MAT1030 – Diskret matematikk

Forelesning 11: Relasjoner

Dag Normann

Matematisk Institutt, Universitetet i Oslo

18. februar 2008

Oppsummering

- Vi har gjort oss ferdige med innføringen av Boolesk mengdelære.
- Bruk av Venn-diagrammer er et av læringsmålene i dette emnet.
- Vi så kort på digital representasjon av mengder.
- Forståelsen av dette blir testet i Oblig. 1
- Definisjonene av kardinaltall og potensmengde, og sammenhengene mellom dem, bør dere kjenne til.
- Vi startet med definisjonene av ordnede par, Cartesiske produkter og relasjoner.
- Dette skal vi fortsette med.

Relasjoner

- Erfarigsmessig faller det stoffet vi nå begynner på vanskeligere for mange enn det vi har gått gjennom til nå.
- Det skyldes at stoffet synes abstrakt og at det er mange nye begreper.
- I eksempler vil vi kunne innføre noen nye symboler som vi gir en spesiell betydning.
- Et eksempel fra forrige uke er relasjonen $a \equiv_p b$ som uttrykker at p er en faktor i $a - b$.
- En av de ferdighetene vi skal oppøve i MAT1030 er evnen til å lese, og forstå, definisjoner.
- De relasjonene vi vil innføre i eksemplene, vil som oftest ikke være pensum, men evnen til å forstå slike eksempler kan bli prøvet til eksamen.

Relasjoner

- Relasjoner med bestemte egenskaper kan dukke opp i så mange forskjellige sammenhenger at det kan være aktuelt å studere dem under ett.
- Det kan også være aktuelt å utvikle program som virker for alle relasjoner av en gitt type.
- Følgende oppgaver trenger strengt tatt det samme programmet:
  - Ordne dagens avisoverskrifter alfabetisk.
  - Ordne deltagerne i kretsmesterskapet på10 km klassisk etter oppnådd slutt-tid.
  - Ordne LOTTO-tallene etter størrelse.
- Det er noe felles ved oppgaven å skulle ordne en mengde, og det er naturlig å isolere de relasjonene som kan oppfattes som ordninger.

Relasjoner

- Vi ordner gjerne studentene etter oppnådde karakterer.

  Er det noen forskjell på en slik "ordning" og en alfabetisk ordning?
- Inklusjon mellom mengder er en form for "større enn", men det finnes mengder, eksempelvis $\{1, 2, 3\}$ og $\{2, 3, 4\}$, som ikke er innehold i hverandre noen vei.
- Hva vil sorteringsalgoritmer gjøre hvis vi bruker dem på slike ordninger?

Relasjoner

- Det er noen egenskaper ved relasjoner som er så vanlig forekommende (hos de *nyttige* relasjonene) at vi har gitt dem egne navn.
- Vi gir listen først og drøfter hver enkelt egenskap etterpå:

Relasjoner

Definisjon

- En relasjon R på en mengde A kalles:
  - Refleksiv hvis xRx for alle $x \in A$.
  - Irrefleksiv hvis vi ikke har noen $x \in A$ slik at xRx.
  - Symmetrisk hvis xRy medfører yRx for alle $x, y \in A$.
  - Antisymmetrisk hvis $xRy \wedge yRx$ medfører at $x = y$ for alle $x, y \in A$.
  - Transitiv hvis $xRy \wedge yRz$ medfører xRz for alle $x, y, z \in A$.
- Vi skal bruke den tiden vi trenger til å lære oss disse begrepene, og å forstå dem.

