MAT1030 – Diskret matematikk

Forelesning 12: Relasjoner, Funksjoner

Dag Normann

Matematisk Institutt, Universitetet i Oslo

20. februar 2008

Oppsummering

- En relasjon på en mengde A er en delmengde $R \subseteq A \times A = A^2$.
- Vi har satt navn på visse egenskaper relasjoner som oppstår i anvendelser ofte kan ha.

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 $x, y, z \in A$.

Oppsummering

- Etter å ha sett på endel eksempler på relasjoner, og deres tilknytning til egenskaper som *refleksiv*, *irrefleksiv*, *symmetrisk*, *antisymmetrisk* og *transitiv*, begynte vi å se på ekvivalensrelasjoner.
- En *ekvivalensrelasjon* er normalt en relasjon som uttrykker at objektene har visse felles egenskaper.
- Den formelle definisjonen var:

Ekvivalensrelasjoner

Definisjon

La R være en relasjon på en mengde A.

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

Merk

- Vi rakk å se på del a) og del b) i følgende eksempel:

Ekvivalensrelasjoner

Eksempel

a) La A være mengden av sammensatte utsagn i utsagnsvariablene p_1, p_2, p_3. Vi lar $\phi R \psi$ hvis $\phi \Leftrightarrow \psi$, det vil si hvis $\phi \leftrightarrow \psi$ er en tautologi.

Da er R en ekvivalensrelasjon.

b) En *vektor* er et par (x, y) av punkter i planet eller rommet.

x kalles *roten* til vektoren og y kalles *spissen* til vektoren.

Det er vanlig å si at to vektorer er like hvis de har samme lengde og retning.

Det uttrykker vi ved

$$(x, y)R(u, v) \Leftrightarrow y - x = v - u.$$

Dette er en ekvivalensrelasjon.

Ekvivalensrelasjoner

Eksempel (Fortsatt)

c) Hvis vi arbeider med en stor programpakke, og ønsker å gjøre den mer effektiv, kan vi vinne en del på å erstatte en subrutine med en raskere en.

Hvis det for eksempel ofte inngår at data må ordnes på en bestemt måte, spiller det ikke så stor rolle for utfallet hvordan vi organiserer en slik ordning, men det kan bety mye for effektiviteten.

To mulige subrutiner er *ekvivalente* hvis de alltid omgjør de samme input-dataene til de samme output-dataene.

Dette er et eksempel på en ekvivalensrelasjon.

Ekvivalensrelasjoner

Merk

- I forbindelse med eksempel c) kan vi bemerke:

  Erstatter vi et underprogram i et program med et ekvivalent underprogram, blir det omskrevne programmet ekvivalent med det opprinnelige.
- Dette er et eksempel på en nyttig egenskap, men hvor vi trenger både ekvivalensrelasjoner og induksjonsbevis for å gi et skikkelig bevis.

Ekvivalensrelasjoner

En viktig egenskap ved en ekvivalensrelasjon R på en mengde A er at R deler A opp i disjunkte mengder av parvis ekvivalente elementer i A.

(Disjunkt betyr at snittet er tomt.)

Disse mengdene kaller vi ekvivalensklasser

Vi skal vise denne egenskaper ved ekvivalensrelasjoner helt generelt, men la oss se på noen eksempler først.

Ekvivalensrelasjoner

Eksempel

- La $A = \{0, 1, 2, 3, 4, 5\}$
- La $R = \{(0,0), (0,1), (1,1), (2,2), (3,3), (3,4),$
  $(3,5), (4,3), (4,4), (4,5), (5,3), (5,4), (5,5)\}$
- I utgangspunktet er det ikke så lett å se hvilke egenskaper R har, men beskriver vi R på matriseform blir bildet klarere:

Ekvivalensrelasjoner

Eksempel (Fortsatt)

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

Vi ser at aRb hvis og bare hvis a og b tilhører den samme av delmengdene $\{0, 1\}$, $\{2\}$ og $\{3, 4, 5\}$.

Ekvivalensrelasjoner

Eksempel

- Vi definerer relasjonen R på $\mathbb{R}^2$ ved $(x, y)R(u, v)$ om $x + y = u + v$.
- R er en ekvivalensrelasjon.
- Hvis $x + y = k$ vil $(x, y)R(u, v)$ om $u + v = k$.
- Denne relasjonen deler planet opp i uendelig mange disjunkte deler, hvor delene er alle linjene med stigningstall -1

Ekvivalensrelasjoner

Definisjon

La R være en ekvivalensrelasjon på en mengde A og la $a \in A$.
Vi lar ekvivalensklassen til a være

$$E(a) = \{b \in A \mid aRb\}.$$

Ekvivalensrelasjoner

Teorem

La R være en ekvivalensrelasjon på mengden A, $E(a)$ ekvivalensklassen til $a \in A$.

a) For alle $a \in A$ vil $a \in E(a)$.
b) Hvis aRb vil $E(a) = E(b)$.
c) Hvis $\neg(aRb)$ vil $E(a) \cap E(b) = \emptyset$

Ekvivalensrelasjoner

Dette teoremet sier nettopp at hvis R er en ekvivalensrelasjon på A, så kan vi dele A opp i disjunkte klasser av parvis ekvivalente elementer.

