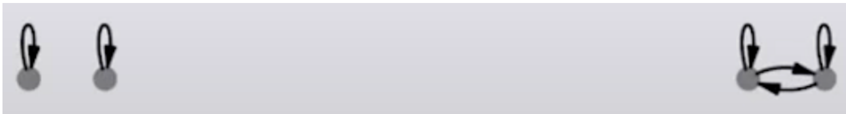
Vi skal studere relasjoner i et matematisk og abstrakt perspektiv
Vi møter på relasjoner hele tiden
Vi bruker mindre eller lik-relasjonen $\geq$ på reelle tal, delmengderelasjonen $\subseteq$ på mengder og logisk konsekvens-relasjonen $\Rightarrow$ på utsagnslogiske formler

- En binær relasjon fra mengden S til mengden T er en delmengde av S $\times$ T
- En binær relasjon på mengden S er en delmengde av S^2 = S$\times$ S
- Mer generelt, en n-ær relasjon er en delmengde av $A_1 \times \ldots \times A_n$, og en n-ær relasjon på en mengde A er en delmengde av A^n.

- Nå vi bruker ordet «relasjon», er det som oftest underforstått at dette betyr en binær relasjon
- Eksemplet
  - Følgende er en binær relasjon fra {a,b,} til {1,2}
    - Dette gir følgende kryssmengde
    - {<a,1>, <a,2>, <b,1>, <b,2>}
  - {<a,1>,<a,2>,<b,2>}
  - Følgende er en binær relasjon på mengden {1,2,3}
    - Dette gir følgende kryssmengde
    - {<1,2>, <1,3>,<2,3>,<3,3>}
  - {<1,2>, <1,3>,<2,3>,<3,3>}
- Ulike relasjoner
  - Identitetsrelasjonen
    - Relasjonen på S, som relaterer alle elementer til seg selv: {<x,x>| x∈S}. Her er identitsrelasjonen på mengden {1,2,3}:
      - {<1,1>, <2,2>, <3,3>}
  - Den tomme relasjonen
    - Relasjonen fra S til T, som. Ikke realterer noen elementer til hverandre: ∅. Her er den tomme relasjonen på mengden {1,2,3}
      - ∅
  - Den universelle relasjonen fra til T, som relaterer alle elementer i S til alle elementer i T. S×T. Dette er altså det samme som kryssproduktet til S og T
- Notasjon
  - Hvis R er en relasjon og <a,b> ∈ R, tillatter vi oss å skrive aRb i stedet for <a,b> R.
  - VI skriver for eksempel 4<5 istedet for <4,5> ∈ <.
  - Dette kalles infiksnotasjon
- Refleksivitet
  - EN binær relasjon R på mengden S er refleksiv hvis det for alle x i S er slik at <x,x> ∈ R
  - **Refleksive relasjoner er de hvor alt er relatert til seg selv.**
  - Eksempel
    - La S være mengden {1,2,3}
      - Er {<1,1>,<1,2>,<1,2>} en refleksiv på S?
        - Nei, fordi <2,2> og <3,3> ikke er med
      - Hva med {<1,1>,<2,2>,<3,3>}?
        - Ja
      - Hva med {<1,2>,<1,2>,<2,2>,<2,3>,<3,3>}?
        - Ja
  - Refleksive relasjoner
    - Likhetsrelasjonen på en mengde er alltid refleksiv
    - Delmengderelasjonen ⊆ er refleksiv
    - Mindre enn eller lik-relasjonen ≤ på tall er refleksiv
    - Logisk konsekvens-relasjonen ⇒ på formler er refleksiv
    - Den universelle relasjonen på en mengde er refleksiv
  - Ikke-refleksive relasjoner
    - Den vanlige mindre enn-relasjonen < er ikke refleksiv

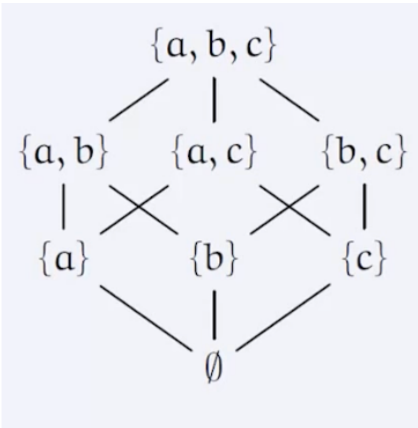
        - Forelder-relasjonen på mennesker er ikke refleksiv
- Symmetri
    - En binær relasjon R på mengden S er symmetrisk hvis det for alle x, y er slik at hvis <x,y> ∈ R, så <y,x> ∈ R
    - **Symmetriske relasjoner er de hvor rekkefølgen på elementene ikke spiller noen rolle**
    - Eksempel
        - La S være mengden {a,b,c}
            - Er {<a,b>,<b,a>,<c,b>,<b,c>} en symmetrisk relasjon på S?
                - Ja
            - Hva med {<a,b>,<b,a>,<a,c>}
                - Nei, har vi <a,c>, må vi ha med <c,a> også for at den skal bli symmetrisk
    - Symmetriske relasjoner
        - Likhetsrelasjonen på en mengde er alltid symmetrisk
        - Logisk ekvivalens-relasjonen ⇔ på formler er symmetrisk
        - Den universelle relasjonen på en mengde er symmetrisk
        - Kjæresterelasjonen er symmetrisk
            - Er A kjæresten til B, er B kjæresten til A.
    - Ikke-symmetriske relasjoner
        - Delmengderelasjonen ⊆ er ikke symmetrisk
        - Mindre enn eller lik-relasjonen ≤ på tall er ikke symmetrisk
        - Logisk konsekvens-relasjonen ⇒ på formler er ikke symmetrisk
        - Den universelle relasjonen på en mengde er ikke symmetrisk
        - Forelder-relasjonen på mennesker er ikke symmetrisk
- Transitivitet
    - En binær relasjon på mengden S er transitiv hvis det for alle x,y,z er slik at hvis <x,y> ∈ R og <y,z> ∈ R, så <x,z>∈ R.
    - **Transitive relasjoner er hvor alt du kan gjøre i to steg kan du også gjøre i ett steg.** 
    - Eksempel
        - La S være mengden {1,2,3}
            - Er {<1,2>,<2,3>,<1,3>} en transitiv relasjon på S
                - Ja
            - Er {<1,2>,<2,3>} transitiv?
                - Nei, fordi <1,3> mangler
            - Hva med {<1,2>,<2,1>}?
                - Nei, fordi <1,2> og <2,1> er med, men både <1,1> og <2,2> mangler.
        - Transitive relasjoner
            - Likhetsrelasjonen på en mengde er alltid transitiv
            - Delmengderelasjonen ⊆ er alltid transitiv
            - Mindre enn eller lik-relasjonen ≤ på tall er alltid transitiv
            - Logisk konsekvens-relasjonen ⇒ og ekvivalens-relasjonen ⇔ på formler alltid transitive

- Etterkommer-relasjonen på mennesker er transitiv
  - Mine etterkommere sine etterkommere er også mine etterkommere
- Ikke transitive relasjoner
  - Forelder-relasjonen på mennesker er ikke transitiv
  - Vennerelasjon er ikke transitiv.
    - Mine venners venner er ikke nødvendigvis ikke nødvendigvis mine venner.
  - Kjæresterelasjonen er ikke transitiv.

- Ekvivalens
  - En binær relasjon på mengden S er en ekvivalensrelasjon hvis den er refleksiv, symmetrisk og transitiv.
  - **Ekvivalensrelasjoner er de som forteller oss om elementer er like**
  - 
  - Eksempler
    - La S være mengden {1,2,3}
      - Er relasjonen {<1,1>,<2,1>,<1,2>,<2,2>,<3,3>} en ekvivalensrelasjon på S?
        - Ja, fordi den refleksiv, symmetrisk og transitiv.

      - Er relasjonen {<1,1>,<2,1>,<1,2>} en ekvivalensrelasjon på S?
        - Nei, denne mangler <2,2>, <3,3>. Denne er hverken refleksiv eller transitiv.
- Anti-symmetri
  - EN binær relasjon R på mengden S er anti-symmetrisk hvis det for alle x,y er slik at hvis <x,y> ∈ R og <y,x>∈ R så x=y.
  - **Anti-symmetriske relasjoner er de hvor det ikke finnes to forskjellige elementer som er relatert til hverandre.**
  - Eksempel
    - La S være mengden {1,2,3}
    - Er {<1,2>,<1,3>} en anti-symmetrisk relasjon på S?
      - Ja
    - Hva med {<1,2>,<2,1>}?
      - Nei, fordi <1,2> og <2,1> er med, men 1≠ 2.
- Irrefleksivitet
  - EN binær relasjon på R mengden S er irrefleksiv hvis det ikke er noen x ∈ R slik at <x,x> ∈ R
  - **Irrefleksive relasjoner er de hvor ingenting er relatert til seg selv.**
  - Eksemplet
    - La S være mengden {1,2,3}
      - Er {<1,2>,<2,1>} en irrefleksiv relasjon på S?

        - Ja
      - Hva med {<3,1>,<3,2>,<3,3>}?
        - Nei, fordi den har med <3,3>
- Ordninger
  - Partiell ordning
    - En binær relasjon på mengden S er en partiell ordning hvis den er refleksiv, transitiv og anti-symmetrisk
    - **Partielle ordninger er relasjoner med en retning.**
    - Eksempel
      - Mindre eller lik relasjonen $\leq$ på reelle tall er en partiell ordning
      - Mindre enn relasjonen $<$ er ikke det. Den er ikke refleksiv
      - Logisk konsekvens-relasjonen $\Rightarrow$ er ikke en partiell ordning.
      - Delmengderelasjonen $\subseteq$ er en partiell ordning.

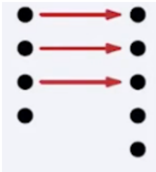
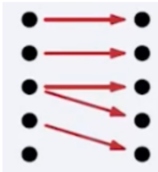
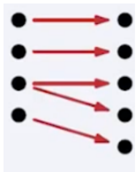


  - Totale ordninger
    - En partiell ordning R på en mengde S kalles en total ordning eller en lineær ordning hvis det for alle x og y i S er slik at xRy eller yRx
    - Totale ordninger er relasjoner som ordner alle elementene i en mengde etter hverandre
    - Eksempel
      - Mindre eller lik relasjonen $\leq$ på reele tall er en total ordning
      - Delmengderelasjonen $\subseteq$ trenger ikke å være en total ordning, fordi det er mulig å ha to mengder A og B uten at Hverken

Kapittel 7 – funksjoner

Definisjon

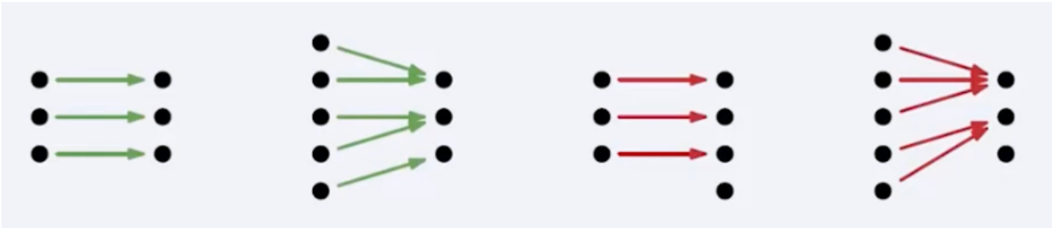
- En funksjon fra A til B er en binær relasjon f fra A til B slik at for enhver $x \in A$, er det nøyaktig ett element $y \in B$ slik at <x,y>$\in$f
- Vi skriver f(x)=y når <x,y> $\in$ f. I dette tilfellet kaller vi x for argumentet og f(x) for verdien til funksjonen
- Vi skriver f: $A \rightarrow B$ for funksjonen f når den er en funksjon fra A til B
- Eksempel
  - Relasjonen {<1,1>,<2,2>,<3,3>} er en funksjon fra {1,2,3} til {1,2,3}
    - Hvis vi kaller denne funksjonen for f, få vi at f(1)=1, at f(2)=2 og at f(3) = 3.
- Eksempel på hva som ikke er en funksjon

        - Relasjonen {<1,b>,<2,a>} fra {1,2,3} til {a,b} er ikke en funksjon, fordi det mangler et tuppel på formen <3,x>
        - Relasjonen {<1,1>,<1,2>} på {1,2} er heller ikke en funksjon, fordi 1 forekommer som første element i to tupler. Det er ikke lov
- Notasjon
    - F(x)=2x står for funksjonen som inneholder alle tupler på formen <x,2x>. F.eks. <1,2>, <2,4>, <0.5, 1>
    - F(x) = y
        - «F av x er lik y»
        - «F sender x til y»
        - «F anvendt på x gir/returnerer y»
- Definisjon- og verdiområde
    - La f være en funksjon fra A til B
    - Mengden A kalles definisjonsområdet til f
    - Mengden B kalles verdiområdet til f.
    - Eksempler på binære relasjoner som ikke er funksjoner
       ,  ,  og 
    - Noen funksjoner
        - En tilordning av sannhetsverdier til utsagnsvariabler er en funksjon fra mengden av utsagnsvariabler til {0,1}
        - En valuasjon er en funksjon fra mengden av alle utsagnslogiske formler til {0,1}
        - Funksjonen s: N→N som er slik at s(x)=x+1 kalles etterfølgerfunksjonen på de naturlige tallene
        - Hvis A er en mengde, er identitetsfunksjonen på A funksjonen id_A som er slik at $id_A(x)= x$ for alle $x \in A$
- Injektiv funksjon
    - En funksjon f: A→B er injektiv hvis det for alle elementer x og y i A er slik at hvis $x \neq y$, så $f(x) \neq f(y)$
    - VI sier i såfall at f er en injeksjon og en-til-en
    - **Injektiv betyr altså at to forskjellige elementer sendes til to forskjellige elementer.**
    - Eksempler, grønt i injektiv og rødt er ikke injektiv

- Bildemengden til en funksjon
    - La f være en funksjon fra A til B, og la X være en delmengde av A
    - Mengden $\{f(x) | x \in X\}$ kalles bildet av X under f og skrives f[X]

- Bilder av hele A under f, f[A], kalles bildemengden til f

- Surjektive funksjoner
  - En funksjon f: A→B er surjektiv hvis det for alle y∈B, finnes en x∈A slik at f(x) = y.
  - Vi sier i så fall at f er en surjeksjon og på
  - Eksempler, grønt i surjektiv og rødt er ikke surjektiv



- Bijektive funksjoner
  - En funksjon er bijektiv hvis den er injektiv og surjektiv
  - Vi sier også at funksjonen er en bijeksjon og en en-til-en korrespondanse.
  - Eksempler, grønt i bijektiv og rødt er ikke bijektiv

- Maling
  - En injektiv maler, maler hele veggen
  - En surjektiv maler, maler aldri samme sted
  - En bijektiv maler, maler hele veggen uten å male samme sted to ganger

- Eksempler
  - F(x)=2x
    - Injektiv og surjektiv
  - F(x)=x^2
    - Hverken surjektiv eller injektiv.
- Funksjoner med flere argumenter
  - Når definisjonsområdet til en funksjon f er et kartesisk produkt av n menfder, skriver vi $f(x_1,....,x_n)$ i stedet for $f(<x_1,....,x_n>)$
- Sammensetning av funksjoner

  - Hvis f: A→B og g: B→C er funksjoner
    - g∘f : A→C
    - definert som funksjonen vi får ved å første anvende f, deretter anvende g på verdien av dette, det vil si (g∘f)(a)= g(f(a))
  - Eksempel

- Hvis f(x)=2x og g(x)= x+3, blir sammensetningen g∘f lik funksjonen som gir 2x+3
  - (g∘f)(x)=g(2x)=2x+3
  - Først multipliseres det med 2. Deretter legges det til 3.
  - Den andre sammensetningen f∘g er lik funksjonen som gir 2(x+3)

- Oppgave

  La f og g være gitt på følgende måte:

  - $f : \{1, 2, 3\} \to \{a, b, c, d\}$ er funksjonen $\{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, d\rangle\}$
  - $g : \{a, b, c, d\} \to \{4, 5\}$ er funksjonen $\{\langle a, 4\rangle, \langle b, 5\rangle, \langle c, 4\rangle, \langle d, 5\rangle\}$

  Hva er $(g \circ f)(1)$?

  - (g∘f)(1)=g(f(1))=g(a)=4
  - Først anvendes f på argumentet 1, noe som gir verdien a, og så anvendes g på og vi ender opp med verdien 4

- Operasjoner
  - En unær operasjon på en mengde A er en funksjon fra A til A
  - En binær operasjon på en mengde A er en funksjon fra A×A til A
  - Mer generelt, en n-ær operasjon på en mengde A er en funksjon fra A^n til A
  - Eksempel
    - Hvorvidt en funksjon er en operasjon, avhenger av definisjonsområdet
    - Det å addere eller multiplisere er operasjoner på de fleste tallmengder, men det samme er ikke tilfellet for det å trekke fra eller dele
    - For eksempel er ikke det å trekke fra, en operasjon på mengden av naturlige tall. Det fordi x-y kan bli et negativt tall, som er utenfor definisjonsområdet
    - På mengden av reelle tall er minusfunksjonen en operasjon
    - I mengdelære har vi at både snitt og union er operasjoner
    - Etterfølgerfunksjonen, som tar et naturlig tall og legger til én, er et eksempel på en unær operasjon på mengden av naturlige tall.
- Funksjoner som objekter
  - Høyreordens funksjon
    - Det er ingenting i veien for at funksjoner kan ta andre funksjoner som argumenter
    - Vi har allerede sett ett eksempel på dette, og det er sammensetningsoperasjonen ∘ som setter sammen to funksjoner til Én

Kapittel 8 – mer mengdelære

- Den universelle mengden
  - Hva er mengden av elementer som ikke er med i en mengde?
  - Hva er mengden av elementene som ikke er med i {1,2,3}?

