

MAT1030 – Forelesning 11

Relasjoner

Dag Normann - 23. februar 2010

(Sist oppdatert: 2010-02-23 14:33)

Kapittel 5: Relasjoner

Kommentarer til forelesningen

På grunn av svikt i dataanlegget, ble forelesningen gitt som tavleforelesning.

Dette resulterte i at noen planlagte momenter uteble, mens foreleser snakket om ordninger, et tema planlagt for 24.02.2010.

Samlet sett vil forelesningene 23.02.2010 og 24.02.2010 dekke pensum om relasjoner, med eksempler i tillegg.

Binære relasjoner

- Forrige uke innførte vi mengdebegrepet, og vi så på Boolske operasjoner som union, snitt og komplement.
- Vi lærte å sette opp Venn-diagrammer for å studere resultatet av sammensatte Boolske operasjoner.
- Vi så på inklusjon, det vil si delmengdebegrepet.
- Vi var en rask tur innom kardinalitet.
- Til slutt så vi på ordnede par (a, b) og og kartesisk produkt $A \times B$.
- $A \times B = \{(a, b) : a \in A \wedge b \in B\}$
- Vi fortsetter der vi slapp.

Eksempel.

- Hvis A er mengden av norske statsborgere, vil $A \times A$ være mengden av par av norske statsborgere.

Det fins mange interessante undermengder av $A \times A$ bestemt av de forskjellige forhold det kan være mellom to personer, eksempelvis

- kollega av
- søster til
- nabo av
- misunnelig på
- ...

Dette vil lede oss over til avsnittet om relasjoner.

Definisjon.

La A være en mengde.

En binær relasjon på A er en delmengde R av $A^2 = A \times A$.

Merk.

- I senere studier kan dere komme borti relasjoner mellom tre eller flere objekter. Disse er da ikke binære.
- Siden vi bare skal studere binære relasjoner, gjør vi som boken, og dropper ordet "binær".

Eksempel.

- I kryptografi er modularegning viktig.
- Hvis p er et primtall og a og b er hele tall, sier vi at $a \equiv_p b$ om p er en faktor i $a - b$.
- Da er \equiv_p en relasjon på de hele tallene.
- Vi kunne like gjerne skrevet

$$(a, b) \in \equiv_p .$$

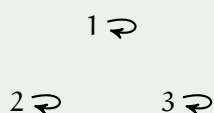
- Relasjonen \equiv_p og beslektede relasjoner (hvor eksempelvis p ikke er et primtall, men i praksis umulig å faktorisere) spiller en stor rolle i kryptografi.

Vi skal se på hvordan vi kan visualisere relasjoner.

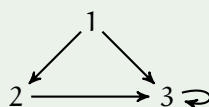
Eksempel.

La $S = \{1, 2, 3\}$.

- $\{(1, 1), (2, 2), (3, 3)\}$ er en binær relasjon på S , skrevet på listeform. På grafisk form ser relasjonen slik ut:



- $\{(1, 2), (1, 3), (2, 3), (3, 3)\}$ er også en binær relasjon på S , skrevet på listeform. Grafisk form blir:



Eksempel (Flere eksempler på relasjoner).

- *Likhetsrelasjonen* på en mengde S , $\{(x, x) : x \in S\}$.
- *Mindre enn-relasjonen* på f.eks. naturlige tall, $\{(x, y) : x, y \in \mathbb{N} \text{ og } x < y\}$
- *Foreldrerelasjonen* på f.eks. mengden av mennesker, $\{(a, b) : a \text{ er forelder til } b\}$
- *Delmengde-relasjonen* på en mengde av mengder.
- Og så videre.

- Noen lærebøker vil definere en relasjon fra A til B som en mengde

$$R \subseteq A \times B.$$

- Det kan fins pedagogiske grunner for å gjøre det slik, men enhver relasjon fra A til B vil samtidig være en relasjon på $A \cup B$.
- Vi vinner ikke tilstrekkelig mye på å arbeide med mere generelle relasjoner sett i forhold til hvor omstendelig det vil bli å formulere det vi ønsker å uttrykke.

Notasjon for relasjoner

- Det å beskrive en relasjon som en mengde av ordnede par gir ikke mye innsikt i hvordan relasjonen ser ut.
- Det å skrive $(a, b) \in R$ representerer også en uvant måte å skrive ting på.
- Ingen av oss har lyst til å begynne å skrive

$$(2, 3) \in <$$

i stedet for $2 < 3$, eller

$$(3, 3) \in =$$

i stedet for $3 = 3$, for ikke å snakke om

$$(\emptyset, \{\emptyset\}) \in \in$$

i stedet for $\emptyset \in \{\emptyset\}$.