Bevis

Siden aRa vil $a \in E(a)$. Dette viser a).

La aRb. Skal vise at $E(a) = E(b)$.

Siden vi da også har at bRa er det nok å vise at $E(b) \subseteq E(a)$ for å vise b).

Så la $c \in E(b)$.

Da vil $aRb \wedge bRc$ så aRc fordi R er transitiv.

Det betyr at $c \in E(a)$.

Siden $c \in E(b)$ var valgt vilkårlig, kan vi slutte at $E(b) \subseteq E(a)$.

Ekvivalensrelasjoner

Bevis (Fortsatt)

Til sist, anta at $c \in E(a) \cap E(b)$.

Da vil $aRc \wedge bRc$.

Ved symmetri og transitivitet for R følger det at aRb.

Snur vi dette argumentet på hodet, får vi at $\neg(aRb) \Rightarrow E(a) \cap E(b) = \emptyset$.

Dette viser c), og teoremet er bevist.

Ekvivalensrelasjoner

Oppgave

La A være en mengde og la R og S være ekvivalensrelasjoner på A.

La $T = S \cap R$

a) Forklar hvorfor vi har at aTb hvis og bare hvis $aRb \wedge aSb$ for alle a og b i A.
b) Vis at T er en ekvivalensrelasjon.
c) Finn et eksempel hvor $R \cup S$ ikke er en ekvivalensrelasjon.

Ordninger

- En annen type relasjoner som forekommer ofte er ordninger.
- Vi har en ordning når vi formaliserer "mindre eller lik" , "er svakere enn" og tilsvarende forhold.
- Vi tar definisjonen først, og illustrerer den med noen eksempler etterpå.
- Vi følger boka og definerer:

Ordninger

Definisjon

La A være en mengde med en relasjon R.

Vi kaller R en partiell ordning hvis

1. R er refleksiv
2. R er transitiv
3. R er antisymmetrisk.

Ordninger

Eksempel

a) La $\mathcal{E}$ være en universell mengde, og $\subseteq$ være inklusjonsordningen på potensmengden til $\mathcal{E}$.

1. $\subseteq$ er *refleksiv* fordi $A \subseteq A$ for alle mengder A.
2. $\subseteq$ er *transitiv* fordi $A \subseteq B$ og $B \subseteq C$ alltid vil medføre at $A \subseteq C$
3. $\subseteq$ er *antisymmetrisk* fordi $A = B$ når $A \subseteq B$ og $B \subseteq A$.

Dette viser at $\subseteq$ er en partiell ordning.

Ordninger

Eksempel (Fortsatt)

b) La $\leq$ være den vanlige "mindre-eller-lik" relasjonen på $\mathbb{J}$.

$\leq$ er opplagt både refleksiv, transitiv og antisymmetrisk, så $\leq$ er en partiell ordning.

$<$ er derimot IKKE en partiell ordning, fordi $<$ ikke er *refleksiv*.

c) Hvis vi ordner studentene i MAT1030 etter oppnådd karakter, med A øverst, F langt nede, men "ikke møtt" og "trukket seg før eksamen" enda lenger nede, har vi ikke en partiell ordning.

Siden det er mer enn 8 studenter, må minst to stykker lide samme MAT1030-skjebne.

Disse vil stå likt, men være forskjellige personer.

Det betyr at denne relasjonen ikke er *antisymmetrisk*

Ordninger

- Det er en viktig forskjell mellom ordningen av potensmengden til $\mathcal{E}$ og ordningen av $\mathbb{J}$.
- Hvis vi har to tall a og b vil en av tre holde:
  1. $a = b$
  2. $a < b$
  3. $b < a$
- For inklusjon har vi en fjerde mulighet, nemlig at ingen av A eller B er inneholdt i den andre.
- Vi fanger opp denne forskjellen i en definisjon:

Ordninger

Definisjon

La R være en partiell ordning på en mengde A.

R kalles total dersom vi for alle a og b i A har at

$$aRb \vee bRa.$$

Merk

- Det er for totale ordninger at vi har gode sorteringsalgoritmer.
- Utviklingen av slike algoritmer overlater vi til foreleserne i programmering, de er flinkere til å finne effektive agoritmer.