- Vi antar at det i alle kontekster er en underliggende universell mengde og at U står for denne mengden. Hvis ingenting annet er spesifisert, antar vi at U står for en vilkårlig universell mengde

- Hva som er den universelle mengden varierer fra sammenheng til sammenheng.
- Noen ganger kan den være mengden av naturlig tall; andre ganger kan den være mengden av utsagnslogiske formler.
- I definisjonene av de andre operasjonene på mengder har ikke den universelle mengden vært nødvendig.
- I definisjonen av snitt er for eksempel (A∪B) definert fra mengdene A og B alene

- Komplementet til mengder
  - Hvis M er en mengde, og U er den universelle mengden, er komplementet til M mengden av alle elementer i U som ikke er med i M.
  - Legg merke til at denne mengden er lik U\M
  - Når vi skriver denne mengden, må den universelle mengden være kjent eller vi må anta at det finnes en vilkårlig universell mengde

  - Eksempler
    - Anta at U = {1,2,3,4,5,6}
    - Komplementmengden til den tomme mengden er {1,2,3,4,5,6}
    - Komplementmengden til {1} er {2,3,4,5,6}
- Regne med Venn-diagrammer
  - https://logiskemetoder.no/nettkurs/innhold/08/02/00
  - Eksempel
    - A = {x|x er et oddetall}
    - B = {x|x>7}
    - C = {x|x er delelig på 3}
    - Hvilke av disse tallene er elementer i $(A \cup B) \cap \overline{C}$?
    - A = {1,3,5,7,9,11,...}
    - B = {8,9,10,11}
    - Komplementet til C = {1,2,4,5,7,8,10,11}
    - (A∪B) = {1,3,5,7,8,9,10,11}
    - {1,2,3,5,7,8,9,10,11}∩ {1,2,4,5,7,8,10,11} = {1,5,7,8,10,11}
    - SVAR: {1,5,7,8,10,11}
- Potensmengder
  - Hvis M er en mengde, er potensmengden til M mengden av alle delmengder av M.
  - Vi skriver P(M) for potensmengden til M
  - Eksempler
    - Potensmengden til Ø

            - {Ø}
        - Potensmengden til {1}
            - Svar: {Ø,{1}}
        - Potensmengden til {1,2}
            - {Ø,{1},{2},{1,2}}
    - Hvis en endelig mengde har n elementr, har potensmengden alltid 2^n elementer
    - Det er fordi det er 2^n delmengder av en mengde med n elementer
    - Én mpte å forstå det på er ved å se at det er to muligheter for hvert av de n elementene: Enten er det med eller er det ikke med.
- Kardinalitet
    - To mengder M og N har lik kardinalitet hvis det finnes en en-til-en korrespondanse mellom elementene i M og N
    - Vi skriver |M| = |N| når det er tilfellet
    - Mengden M har kardinalitet mindre eller lik N hvis det finnes en en-til-en korrespondanse mellom M og en delmengde av N.
    - Hvis M er en endelig mengde, er kardinalitet til M lik antall elementer i M, og i så fall bruker vi notasjonen |M| for antall elementer i M
    - Eksempel (Lik kardinalitet, endelige mengder)

    - Eksempel (uendelige mender)
        - N er mengden av naturlige tall
        - 2N er mengden av alle naturlige partall
        - Funksjonen f(x) = 2x fra N til 2N gir en en-til-en korrespondanse mellom N og 2N
        - Det betyr at N og 2N har samme kardinalitet
    - Kardinalitet er set.len()

- Tellbarhet
    - En uendelig mengde M er tellbar hvis det er en-til-en korrespondanse mellom elementene i M og de naturlige tallene. Hvis ikke, er M overtellbare. Alle endelige mengder er tellbare.
    - En mengde er med andre ord tellbar hvis den har samme kardinalitet som de naturlige tallene
    - Det betyr at alle elementene i mengden kan telles opp og at ethvert element får hvert sitt naturlige tall
    - Eksempel
        - Mengden av heltall, Z , er tellbar
        - For å bevise dette, må vi lage en en-til-en korrespondanse mellom denne mengden og mengden av naturlige tall.
        - Dette kan vi gjøre på følgende måte

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f(x)	0	−1	1	−2	2	−3	3	−4	4	−5	5	−6	6	−7	7

- Overtellbarhet
  - Det finnes mengder som er så store at de ikke er tellbare
  - Georg Cantor var den første som beviste dette
    - I en artikkel i 1874 ga han et bevis for at mengden av reelle tall ikke hadde samme kardinalitet som de naturlige tallene, med andre ord at mengden av reelle ikke var tellbar
  - Generelt sett er det slik at potensmengden til en mengde altid har større kardinalitet enn mengden selv
  - Potensmengden er også definert for uendelige mengder, og vi kan bevise at det aldri eksisterer en surjektiv funksjon fra en mengde til dens potensmengde
  - Overtellbarhet via diagonalisering
    - La oss se på mengden av uendelige sekvenser på formen hvor hver b er enten 0 eller 1.
    - Vi kan godt tenke på en slik sekvens som en funksjon fra naturlige tall til {0,1}
    - Nå skal vi bevise at mengden av alle sekvensene er overtellbar ved et motsigelsesbevis. Anta for motsigelse at det finnes en en-til-en korrespondanse mellom denne mengden og de naturlige tallene.

sekvens 0:	1	1	0	1	1	0	1	0	1	1	...
sekvens 1:	0	0	1	1	0	1	1	1	1	1	...
sekvens 2:	1	1	1	0	0	0	0	0	0	1	...
sekvens 3:	1	1	0	0	1	0	1	0	0	0	...
sekvens 4:	0	1	1	0	0	1	0	0	1	1	...
sekvens 5:	1	0	0	0	1	0	1	0	1	0	...
sekvens 6:	1	0	1	1	0	1	0	1	0	0	...
sekvens 7:	1	1	0	0	1	1	0	1	0	0	...
sekvens 8:	1	0	1	1	0	1	1	0	0	1	...
sekvens 9:	1	1	1	0	0	0	1	0	0	1	...
⋮											⋱
sekvens x:	0	1	0	1	1	1	1	0	1	0	...

Kapitttel 9 – Tillukninger og induktivt definerte mengder

- Definere mengder
  - Å definere mengder induktivt er en måte å definere mengder på som er nyttig og som brukes mye i både informatikk og matematikk
  - Å definere mengder induktivt betyr å bygge dem opp nedenfra eller innenfra
  - Det er måte å konstruere mengder på steg for steg
  - Når vi har definert en mengde induktivt, har vi god kontroll på hvilke elementer som er i mengden

- Det blir enklere å behandle og bevise påstander om mengden, enn om vi definerte den på en mer abstrakt måte
- Vi vil også se at det å definere en mengde induktivt er å fange inne noe komplekst ved hjelp av enkle regler
- Som en viktig forberedelse og oppvarming, ser vi først på tillukninger av relasjoner og mengder

- Tillukning av mengder
  - En viktig egenskap ved induktivt definerte mengder er at de er lukket under gitte operasjoner, og derfor ser vi først på det:
  - At en mengde er lukket under en gitt operasjoner, betyr at når vi utfører denne operasjonen på ett eller flere elementer i mengden, er vi garantert at resultatet er et element i den samme mengden
  - Hvis M er en mengde, kalles den minste mengden som inneholder M og som er lukket under en eller flere operasjoner, tillukningen av M under disse operasjonene.
  - Eksempel
    - Er mengden av naturlige tall lukket under addisjon.
      - Hvis du adderer to naturlige tall, får du et nytt naturlig tall
    - Er mengden av naturlige tall lukket under multiplikasjon.
      - Hvis du ganger to naturlige tall, får du et nytt naturlig tall
    - Er mengden av naturlige tall lukket under subtraksjon.
      - Den er ikke lukket, fordi du kan ta et naturlig tall minus et annet naturlig tall og få et negativt tall
    - Er mengden av rasjonale tall(brøker) lukket under addisjon
      - Ja
    - Er mengden av rasjonale tall(brøker) lukket under multiplikasjon
      - Ja
    - Er mengden av rasjonale tall(brøker) lukket under kvadratrot
- Tillukning av binære relasjoner
  - Hvis R er en relasjon, kalles den minste relasjonen som inneholder R og som har en gitt egenskap, tillukningen av R med hensyn til denne egenskapen.
  - Hvis egenskapen dert er snakk om er refleksivitet, symmetri eller transitivitet, kalles tillukningen henholdsvis den refleksive, symmetriske eller transitive tillukningen av R.
  - Eksempel

    La $R = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,1\rangle, \langle 2,2\rangle\}$ være en relasjon på mengden $\{1,2,3,4\}$.

    Det kan være lurt å tegne relasjonen som prikker og piler slik som i videoen!

    - Hvilken av disse er den refleksive tillukningen av R?
      - R ∪ {⟨1,1⟩,⟨3,3⟩,⟨4,4⟩}
    - Hva er den transitive tillukningen av {<1,2>,<2,3>,<3,4>}
      - {<1,3>, <2,4>, <1,4>}

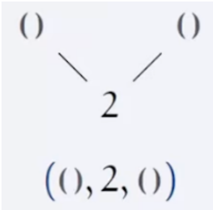
- Induktivt definerte mengder

- En induktivt definert mengde er den minste mengden som inneholder en gitt mengde – kalt en basismengde – og som er lukket under gitte operasjoner. En mengde defineres induktivt i følgende tre steg:
    - Basisteget: å spesifisere en basismengde
    - Induksjonssteget: å spesifisere operasjonene
    - Tillukningen: å ta den minste mengden som inneholder basismengden og som er lukket under operasjonene

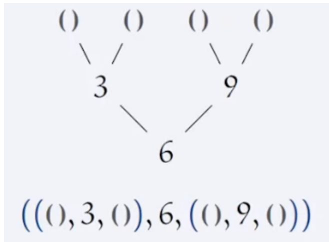
- Tallmengder
  - Mengden av naturlige tall kan defineres induktivt som den minste mengden N som er slik at
    - $0 \in N$ og
    - Hvis $x \in N$, så $x+1 \in N$
  - Mengden av partall er den minste mengden som inneholder 0 og som er lukket under operasjonene som henholdsvis legger til og trekker fra to.
- Utsagnslogiske formler
  - Mengden av utsagnslogisk formler er den minste mengden X slik at følgende holder
    - Enhver utsagnsvariabel er med i X
    - Disse utgjør basismengden og kalles atomære formler
    - Hvis F er med i X, er $\neg F$ med i X
    - Hvis F er med i X, så er $(F \wedge G)$, $(F \vee G)$ og $(F \rightarrow G)$ med i X

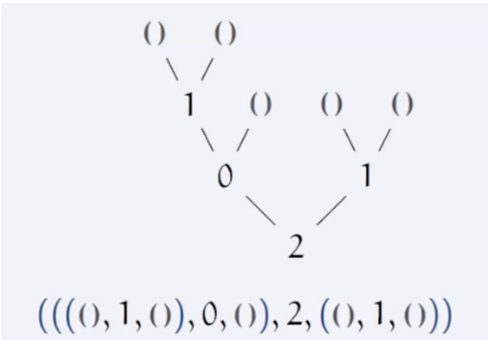
- Lister
  - Lister likner på tupler, men er ikke det samme som tupler
  - VI skriver lister ved å angi elementene i listen med komma mellom og ved å sette parentesene utenfor:
    - ()
    - (1)
    - (2,3,4)
    - (1::(2,3,4)) = (1,2,3,4)
    - (4::()) = (4)
  - Så lenge det er entydig, kan vi droppe parentesene rundt (x::L) g skrive x::L, men parentesen som angir listen må være på plass.
  - Mengden av lister over en mengde A er induktivt definert som den minste mengden slik at følgende holder:
    - () er en liste over A
      Dette er den tomme listen over A
    - Hvis $x \in A$, og L er en liste over A, er x::L en liste over A.
  - Eksempel
    - For å få listen (1,2,3), kan vi begynne med dne tomme listen og legge til elementer ved hjelp av :: på følgende måte
      - 1::(2::(3::())).
- Binære trær
  - En annen type struktur som brukes mye, spesielt i informatikk, er såkalte binære trær
  - Trær er viktige fordi de gjør det mulig for oss å lage og representere informasjon på en måte som ikke er flat, men som har mer struktur.

- Mengden av binære trær over en mengde A er den minste mengden slik at følgende holder:
  - () er binært tre over A
    Dette kalles det tomme binære treet eller bare det tomme treet
  - Hvis x∈A, og V og H er binære trær over A, er (V,x,H) et binært tre over A
    Elementet x kalles en node i det binære treet
    Når et binært tre på formen ((),x,()), kalles x en bladnode eller en løvnode
- Eksempel



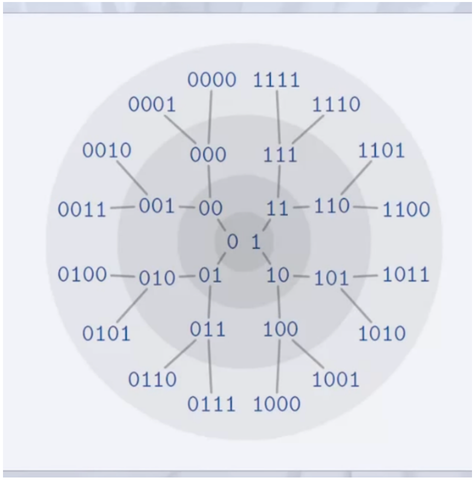
  - ((),2,())
  - ((( ),3,( )),6,(( ),9,( )))
  - ((((), 1, ()), 0, (),2,((), 1, ()))





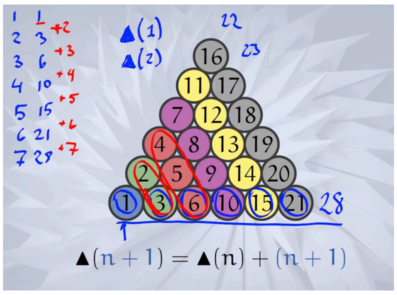
- Programmeringsspråk
- Alfabeter, tegn, strenger og formelle språk
  - Anta at A er en mengde av tegn
  - Mengden A kalles et alfabet
  - Mengden av strenger over A er den minste mengden A* slik at:
    - Λ∈A*, hvor symbolet står for den tomme strenger og
    - Hvis s∈ A* og x∈A, er sx ∈ A*, hvor sx står for resultatet av å slå sammen s og x.
  - Vi skriver s i stedet for Λs
  - Et språk over A er en delmengde av A
- Mengder av strenger
  - Her er mengden av strenger over noen enkle alfabeter
    - Ø* = { Λ }
    - {a}* = { Λ , a, aaa, aaaa, aaaaaa...}
    - {0,1} = { Λ , 0, 1, 00, 01, 10, 11, 000, 001,...}
    - {a,b,c} = { Λ , a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, ...}
- Alle strenger med et partall antall tegn
  - La S være den minste mengden slik at
    - Λ∈S
    - Hvis t ∈ S, så taa, tab , tba, tbb ∈ S
  - Vi får at aaaa ∈ S

- Men aaa ∈ S
- Hvordan ser S ut?
- Mengden S inneholder alle strenger over (a,b) som har et partall antall tegn

- Konkatenering
  - Operasjonen som består av å slå to strenger s og t sammen til én, st, kalles konkatenering
  - Skrvemåten s^n brukes som en forkortelse for strengen s gjentatt n ganger etter hverandre
  - For eksempel er a^3b^3 det samme som aaabbb.
  - Vi antar at $s^0 = \Lambda$
  - Vi tillater oss her å se bort fra alle forekomster av den tomme strengen
  - Resultatet av å konkatenere en streng s med den tomme strengen blir s, det vil si at $\Lambda s = s\Lambda = s$
  - Eksempel
    - Ett språk over alfabetet {},ba er mengden av alle strenger på former a^nb^n.
    - Det vil si mengden {b, aba, aabaa,...}
    - VI kan beskrive dette språket som $\{a^nba^n \mid n = 0,1,2,...\}$
    - Dette språket kan defineres induktivt som den minste mengden S som er slik at b ∈ S og hvis t ∈ S, så ata ∈ S.
- Bitstrenger
  - EN bitstreng kan godt defineres som en endelig sekvens av 0-er og 1-ere, men ved å definere bitstrenger induktivt, får vi mer kontroll
  - Mengden av bitstrenger er induktivt definert som den minste mengden som er slik at
    - 0 og 1 er bitstrenger
    - Hvis b er en bitstreng er b0 og b1 også bitstrenger
  - 

Kapittel 10 – Rekursive funksjoner

- De triangulære tallene

    - 

- Plassholdere
    - VI bruker plassholdere hele tiden
    - En plassholder er et ord eller en variabel som kan stå for noe annet.
        - F(x) = 2x + 1
        - F(y) = 2y + 1
        - F(input) = 2 input + 1
    - Det er viktig å være klar over at i en gitt kontekst, kan enkelte symboler være reserverte og ikke brukes som plassholdere.
        - f(+)=2+ + 3. Dette er ikke lov
    - Noen ganger ønsker vi å oppgi hva slags form et uttrykk er på, og da bruker vi plassholdere
        - (1+4)/(2+3) er på formen x/y
        - 17 = 16+1 er på formen n+1
        - $(P \to Q) \to (Q \to R)$ er på formen $F \to G$
- Bytte likt med likt
    - Det er ofte underforstått at vi kan bytte ut likt med likt
    - Anta for eksempel at A=B
    - I et stort uttrykk hvor A forekommer, kan vi bytte it A med B fordi de er antatt å være like
    - For eksempel vil (2+3A) være lik (2+3B)
    - Logiske ekvivalenser blir ofte brukt på denne måten, ved at et deluttrykk med ett som er ekvivalent
- Rekursive funksjoner
    - Hvis en mengde M er induktivt definert, kan vi definere en rekursiv funksjon f med definisjonsområdet M på følgende måte:
        - For hvert element x i basismengden til M, spesifiserer en verdi for f(x)
        - Dette kalles basissteget eller basistilfellet for funksjonen
        - For hvert element x i M som fremkommer i et induksjonssteg definer verdien til f(x) ved å bruke de tidligere definerte verdiene for f
        - Dette kalles rekursjonssteget.
    - Eksempel
        - La d(0) = 0
        - La d(n+1) = d(n) + 2, for alle $n \in N$
          Med utgangspunkt i dette kan vi regne ut de første verdiene:
        - D(1) = d(0) + 2 = 0 + 2 = 2
        - D(2) = d(1) + 2 = 2 + 2 = 4
        - D(3) = d(2) + 2 = 4 + 2 = 6

    - Fakultetsfunksjonen
        - La 0! = 1

- La (n+1)! = (n+1)*n!, for alle n ∈ N
  VI regner ut de første verdiene til f ved å følge definisjonen:
- 1! = (0+1)*0! = 1*1 = 1
- 2! = (1+1)*1! = 2*1 = 2
- 3! = (2+1)*2! = 3*2 = 6
- 4! = (3+1)*3! = 4*6 = 24
  Det er formen på argumentet til funksjonen som bestemmer verdien.

- Fibonacci-tallene
  1,1,2,3,5,8
  - Disse kan defineres rekursivt på følgende måte:
  - F(0) = 1 og F(1) = 1
  - F(n+2) = f(n)+ F(n+1) for alle naturlig tall n.