Refleksive relasjoner

Eksempel (Refleksiv: xRx for alle x)

- For enhver mengde A vil likhetsrelasjonen $x = y$ være refleksiv på A.
- Hvis X er mengden av delmengder av en mengde $\mathcal{E}$, vil inklusjonsrelasjonen $A \subseteq B$ være refleksiv på X.
- $\leq$ er en refleksiv relasjon, uansett om vi ser på den som en relasjon på $\mathbb{N}$, på $\mathbb{Q}$, på $\mathbb{J}$ eller på $\mathbb{R}$.
- $<$ er normalt ikke en refleksiv relasjon, spesielt ikke nå vi bruker tegnet på vanlig måte for $\mathbb{N}$ etc.
- Hvis A er mengden av sammensatte utsagn i utsagnsvariablene p, q og r, og ϕ og ψ er sammensatte utsagn, kan vi definere $\phi R \psi$ som

  $$\phi \to \psi \text{ er en tautologi.}$$

  Da er R en refleksiv relasjon.

Refleksive relasjoner

Hvis en relasjon gis på matriseform, er det lett å se om relasjonen er refleksiv eller ikke:

$$\begin{bmatrix} \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} \end{bmatrix}$$

Ved å se at vi har bare T på diagonalen, ser vi at relasjonen er refleksiv.

Gjør vi en liten forandring, trenger ikke relasjonen lenger å være refleksiv:

Refleksive relasjoner

$$\begin{bmatrix} \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \color{red}{\mathrm{F}} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} \end{bmatrix}$$

Irrefleksive relasjoner

Eksempel (Irrefleksiv: $\neg(xRx)$ for alle x)

- $\neq$ er irrefleksiv på alle mengder.
- *Far til* og *Mor til* er irrefleksive relasjoner på enhver forsamling av mennesker.
- $<$ og $>$ er irrefleksive relasjoner på $\mathbb{N}$, $\mathbb{J}$, $\mathbb{Q}$ og $\mathbb{R}$.
- *Ekte inklusjon* er en irrefleksiv relasjon.

Irrefleksive relasjoner

Eksempel

- La X være mengden av sammensatte utsagn i utsagnsvariablene p, q og r, la ϕ og ψ være sammensatte utsagn, og definer relasjonen S ved

  $$\phi S \psi$$

  når

  $$\phi \wedge \psi \to \mathrm{F}$$

  er en tautologi.
- Da er S hverken refleksiv eller irrefleksiv.

Irrefleksive relasjoner

Hvis relasjonen blir beskrevet ved hjelp av en matrise, er det også enkelt å kontrollere om relasjonen er irrefleksiv:

$$\begin{bmatrix} \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \mathrm{F} \end{bmatrix}$$

Det er bare å sjekke om det står F langs diagonalen.

Symmetriske relasjoner

Eksempel (Symmetrisk: xRy medfører yRx for alle x og y.)

- Symmetriske relasjoner er de relasjonene hvor rekkefølgen ikke spiller noen rolle.
- x er gift med y.
- $\phi \wedge \psi$ er ikke en kontradiksjon.
- $\phi \wedge \psi$ er en kontradiksjon.
- n og m har en felles faktor > 1, som en relasjon på $\mathbb{N}$.
- $A \cap B = \emptyset$ som relasjon på potensmengden til $\mathcal{E}$.

Symmetriske relasjoner

Vi kan undersøke om en relasjon er symmetrisk ved å studere matriserepresentasjonen:

Eksempel

$$\begin{bmatrix} \mathrm{T} & \mathrm{T} & \mathrm{T} & \mathrm{F} \\ \mathrm{T} & \mathrm{F} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} \end{bmatrix}$$

Denne relasjonen er symmetrisk

Eksempel

$$\begin{bmatrix} \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{F} \\ \mathit{T} & \mathrm{F} & \mathrm{F} & \mathrm{T} \\ \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{T} \\ \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} \end{bmatrix}$$

Denne relasjonen er ikke symmetrisk

Antisymmetriske relasjoner

Eksempel (Antisymmetrisk: $xRy \land yRx$ medfører $x = y$)

- I en antisymmetrisk relasjon skal vi ikke ha andre positive speilsymmetrier om diagonalen enn de som ligger på diagonalen.
- Inklusjon av mengder.
- $\leq$ og $<$ i vanlige sammenhenger.
- Antisymmetri er svært ofte knyttet til former for ordninger, og vi kommer tilbake til dette senere

Transitive relasjoner

Eksempel (Transitiv: $xRy \wedge yRz$ medfører xRz)

- $<$ og $\leq$ er transitive relasjoner i alle vanlige sammenhenger.
- $\subseteq$ er en transitiv relasjon på potensmengden til $\mathcal{E}$.
- "ϕ er en logisk konsekvens av ψ" er transitiv.
- *Far til* og *Mor til* er ikke transitive, men *etterkommer* er transitiv.
- *Søsken til* er transitiv hvis vi mener helsøsken, men ikke hvis vi inkluderer halvsøsken.