En utfordring

- Dette er en oppgave for de som har lyst til å se hvor gode de er til å resonere rundt de generelle definisjonene vi har gitt.
- Vi forventer ikke at studentene skal kunne løse slike oppgaver til eksamen.

Oppgave

La R være en relasjon på en mengde A.

Vi kaller R en preordning hvis R er transitiv og refleksiv.

Definer relasjonen S på A ved aSb når $aRb \wedge bRa$.

a) Vis at S er en ekvivalensrelasjon på A.

Der er vanlig å skrive A/S for mengden av ekvivalensklasser $E(a)$ til ekvivalensrelasjonen S.

En utfordring

Oppgave (Fortsatt)

Vi definerer en relasjon $\hat{R}$ på A/S ved

$$E(a)\hat{R}E(b)$$

om aRb

b) Vis at det ikke spiller noen rolle hvilke elementer i ekvivalensklassene $E(a)$ og $E(b)$ vi bruker.

c) Vis at $\hat{R}$ er en partiell ordning på mengden av ekvivalensklasser.

OVER TIL KAPITTEL 6

Funksjoner

- Fra skolematematikken kjenner man funksjoner definert ved uttrykk som
  - $f(x) = x^2 + 3x + 4$
  - $g(x) = \sin x$
  - $h(x) = e^{2\ln(x)+27}$
- Vi har også støtt på tallteoretiske funksjoner som
  - Heltallsverdien til $\frac{n}{m}$
  - Primtall nr. n.
  - Største felles mål av n og m.

Funksjoner

Felles for alle disse eksemplene er at det er en sammenheng mellom

argumentet eller argumentene

til funksjonen, og

verdien

til funksjonen.

Funksjoner

Det er vanlig å fremstille en funksjon som en slags svart boks hvor

- Vi fôrer boksen med funksjonsargumentene.
- Boksen bearbeider dataene.
- Boksen gir oss funksjonsverdien.

Som intuitivt bilde er dette en grei beskrivelse.

Som presis matematisk definisjon holder det ikke helt.

Vi skal holde oss til presisjonsnivået i boka.

Hovedpoenget er at vi skal tolke ordet *regel* på neste side så liberalt som mulig.

Funksjoner

Definisjon

La X og Y være to mengder.

En funksjon $f : X \to Y$ er en regel som for hver $x \in X$ gir oss en, og bare en, $y = f(x)$ i Y.

Merk

- Som sagt skal ordet *regel* tolkes så liberalt som mulig, men, som vi skal se, med en smule forsiktighet.
- Det er ikke noe krav om at det skal foreligge noen regler som mennesker eller maskiner kan følge.
- Det eneste kravet er at $f(x)$ skal finnes i Y, og at uttrykket $f(x)$ ikke kan være flertydig.

Funksjoner

Eksempel (Funksjoner)

- Vi skal se på noe av det vi har snakket om før, og se hvorvidt funksjoner er involvert.
- Vi skal legge vekt på andre eksempler enn de dere kjenner fra skolematematikken.
- La $\mathcal{E}$ være en universell mengde, og la A være en delmengde av $\mathcal{E}$
- Vi definerte $\overline{A} = \{x \in \mathcal{E} \ : \ x \notin A\}$.
- Hver A har en og bare en komplement-mengde, så $f(A) = \overline{A}$ er en funksjon.
- Her er X lik Y lik potensmengden til $\mathcal{E}$.

Funksjoner

Eksempel (Fortsatt)

- På samme måte kan vi oppfatte $\cap$ og $\cup$ som funksjoner.
- Hvis Y er potensmengden til $\mathcal{E}$ og $X = Y^2$, vil $\cap$ og $\cup$ være funksjoner fra X til Y.
- Vi har sett på binærrepresentasjonen til hele tall.
- I hvilken forstand er
  $$REP(a) = \text{binærrepresentasjonen til } a$$
  en funksjon?

Funksjoner

Eksempel (Fortsatt)

- Vi vet at ikke alle tall har en binær representasjon.
- Det betyr at REP ikke oppfyller kravet
  $$\forall x \in X \exists y \in Y(REP(x) = y)$$
  hvis vi lar $X = \mathbb{J}$.
- Lar vi X være mengden av tall med en binær representasjon, blir REP en funksjon.

Funksjoner

Eksempel (Fortsatt)

- Quicksort er en algoritme som sorterer elementene i en liste etter størrelse.
- Quicksort gir mening hver gang listen er hentet fra en totalt ordnet mengde.
- Da beregner Quicksort funksjonen som tar en vilkårlig liste som argument og gir den sorterte listen som verdi.
- Vi kan finne en annen algoritme Slowsort for sortering av elementene i en liste, og den vil definere den samme funksjonen, men være en annen algoritme.
- Det er forbindelsen mellom argument og verdi som bestemmer hvilken funksjon vi har, ikke hvordan vi kommer fra argument til verdi.