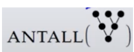
- Bitstregner
  - Eksempel
    - La v(0) = 0 og v(1) = 1
    - Hvis b er en bitstreng, la
      v(b0) = 2 * v(b)
      v(b1) = 2 * v(b) + 1
    - V(100) = v(b0) = 2*v(10)
      - 2*(2*v(1))
      - 2*(2*1)
      - 2*2 = 4
    - V(101) = 2*v(10) + 1
      - 2*(2*v(1)) + 1
      - 2*(2*1) + 1
      - 2 * 2 + 1 = 5
- Valuasjon
  - La t være en tilordning av sannhetsverdier til utsagnsvariabler, vil is en funksjon fra mengden av utsagnsvariabler til {0,1}
  - En valuasjon kan nå defineres rekursivt som en funksjon v fra utsagnslogiske formler til {0,1} på følgende måte:
  - V(P) = 1 hvis og bare hvis t(P)= 1, for alle utsagnsvariabler P
    Dette er basistilfellet i definisjonen.
  - V(¬F) = 1 hvis og bare hvis v(F) = 0
  - V(F∧G) = 1 hvis og bare hvis v(F) = 1 **og** v(G) = 1
  - V(F∨G) = 1 hvis og bare hvis v(F) = 1 **eller** v(G) = 1
  - V(F→G) = 1 hvis og bare hvis v(F) = 1 impliserer v(G) = 1
    Disse fire punktene utgjør rekursjonssteget i definisjonen.
- Lister
  - Lengden av en liste
    - Vi ønsker å definere en funksjon, len, fra lister til naturlige tall slik at hvis L er en liste, fir len(L) lengden til L, det vil si antall elementer i L. Vi definerer len rekursivt på følgende måte;
    - (1) len (())= 0
    - (2) len (x::L) = 1 + len(L)
      Len((a,b,c)) a::(b,c)
      = 1+ len ((b,c))

= 1+1+ len ((c))
=1+1+1+ len (())
=1+1+1+0
= 3

- Sammensetning av lister
  - (1,2,3)+(4,5,6) = (1,2,3,4,5,6)
    Følgende er en rekursiv definisjon av +.
    1. ()+M = M
    2. (x::L) + M = x::(L+M)
       (1,2)+(3,4)
       = 1 :: 2 + (3,4)
       = 1 :: 2 :: () + (3,4)
       = 1 :: 2 :: (3,4)
       = 1 :: (2,3,4)
       = (1,2,3,4)
- Bildet av en liste
  Vi definerer funksjonen map på følgende måte.
  1. map(f, ()) = ()
  2. map(f, x::L) = (f(x)::map(f,L))

  La f være funksjonen som ganger et tall med fire
  Map(f,(1,2,3))
  = 4 :: map(f,(2,3))
  = 4 :: 8 :: map(f,(4))
  = 4 :: 8 :: 12:: map(f())
  = 4 :: 8 :: 12 :: ()
  = 4 :: 8 :: (12)
  = 4 :: (8,12) = (4,8,12)

- Binære trær
  - Mengden av binære trær over en mengde A er den minste mengden slik at følgende holder:
    - () er et binært tre over A
    - Hvis x∈ A, og V og H er binære trær over A, er (V,x,H) et binært tre over A
  - Antall noder i et binært tre definert rekursivt
    - La funksjonen antall fra binære trær til naturlige tall være definert på følgende måte.
      1. antall() = 0
      2. antall(V,x,H) = antall(V)+1+Antall(H)
         antall((),x,()) = antall() + 1 + antall() = 0+1+0 = 1
    - 

      Antall(●)+1+antall(●) = 1+1+1 = 3
    - 

  - Høyden til et binært tre definert rekursivt

        - La høyden til et binært tre være definert på følgende måte, som en rekursiv funksjon høyde fra binære trær til naturlige tall. Funksjonen gir eantallet noder i den lengste grenen ti det binære treet som verdi
          1. Høyde() = 0
          2. Høyde(V,x,H) = 1+max(høyde(V)),høyde(H))

          Som i forrige eksempel får vi at $\text{HØYDE}(\bullet) = 1$, og vi kan regne ut høyden til det binære treet slik:

          $$\text{HØYDE}() = 1 + \max(\text{HØYDE}(\bullet), \text{HØYDE}(\bullet)) = 1 + \max(1, 1) = 1 + 1 = 2$$

- Formelle språk
    - Rekursiv funksjon på et formelt språk
        - Vi definerte språket $a^n b a^n$ som den minste mengden S slik at b∈S og hvis t∈ S, så ata∈ S
        - Nå kan vi for eksempel definere en rekursiv funksjon f: S→N slik at f(b) = 0 og f(ata) = 2 + f(t)
        - Vi regner ut hva f gjør på strengen aaabaaa slik:

          F(aaabaaa) = 2 +f(aabaa)
          = 2+2+f(aba)
          = 2+2+2+f(b)
          = 2+2+2+0 = 6
          Funksjonen gir antall a-er i strengen
    - Konkatenering av strenger
        - Mengden av strenger over et alfabet A er den minste mengden A* slik at $\Lambda \in A^*$, og hvis $s \in A^*$ og $x \in A$, så $sx \in A^*$.
        - Vi kan definere konkatenering av strenger rekursivt på gølgende måte. For å gjøre det helt tydelig, skriver vi nå (t*s) for konkateneringen av t og s, men vanligvis skriver vi bare ts. Vi definerer funksjonen rekursivt uten å gjøre noe med t, og vi kan derfor anta at t er en vilkårlig streng.

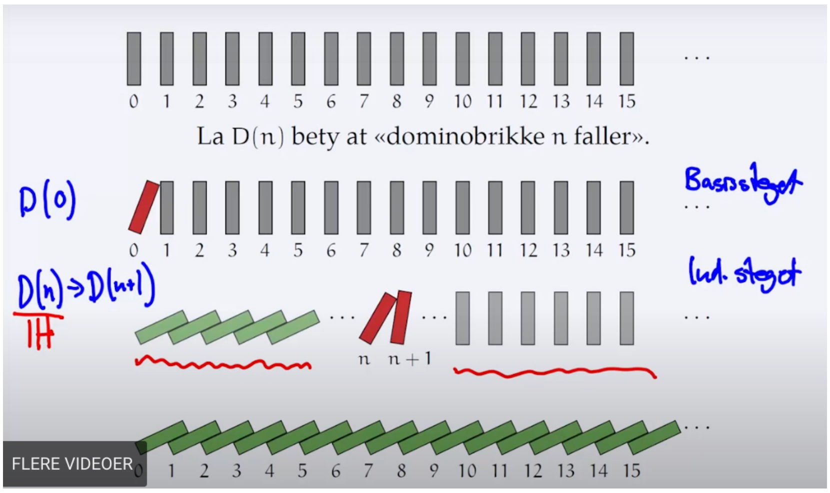
          La (t*Λ)= t, og hvis s∈A* og x∈A, la (t*sx) = (t*s)x
          (ab*ab) = (ab*a)b = (ab*Λ)ab = abab

Kapittel 11 – matematisk induksjon

Matematisk induksjon er en kraftig og nyttig bevismetode for påstander om naturlige tall. Du får se mange eksempler på bruk av induksjonsbevis og lærer om hvordan rekursive funksjoner og induksjonsbeis er relatert til hverandre. Du lærer også om det matematiske spillet Hanois tårn og hvordan dette kan analyseres ved hjelp av rekursive funksjoner

- Et matematisk eksempel
    - La oss legge sammen etterfølgende oddetall og se hva vi får
        - 1 = 1 = 1*1
        - 1+3 = 4 = 2*2
        - 1+3+5 = 9 = 3*3
        - 1+3+5+7 = 16 = 4*4
        - 1+3+5+7+9 = 25 = 5*5
        - 1+3+5+7+9+11 = 36 = 6*6
    - Det virker som at summene blir kvadrattall, det vil tall på formen n*n

    - Ved nærmere ettersyn virker det også som om summen av de n første oddetallene blir n^2.
        - $1 + 3 + 5 + ... + (2n-1) = n^2$
    - Spørsmålet er nå hvordan vi kan bevise at dette er sant for alle tall
- Motivasjon
    - Ett svar er matematisk induksjon, en bevismetode for å vise at noe er sant for alle naturlige tall.
    - I dette kapittelet skal vi generalisere denne metoden og se på strukturell induksjon, en bevismetode for å vise at noe er sant for alle elementer i en induktivt definert mengde.
    - Vi kan se på matematisk induksjon som et spesialtilfelle av strukturell induksjon
    - Induksjon er generelt sett en kraftig og anvendbar metode for å vise at alle elementene i en uendelig mengde har en bestemt egenskap
- Matematisk induksjon
    - For å bevise at en påstand er sann for alle naturlige tall, er det tilstrekkelig å bevis
        - Basissteget: at påstanden holder for tallet 0
        - Induksjonssteget: at hvis påstanden holder for et vilkårlig naturlig tall n, så holder den også for n+1. Antakelsen om at påstanden er sann for n, kalles induksjonshypotesen
    - Hvis begge disse holder, kan vi med matematisk induksjon konkludere med at påstanden er sann for alle naturlige tall
- Domino-metaforen
    - La D(n) bety at «dominobrikke n faller»



- Notasjon
    - Hvis P står for en påstand, er det vanlig å skrive P(x) for å indikere at x forekommer i P
    - Det gjør det enkelt å bytte ut x med noe annet; symbolet x fungerer her som en plassholder
    - Hvis for eksempel P(x) er påstanden «x pluss x er lik 2*x», vil P(5) være påstanden 5 pluss 5 er like 2*5
- Verdt p merke seg
    - Et induksjonsbevis består av to steg: et basissteg og et induksjonssteg

- Med notasjonen over kan vi skrive disse to stegene på følgende måte:
  - Basissteget: P(0) er sann
  - Induksjonssteget: P(n)→P(n+1) er sann for alle naturlige tall n
- Hvis disse to punktene er oppfylt, må påstanden være sann for alle naturlige tall.
- Overbevis deg selv om at dette er sant
- Hvordan skulle det være mulig at disse punktene var oppfylt uten at påstanden var sann for alle naturlige tall?
- Det å vise at hvis P(n)→P(n+1) er sann for alle n, er det samme som å vise at hvis P(n) er sann for en vilkårlig n, så er også P(n+1) sann
- Merk at vi ikke antar at P(n) er sann for alle n
- Det er det vi konkluderer med helt til slutt
- Det skal være slik at P(n+1) er sann under antakelsen, eller hypotesen, om at P(n) er sann
- Det er derfor den kalles induksjonshypotesen
- Legg også merke til at matematisk induksjon nøyaktig følger strukturen til hvordan naturlige tall er induktivt definert
- Og det er alltid universelle påstander som bevises ved induksjon; i dette tilfellet er det slik at dor alle naturlige tall n, holder påstanden
- Påstanden det er snakk om kan være sammensatt, og det lønner seg ofte å vende tilbake til den og sjekke nøyaktig hva den sier.

- Et induksjonsbevis steg for steg
  - Påstanden P(n) vi ønsker å bevise er

    $1+3+5+...+(2n-1) = n^2$
  - Det er naturlig å begynne med tallet 1 i dette tilfellet
  - For å bevise basissteget, at P(1) er sann, erstatter vi n med 1 pg får følgende påstand

    $P(1)=(2*1-1) = 1^2$
  - Ved p regne ut venstre- og høyresiden, får vi 1 på hver side og ser at påstanden er sann for tallet 1
  - Nå skal vi vise induksjonssteget, at hvis P(n) er sann, er P(n+1) sann, for alle positive heltall n.
  - Anta derfor at P(n) er sann for en vilkårlig n:

    $1+3+5+...+(2n-1) = n^2$
  - Det som står her er påstanden P(n), og dette er induksjonshypotesen vår. Fra denne må vi vise at P(n+1) er sann

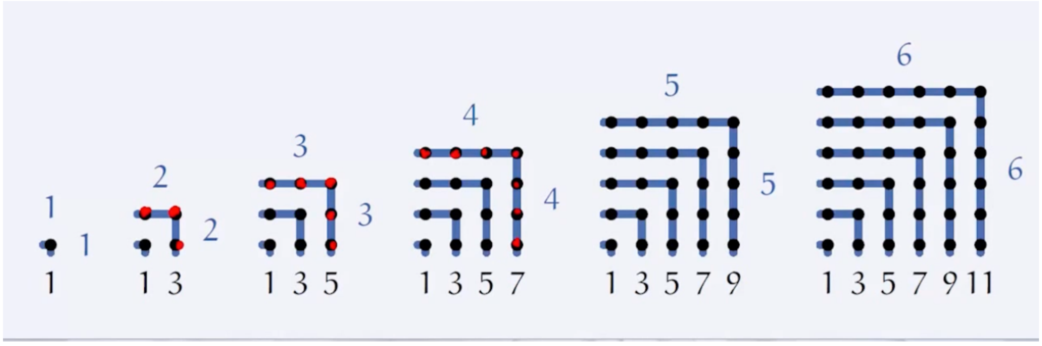
    $1+3+5+...+(2n-1)+(2n+1) = (n+1)^2$
  - Det som står her er P(n+1), påstanden for tallet n+1
  - Fordi vi har antatt at påstanden er sann ofr tallet n, kan vi bytte ut den første biten, 1+3+5+..+(2n-1), med n^2. Da får vi følgende:

    $N^2+(2n+1) = (n+1)^2$

  - Vi kan konkludere med at påstanden er sann for alle n+1
  - VI har altså bevist at hvis P(n) er sann, er P8n+19 sann
  - Ved matematisk induksjon følger det at påstanden er sann for alle positive heltall

- Nå har vi bevist, for all fremtid og med 100 prosent sikkerhet, at summen av de n første oddetallene er et kvadrattall, nærmere bestemt n^2

- Et geometrisk bevis for den samme påstanden.



- Hva er det egentlig som foregår i et induksjonsbevis
  - Intuisjon
    - Det å bevise induksjonssteget, at «hvis P(n) er sann, så er P(n+1) sann» fro alle naturlige tall n, gir oss egentlig uendelig mange minibevis, ett for hvert tall n
    - Hvis vi for eksempel erstatter n med 5, får vi et bevis for P(5) →P(6), og hvis vi erstatter n med 6, får vi et bevis for P(6) →P(7)
    - Hvis vi ønsker å bevise at påstanden P holder for tallet 27, kan vi sette sammen beviset for P(0) med alle minibevisene for n = 0,1,2,...,26
      - Beviset for p(0) og beviset for P(0) →P(1)gir et bevis for P(1)
      - Beviset for p(1) og beviset for P(1) →P(2)gir et bevis for P(2)
      - ...
      - Beviset for p(26) og beviset for P(26) →P(27)gir et bevis for P(27)
    - Uansett hvor stort tallet n er , kan vi finnet et bevis fro p(n)
    - Det er nøyaktig dette et induksjonsbevis generaliserer
    - Konklusjonen i induksjonsbeviset er at påstanden holder for alle naturlige tall n
- Begrunnelser

  Hvorfor funker induksjon?
  - Et enkelt svar er at vi antar at den gjør det
  - Det er vanlig å ta med aksiomer for matematisk induksjon for å gjøre denne antakelsen presis
  - Vi kunne også ha bevist at matematisk induksjon er et gyldig prinsipp, men da ville vi ha antatt og tatt i bruk et annet prinsipp som var tilsvarende sterkt.
- Sterk/komplett induksjon
  - Det betyr at vi i induksjonssteget antar at påstanden holder for alle naturlige tall mindre eller lik n, og ikke bare n, og fra det viser at påstanden holder for n+1
  - Dette er ekvivalent med det vi har sett, men det kan være praktisk å kunne referere til alle de foregående påstandene og ikke bare den forrige.
- Summen av de første tallene
  - La oss legge sammen etterfølgende tall og se hva vi får
    - 1=1

        - 1+2=3
        - 1+2+3=5
        - 1+2+3+4=10
        - 1+2+3+4+5=15
    - Dette er de samme triangulære tallene.
    - 1+2+3+...+n = $\frac{n*(n+1)}{2}$
    - Basissteget er å vise at påstanden holder n=1
    - Hvis vi erstatter n med tallet 1, får vi $\frac{1*(1+1)}{2}$ = 1
    - HS=VS
    - For å vise induksjonssteget, antar vi at påstanden er sann for n = k
      Dette er induksjonshypotesen vår ser og ser slik ut
    - 1+2+3+...+k= $\frac{k*(k+1)}{2}$
    - Nå må vi vise at påstanden er sann for n=k+1
    - 1+2+3+...+k+(k+1) = $\frac{(k+1)*((k+1)+1)}{2}$
    - Fordi vi har antatt at påstanden er sann for n=k, kan vi bytte ut den første biten 1+2+3+...+k, med $\frac{k*(k+1)}{2}$+(k+1) = $\frac{(k+1)*((k+1)+1)}{2}$
    - Det som nå gjenstår er å bevise at dette er sant, dvs, at venstre- og høyresiden er like.

$$\begin{aligned}\frac{k(k+1)}{2}+(k+1) &= \frac{k(k+1)}{2}+\frac{2(k+1)}{2}\\ &= \frac{k(k+1)+2(k+1)}{2}\\ &= \frac{(k+2)(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}\\ &= \frac{(k+1)((k+1)+1)}{2}\end{aligned}$$

    - Vi har altså bevist at hvis påstanden er sann for k, er påstanden sann for (k+1)
    - Ved induksjon følger det at påstanden er sann fro alle positive heltall

Kapittel 12 – Strukturell induksjon

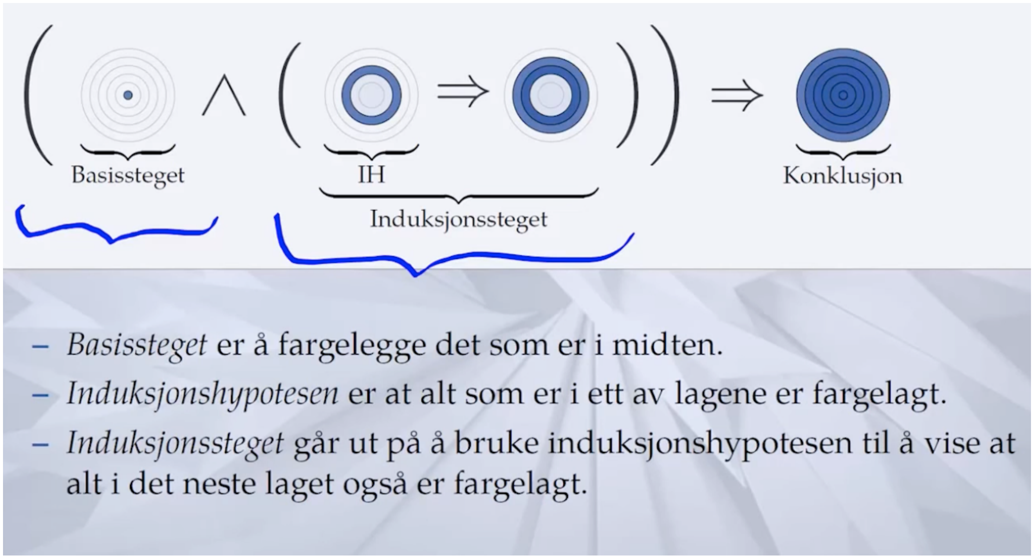
- Strukturell induksjon
    - I matematisk induksjon benytter vi oss egentlig av den induktive definisjonen av mengden av naturlige tall
    - Nå skal vi generalisere matematisk induksjon slik at metoden kan brukes for alle induktivt definerte mengder, ikke naturlige tall

      $0 \in N$

      $x \in N \rightarrow x+1 \in N$
    - Denne mer generelle bevismetoden kalles strukturell induksjon og er kraftig og allsidig metode

- Vi kan bruke denne når vi ønsker å vise at alle elementene i en induktivt definert mengde har en bestemt egenskap
- Et bevis ved strukturell induksjon har et basissteg og et induksjonssteg som følger strukturen til den induktive definisjonen til punkt og prikke

- Definisjon av strukturell induksjon
  - Anta at en mengde er induktivt definert. For å vise at en påstand er sann for alle elementer i denne mengden er det nok å vise følgende:
    - Påstanden holder for alle elementer i basismengden. Dette steget kalles basissteget
    - Hvis mengden er lukket under en operasjon som gjør at x fremkommer fra $x_1, x_2, \ldots, x_n$, og påstanden holder for alle disse, holder påstanden også for x. Dette steget kalles for induksjonssteget. Antakelsen om at påstanden holder for $x_1, x_2, \ldots, x_n$ kalles induksjonshypotesen
  - Hvis begge disse punktene holder, kan vi ved strukturell induksjon konkludere med at påstanden er sann for alle elementer i mengden.
- Språkbruk
    - «ved strukturell induksjon på mengden av formler»
    - «ved induksjon på formler»
    - «ved induksjon på strukturen til formler»
  - Dette betyr det samme
  - Med den samme notasjonen som tidligere, hvor P(x) står for påstanden, kan vi skrive de to stegene i et bevis ved strukturell induksjon på følgende måte.
    - Basissteget: at P(x) er sann for alle x i basismengden
    - Induksjonssteget: at hvis $P(x_1), P(x_2), \ldots P(x_n)$ er sanne, og x fremkommer fra $x_1, x_2, \ldots, x_n$, så er P(x) også sann
  - Visualisering



- Strukturell induksjon på bitstrenger
  - Vi definerte bitstrenger induktivt som den minste mengden som inneholder 0 og 1 og som er slik av hvis b er med, er b0 og b1 også med
  - For å vise at en påstand er sann for alle bitstrenger ved strukturell induksjon, må vi vise basissteget og induksjonssteget