- Den første forenklingen vi skal gjøre er å skrive aRb når vi mener $(a, b) \in R$.

Beskrivelser av relasjoner

- Hvis A er en liten mengde, fins det to måter å beskrive R på,
 - Ved hjelp av en matrise
 - Ved hjelp av en graf
- Vi skal se på noen eksempler.
- For begge måter å beskrive relasjoner på spiller det en stor rolle hvordan man organiserer elementene i mengden A ,

- i rekkefølge som koordinater
- som punkter på en tavle eller et ark
- La $A = \{1, 2, 3, 4, 5\}$ og la $R = \{(1, 3), (2, 4), (3, 5), (4, 1), (5, 2)\}$
- Vi skal illustrere R ved hjelp av en 5×5 -matrise.
 - Radene, regnet ovenfra, vil representere 1. koordinat.
 - Søylene, regnet fra venstre, vil representere 2. koordinat.
 - Vi markerer elementene i R med **T** og de andre med **F**.
 - Det er like vanlig, og ofte bedre, å bruke 1 og 0.

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

- Den grafiske fremstillingen tar vi på tavlen.
- La $A = \{1, 2, 3, 4\}$ og $R = \{(1, 2), (1, 3), (1, 4), (4, 1), (3, 1), (2, 1), (3, 3)\}$
- Matrisereformen blir

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

- Den grafiske fremstillingen tar vi på tavlen.

Flere begreper

- Erfaringsmessig faller det stoffet vi nå begynner på vanskeligere for mange enn det vi har gått gjennom så langt.
- 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 vi har sett på 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 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 et løp etter oppnådd sluttid.
 - Ordne LOTTO-tallene etter størrelse.
 - Ordne studenter etter oppnådde karakterer.

- Det er noe felles ved oppgaven å skulle ordne en mengde, og det er naturlig å isolere de relasjonene som kan oppfattes som ordninger.
 - Det er blant annet noe av det vi skal lære nå.
- Inklusjon mellom mengder er en form for “større enn”, men det fins mengder, eksempelvis $\{1, 2, 3\}$ og $\{2, 3, 4\}$, som ikke er inneholdt i hverandre noen vei.
- Hva vil sorteringsalgoritmer gjøre hvis vi bruker dem på slike ordninger?
- 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:

Egenskaper ved binære relasjoner

Definisjon.

- En relasjon R på en mengde A kalles:
 - Refleksiv hvis xRx for alle $x \in A$.
 - Irrefleksiv hvis det ikke fins 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 når 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

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

Da er R en refleksiv relasjon.

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

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

- 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.

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

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.

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

$$\text{når} \quad \phi S \psi$$

$$\phi \wedge \psi \rightarrow \mathbf{F}$$

er en tautologi.

- Da er S hverken refleksiv eller irrefleksiv.

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

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

- 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} .

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

Eksempel.

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

Denne relasjonen er symmetrisk

Eksempel.

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

Denne relasjonen er *ikke* symmetrisk

Antisymmetriske relasjoner

Eksempel (Antisymmetrisk: $xRy \wedge yRx$ 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.

Et eksempel

- 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.
- 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 $x > 0 \Rightarrow x > 0 \vee x = 0$, men omvendingen gjelder ikke.
 2. Utsagnene $\neg(x < 0) \vee x > 0$ 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 $B \Rightarrow C$.

Enda et eksempel

- 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, \dots, x_n i programmet.
- Underveis vil verdiene på disse variablene endre seg, gjennom instruksjoner som

$$x_i \leftarrow t(x_1, \dots, x_n).$$

- En fordeling av verdier på variablene kaller vi en *valuasjon* eller en *tilstand*.
- 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 .

- Hvis $\llbracket \mathcal{P} \rrbracket$ er *refleksiv*, betyr det at programmet i realiteten lar alle inputvaluasjoner være uforandret.
- Hvis $\llbracket \mathcal{P} \rrbracket$ er *irrefleksiv*, betyr det at programmet gjør endringer uansett input.
- Hvis $\llbracket \mathcal{P} \rrbracket$ 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 $\llbracket \mathcal{P} \rrbracket$ er *antisymmetrisk*, betyr det at vi aldri kommer tilbake til input-dataene ved å kjøre programmet på output-dataene.
- $\llbracket \mathcal{P} \rrbracket$ 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.
- 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 $\vdash_{\mathcal{P}}^*$.
- 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.