Funksjoner

Definisjon

a) Hvis $f : X \to Y$ er en funksjon kaller vi
   - X for definisjonsområdet til f.
   - Y for verdiområdet til f.

b) Bildet eller bildemengden til f er

$$\{f(x) \ : \ x \in X\}$$

c) Vi kan skrive $f[X]$ for bildet til f.

Funksjoner

Eksempel (Funksjoner)

- Definer $f(x) = e^x$ som en funksjon fra $\mathbb{R}$ til $\mathbb{R}$.
  Da vil:
  - *Definisjonsområdet* til f være hele $\mathbb{R}$.
  - *Verdiområdet* til f være hele $\mathbb{R}$.
  - *Bildet* til f være mengden av positive reelle tall.

Funksjoner

Eksempel (Fortsatt)

- La $A \subseteq \mathcal{E}$ være en mengde, og definer

$$f_A(B) = A \cap B$$

  som en funksjon fra potensmengden X til $\mathcal{E}$ til seg selv.
- Da er X både definisjonsområdet og verdiområdet til f_A, mens bildemengden vil være potensmengden til A.

Funksjoner

Eksempel (Fortsatt)

- Innledningsvis i disse forelesningene konstruerte vi en pseudokode for å beregne $|n-m|$ fra n og m.
- I dette tilfellet var definisjonsområdet mengden av par av ikke-negative hele tall, verdiområdet og bildemengden lik mengden av ikke-negative hele tall.
- Da vi satte opp sannhetsverditabeller for sammensatte utsagn i utsagnsvariablene p, q og r, konstruerte vi i virkeligheten funksjoner fra mengden X av trippler fra $\{\mathrm{T}, \mathrm{F}\}$ til $Y = \{\mathrm{T}, \mathrm{F}\}$.

  To sammensatte utsagn er logisk ekvivalente når disse funksjonene er like.

Funksjoner

Merk

- Læreboka bruker *domain* for definisjonsområde og *codomain* for verdiområde.
- Det er ikke uvanlig å bruke ordene *domene* og *kodomene* på norsk.
- Vi skal holde oss til betegnelsene *definisjonsområde* og *verdiområde* i disse forelesningene.

Funksjoner

- Funksjoner har en ting felles med relasjoner:

  Noen av dem har spesielle egenskaper som er verd en egen betegnelse.
- Vi skal først se på injektive funksjoner.
- Andre betegnelser er 1-1-funksjoner og enentydige funksjoner.

Funksjoner

Eksempel (Injektive funksjoner)

- La w være et 32-bits binært tall, og la $f(w)$ være det heltallet som har w som 4-bytes representasjon.
- Hvis $v \neq w$ vil $f(v) \neq f(w)$ siden vi ikke bruker to forskjellige binære representasjoner av det samme tallet.
- Hvis vi oppfatter f som en *input-output*-forbindelse, ser vi at det er én input pr. output.
- Dette er et eksempel på en en-til-en-funksjon, eller *injektiv* funksjon.

Funksjoner

Eksempel (Fortsatt)

- En telefonselger vil ha datastøttet oppringing til kunder.
- For ikke å irritere kundene unødig, bør ikke telefonselgeren kontakte samme kunde to ganger.
- Hvis $R(n)$ er kunde nummer n selgeren kontakter, betyr dette kravet at $R(n) \neq R(m)$ når $n \neq m$.
- Programmet selgeren støtter seg på må være slik at oppringningsfunksjonen R blir injektiv, eller enentydig.

Funksjoner

Den formelle definisjonen vil være:

Definisjon

La $f : X \to Y$ være en funksjon.

f kalles injektiv hvis vi for alle x og y i X har at

$$x \neq y \Rightarrow f(x) \neq f(y).$$

Funksjoner

Merk

- Vi har brukt den kontrapositive versjonen i definisjonen.
  En ekvivalent formulering vil være

$$f(x) = f(y) \Rightarrow x = y.$$

Funksjoner

Eksempel (Injektive funksjoner)

- La $f(x) = x^2$ være en funksjon fra $\mathbb{R}$ til $\mathbb{R}$.
  Da er ikke f injektiv fordi $1 \neq -1$ mens $f(1) = f(-1)$.
- Hvis vi begrenser definisjonsområdet til de ikke-negative tallene $\mathbb{R}_{\geq 0}$ blir funksjonen injektiv.
- Funksjonen som ordner en sekvens av ord alfabetisk er ikke injektiv, fordi ord-sekvensene "Per,Pål,Espen" og "Espen,Pål, Per" er forskjellige, men de blir like når vi ordner dem alfabetisk.