  - Basisstege består av å vise at påstanden er sann for alle elementene i basismengden, nemlig 0 og 1
  - Induksjonssteget består av å vise følgende to deler, én for hver operasjon mengden er lukket under
    - For alle bitstrenger b:
      - Hvis påstanden er sann for b, er den sann for b0
    - For alle bitstrenger b:
      - Hvis påstanden er sann fro b, er den sann for b1
- En rekursiv funksjon fra bitstrenger til naturlige tall
  - La funksjonen v fra bitstrenger til naturlige tall være definert rekursivt på følgende måte:
    - V(0) = 0 og v(1) = 1
    - V(b0) = 2*v(b)
    - V(b1) = 2*v(b)+2
  - Vi kan regne ut at v(11) = 2*v(1)+1, og at funksjonen returnerer det samme uansett hvor mange forekomster av 0 vi legger til venstre side v(011)=v(0011)=v(00011) = ... = 3
  - Det virker som om v(b) = v(0b) holder for alle bitstrenger b.
  - Det er det vi skal nå skal bevise ved strukturell induksjon
  - Vi lar P(b) stå for påstanden v(b)=v(0b)

- Påstanden bevist ved strukturell induksjon
  - Vi beviser nå at v(b) = v(0b), for alle bitstrenger b, ved strukturell induksjon. La P(b) stå for påstanden v(b)=v(0b)
    - Basissteget består av å vise at P(0) og P(1) er sanne
      - P(0) er sann: v(0) = 0 = 2*0 = 2*v(0) = v(00)
        - Det følger fra en definisjon.
      - P(1) er sann: v(1) = 1 = 2*0+1 = 2*v(0) + 1 = v(01)
    - Induksjonssteget består av å vise at hvis P(b) er sann, er også P(b0) og P(b1) sanne Anta derfor at P(b) er sann, de vil si at v(b) = v(0b), for en vilkårlig bitstreng b; dette er induksjonshypotesen
      - P(b0) er sann: v(b0) = 2*v(b) = 2*v(0b) = v(0b0)
      - P(b1) er sann: v(b1) = 2*v(b) + 1 = 2*v(0b)+1 = v(0b1)
      - I begge linjene over, holder første og siste likhet som følge av definisjonen av v, og den midterste likheten holder på grunn av induksjonshypotesen, som sier at v(b) = v(0b)
    - Ved strukturell induksjon på mengden av bitstrenger følger det at v(b) = v(0b) er sann fro alle bitstrenger b
- Strukturell induksjon på utsagnslogiske formler
  - Mengden av utsagnslogiske formler
    - Mengden av utsagnslogiske fomler er induktivt definert
    - Dermed kan vi bruke strukturell induksjon til å vise at en påstand holder for alle utsagnslogiske fomler
    - For å vise at en påstand er sann for alle utsagnslogiske formler må vi vise:
      - Basissteget, at påstanden er sann for alle utsagnsvariabler
      - Induksjonssteget, som her består av fire, like viktige, deler

- Hvis påstanden er sann for formelen F, er den sann for $\neg F$.
- Hvis påstanden er sann for formlene F og G, er den sann for $(F \wedge G)$.
- Hvis påstanden er sann for formlene F og G, er den sann for $(F \vee G)$.
- Hvis påstanden er sann for formlene F og G, er den sann for $(F \rightarrow G)$.

        - Hvordan kan vi bevise at et uttrykk $((Q\wedge P)$ ikke er en utsagnslogisk formel?
        - Det er som regel mye vanskeligere å bevise at noe er umulig enn å vise at noe er mulig
        - Det kan noen ganger være både bedre og enklere, å bevise en påstand som er sterkere enn den vi egentlig ønsker å bevise
        - I dette tilfellet kan vi for eksempel bevise at hvis et uttrykk har forskjellig antall venstre- og høyreparentes, er det ikke en utsagnslogisk formel
        - Det kontrapositive av dette er at hvis noe er en utsagnslogisk formel, har det like mange venstre- og høyreparenteser
        - Dette er en sterkere påstand, og den har som konsekvens at $((Q\wedge P)$ ikke er en utsagnslogisk formel fordi den har to venstreparenteser og en høyreparentes
        - Vi beviser den sterkere påstanden ved strukturell induksjon
    - Påstanden bevist ved strukturell induksjon
        - VI beviser at alle utsagnslogiske fomler F har like mange venstre- og høyreparenteser. Påstanden vi viser at holder for alle formler F er: «F har like mange venstre- og høyreparenteser»
            - Basissteget: Hvis F er en utsagnsvariabel, inneholder den ikke parenteser, og da er påstanden sann.
            - Induskjonssteget:
            - Anta at $F = \neg G$ og at påstanden holder for G. Formelen F har like mange parenteser som G. Dermed holder påstanden også for F
            - La F være $(G\circ H)$ for $\circ\in\{\wedge,\vee,\rightarrow\}$, og anta at påstanden holder for både G og H. Formelen F har dermed en venstre- og en høyreparentes i tillegg til de som finnes i G og H. Siden påstanden holder for G og H, holder den også for F
        - Det følger ved strukturell induksjon på mengden av utsagnslogiske formler at alle utsagnslogiske formler F har like mange venstre- og høyreparenteser.

- Strukturell induksjon på lister
    - Definisjon liste
        - Mengden av lister over en mengde A er induktivt definert som den minste mengden slik at følgende holder:
            - () er en liste over A
            - Hvis $x\in A$ og L er en liste over A, er x::L en liste over A
    - Definisjon sammensetning av lister
        - Følgende er en rekursiv definisjon av +
            - () + M = M

      - (x::L)+ M = x::(L+M)
  - Bevis ved induksjon på lister at L+() = ()+L for alle lister L
    - Basissteget er at påstanden holder hvis L erstattes med den tomme listen. Dette er sant for ()+() = ()
    - Induksjonssteget: Anta at påstanden holder for listen L, det vil si at L+() = () + L. Dette er induskjonshypotesen. Fra denne må vi vise at påstanden holder for x::L, det vil si at (x::L)+()=()+(x::L)
      - x::L + () = x::(L+()) ved punkt (2) i definisjonen av +
        = x::(()+L) ved induksjonshypotesen
        = x::L ved punkjt (1) i definisjonen av +
        = () + (x::L) ved punkt (1) i definisjonen av +
    - Ved strukturell induksjon følger det at L + () = () + L for alle lister L
- Strukturell induksjon på binære trær
  - Definisjon binære trær
    - Mengden av binære trær over en mengde A er den minste mengden slik at følgende holder
      - () er et binært tre over A
      - Hvis $x \in A$, og V og H er binære trær over A er (V,x,H) et binært tre over A
  - Definisjon antall noder i et binært tre
    - La funksjonen allant fra binære trær til naturlige tall vre definert på følgende måte:
      - Allant() = 0
      - Allant(V,x,H) = Allant(V) + 1 + allant(H)
  - Egenskaper ved alle binære trær
    - Det virker som om funksjonen allant gir antallet noder i de forskjellige binære trærne som verder
    - Dette er en enkel egenskap ved funksjonene allant, og vi skal – for treningens skyld – bevise ved strukturell induksjon at dette alltid holder
    - Påstanden vi beviser for alle binære trær T er altså «allant(T) er lik antall noder i T»
  - Påstanden bevist ved strukturell induksjon
    - Basissteget går ut på å vise at påstanden holder for det tomme binære treet(). Antall noder i det tomme binære treet er null, og påstanden holder fordi allant() = 0 per definisjon av allant
    - Induksjonssteget går ut på å vise at hvis påstanden holder for to binære trær V og H, så holder den også for treet (V,x,H)
      - Anta derfor at påstanden holder for trærne V og H, det vil si at antall noder i V er lik allant(V) og at antall noder i H er lik allant(H)
      - Antall noder i treet (V,x,H) er lik summen av antall noder i V og H pluss én

        Allant(V,x,H) = allant(v) + 1 + allant(H)

    - Da er antall noder i (V,x,H) lik allant(V,x,H)

- Ved induksjon følger det at funksjonen allant for antall noder i treet som verdi.

Kapittel 13 - Førsteordens språk

- Se Fra timer

Kapittel 14 – Representasjon av kvantifiserte utsagn

- Predikater
        - «x + y er et partall»
        - «5 + y er et partall»
        - «5 + 3 er et partall»
    - Et predikat er et uttrykk som inneholder en eller flere plassholdere som blir sant eller usant når vi erstatter plassholderne med verdier
    - VI kjenner predikater godt fra induksjonsbevis
    - Her er det som regel en påstand med én eller flere plassholdere som bevises for alle elementer i en induktivt definert mengde
    - Eksempel
        - «x er en god person» er et predikat
        - Dette kan representere ved den atomære formelen Gx
        - Her et G et relasjonssymbol med aritet én
        - Det er naturlig med aritet én fordi predikatet som representeres har én plassholder
        - Når vi har representert predikater som atomære formler, kan vi legge på kvantorer og få sammensatte førsteordens formler
        - $\exists x G x$ kan leses som:
            - Det finnes en x slik at Gx
            - Det finnes en x slik at x er en god person
            - Det finnes en god person
        - $\forall x G x$ kan leses som:
            - For alle x, er det slik at Gx
            - For alle x, x er en god person
            - Alle er gode personer
    - Kommentarer
        - Det er ingenting i veien for å legge på en kvantor med en annenvariabel, men det er ganske meningsløst
        - Formelen $\exists y G x$ kan leses som «det finnes en y slik at x er god»
        - I dette utsagnet fungerer x fortsatt som en plassholder, og hele uttrykket kan derfor fremdeles tolkes som et predikat, selv om det er en kvantor ytterst
        - Vi sier at x er en fri variabel i formelen $\exists y G x$
- Frie variabler og lukkede formler
    - En variabelforekomst i en førsteordens formel er fri hvis den ikke er bundet, det vil si hvis den ikke er innenfor skopet til en kvantor. EN formel er lukket hvis den ikke inneholder noen frie variabler

  - Motivasjon
    - Skillet mellom lukkede og ikke-lukkede formler er nyttig
    - Tidligere definerte vi et utsan som noe som enten er sant eller usant
    - En lukket formel er i praksis et utsagn
    - Når vi kommer til semantikken, skal vi se på hvordan lukkede formler kan tolkes, slik at de fpr en sannhetsverdi, sann eller usann.
- Et førsteordens språk for å uttrykke beundring
  - NÅ definerer vi et førsteordens språk for å representere utsang om beundring ved å øa signaturen være <a,b; ; Idol, Liker>
  - Det vil si at a og b er konstantsymboler, det er ingen funksjonssymboler og relasjonssymbolene er Idol og Liker
  - VI antar at Idol har aritet én og at Liker har aritet to
  - Følgende er eksempler på uttrykk som representeres med atomære formler
    - Idol(a) Alice er et idol
    - Liker(a,b) Alice liker Bob
    - Liker(x,a) x liker Alice
  - Følgende er eksempler på uttrykk som representeres med sammensatte former. Lergg merke til at alle formlene er lukkede
    - $\forall x \mathrm{Liker}(a,x)$ Alice liker alle
    - $\exists x \mathrm{Idol}(x)$ Det finnes et idol
    - $\forall x(\mathrm{Liker}(b,x) \rightarrow \mathrm{Liker}(a,x))$ Alice liker de Bob liker
    - $\exists \mathrm{Liker}(x,x)$ Noen liker seg selv
    - $\forall x(\mathrm{Liker}(x,x) \rightarrow \mathrm{Liker}(b,x))$ Bob liker alle som liker seg selv
    - $\neg \exists x(\mathrm{Liker}(x,a) \wedge \mathrm{Liker}(x,b))$ Det finnes ikke noen som liker både Alice og Bob
    - $\exists x \neg \mathrm{Liker}(x,x)$ Det finnes noen som ikke liker seg selv
    - $\exists x(\mathrm{Liker}(b,x) \wedge \mathrm{Liker}(x,a))$ Bob liker noen som liker Alice
    - $\forall x \exists y \mathrm{Liker}(x,y)$ Alle liker noen
    - $\forall x(\forall y \mathrm{Liker}(y,x) \rightarrow \mathrm{Idol}(x))$ De som likes av alle er idoler
  - Forskjellige språk brukes til forskjellige formål
    - Noen ganger ønsker vi et rikt språk med mange symboler for å uttrykke mye på en kompakt måte
    - Andre ganger ønsker vi et lite språk for å beholde kontroll og gjøre mye med enkle midler
    - Her er det ingen fasit, og hvilken signatur vi velger, avhenger av hva vi ønsker å gjøre
    - Sånn er det med programmeringsspråk også
  - Et annet språk for tallteori
    - Signaturen <0; s+; => har vi sett
    - Signaturen <0,1;+,*;=,<> beskriver et annet fspråk for tallteori
    - Her har vi ikke lenger funksjonssymbolet s, men i stedet har vi:
      - Konstantsymbolet 1
      - Funksjonssymbolet *
      - Relasjonssymbolet <
    - Vi antar at alle funksjons- og relasjonssymboler har aritet to
    - De enkleste termene i dette språket er konstantsymbolene 0 pg 1 og alle variablene

        - Ved å bruke + og * får vi termer som:
            - 1+1   0*1   x+0   x*x   (1+1)*(1+1)
              Her bruker vi infiksnotasjon for både + og *
        - Her er noen atomære formler i dette språket, sammen med hva de uttrykker
            - $X<1$ x er mindre enn 1
            - $X=x$ x er lik x
            - $X*1 = x$ x ganget med 1 er lik x
            - $(1+0)<(1+1)$ 1+0 er mindre enn 1+1
        - Her er noen sammensatte fomler i språket, sammen med hva de uttrykker
            - $\neg(x<x)$ x er ikke mindre enn seg selv
            - $\forall x(x<x+1)$ x er alltid mindre enn x+1
            - $\forall x(x*0=0)$ x multiplisert med 0 blir alltid 0
            - $\forall x \exists y(x<y)$ for alle tall finnes det et som er større
            - $\neg\forall x \exists y(x<y)$ det finnes ikke et største tall
            - $\forall x(0<x)$ 0 er det minste tallet
        - Hvorvidt formelen er sanne eller ikke, har vi ikke sagt noe om ennå. Alle disse formlene kan faktisk gjøres sanne eller usanne, avhengig av hvilken tolkning vi legger til grunn
    - Noen praktiske tips
        - Det er en del mønste som går igjen når vi representerer utsagn med førsteordens logikk
        - $\forall x(\ldots\rightarrow\ldots)$ brukes som oftest for å representere utsagn på formen «alle[...] er [...]» En vanlig feil er å skrive $\forall(\ldots\wedge\ldots)$
        - $\exists x(\ldots\wedge\ldots)$ brukes som oftest for å representere utsagn på formen «det fines noe som både er [...] og [...]» En vanlig feil er å skrive $\exists x(\ldots\rightarrow\ldots)$
        - $\neg\exists x(\ldots)$ eller $\forall x\neg(\ldots)$ brukes som oftest for å representere utsagn på formen «det fins ingen som er slik at [...]». EN vanlig feil er å skrive $\exists x\neg$ [] eller $\neg\forall x$[...]

Kapittel 15 – Tolkning av modeller

Introduksjon

- Hvordan skal vi tolke førsteordens formler?
- Hva skal $\forall x$ og $\exists x$ bety?
- Hva kan vi bruke førsteordens formler til å uttrykke?
    - Og hva er det man ikke kan uttrykke?
- Hva gjør en formel sann, usann, gyldig, kontradiktorisk, oppfyllbar eller falsifiserbar?
- Når er en førsteordens formel en logisk konsekvens av andre førsteordens formler?
- Å gi en semantikk er å si noe om forholdet mellom språk og virkelighet
    - I utsagnlogikken er det valuasjonene som gir oss semantikken
    - I førsteordens logikk er det modellene som gir oss semantikken
- En modell står intuitivt av
    1. En mengde, kalt domenet til modellen, og
    2. En tolkning av alle ikke-logiske symboler slik at
        - Et konstantsymbol tolkes som et element i mengden

        - Et funksjonssymbol tolkes som en funksjon på mengden
        - Et relasjonssymbol tolkes som en relasjon på mengden
    - En modell forteller oss hvilke førsteordens formler som er sanne og hvilke som er usanne
    - En gitt førsteordens formel kan være sann eller usann, og det avhenger av modellen den tolkes i.
    - VI skal først definere hva en modell er, og så skal vi definere hvordan modeller fir oss sannhetsverdier for førsteordens formler

Eksempel

- Sannhet avhenger av tolkning – 1
    - Se på formelen $\forall xPx$
    - Vi leser den som «for alle x, så er Px sann»
    - Hvorvidt denne formelen er sann eller usann avhenger av hvordan relasjonssymbolet P tolkes i en modell
        - Hvis P tolkes som mengden av alle elementer, så er formelen sann
        - Hvis ikke, er den usann
- Sannhet avhenger av tolkning – 2
    - Se på formelen $\forall x\exists y(x<y)$
    - Vi leser den som «for alle x, så finnes det en y slik at $x<y$»
    - Hvorvidt denne formelen er sann eller usann avhenger av hvordan relasjonssymbolet $<$ tolkes i en modell
        - Hvis en tolkes som mindre enn-relasjonen over de naturlige tellene, er den sann
        - Grunnen er at for alle naturlige tall så finnes det ett som er større
        - Hvis $<$ tolkes som mindre enn-relasjonen over mengden {1,2,3,4,5,6,7}, er den usann
        - Grunnen er at det finnes et tall, nemlig 7, slik at det ikke finnes noe større tall.
- Modeller
    - Hva betyr det å gi en modell for et språk?
        - Det er å spesifisere et domene, samt å si hvordan alle de ikke-logiske symbolene skal tolkes
        - VI bruker så en modell til å tolke førsteordens termer og formler
        - Hvis språket for eksempel kun består av ett relasjonssymbol R, er det nok til å spesifisere domenet, som er en mengde, og tolkningen av R, som er en relasjon på denne mengden
        - Hvis domenet er de naturlige tallene, og R har aritet to, må tolkningen av R være en binær relasjon på de naturlige tallene
    - En modell M for et gitt førsteordens språk består av en ikke-tom mengde D, kal domenet til modellen, og en funksjon som tolker alle ikke-logiske symboler på følgende måte:
        - Hvis k er et konstantsymbol er $k^M \in D$
        - Hvis f er et funksjonssymbol med aritet n, er f^M en funksjon fra D^n til D.
        - Hvis R er et relasjonssymbol med aritet n, er R^M en n-ær relasjon på D, det vil si en delmengde av D^n
    - VI skriver $|M|$ for domenet D til modellen M
- Tolkning av termer

- En lukket term
    - En term kalles lukket hvis den ikke inneholder noen variabler
- La et førsteordens språk være gitt, og la M være en modell for dette språket. Da tolker vi en lukket term $f(t_1,...,t_n)$ på følgende måte:
    - $f(t_1,...,t_n)^M = f^M(t_1^M,...,t_n^M)$
- Eksempel
    - La M være en modell med domene {0,1,2,3,4} slik at
        - Konstantsymbolet a tolkes som 3, og vi skriver dette som $a^M = 3$
        - Konstantsymbolet b tolkes som 4, og vi skriver dette som $b^M = 4$
        - Funksjonssymbolet f med aritet én tolkes som en funksjon på {0,1,2,3,4} som gir 0 hvis argumentet er et partall og 1 hvis argumentet er et oddetall
    - Nå kan vi tolke alle termer som inneholder disse symbolene
        - Tolkningen av f(a) skriver vi som $f(a)^M$
            - Ved å regne oss innover får vi $f(a)^M = f^M(a^M) = f^M(3) = 1$
        - Tolkningen av f(b) skriver vi som $f(b)^M$
            - Ved å regne oss innover får vi $f(b)^M = f^M(b^M) = f^M(4) = 0$