Noen eksempler

- Vi skal ta utgangspunkt i noen relasjoner som det kan være aktuelt å studere av praktiske eller teoretiske grunner.
- Vi skal se på hvilke av de fem egenskapene vi har sett på disse relasjonene vil ha.

Noen eksempler

- Hvis A og B er utsagn i predikatlogikk, lar vi $A \Rightarrow B$ bety at B er en logisk konsekvens av A. Vi sier at A impliserer B.
- Det betyr at B er sann i enhver situasjon som gjør A sann.
- Vi oppfatter $\Rightarrow$ som en relasjon på mengden av utsagn i predikatlogikk.
- $\Rightarrow$ er *refleksiv* fordi $A \Rightarrow A$ for alle utsagn A.
- $\Rightarrow$ er da ikke *irrefleksiv*.
- $\Rightarrow$ er ikke *symmetrisk* (se 1.) eller *antisymmetrisk* (se 2.)
    1. Vi har $x > 0 \Rightarrow x > 0 \lor x = 0$, men omvendingen gjelder ikke.
    2. Utsagnene $\neg(x < 0) \lor x > 0$ og $x < 0 \rightarrow x > 0$ impliserer hverandre, men de er ikke like.
- $\Rightarrow$ er transitiv siden $A \Rightarrow C$ når $A \Rightarrow B$ og $B \Rightarrow C$.

Noen eksempler

- Når man skal gi en matematisk beskrivelse av hva et program P "gjør", er det ofte to relasjoner som det er aktuelle å studere.
- Vi begrenser oss til språk som minner om pseudokoder.
- Da har vi variable $x_1, \ldots, x_n$ i programmet.
- Underveis vil verdiene på disse variablene endre seg, gjennom instruksjoner som
$$x_i \leftarrow t(x_1, \ldots, x_n).$$
- En fordeling av verdier på variablene kaller vi en valuasjon eller en tilstand.

Noen eksempler

- La V være mengden av valuasjoner, og la u og v være elementer i V.
- Hvert program $\mathcal{P}$ vil bestemme en relasjon $[\![\mathcal{P}]\!]$ på V, hvor

  $$u[\![\mathcal{P}]\!]v$$

  hvis output-valuasjonen er v når inputvaluasjonen er u.

Noen eksempler

- Hvis $[\![\mathcal{P}]\!]$ er *refleksiv*, betyr det at programmet i realiteten lar alle inputvaluasjoner være uforandret.
- Hvis $[\![\mathcal{P}]\!]$ er *irrefleksiv*, betyr det at programmet gjør endringer uansett input.
- Hvis $[\![\mathcal{P}]\!]$ er symmetrisk, betyr det at hvis vi kjører programmet en gang til, kommer vi tilbake til utgangspunktet.
- Krypteringsmaskinen ENIGMA brukt av tyskerne under krigen hadde den egenskapen.
- Hvis $[\![\mathcal{P}]\!]$ er antisymmetrisk, betyr det at vi aldri kommer tilbake til input-dataene ved å kjøre programmet på output-dataene.
- $[\![\mathcal{P}]\!]$ er i praksis aldri transitiv, siden dette ville medført at vi oppnår det samme om vi kjører programmet to ganger, hvor output overføres til input mellom gangene.

  Dette vil imidlertid være tilfelle om output-dataene alltid inneholder en form for stopp-ordre.