- Tolkning av atomære formler
    - Først skal vi gi sannhetsverdier til atomære formler
    - Deretter skal vi definere sannhetsverdier for førsteordens formler
    - For å finne ut hvorvidt en lukket atomær formel er sann i en modell, må alle relasjonssymbolene og termene i formelen være tolket.
    - Deretter kan vi sjekke om tolkningen av relasjonssymbolene er i samsvar med tolkningen av termene
    - Definisjon
        - Anta at M er en modell for et førsteordens språk, og la $R(t_1,...,tn)$ være en lukket atomær formel
        - Vi sier at formelen $R(t_1,...,tn)$ er sann i M og skriver $M \models R(t_1,...,tn)$ hvis følgende holder:
            - $\langle t_1^M,...,t_n^M \rangle \in R^M$
    - Eksempel
        - Anta at M er en modell med de naturlige tallene som domene
        - Anta at $a^M = 3$, $b^M = 4$ og at R^M er mindre enn-relasjonen på de naturlige tallene
        - Da er Rab sann i M, fordi a^M, som er lik 3, er mindre enn b^M, som er lik 4
        - Her er det samsvar mellom den lukkede atomære formelen Rab som er noe rent syntaktisk, og den binære relasjonen som utgjør tolkningen av R
        - Vi ser at Rab er sann i modellen M fordi $\langle a^M,b^M \rangle \in R^M$
- Substitusjon
    - For å gi definisjonen av hvordan formler tolkes i en modell, trenger vi begrepet substitusjon
    - Grunnen til at substitusjoner introduseres akkurat nå, er at de brukes for å tolke formler med kvantorer
    - Som en foreløpg intuisjon , skal vi si at $\forall xPx$ er sann i en modell hvis Px er sann uansett hva vi setter inn for x

- Vi trenger begrepet substitusjon for å gjøre det helt presist hva vi mener med å «sette inn for x»
- Først definerer vi substitusjon i termer, deretter i formler

- Substitusjon i termer
  - La s og t være termer og x en variabel
  - Da er s[x/t] resultatet av å erstatte, eller substituere alle forekomster av x i s med t
  - Vi kan se for oss [x/t] som en funksjon som bytter ut alle x-er med t-er
  - En måte å gjøre det helt eksplisitt på er ved å definere en substitusjon som en rekursiv funksjon
  - Eksempel
    - F(x,y)[x/a]=f(a,y)
    - F(x,y,a)[x/y] = f(y,y,a)
    - F(y,y,a)[y/b] = f(b,b,a)
    - (x+y)[x/3] = 3 + y
    - (x+y)[y/3] = x + 3
- Substitusjon i former
  - Hvis p er en formel, t en term og x en variabel, er p[x/t] resultatet av å erstatte, eller substituere, alle frie forkomster av x i p med t
  - Eksempel
    - $\exists$x(x+y=100)[y/25] = $\exists$x(x+25 = 100)
    - (Pxy$\wedge\forall$xPxy)[x/a] = P(ay$\wedge\forall$xPxy)
    - (Pxy$\wedge\forall$xPxy)[y/a] = P(xa$\wedge\forall$xPxa)
- Tolkning av sammensatte former
  - Vi antar at språkene er rike nok
    - I tidligere eksempler har vi ofte hatt konstantsymboler for alle elementene i et domene
    - Det er nyttig, men det ikke alltid slik at disse konstantsymbolene er i språket
    - Strengt tatt har vi ingen garanti for at et språk er så rikt
    - For enkelhets skyld – og for å definere semantikken – skal vi anta at for enhver modell og ethvert språk, inneholder språket konstantsymboler for alle elementer i domenet til modellen:
      - Hvi M er en modell for et fitt førsteordens språk, antar vi at for ethvert element a i |M|, finnes det et konstantsymbol $\bar{a}$ i språket. Vi antar at enhver modell M tolker $\bar{a}$ som a, med andre ord at $\bar{a}^M$ = a
  - Intuisjon
    - Intuitivt skal $\exists$- og $\forall$-formler tolkes på følgende måte:
    - EN formel $\exists$xp er sann hvi vi kan sette inn noe for x i p slik at p blir sann
      - For eksempel er formelen $\exists$x(x-5=0) sann fordi uttrykket (x-5=0) blir sant når vi setter inne 5 for x
    - På tilsvarende måte er en formel $\forall$xp sann hvis p blir sann uansett hva vi setter inn for x
      - For eksempel er formelen $\forall$x(x-x=0) sann, fordi (x-x=0) blir sann uansett hva vi setter inn for x

- Tolkning av lukkede formler
  - Anta at M er en modell for et gitt førsteordens soråk. VI definerer rekursivt hva det vil si at en lukket formel p er sann i M. Skrivemåten M|= p betyr at p er sann i modellen M
    - $M|=R(t_1,...,tn)$ hvis $<t_1^M,...,t_n^M> \in R^M$
    - $M|= \neg p$ hvis det ikke er tilfellet at $M|=p$
    - $M|=p\wedge q$ hvis $M|= p$ og $M|=q$
    - $M|=p\vee q$ hvis $M|= p$ eller $M|=q$
    - $M|=p\rightarrow q$ hvis $M|=q$ impliserer $M|=q$
    - $M|=\forall xp$ hvis $M|=p[x/\bar{a}]$ for alle a i |M|
    - $M|=\exists xp$ hvis $M|=p[x/\bar{a}]$ for minst en a i |M|
  - Når p er sann i M, sier vi også at M er en modell for p, at M gjør p sann og at M oppfyller p.
- Oppfyllbarhet og gyldighet i førsteordens formler
  - En lukket formel er oppfyllbar hvis det finnes en modell som gjør den sann, ellers er den kontradiktorisk
  - En lukket formel er gyldig hvis alle modeller gjør den sann, ellers er den falsifiserbar
  - En mengde lukkede formler er oppfyllbar/falsifiserbar hvis det finnes en modell som gjør alle formlene sanne/usanne
- Førsteordens språk og likhet
  - Når vi har med likhetssymbolet = i et førsteordens språk, er vi nødt til å være litt oppmerksomme
  - I utgangspunktet har vi lov til å behandle dette som et hvilket som helst annet relasjonssymbol, men det er ofte nyttig å anta at enhver modell tolker = som identitetsrelasjonen
  - Hvis vi ikke gjør denne antakelsen, men vi allikevel ønsker at = tolkes på riktig måte, må vi sørge for dette på andre måter, for eksempel ved å ta med formler som aksiomatiserer likhet
    - Hvis relasjonssymbolet = er med i en signatur, antar vi at dette er et relasjonssymbol med aritet to og at enhver modell tolker = som identitetsrelasjonen, det vil si at =M er lik $\{<x,x>|x\in|M|\}$
  - Eksempler
    - Se side 176
- Oppgaver
  - Vis at formelen $\forall x(Px\vee\neg Px)$ er gyldig
    - La M være en vilkårlig modell, og la e være et vilkårlig element i domenet til M
    - Uansett hvordan P tolkes, vil enten $e\in P^M$ eller $e\notin P^M$
    - I det første tilfellet vil $M|=P\bar{e}$
    - I det andre tilfellet vil $M|=\neg P\bar{e}$
    - Det betyr at $M|=P\bar{e}\vee\neg P\bar{e}$ for alle e, og det betyr at $M|=\forall x(Px\vee\neg Px)$

Kapittel 16 – resonnering om modeller

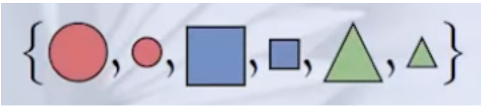
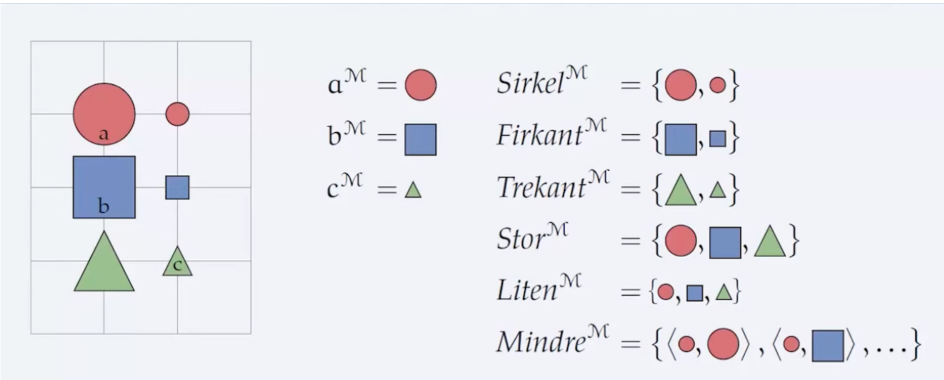
- Logisk ekvivalens

    - To lukkede førsteorden formler p og q er ekvivalente hvis enhver modell som gjør p sann, også gjør q sann, og vice versa
    - Sagt på en annen måte, for enhver modell M, vil $M|=p$ hvis og bare hvis $M=q$. Vi skriver $p \Leftrightarrow q$ når p q er ekvivalente
    - Formlene q og q er ekvivalente hvis og bare hvis $(p \rightarrow q) \wedge (q \rightarrow p)$ er gyldig
    - Alle gyldige formler er ekvivalente med hverandre

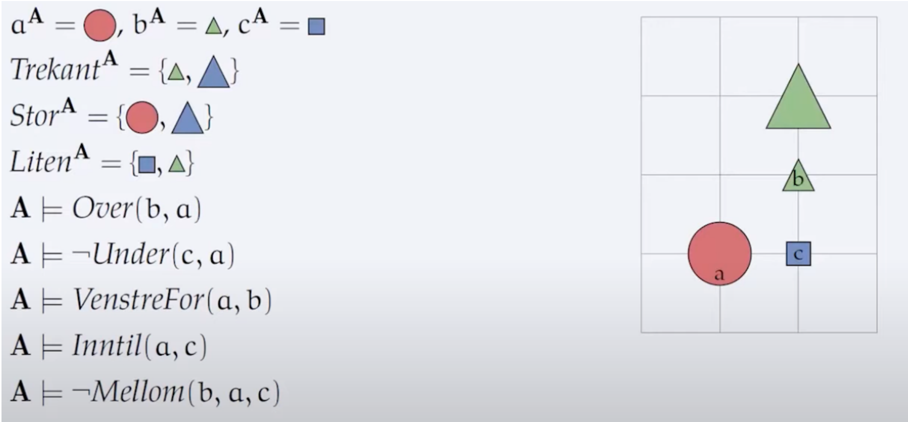
- Logisk konsekvens
    - La M være en mengde av førsteordens formler, og la p være en lukket førsteordens formel. Hvis p er sann i enhver modell som gjør alle formlene i M sanne samtidig, er p en logisk konsekvens, eller bare konsekvens, av formlene i M. VI skriver $M|= p$ når p er en logisk konsekvens av M. Med skrivemåten $p \Rightarrow q$ mener vi at q er en logisk konsekvens av mengden som består av p
    - Formelen q er en logisk konsekvens av p hvis og bare hvis formelen $(p \rightarrow q)$ er gyldig
    - En gyldig formel er en logisk konsekvens av alle formler
    - Alle formler er en logisk konsekvens av kontradiksjoner
- Kvantorer og negasjon
    - $\neg \forall x Px$ er ekvivalent med $\exists x \neg Px$
            - Hvis ikke alle kommer på festen, er det noen som ikke kommer
            - Hvis det er noen som ikke kommer på festen, kommer ikke alle
        - La M være en vilkårlig modell
        - $M|= \neg \forall x Px$
        - $\Leftrightarrow$ det er ikke slik at $M|= \forall x Px$
        - $\Leftrightarrow$ det er ikke slik at for alle elementer $a \in |M|$, så $M|=P\bar{a}$
        - $\Leftrightarrow$ det finnes et element $a \in |M|$ slik ar ikke $M|= P\bar{a}$
        - $\Leftrightarrow$ det finnes et element $a \in |M|$ slik at $M|= \neg P\bar{a}$
        - $M|= \exists x \neg Px$
        - $\neg \forall \neg x Px$ er ekvivalent med $\exists x Px$
        - $\neg \exists x \neg Px$ er ekvivalent med $\forall x Px$

    - $\neg \exists x Px$ er ekvivalent med $\forall \neg Px$
            - Hvis det ikke er noe som er farlig, er alt ufarlig
            - Hvis alt er ufarlig, er det ikke noe som er farlig
- Kvantorer og konnektiver
    - $\exists x(Px \vee Qx)$ er ekvivalent med $\exists x Px \vee \exists x Qx$
        - Hvis det finnes en som danser eller er glad, finnes det en som danser eller det sinnes en som er glad, og vice versa
    - $\forall x(Px \wedge Qx)$ er ekvivalent med $\forall x Px \wedge \forall x Qx$
        - Hvis alle danser og er glade, danser alle og er glade, og vice versa
    - $\forall x(Px \vee Qx)$ er ikke ekvivalent med $\forall x Px \vee \forall x Qx$
        - $\Leftarrow$
        - Alle er menn eller kvinner, men det er ikke slik at alle er menn eller alle er kvinner
    - $\exists x(Px \wedge Qx)$ er ikke ekvivalent med $\exists x Px \wedge \exists x Qx$
        - $\Rightarrow$

        - Det finnes et partall og det finnes et oddetall, men det finnes ikke noe som er både partall og oddetall.

- Modellering med figurer og figurspråk
    - Anta at a, b og c er konstantsymboler
    - Vi tar ikke med noen funksjonssymboler
    - Anta at Sirkel, Firkant, Trekant, Stor, Liten og Mindre er relasjonssymboler
    - Vi leser de atomære formlene på følgende måte:
        - Sirkel(x) x er en sirkel
        - Firkant(x) x er en firkant
        - Trekant(x) x er en trekant
        - Stor(x) x er stor
        - Liten(x) x er liten
        - Mindre(x,y) x er mindre enn y
    - Nå skal vi lage noen forskjellige modeller for dette språket, og alle har en delmengde av følgende mengde som domene:
        - 
    - Vi tolker alltid relasjonssymbolene på den mest naturlige måten, det vil si at $Sirkel^M$ er mengden av sirkler, $Firkant^M$ er mengden av Firkanter, etc.
    - Vi spesifiserer tolkningen av konstantsymbolene for hver modell
    - 

    - Her er formlene Sirkel(a), Firkant(b), Liten(c) og Mindre (c,b) sanne.
    - Men formlene Trekant(a), Stor(c) og Mindre(a,b) er usanne
    - VI kan gjøre språket litt mer interessant ved å legge til noen flere relasjonssymboler
        - Over(x,y) x er nærmere toppen enn y
        - Under(x,y) x er nærmere bunnen enn y
        - VenstreFor(x,y) x er lenger til venstre enn y
        - HøyreFor(x,y) x er lenger til høyre enn y
        - Inntil(x,y) x er rett ved siden av, rett over eller rett under y
        - Mellom (x,y,x) x, y og z er i samme kolonne, rad eller diagonal, og x er mellom y og z
    - Neste modell kaller vi modell a

    - 

- Teorier og aksiomatisering
    - VI kan bruke det vi har lært til å presisere noen velkjente logiske begreper
    - En teori er en mengde med formler. Formlene i en teori kalles aksiomer. Alle logiske konsekvenser av teorien kalles teoremer.
    - Når er teori er gitt, kan vi se på mengden av modeller som oppfyller teorien
    - Hvis disse modellene har noen egenskaper til felles, sier vi gjerne at teorien aksiomatiserer disse egenskapene

Kapittel 17 – Abstraksjon med ekvivalenser og partisoner

- Abstraksjon
        - 2+2=2*2
        - 3+3=2*3
        - 4+4=2*4
        - 5+5=2*5
        - x+x = 2*x
    - Det er uendelig mange måter å skrive bokstaven s på
    - Vi har abstrahert over formen på alle tegnene vi har sett
    - Når vi møter nye tegn, kjenner vi dem igjen tikl tross for at vi aldri har sett dem før
    - PÅ sett og vis har vi laget oss en ekvivalensrelasjon mellom tegn
    - VI tenker på enkelte tegn som ekvivalente og skiller ikke mellom dem.
    - Ekvivalensrelasjoner kan brukes til å abstrahere over, slå sammen, eller identifisere, objekter som man ikke ønsker å se på som forskjellige
    - Eksempler (Abstraksjoner og ekvivalensrelasjoner)
        - Gjester
        - Actionfilmer og romantiske komedier
        - Kaffe
        - Programmer
        - Mennesker
    - Vi abstraherer hele tiden, og språket vårt er fullt av abstraksjoner
    - Når vi er ute etter essensen av noe, så ser vi bort fra de uvesentlige detaljene; vi abstraherer vekk det som er uinteressant
    - En ekvivalensrelasjon er en form for identifikasjon mellom elementer og en måte å gjøre abstraksjon eksplisitt på.
    - Den forteller hvilke elementer som er ekvivalente og ikke
    - Det å bruke ekvivalensrelasjon er som å ta på seg briller med farge på

- Ekvivalensklasser
    - Samle alle elementer som er ekvivalente
        - I praksis bruker vi ekvivalensrelasjoner for å identifisere elementer som vi ikke ønsker å se forskjell på
        - Det å samle alle elementer som er ekvivalente, i én felles mengde er så nyttig at det har fått et eget navn: en ekvivalensklasse
        - Det som er nyttig med ekvivalensklasser er at vi kan behandle alle i den samme ekvivalensklassen på lik – og ekvivalent – måte.
    - Anta at ~ er en ekvivalensrelasjon på en mengde M
    - Vi sier at ekvivalensklassen til et element x∈M er mengden
        - {y∈M | y ~x}   {y|y∈M og y~x}
    - Dette er mengden av elementer i M som er relatert til x
    - Vi skriver [x] for ekvivalensklassen til x
    - Vi skriver M/~ for mengden av alle ekvivalensklasser
    - Denne mengden kalles kvotientmengden av M under ~.

La oss lage en ekvivalensrelasjon R på mengden $M = \{1, 2, 3, 4, 5\}$. En ekvivalensrelasjon er en binær relasjon på en mengde som er refleksiv, transitiv og symmetrisk (definisjon 6.5).

- Siden R skal være refleksiv må $\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle \in R$.
- La oss også si at $\langle 1, 2\rangle \in R$. Da må også $\langle 2, 1\rangle \in R$ siden R skal være symmetrisk.
- La oss også si at $\langle 1, 4\rangle \in R$. Da må $\langle 4, 1\rangle, \langle 2, 4\rangle, \langle 4, 2\rangle \in R$ siden R skal være transitiv og symmetrisk.
- La også $\langle 3, 5\rangle \in R$. Da må også $\langle 5, 3\rangle \in R$ siden R er symmetrisk.

Tegn først opp denne relasjonen som fem prikker med piler mellom seg. Ser du at ekvivalensrelasjonen «binder sammen» elementene i ulike grupper?

Hvor mange ekvivalensklasser gir denne ekvivalensrelasjonen opphav til?

2

De to ekvivalensklassene er $\{1, 2, 4\}$ og $\{3, 5\}$, for elementene i disse mengdene blir relatert med hverandre gjennom ekvivalensrelasjonen.

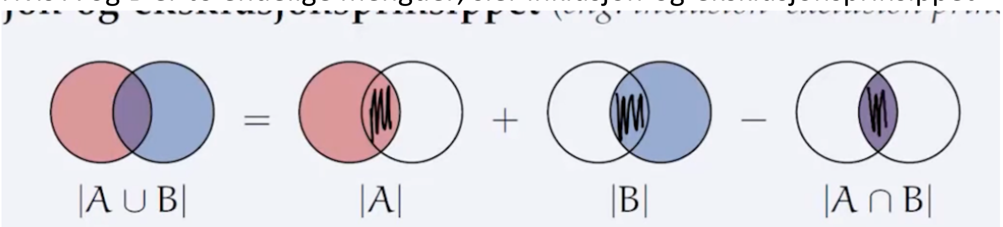
Dette er det korrekte svaret

    - Eksempel på ekvivalensklasse
        - La ~ være relasjonen {<1,1,>,<2,1>,<1,2>,<2,2>,<3,3>} på mengden M = {1,2,3}
        - Vi kan tegne den slik 
        - Dette er en ekvivalensrelasjon på M, fordi den er refleksiv, symmetrisk og transitiv
        - Definisjonen gir oss at   [x] = {y∈M|y~x}
            - Ekvivalensklassen til 1 er [1] som er lik {1,2}
            - Ekvivalensklassen til 2 er [2] som er lik {1,2}
            - Ekvivalensklassen til 3 er [3] som er lik {3}
            - Mengden av alle ekvivalensklassene, kvotientmengden til M er lik M/~ = {[1],[2],[3]}
            - {[1],[2],[3]} = {{1,2},{3}}
    - Eksempel – like gammel som

        - Anta at mengden M er mengden av alle nåværende mennesker
        - Anta at x~y betyr at x er like gammel som y.
        - Dette er en ekvivalensrelasjon på mengden av alle nålevende mennesker, fordi den er refleksiv, symmetrisk og transitiv
        - Her får vi nøyaktig én ekvivalensklasse for hver alder
        - Alle som for eksempel er 18 år gamle er relatert til hverandre og bare hverandre, og havner i samme ekvivalensklasse
    - Et kraftig matematisk verktøy
        - Det å gå fra en mengde M, via en ekvivalensrelasjon på M, til mengden av tilhørende ekvivalensklasser
        - Hvis vi har en mengde, og den av en eller annen grunn er for stor eller for finkornet, kan vi erstatte den med mengden av ekvivalensklasser for en passende ekvivalensrelasjon
        - Det er to ytterligheter her:
            - Identitetsrelasjonen: vi får én ekvivalensklasse per element
            - Den universelle relasjonen: vi får én stor ekvivalensklasse
    - Binære tall
        - En naturlig ekvivalensrelasjon på mengden av bitstrenger er den som sier at to bitstrenger, for eksempel 01 og 001, er ekvivalente hvis de representerer den samme verdien
        - Mengden av ekvivalensklasser av bitstrenger kan sees på som mengden binære tall
- Partisjoner
    - Ofte når vi tenker på mengde, deler vi elementer inn i naturlige delmengder, hvor det ikke er så interessant å skille mellom elementene i delmengdene
    - For eksempel deles mengden av studenter inn i bachelorstudenter og masterstudenter
    - Mengden av heltall deles inn i partall og oddetall
    - Mengden av utsagnslogiske formler deles inn i gyldige og falsifiserbare formler
    - Det som kjennetegner alle disse inndelingene, er at de både dekker hele den underliggende mengden og at de ikke overlapper hverandre.
    - Definisjon: En partisjon av en mengde S er en mengde X av ikke-tomme delmengder av S slik at følgende betingelser holder:
        - Unionen av alle mengden i X er lik S
        - Snittet mellom to forskjellige mengder fra X er tomt
    - Eksempel
        - La S={a,b,c}   Det er nøyaktig fem partisjoner av S, og det er:
            - {{a,b,c}}
            - {{a},{b,c}}
            - {{b},{a,c}}
            - {{c},{a,b}}
            - {{a},{b},{c}}
- Relasjon mellom partisjoner
    - Vi skal nå se at vi kan ordne mengden ved å kalle en partisjon finere enn en annen
    - La X og Y være partisjoner av en mengde M

    - Hvis ethvert element i X er en delmengde av et element i Y, skriver vi X <= Y og sier at X er en forfining av Y og er finere enn Y
    - Denne relasjonen er et eksempel på en partiell ordning.
    - Partisjonen {{1},{2},{3,4}} er finere enn partisjonen {{1,2},{3,4}}
- Sammenheng mellom ekvivalensklasser og partisjoner
    - Hvis vi tar mengden av alle ekvivalensklasser for en gitt ekvivalensrelasjon, får vi en partisjon
    - En ekvivalensrelasjon deler altså en mengde opp i ekvivalensklasser som utgjør en partisjon

Kapittel 18 – kombinatorikk

- Hva er kombinatorikk
    - Handler om å telle og om å finne svar på spørsmål av typen «på hvor mange måter kan vi ...»
    - Kombinatorikk er studiet av såkalte opptellinger, kombinasjoner og permutasjoner
    - VI dekker ikke så mye her, men går gjennom de viktigste begrepene
    - Kombinatorikk er viktig iblant annet sannsynlighetsregning og i kompleksitetsanalyse av algoritmer
- Å legge til og trekke fra
    - Hvis A og B er to endelige mengder, sier inklusjon-og-eksklusjonsprinsippet
    - 

    - Eksempel
        - La A være {a,b}
        - La B være {b,c,d}
        - Da er A∪B = {a,b,c,d}
        - Og A∩B = {b}
        - Vi ser at prinippet stemmer
        - |A∪B| = |A|+|B|-|A∩B|
        - 4. = 2 + 3. − 1
    - Eksempel 2
        - |A∪B∪C|= |A|+|B|+|C|-(|B∩C|+|A∩C|+|A∩Bs|) + |A∩B∩C|
- Multiplikasjonsprinsippet
    - Hvis vi skal treffe en reke uavhengige valg, er det totale antallet muligheter produktet av antall muligheter ved hvert valg. Dette kalles multiplikasjonsprinsippet
    - Eksempel

        - $A = \{1,2\}$
        - $B = \{x,y\}$
        - $A \times B = \{\langle 1,x\rangle,\langle 1,y\rangle,\langle 2,x\rangle,\langle 2,y\rangle\}$
        - $|A \times B| = |A|*|B| = 2*2 = 4$
    - Eksempel 2
        - $A = \{1,2,3\}$
        - $A \times B = \{\langle 1,x\rangle,\langle 1,y\rangle,\langle 2,x\rangle,\langle 2,y\rangle,\langle 3,x\rangle,\langle 3,y\rangle\}$
        - $|A \times B| = |A|*|B| = 2*3 = 6$
    - Dette prinsippet kan brukes til å regne ut størrelsen av et kartesisk produkt
    - $|A_1 \times A_2 \times \ldots \times A_n| = |A_1|*|A_2|\ldots|A_n|$
    - For to mengder, A og B, får vi $|A \times B| = |A|*|B|$
- Eksempler
    - Antall bitstrenger av en gitt mengde
        - Antall mulige er lik $2^{\text{lengden av bitstrengen}}$
        - Dette er fordi man har to muligheter hver gang man legger inn et tall
    - Antall strenger over et alfabet
        - Antall mulige strenger er lik $|\text{alfabetet}|^{\text{lengden av strengen}}$
    - Antall relasjoner på en mengde med 2 elementer
        - $A = \{1,2\}$
        - En relasjon kan være $R = \{\langle 1,1\rangle,\langle 1,2\rangle,\langle 2,2\rangle\}$
        - Antall relasjoner på $A = |A|^4 = 16$
    - Antall relasjoner på en mengde med 3 elementer
    - $A = \{1,2,3\}$
    - For hvert element har man tre valg, relatert til seg selv eller relatert til en av de to andre
    - Da får man 9 piler
    - Og for hver pil, kan man velge om man skal ha den med eller ikke
    - Da har man $2^9 = 512$
- Permutasjon
    - Et annet ord for en endring av en rekkefølge, en ordning eller en omstokking
    - Ordet «permutasjon» kommer fra latin og betyr en fullstendig endring eller å endre noe fullstendig
    - Når vi for eksempel stokker en kortstokk, permuterer vi kortene
    - En permutasjon av en mengde er en ordning av elementene i den
    - Hvis vi allerede har en ordning, er en permutasjon en endring av rekkefølgen
    - Eksempler
        - Det er 2 måter å ordne mengden {1,2} på
            - 12 og 21
            - 2! = 2
        - Det er 6 måter å ordne mengden {1,2,3} på
            - 123 132 213 231 312 321
            - 3! = 6
- Hvor mange permutasjoner finnes det
    - PÅ hvor mange forskjellige måter kan vi ordne n elementer?
    - Vi har:
        - N muligheter for det første elementet
        - (n-1) muligheter for det andre elementet

        - (n-2) muligheter for det tredje elementet
    - Det betyr at det er
        - N måter å velge det første elementet på
        - N(n-1) måter å velge to elementer i rekkefølge på
- Ordnet utvalg
    - Hvis en mengde med n elementer er gitt, og vi ønsker å velge k av disse i rekkefølge, er det n(n-1)(n-2)...(n-(k-1)) måter å gjøre dette på.
        - N = 8 K = 3
        - (8-(3-1)) = 6
        - 8*7*6
    - Eksempel
        - Hvor mange måter kan ci velge 3 elementer i rekkefølge på fra mengden {1,2,3,4,5,6,7,8,9,10}?
        - Mengden har 10 elementer, og det er 10*9*8 = 720 måter å velge tre elementer i rekkefølge på
    - Notasjon
        - $$20 \cdot 19 \cdot 18 = \frac{20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdots 2 \cdot 1}{17 \cdot 16 \cdots 2 \cdot 1} = \frac{20!}{(20-3)!}$$
        - $${}^{n}P_{k} = \frac{n!}{(n-k)!}$$

- Kombinasjoner
    - Når vi snakker om permutasjoner, handler det om hvor mange måter ci kan velge elementer i rekkefølge på
    - Men ofte er vi ikke interessert i rekkefølgen
    - En kombinasjon er et utvalg av elementer fra en mengde hvor rekkefølgen ikke spiller noen roller. EN k-kombinasjon av en mengde A er en delmengde av A med k elementer
    - Eksempel
        - Vi skal fargelegge tre av fem bokser.
        - Antall måter å velge tre elementer i rekkefølge på er ${}^{5}P_{3}$ = 5*4*3 = 60
        - Men da vil hver av disse ti kombinasjonene bli telt 3! = 6 ganger, som er antall permutasjoner av en mengde med tre elementer
        - Hvis vi skal ta høyde for dette, må vi dele på 6 for å få antallet kombinasjoner
- Skrivemåte for antall kombinashoner
    - En av disse er ${}^{n}C_{k}$, hvor «C» kommer fra ordet «combination»
    - En annen er $\binom{n}{k}$, som leses «n velg k»

- Tallet $\binom{n}{k}$ angir hvor mange forskjellige delmengder med k elementer det er av en mengde med n elementer.
- $${}^{n}P_{k} = \binom{n}{k}k!$$
- $$\binom{n}{k} = \frac{{}^{n}P_{k}}{k!} = \frac{n!}{(n-k)!}$$

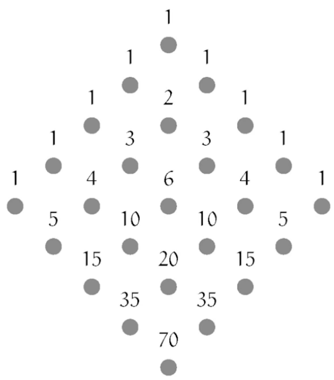
- Binominalkoeffisent
  - Hvis n og k er naturlige tall slik at k n, defineres $\binom{n}{k}$ ved
    $$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$
  - Vi leser som «n velg k», og et slikt tall kalles en binominalkoeffisient
  - Legg merke til at $\binom{n}{k} = \binom{n}{n-k}$ for alle n og k. For eksempel er like $\binom{10}{7}$ lik $\binom{10}{3}$

- Gjentakelser og overtelling
  - Noen ganger teller vi for mye og da må vi kompensere for det på riktig måte.
  - Vi har allerede sett dette i inklusjon-og-eksklusjonsprinsippet, hvor vi teller elementene i snittet to ganger og må trekke fra dette én gang for å få riktig tall
  - Men vi må også telle for mye når vi teller permutasjoner
  - Eksempel
    - Hvor mange strenger kan vi få ved å stokke om på tegnene i strengen koko?
      - Svaret er 6
    - Hvor mange strenger kan vi få ved stokke om på tegnene i strengen pappa?
      - 5! = 60
      - Hver streng blir da telt 2!*3! = 12 ganger
      - Vi må derfor dele antall permutasjoner av fem tegn på dette tallet
      - Vi får $\frac{5!}{2!*3!} = 10$ mulige strenger
  - Generelt er det slik at hvis vi har n objekter, hvorav n_1 har én type, n_2 har en annen type,... og n_r som har siste type – og vi ikke kan se forskjell på objekter

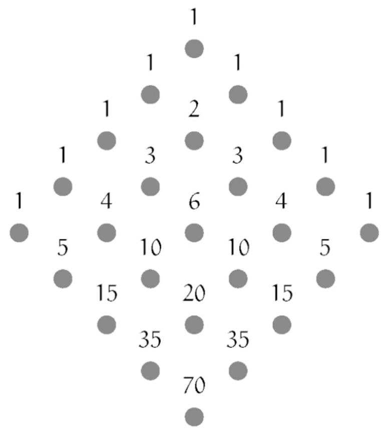
av samme type – er det $\frac{n!}{n_1! \cdot n_2! \cdots n_r!}$ unike permutasjoner av disse objektene.

Kapittel 19 – litt mer kombinatorikk

- Polyas eksempel



Pascals trekant



-
- Binominalkoeffisientene
  - Det at hvert tall i Pascals trekant er lik summen av de to tallene over, betyr at det går an å definere binominalkoeffisientene rekursivt, på følgende måte:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

  - For å gjøre dette mer konkret, la oss gå tilvake til eksemplet hvor vi skulle fargelegge nøyaktig tre av fem bokser. Da får vi

$$\binom{5}{3} = \binom{4}{2} + \binom{4}{3}$$

  -

Kapittel 20 – litt abstrakt algebra

Abstrakt algebra

- Motivasjon
  - Algebra er en sentral del av matematikken
  - Abstrakt algebra regnes som den delen av algebraen som handler om såkalte algebraiske strukturer
  - En algebreaisk struktur betyr bare en mengde sammen med en eller flere operasjoner på denne mengden
- Inverse relasjoner
  - En relasjon er mengde med tupler
  - VI kan alltid finne den motsatte relasjonen ved å bytte ut ethvert tuppel <x,y> med <y,x>
  - Dette er det samme som å snu pilene i tegningene
  - Resultatet kalles den inverse relasjonen
  - Definisjon
    - Hvis R er en relasjon fra A til B er den inverse relasjonen til R relasjonen {<y,x>|<x,y>} fra B til A. VI skriver R^{-1} for inversen til r.
  - Eksempel
    - Den inverse relasjonen til {<a,1>,<b,2>} er {<1,a>,<2,b>}
    - Hvis R er mindre enn-relasjonen på naturlige tall, er R^{-1} større enn-relasjonen på naturlige tall
- Inverse funksjoner
  - Alle relasjoner har en invers
  - Men det er ikke slik at vi alltid får en funksjon hvis vi tar den inverse relasjonen til en funksjon
  - Relasjonen {<a,1>,<b,2>,<c,2>} er for eksempel en funksjon fra {a,b,c} til {1,2}
  - Definisjon
    - La f vøre en en-til-en korresponanse fra mengden A til mengden B
    - Den inverse funksjonen til f er funksjonen fra B til A som er slik at $f^{-1}(b) = a$ hvis $f(a) = b$. Vi skriver f^{-1} for den inverse funksjonen til f.
  - Eksempler
    - La f vøre funksjone fra {1,2,3} til {a,b,c} slik at
      F(1) = a, f(2) = b og f(3) = c
    - Har denne funksjonen en invers=
    - Ja, den er en bijeksjon
    - Den inverse funksjonen f^{-1} er slik at $f^{-1}(a) = 1$, $f^{-1}(b) = 2$ og $f^{-1}(3) = c$
- Kommutativitet
  - En binær operasjon * på en mengde S er kommutativ hvis det slik at for alle $x,y \in S$ er slik at $x*y = y*x$
  - At en binær operasjon er kommutativ, betyr intuitivt at rekkefølgen på argumentene ikke spiller noen rolle.
  - Eksempler på kommutative operasjoner
    - Addisjon
    - Multiplikasjon
    - $\cup$ og $\cap$
- Assosiativitet
  - En binær operasjon * på en mengde S er assosiativ hvis det for alle $x,y,z \in S$ er slik at $x*(y*z) = (x*y)*z$
  - At en operasjon er assosiativ, betyr intuitivt at parentessettingen ikke er viktig

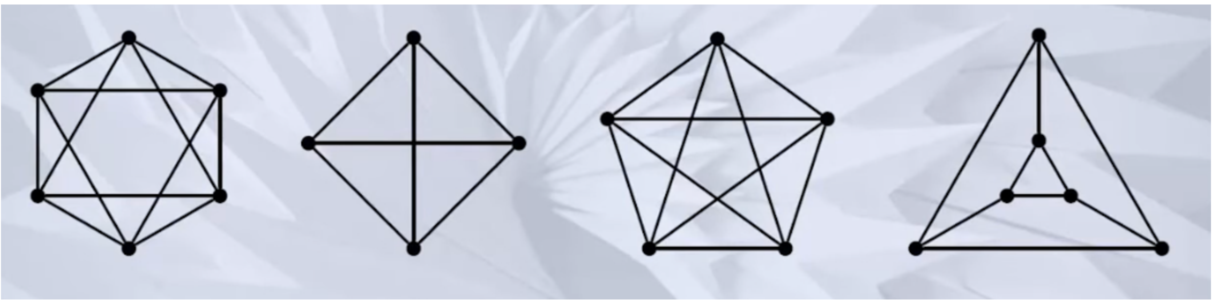
- Eksempler
    - Addisjon
    - Multiplikasjon
    - $\cup$ og $\cap$
- Idempotens
  - Den siste egneskapen vi skal se på handler om hvorvidt det har noen effekt å anvende en operasjon mer enn én gang
  - Definisjon
    - EN unær operasjon f på en mengde S er idempotent hvis det for alle $x \in S$ er slik at $f(f(x)) = f(x)$
    - En binær operasjon * på en mengde S er idempotent hvis det for alle $x \in S$ er slik at $x*x = x$
  - Eksempler
    - Absoluttverdien på reelle tall er idempotent
    - $\cup$ og $\cap$
- Identitetselementer
  - Noen elementer er nøytrale i den forstand at de ikke har noen effekt på andre elementer
  - Definisjon
    - La en binær operasjon * på en mengde S være gitt
    - Hvis $x * e = e*x = x$ for alle $x \in S$, sier vi at e er et identitetselement eller et nøytralt element for operasjonen *
  - Eksempler
    - For de fleste tallmengder har vi at:
      - Et identitetselement for addisjon
        - 0
      - Et identitetselement for multiplikasjon
        - 1
      - Et identitetselement for $\cup$
        - $\varnothing$
- Inverse elementer
  - Det hender også at noen elementer i en mengde nøytraliserer hverandre, og vi sier at elementer kan ha inverser
  - Definisjon
    - La en binær operasjon * på en mengde S være gitt
    - Anta at e er et identitetselement for *
    - Hvis $a*a^{-1} = a^{-1}*a = e$ sier vi at a og a^{-1} er inverse elementer, og at de er inversene til hverandre
  - Legg merke ti at hvorvidt elementer er inverse, avhenger av både mengden, operasjonen og identitetselementet e.
  - Eksempler
    - Det er ikke alltid slik at elementer har inverser
    - Hvis vi ser på naturlige tall og addisjon, er det kun 0 som har en invers, og det er 0 selv: $0+0 = 0$
    - Hvi vi ser på naturlige tall og multiplikasjon, er det kun 1 som har en invers, og det er 1 selv: $1*1 = 1$

        - Hvis vi ser på heltallene og addisjon, har alle elementer en invers: Inversen til x er -x, fordi x+(-x) = 0
        - Hvis vi ser på de rasjonale tallene og multiplikasjon, har alle elementer, bortsett fra 0, en invers: Inversen til x er 1/x, fordi x*(1/x) = 1
- Grupper
    - Følgende definisjon er abstrakt måte å karakterisere alle disse strukturene på
    - Definisjon
        - La en binær operasjon Æ på en mengde G være gitt
        - Da er <G,*> en gruppe hvis følgende betingelser, kalt gruppeaksiomene er oppfylt
            - Operasjonen * er assosiativ $x*(y*z) = (x*y)*z$
            - Det finnes et identitetselement $x*e = e*x = x$
            - Alle elementer har en invers $x*x^{-1} = x^{-1}*x = e$
        - Hvis vi i tillegg har at * er kommutativ, kalles gruppen abelsk
    - Eksempler
        - <Z,+>, heltallene under addisjon, er en gruppe, fordi + er assosiativ, 0 er et identitselement, og alle elementer x har en ionvers -x. Det er en abelsk gruppe fordi + er kommutativ
        - <Z,*>, heltallene undermultiplikasjon, er ikke en gruppe fordi ikke alle elementer har en invers.