Noen eksempler

- En annen viktig relasjon i studiet av hva programmer "gjør" er $\vdash^*$
- Et program P er normalt en form for tekst, og den teksten består av punkter eller instruksjoner.
- Typisk har vi nummerert alle linjene i en pseudokode, slik at vi kan snakke om at vi er i en bestemt posisjon i programmet underveis i kjøringen av programmet.
- La P være mengden av posisjoner og la fortsatt V være mengden av valuasjoner.
- $\vdash^*$ er relasjonen på $P \times V$ hvor

  $$(p, v) \vdash^* (q, u)$$

  hvis programmet $\mathcal{P}$, om vi er i posisjon p og med valuasjon v vil komme til posisjon q og med valuasjon u etter ingen, ett eller flere regneskritt.
- Denne relasjonen er selvfølgelig avhengig av $\mathcal{P}$, og vi kan skrive den $\vdash^*_{\mathcal{P}}$.

Noen eksempler

- Denne relasjonen er *refleksiv*, fordi vi tillater at vi ikke tar noen regneskritt.

  Den er da normalt ikke irrefleksiv.
- Denne relasjonen er *transitiv*.
- Hvis relasjonen er symmetrisk, er det en katastrofe for programmereren, siden vi da bare har løkkeberegninger.
- Hvis relasjonen er *antisymmetrisk*, vil beregningen aldri gå i løkke.

Ekvivalensrelasjoner

En viktig klasse av relasjoner er ekvivalensrelasjonene. La oss se på noen eksempler før vi gir den formelle definisjonen.

Eksempel

a) La $A = \{0, \ldots, 9\}$.

Hvis a og b er elementer i A lar vi aRb hvis $a - b$ er delelig med 3.

Vi ser at R deler A opp i tre disjunkte mengder $B = \{0, 3, 6, 9\}$, $C = \{1, 4, 7\}$ og $D = \{2, 5, 8\}$, hvor hver mengde bestrår av tall som står i innbyrdes relasjon til hverandre, mens vi ikke har noen R-forbindelser på mengdene imellom.

Ekvivalensrelasjoner

Eksempel (Fortsatt)

b) La $A = \mathbb{R}^2$ og la

$$(x, y)R(u, v) \Leftrightarrow x^2 + y^2 = u^2 + v^2.$$

Vi ser at to punkter står i R-relasjon til hverandre nøyaktig når avstanden til origo er den samme.

Denne relasjonen deler $\mathbb{R}^2$ opp i uendelig mange disjunkte mengder, nemlig sirklene om origo med radius r for $r \geq 0$.

Ekvivalensrelasjoner

Eksempel (Fortsatt)

c) La $A = \mathbb{Q}$ og la pRq om p og q har den samme *heltallsverdien*. Heltallsverdien til et tall p er det største hele tallet $a \leq p$.

I alle disse eksemplene har vi definert en relasjon R ved at to objekter står i relasjon til hverandre når de deler en viss felles egenskap.

Det er denne typen relasjoner vi vil kalle *ekvivalensrelasjoner*.

Ekvivalensrelasjoner

- Uansett hvilken egenskap det vil være snakk om, vil ethvert objekt dele denne egenskapen med seg selv.

  Vi vil altså kreve av en ekvivalensrelasjon at den skal være *refleksiv*.
- Hvis a og b deler en egenskap, kan vi også snu på ordstillingen og si at b og a deler denne egenskapen.
- Det er altså et rimelig krav til at en relasjon skal kalles en ekvivalensrelasjon at den er *symmetrisk*.
- Hvis a og b deler en egenskap, og b og c deler den samme egenskapen, er den også felles for a og c.

  Vi vil kreve av en ekvivalensrelasjon at den skal være *transitiv*.

Ekvivalensrelasjoner

- Det viser seg at disse tre egenskapene er tilstrekkelige til å fange opp inutisjonen vår om å formalisere det uformelle "dele visse egenskaper".

  Den formelle definisjonen er:

Definisjon

La R være en relasjon på en mengde A.

Vi kaller R en ekvivalensrelasjon om R er refleksiv, symmetrisk og transitiv.