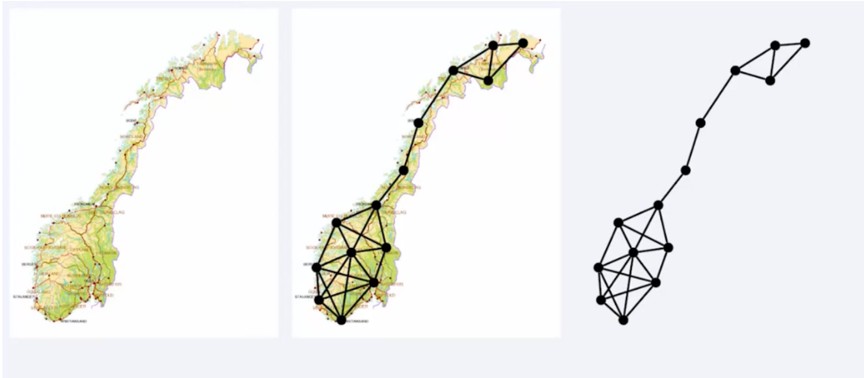
Kapittel 21 – Grafteori

Hva er en graf?

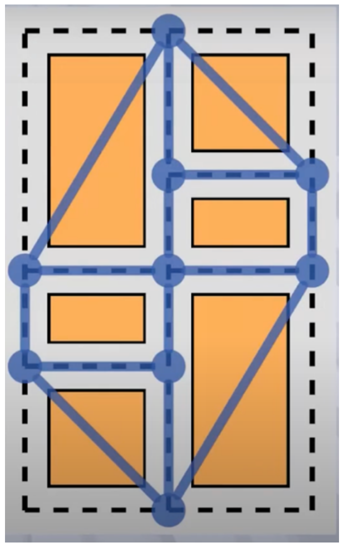
- En grad består av noder(•) g kanter (---). Her er noen grafer



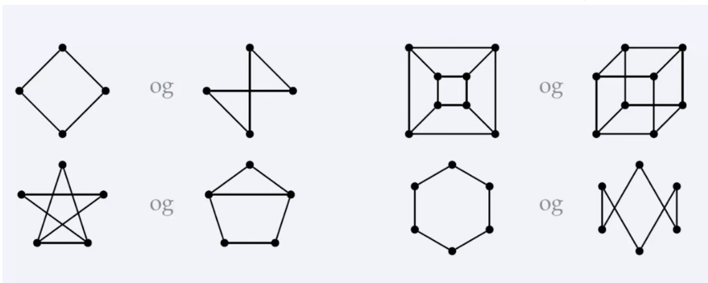
-
- Klarer du å tegne en eller flere av disse gradene på et ark uten å løfte blyanten pg uten å gå over en kant to ganger? Med litt grafteori så er det enkelt å nesvare dette spørsmålet umiddelbart. Vi skal se at oppgaven er ekvivalent med å finne en såkalt eulersvei.
- Eksempler på grafer
    - Grafer kan representere mange forskjellige ting
    - Nodene kan være studentene på Blinder, og kantene kan representere at to kjenner hverandre
    - Nodene kan være tilstandene som et dataprogram er i, og kantene kan representere overganger mellom tilstandene.
- Eksempel – kart som grafer

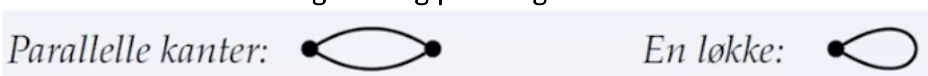
- 

- Et veinett kan representeres som en graf
- Vi kan la hvert kryss svare til en node.
- VI kan la veiene som forbinder kryssene svare til kantene.



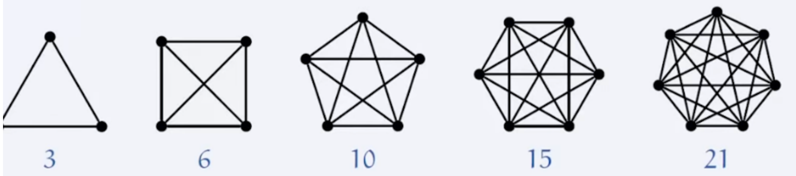
Graf

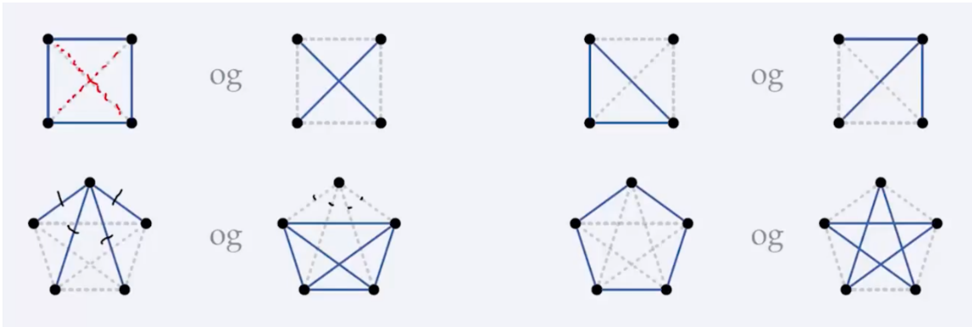
- Definisjon
    - En graf G består av en endelig, ikke-tom mengde V av noder, og en mengde E av kanter. Hver kant i E er en mengde {u,v} der u og v er to forskjellige noder. Vi sier at {u,v} forbinder u og v og at {u,v} ligger inntil u og v. To noder kalles naboer hvis de forbindes av en kant.
- Struktur og form
    - Det at det ikke er noen unik måte å tegne opp en graf på, er ikke begrenset til hvordan vi tegner nodene og kantene
    - Følgende par av grafer har samme underliggende struktur, men er tegnet opp på forskjellige måter.
    - Vi kan forestille oss at kantene er elastiske og at vi flytter om på nodene.
    - 

- Andre måter å definere en grad på
    - Ved å endre på definisjonen av en kant, får vi andre begreper, og vi skal se på to slike:
    - Hvis en kant defineres slik at flere kanter kan ligge inntil de samme nodene, eller slik at en kant kan forbinde en node med seg selv, får vi det som henholdsvis kalles multigrafer og pseudografer
    - 

- Vi kan også endre på definisjonen av en kant slik at kantene får retning; da får vi rettede grafer
    - Definisjon

        - En rettet graf er definert som en graf, men hvor kantene er ordnede par <u,v> i stedet for mengder {u,v}
        - F.eks. kantene {<A,B>,<B,A>,<A,C>} over nodene A, B og C
- Tomme grafer
    - En graf uten kanter kalles en tom graf eller en nullgraf
    - 

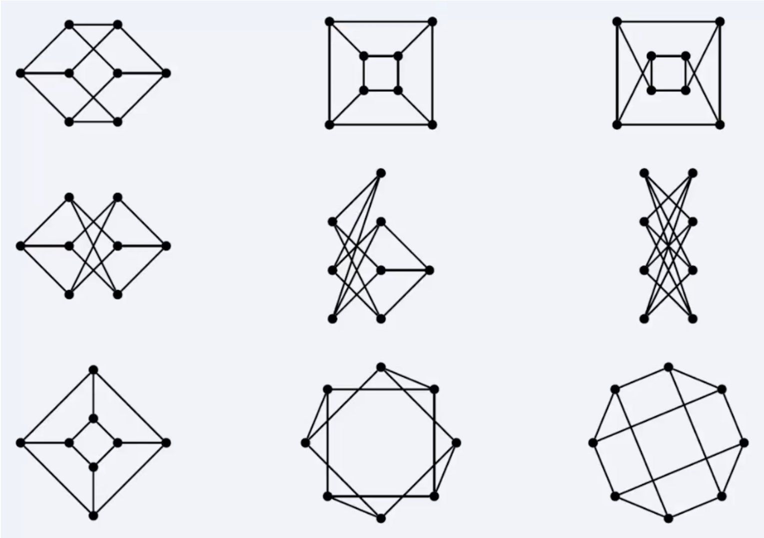
      Tomme grafer.
- Komplette grafer
    - En enkel graf er komplett hvis hver node er nabo med enhver annen node. Den komplette grafen med n noder kalles K_n.
    - 

    -
- Komplementet til grafer
    - Hvis G er en graf, er komplementet til G grafen som har de samme nodens som G, men hvor to noder er naboer hvis og bare hvis nodene ikke er naboer i G. Vi skriver $\overline{G}$ for komplementet til G
    - 

Noder
- Graden til en node
    - Graden til en node v er antall kanter som ligger inntil v.
    - En løkke teller som to kanter.
    - Med deg(v) mener vi graden til v.
    - En node med grad 0 kalles isolert
    - Eksempel
        - En enkel måte å finne graden til en node på er ved å tegne en sirkel rundt noden og telle hvor mange kanter som skjærer sirkelen. Denne metoden fungerer også med løkker og parallelle kanter, som i følgende multigraf.
- Summen av gradene
    - Det første resultatet er at summen av gradene til nodene i en graf alltid er lik det dobbelte av antallet kanter.
    - Hvis V er mengden av noder og E er mengden av kanter, kan dette uttrykkes på følgende måter: $\sum_{v \in V} \deg(v) = 2|E|$

  - Dette leser vi som «summen av deg(v), for alle v i V, er like 2 ganger antall elementer i E.»
  - Vi kan forestille oss at vi begynner med kun nodene og legger til alle kantene, én etter én.

Isomorfi

- Begrepet er et av de viktigste i matematikk
- Isomorfe objekter har samme form, men kan ha ulikt innhold.
- Vi sier at to matematiske objekter er isomorfe hvis de er «strukturelt like»
- Hvis vi har tegnet opp to grafer og kan komme fra den ene til den andre ved å flytte rundt på nodene og endre på lengdene på kantene, er grafene isomorfe
- 
- Definisjon
  - La G og H være to grafer. En isomorfi fra G til H er en bijektiv funksjon f fra nodene i G til nodene i H som er slik at nodene u og v er naboer i G hvis og bare hvis nodene f(u) og f(v) er naboer i H.
- Notasjon
  - Det er vanlig å skrive V(G) for mengden av nodene i en graf G.
  - Bokstaven V brukes fordi noder kalles «vertices» på engelsk
  - Når en graf er enkel, er det vanlig å skrive ab for en kant som ligge rinntil to noder a og b
  - Dette går ikke hvis grafen har parallelle kanter eller løkker.
- Avgjøre om to grafer er isomorfe
  - For å vise at to grafer er isomorfe, må vi gi en funksjon og argumentere for at funksjonen har egenskapene som er nødvendige
  - For å vise at to grafer ikke er isomorfe, er det tilstrekkelig å finne en grafteoretisk egenskap som kun den ene av grafene har.
  - En grafteoretisk egenskap er en egenskap som bevares under lovlige transformasjoner, som å flytte rundt på nodene, gjøre kantene lengre/kortere
  - Noen av de enkleste grafteoretiske egenskapene er følgende:
    - Hvor mange noder en graf har
    - Hvor mange kanter en graf har
    - Hvor mange noder av en bestemt graf har

Kapittel 22 – vandring i grafer

- Eulerveier og eulerkretser
  - La G være en sammenhengende graf. En eulervei er en vandring som inneholder hver kant fra G nøyaktig én gang. En eulerkrets er en eulervei hvor den første og den siste noden sammenfaller. En sammenhengende grad som har en eulerkrets kalles en eulersk graf.
  - EN eulervei kalles også ofte en eulersti, men vi har definert en sti som en vandring hvor ingen node forkommer mer enn én gang
  - I en eulervei har vi lov til å gjenta noder, men ikke kanter.

Fra timer

Logiske gåter

1. Briten bor i det røde huset
2. Svensken har hunder som kjæledyr
3. Dansken drikker te
4. Det grønne huset er like til venstre for det hvite huset
5. Det grønne husets eier drikker kaffe

  - Vi løser dette ved logisk argumentasjon
  - Dvs. : det kommer an på formen
- Formell logikk
  - Det meste av logisk argumentasjon foregår i naturlig språk
    - P $\wedge$ q er samme som p <u>og</u> q
    - P $\vee$ q er samme som p <u>eller</u> q
    - P $\Leftrightarrow$ q er samme som p <u>ekvivalens</u> q
  - Men: det er ganske tydelige mønstre
  - Vi kan lage regler og algoritmer for det.
- Hvorfor?
  - Det er viktig å lære klar logisk argumentasjon
    - Det blir ikke klarene enn ved å formalisere
    - Formalisering hjelper å forstå hvorfor noen mønstre fungerer eller ikke og dermed forbedre argumentasjonen eller avkrefte dem
  - Formal logikk er et paradeeksempel for å lære om
    - Forskjell på syntax og semantikk
    - Hvorfor man får de to til å henge sammen
    - Rekursjon og induksjon

F	¬F
1	0
0	1

F	G	(F ∧ G)
1	1	1
1	0	0
0	1	0
0	0	0

F	G	(F ∨ G)
1	1	1
1	0	1
0	1	1
0	0	0

F	G	(F → G)
1	1	1
1	0	0
0	1	1
0	0	1

Ulike tegn:

- ∨ betyr eller
- ∧ betyr og
- ∩ er en mengde av det som er felles mellom to mengder {1,2}∩{2} = {2}
- ∪ er en samlet mengde av to mengder {1,2} ∪ {2} = {1,2}
- ⊆ sier at mengden på venstre side er delmengden til mengden på høyre side. F.eks. {1} ⊆ {1,2, {1,2}, {1,3}, {1,2,3}}. Og {1,2{1,2}} ⊆ {1,2, {1,2}, {1,3}, {1,2,3}}.
- ¬ evaluerer at et utsagn er usant.

Abstraksjon

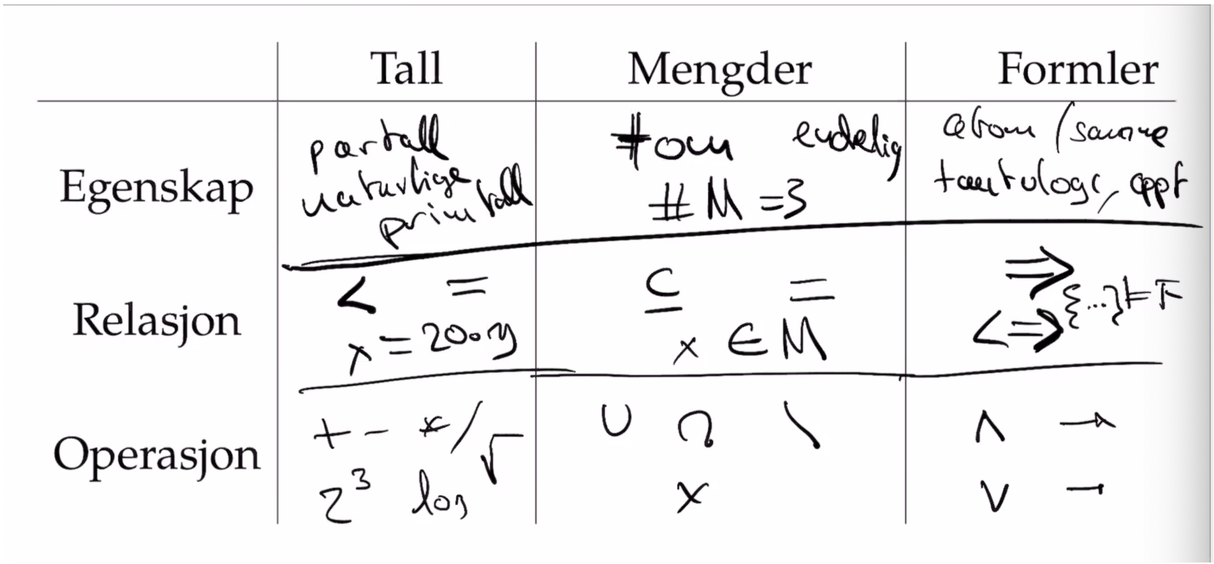
- Er det en personbil så har den ikke brøyteskuff
  - Kan ikke være personbil og ha brøyteskuff
- Er tallerkenen gul så er den ikke fin
  - Kan ikke være gul og din
- Det er felles struktur i resonnementene
- Resonnementet er uavhengig av biler eller tallerkener
- D.v.s.: dette er et logisk resonnement
  - Hvis P→ ¬ Q så ¬(P∧Q)

P	Q	P	→	¬	Q	¬	(P	∧	Q)
1	1	1	0	0	1	0	1	1	1
1	0	1	1	1	0	1	1	0	0
0	1	0	1	0	1	1	0	0	1
0	0	0	1	1	0	1	0	0	0

- Formelen F er en logisk konsekvens av formelen G, med symboler G ⇒ F, hvis F er sann for alle valuasjoner som gjør G sann.
  - F.eks. P→ ¬ Q ⇒¬(P∧Q)
- Formelen F er logisk ekvivalent med formelen G, med symboler G⇔F, hvis F og G har samme sannhetsverdi for alle valuasjoner
- Formelen F er en logisk konsekvens av mengden M, med symboler M |= F, hvis F er sann for alle valuasjoner som gjør alle formlene i M sanne samtidig,
- Et gylig eller holdbart resonnement er et hvor konklusjonen er en logisk konsekvens av mengden av premisser.

- Formelen F er oppfyllvar hvis det Finnes en valuasjon v som oppfyller den, med symboler |= F, det vil si gjør den sann.
- Formelen F er falsiferbar hvis det finnes en valuasjon v som falsifiserer den, med symboler v|≠ F, det vil si gjør den usann.
- Formelen F er gyldig eller en tautologi hvis dne er sann for alle valuasjoner, med symboler v |= F

Egenskaper, Relasjoner og Operasjoner



	Tall	Mengder	Formler
Egenskap	partall naturlige primtall	tom endelig $\#M = 3$	atom (samme tautologi, oppf
Relasjon	$<$ $=$ $x = 2009$	$\subseteq$ $=$ $x \in M$	$\Rightarrow$ $\Leftrightarrow$ $\{\ldots\} \models F$
Operasjon	$+$ $-$ $*$ $/$ $\sqrt{}$ 2^3 log	$\cup$ $\cap$ $\setminus$ $\times$	$\wedge$ $\rightarrow$ $\vee$ $\neg$

Abstraksjoner:

	Egenskap	Relasjon	Operasjon
Tall	Partall, primtall, oddetall	> ≥ =	+, -, *, /, x^2
Mengde	Tom	⊆ =	∩, ∪, \, ×
Relasjon	Symmetrisk, refleksiv, transitiv, anti-symmetrisk Funksjon	=	∩, ∪
Funksjoner	Injektiv, surjektiv, bijektiv	=	f∘g
Formler	Gydlighet, oppfyllbarhet, falsifiserbarhet, motsigelse	Ekvivalens⇔ Logisk konsekvens⇒	∧

- Vi har ikke definert et begrep «relasjon»
- Heller ikke et begrep «funksjon»
- Vi har definert «relasjon fra A til B»
- Vi har definert «relasjon på A»
- Vi har definert «funksjon fra A til B»
- Uten å kjenne til A vet du ikke om en relasjon er refleksiv
- Uten å kjenne til A vet du ikke om en relasjon er en funksjon

- Uten å kjenne til B vet du ikke om en relasjon er surjektiv

Puzzle

1. Ole, Dole Doffen er hannhunder, Daisy og Minnie er tisper
2. Alle liker én av: få kos, hente ting, sove, grave ned ting, går tur
3. Ingen to hunder liker det samme
4. Å hente ting, grave ned, eller gå på tur er aktivt; men ikke å få kos eller sove
5. Ole liker enten å hente eller å grave ned
6. Hverken Dole eller Daisy eller minnie liker å gå på tur
7. En av hannhundene liker å få kos.
8. En av tispene liker å hente
9. Minnie liker å være aktiv

P.g.a. 1 (5 hunder),2,3. For hver ting er det en hund som liker å gjøre det (10)
P.ga. (6) og (10) liker enten Ole eller Doffen å gå på tur. (11)
Tilfelle 1: Ole går på tur
    (5): Ole liker ikke å gå på tur
Dermed, Tilfelle 2: Doffen liker å gå tur. (12)

7: En av Ole, Dole, Doffen liker å få kos
    p.g.a (12) er det ikke Doffen
    p.g.a (5) er det ikke Ole
        Da er det Dole som liker kos (13)
8: En av tispene liker å hente
    p.g.a (9) og (8) liker Minnie å hente. (14)

Dole = kos, Doffen = tur, Minnie = hente
Mangler grave ned ting, og å sove.

    p.ga. (5) og (14) liker Ole å grave ned (15)

    p.g.a (2) liker Daisy å sove
SVAR:
Ole – grave ned
Dole – kos
Doffen – tur
Daisy - sove
Minnie – hente

Bevisformer

Dette er ekvivalente utsagn

$A \Rightarrow B$

$\neg B \Rightarrow \neg A$ Kontrapositivt bevis

$A \wedge \neg B$ er oppfyllbar Motigelsesbevis

Dette er også ekvivalente utsagn:
$\{A_1, A_2, A_3\} \models B$
$\{\neg B, A_2, A_3\} \models \neg A_1$
$\{A_1, A_2, A_3, \neg B\}$ er uoppfyllbar

La A, B, C være tre mengder
- Anta at $A \subseteq B$ (1) og $B \subseteq C$ (2)
- Vis at $A \subseteq C$

Jeg må vise at alle $x \in A$, er $x \in C$. (def av $\subseteq$)

La x være et vilkårlig element av A
P.g.a (1) er også $x \in B$
P.g.a (2) er også $x \in C$

X var vilkårlig med $x \in A$. Derfor for alle $x \in A$ er $x \in C$
$A \subseteq C$ ihht definisjon av $\subseteq$

Kontrapositivt bevis
Vis at $A \not\subseteq B$ fra $B \subseteq C$(2) og $A \not\subseteq C$(3)
p.g.a (3) finnes $x \in A$ med $x \notin C$
Anta at $x \in B$, da må fra (2) også $x \in C$
$x \notin B$ kan ikke være sant, altså $x \notin B$
$x \in A$ og $x \notin B$, altså (def $\subseteq$) $A \not\subseteq C$

Motsigelsesbevis
Anta for motsigelsen at $A \not\subseteq C$ (3)
p.g.a (3) finnes $x \in A$ med $x \notin C$
Men p.g.a (1) og $x \in A$ så $x \in B$
p.g.a(2) og $x \in B$ så $x \in C$

Motsigelse

Transitivitet
Noen relasjoner på mengden av person:
- X er like gammel som y
  - Hvis a(x)= a(y) og a(y)=a(z)
  - Så a(x) = a(z)
- X er eldre enn y
  - Hvis a(x) > a(y) og a(y) > a(z)
  - Så a(x) > a(z)
- X er yngre enn y
  - Hvis a(x) < a(y) og a(y) < a(z)
  - Så a(x) < a(z)
- X kjenner y
  - Hvis a(x) kjenner a(y) og a(y) kjenner a(z)
  - Så kjenner ikke nedvendigvis a(x) a(z)

- Altså er denne relasjonen ikke transitiv
- X er gift med y
    - Den er ikke transitiv. Man er gift med en person som også er gift med deg.
    - Hvis den skal være transitiv må du være gift med deg selv.
- X er i slekt med y
    - Den er transitiv
- X eier huset y
    - Den er ikke transitiv

Matematisk induksjon

Å bevise noe for alt

- Bevise at for alle $x \in A$, så holder påstanden P(x)
- La $x \in A$ være et vilkårlig element av A
    - Så beviser vi P(a)
- Siden A var vilkårlig valgt, gjelder P for alle elementer av A
- VI beviser P(a) for alle elementer, uavhengig av hverandre.

Å bevise noe for alle naturlige tall

- N = {0,1,2,3,4,5,...}
- VI starter med å bevise P(0)
- Så beviser vi P(1), og vi kan bruke P(0)
- Så beviser vi P(2), og vi kan bruke P(1)
- Så beviser vi P(3), og vi kan bruke P(2)
- ...
- Da beviser vi etter hvert P(n) for alle $n \in N$
- Merk at det fordi N er induktivt definert.

Vilkårlige steg

- VI starter med å bevise P(0)
- Så velger vi et vilkårlig tall $k \in N$
    - Og beviser P(k+1),og vi kan bruker P(k)
    - D.v.s.: Vi beviser at hvis P(k) så holder P(k+1)
- Siden $k \in N$ var vilkårlig valgt, har vi bevist:

  Hvis P(n) gjelder så gjelder P(n+1)

  For alle $n \in N$.
- Da har vi bevist P(0), og derfor P(1), og derfra P(2),...
- Vi har altså bevist at P(n) holder for alle $n \in N$

Eksempel

- Påstand: n^2+n er et partall for alle $n \in N$
- P(n): n^2+n er et partall
- Vi viser at P(n) holder for alle $n \in N$
- Vi starter med å bevise P(0), d.v.s. 0^2+0 er et partall
- Nå viser vi at hvis n^2+n er et partall så er $(n+1)^2+(n+1)$ partall, for alle $n \in N$
    - La $k \in N$ være et vilkårlig naturlig tall
    - Anta at P(k), d.v.s. k^2+k er et partall
    - Vi må vise P(k+1), d.v.s. $(k+1)^2 + (k+1)$ er et partall
    - $(k+1)^2 + (k+1) = k^2+2k+1+k+1 = (k^2+k)+2k+2$
    - ... som er en sum av partall og derfor et partall

- Vi har altså bevist 0^2+0 er et partall, derfra at 1^2+1 er et partall,...

Bevis ved matematisk induksjon
- For å bevise matematisk induksjon at en påstand er sann for alle naturlige tall, er det tilstrekkelig å bevise:
- Basissteget: at påstanden holder for tallet 0
- Induksjonssteget: at hvis påstanden holder fro et vilkårlig naturlig tall n, så holder den også for n+1
- Antakelsen om at påstanden er sann for n, kalles induksjonshypotesen.
- Hvis begge disse stegene kan bevises, kan vi ved matematisk induksjon konkludere med at påstanden er sann for alle naturlige tall
- Matematisk induksjon er en bevismetode som skiller seg fra de andre bevismetodene i kapittel 5
- Det er for eksempel ikke mulig å bevise noe ved induksjon ved å bare manipulere noen symboler eller sette noe inn i en formel.
- Et bevis ved matematisk induksjon har en bestemt logisk struktur som skiller seg fra andre bevismetoder
- Det er ikke vanskelig å lære seg denne metoden, men det krever øvelse og at man faktisk tester seg selv.
- Matematisk induksjon handler om å vise at en egenskap holder, at en påstand er sann, for alle de naturlige tallene
- Først viser vi at egenskapen holder for det minste tallet, som er 0, og så viser vi at hvis egenskapen holder fro ett tall, så holder egenskapen også for det neste tallet.

Eksempel som induksjonsbevis
- Påstanden vi skal bevise at er sann fro alle naturnlige tall n er:
- «n^2+n er et partall»
- Basissteget er å bevise at påstanden holder for tallet 0
- Siden P(0), d.v.s. 0^2+0 er et partall, får vi at påstanden holder
- Induksjonssteget går som følger: Anta at påstanden holder for et tall km det vil si at k^2+k er et partall
- Dette er induksjonshypotesen
- Fra denne må vi vise at påstanden også holder for k+1, det vil si at k^2+k er et partall
    - $(k+1)^2 + (k+1) = k^2+2k+1+k+1 = (k^2+k)+(2k+2)$
- K^2+k er et partall ved induksjonshypotesen
- $2k+2 = 2(k+1)$ er et partall
- $(K+1)^2+(k+1)$ er en sum av partall og derfor et partal, som var det vi skulle fram til
- Ved matematisk induksjon følger det at n^2+n er et partall for alle naturlige tall n

Kapittel 13 – Førsteordens språk

Språk med større utsagnskraft
- Utsagnslogikk beskriver strukturen til utsagn
- Husk: et utsagn er noe som kan vøre sant eller usant
- Semantikken tillater å definere begrep ‘konsekvens’ og ‘ekvivalens’ mellom formler
    - Som tilsvarer hvordan vi resonnerer
    - Selv når vi ikke bruker formal logikk

- For alle formler F og G:
    - $F \rightarrow G$ er en logisk konsekvens av $\neg G \rightarrow \neg F$
  - Dette kan vi sjekke, for eksempel ved bruk av sannhetsverditabeller
  - Derfor vet vi, at hvis vi skal bevise et utsagn på formen:
    - Hvis F gjelder, så gjelder også G
  - Så holder det å bevise at:
    - Hvis G ikke gjelder, så gjelder heller ikke F, fordi den første er en konsekvens av nr 2.
- Vi har lært å bevise et utsagn på formen
    - For alle $x \in A$ gjelder påstanden P for x
  - Så er det nok å bevise
    - Påstanden P gjelder for a hvor a er et vilkårlig valgt element av A
  - VI har også litt forklaring av hva «vilkårlig valgt» innebærer
  - Og en del forklaringer på hvorfor dette gir mening.
  - Men vi har ingen forklaring innenfor utsagnslogikken.

Introduksjon

- I utsagnlogikk har vi kun utsagnsvariablene og konnektivene
- Med disse kan vi analyserer og representere utsagn
- Førsteordens logikk, også kalt predikantlogikk, utvider utsagnslogikk med blant annet kvantorer:
  - $\exists$ Eksistenskvantoren, og
  - $\forall$ Allkvantoren.
- Ved hjelp av disse kan vi analysere og representere kvantifiserte utsagn, det vil si utsagn om at det finnes et objekt med en bestemt egenskap eller at alle objekter har en bestemt egenskap.
- Slike påstander er det vanskelig å representere i utsagnslogikk
- Eksempler fra matematikk
  - Ethvert heltall er enten et partall eller et oddetall
  - Det finnes uendelig mange primtall
  - Mellom to brøktall finnes det et annet brøktall
  - Alle partall større enn 2 er lik summen av to primtall
- Slike universelle og eksistensielle utsagn inngår ofte i resonnementer.

Formen på et resonnement

- Følgende to resonnementer har forskjellig *innhold*, men nøyaktig samme *form*.
  - Alle mennesker er dødelige
    <u>Kurt er ikke dødelig</u>
    Kurt er ikke et menneske
  - Alle perfekte tall er partall
    <u>X er ikke et partall</u>
    X er ikke et perfekt tall
- Legg merke til at begge resonnementene er gyldige i kraft av sin form og ikke sitt innhold
- Ved hjelp av førsteordens logikk kan vi analysere slike resonnementer.

Skille mellom syntaks og semantikk

- Vi skiller skarpt mellom syntaks, som består av formler, symboler og tegn, og semantikk, som består av tolkninger, sannhetsverdier og modeller
- Syntaks er i utgangspunktet bare tegn som kan bety hva som helst, mens semantikken forteller hvordan tegnene skal tolkes
- Vi begynner med å definere syntaksen til førsteordens logikk
  - I dette kapitlet defineres syntaksen til førsteordens logikk via to induktivt definerte mengder
  - Den første er mengden av førsteordens termer
  - Den andre mengden er mengden av førsteordens formler
  - Utgangspunktet for å definere førsteordens termer er variabler, konstantsymboler og funksjonssymboler
  - Alle variabler og konstantsymboler er førsteordens termer.
  - En typisk sammensatt førsteordens term ser slik ut:
    - F(a,x)
      F - funksjonssymbol
      A – førsteordens term (konstantsymbol)
      X – førsteordens term (variabel)
  - Deretter defineres mengden av atomære formler
  - Dette er med utgangspunkt i relasjonssymboler og termer
  - En typisk atomær formel ser slik ut:
    - R(a,f(a,x))
      R – relasjonssymbol
      A – førsteordens term(konstantsymbol)
      F(a,x) – førsteordens term (sammensatt)
  - For å lage sammensatte førsteordens formler kan de atomære formlene settes sammen med de logiske konnektivene
  - Dette er på akkurat samme måte som utsagnsvariablene i utsagnslogikk
  - I tillegg bruks kvantorene $\forall$ og $\exists$, sammen med variabler, for å lage kvantifiserte formler på følgende form:
    - $\forall$x(P(x)$\vee$Q(f(a,x)))
      $\forall$ - kvantor
      X – variabel
      P(x) og f(a,x) – førsteordens formler (atomære)
      $\vee$ - logisk konnektiv

  - Hvilke førsteordens formler som finnes i en gitt kontekst, avhenger kun av konstantsymbolene, funksjonssymbolene og relasjonssymbolene
  - Dette kalles de ikke-logikse symbolene
  - De ikke-logiske symbolene utgjør det som kalles en signatur

Definisjon (Signatur)

- De ikke-logiske symbolene utgjør det som kalles en **signatur** (*eng: signature*).
- En signatur angis som et tuppel av tre mengder på følgende måte:

$$\langle \underbrace{a, b, c, \ldots}_{\text{konstantsymboler}} \; ; \; \underbrace{f, g, h, \ldots}_{\text{funksjonssymboler}} \; ; \; \underbrace{R, S, T, \ldots}_{\text{relasjonssymboler}} \rangle$$

Her er konstant-, funksjons- og relasjonssymbolene adskilt med semikolon.

    - Vi krever at disse er disjunkte, det vil si at de ikke har noen elementer felles
- Konvensjonen om å droppe parenteser
    - Aritet = antall argumenter noe må ta inn.
    - Så lengde det er entydig og ariteten er kjent, kan vi droppe parentesene og skrive for eksempel
      fa i stedet for f(a)
      fx i stedet for f(x)
      gaa istedet for g(a,a)
      gfaa i stedet for g(f(a),a)
    - Men noen ganger bør parenteser brukes for å gjøre en term mer leselig.

Kapittel 14 – representasjon av kvantifiserte utsagn

Å brukes førsteordenslogikk må læres

- L(x,y) representerer at x liker y
- S(x) representerer at x er student
- M representerer Martin
- «Martin liker alle studenter»
- L(m, ∀s)?
- Som å oversette naturlige språk ord for ord.

Hva? Hvordan?

- VI må første forstå hva utsagnet innebærer
- ... og så hvordan vi får brukt logikken til å uttrykke det
- «Martin liker alle studenter»
- Her sier vi noe om alle studenter
- Vi sier altså noe om alle x slik at s(x) holder
- Nemlig at Martin liker dem. Altså at l(m,x) holder
- Logikken lar oss ikke si noe om «alle x med s(x)» direkte
- Men vi kan si noe om «alle x»
- Det blir altså: for alle x, hvis x er en student, så liker Martin x
- Det kan vi skrive som formel:

$$\forall x.(s(x) \rightarrow l(m,x))$$

- Et predikat er et uttrykk som får en sannhetsverdi når vi erstatter plassholderne med verdier

- For eksempel blir predikatet «tallet x er et partall» sant når vi erstatter x med (et partall) og usant når vi erstatter x med 3 (ikke et partall)
- En variabel er bundet i en formel hvis den er innenfor skopet til en kvantor; ellers er den fri.
- En lukket førsteordens formel er en formel uten frie variabler
- Når vi representerer utsagn med førsteordens formler, er det helt essensielt å se på strukturen til utsagnene vi representerer
- Her kommer alt vi lærte om utsagnslogikk til nytte.
- I tillegg må vi holde styr på kvantorene

Et enkelt eksempel
- La Bx representere predikatet «x har det bra» B(x)
- Da representeres ¬Bx predikatet «det er slik at x har det bra»
- Det er naturlig å tolke dette på samme måte som «x har det dårlig»
- Da får vi følgende representasjon
  - ∃xBx noen har det bra denne er lukket.
  - ∀xBx alle har det bra
  - ¬∃xBx ingen har det bra
  - ¬∀xBx ikke alle har det bra
  - ¬∀x¬Bx ikke alle har det dårlig
  - ¬∃x¬Bx ingen har det dårlig
  - ∀x¬Bx alle har det dårlig
  - ∃x¬Bx noen har det dårlig

Enda et eksempel
- La nå Rxy stå for det generelle predikatet «x er relatert til y»
- For å uttykke «alle er relatert til noen» skriver vi ∀x∃yRxy
- VI kan godt velge andre variabler og skrive ∀w∃zRwz
  - Rab a er relatert til b
  - ∀x∀yRxy relasjonen er universell / alle er relatert til alle
  - ∃x∃yRxy relasjonen er ikke tom / noen er relatert til noen
  - ¬∃x∃yRxy relasjonen er tom / ingen er relatert til noen
  - ∃x∀yRxy det finnes et noen som er relatert til alle
  - ∀x∃yRxy for alle finnes det noen som det er relatert til
  - ∃xRxx noen er relatert til seg selv
  - ∀x(Px→Rxx) hvis P er sann for x, så er x relatert til seg selv
  - ∀x(Rxx→Px) P er sann for alle som er relatert til seg selv

Modeller
- Modeller gjør det samme for førsteordens formler som valuasjoner gjør for utsagnslogiske formler
- De gir alle fomler en definitiv sannhetsverdi
- Fordi en modell per definisjon har et domene og en tolkning til alle konstantsymboler, funksjonssymboler og relasjonssymboler.
- EN modell M består av en ikke-tom mengde D, kalt domenet til modellen, og en tolkning av alle ikke-logiske symboler