MS-A0409 Grundkurs i diskret matematik Sammanfattning

G. Gripenberg

Aalto-universitetet

10 september 2013

Mängder

Det enklaste sättet att beskriva en mängd är att räkna upp de elementen i mängden, tex. $A = \{2, 4, 5, 8\}$ *och* $B = \{4, 5, \ldots 2004\}$. *Man skriver* $x \in A$ *om* x *är ett element i* A *och* $x \notin A$ *om* x *inte är det, så att tex.* $2 \in A$, $375 \in B$ *men* $6 \notin A$ *och* $3 \notin B$.
Mängderna $\{2, 3, 2\}$ *och* $\{3, 2\}$ *är desamma eftersom de innehåller samma element och upprepningar och ordningen inte har någon betydelse.*
Ofta anges mängder som de element i en mängd A *som har en viss egenskap* P, *dvs.* $B = \{\, x \in A : P(x) \,\}$ *där* $P(x)$ *för varje* $x \in A$ *antingen är sant eller falskt. Tex. är* $\{\, x \in \mathbb{R} : x \leq 4 \,\}$ *alla reella tal som är mindre eller lika med* 4.

- $\emptyset = \{\}$ *är den tomma mängden som inte har några element alls.*
- $A \cup B = \{\, x : x \in A$ *eller* $x \in B \,\}$
- $A \cap B = \{\, x : x \in A$ *och* $x \in B \,\}$
- $A \setminus B = \{\, x : x \in A$ *och* $x \notin B \,\}$
- $A \subset B$ *om* $x \in B$ *för alla* $x \in A$
- $A^c = \Omega \setminus A$ *ifall* $A \subset \Omega$ *och det är klart vad* Ω *är.*

Satslogik

Om a och b är satser eller påståenden som kan vara sanna eller falska, men inte någonting mitt emellan, så gäller

- *satsen a & b är sann då a och b är sanna,*
- *satsen a | b är sann då a eller b är sann (och också då både a och b är sanna).*
- *satsen !a är sann då a inte är sann, dvs. falsk.*
- *satsen $a \to b$ är sann då (!a) | b är sann, dvs. då antingen b är sann eller a är falsk.*

I matematisk logik används vanligen $\wedge$ istället för &, $\vee$ istället för | och $\neg$ istället för ! och $a \leftrightarrow b$ är en förkortning av $(a \to b)$ & $(b \to a)$.

Implikationen $\to$

Observera att implikationen $a \to b$ som logisk sats inte alltid motsvarar vad man i dagligt tal menar med en implikation, dvs. "av a följer b" eftersom $a \to b$ är sann då a är falsk och den inte nödvändigtvis har något med orsakssamband att göra.

Predikatlogik

Predikatlogiken är en utvidgning av satslogiken så att man förutom satser har variabler $x, y, \ldots$ och predikat $P, Q, \ldots$ (eller hur man nu vill beteckna dem). Predikaten har ett ändligt antal argument, tex. $P(x)$, $Q(x, y)$, osv. och ett predikat utan argument är en sats.
Förutom de operationer (!, &, | och $\to$) som finns i satslogiken använder predikatlogiken all- och existenskvantorerna $\forall$ och $\exists$ som uttrycker "för alla" och "det existerar".
Förutom predikat kan man också använda funktioner vars värde hör till det område som behandlas ("domain of discourse"). En funktion med noll argument är då en konstant. Funktioner och konstanter kan också uttryckas med hjälp av predikat, men det blir lätt onödigt klumpigt.

Operatorordning

Om man inte vill använda parenteser, som naturligtvis har högsta prioritet) kan man utnyttja att de logiska operatorerna (vanligtvis) evalueras i följande ordning: Först !, sedan $\forall$ och $\exists$, sedan & och | och till sist $\to$.

Peanos axiom och de naturliga talen

Vi har en konstant o (”det första talet”, ursprungligen 1, nu ofta 0), en funktion $S(x)$ (”successor”, dvs. ”följande tal”) och ett predikat $L(x, y)$ med två argument (som uttrycker att x och y är lika) som här skrivs i formen $x == y$.
De två första axiomen är

- P1 $\forall x(!(S(x) == o))$ *(det första talet följer inte efter något tal)*
- P2 $\forall x(\forall y((S(x) == S(y)) \to (x == y)))$ *(om de följande talen är lika är talen lika)*

Det tredje axiomet är egentligen ett axiomschema eller oändligt många axiom eftersom det skall gälla för alla predikat P:

- P3 $(P(o)\ \&\ (\forall x(P(x) \to P(S(x))))) \to (\forall x P(x))$ *(induktionsprincipen)*

Eftersom P3 egentligen säger vad som gäller för alla predikat, $\forall P$ är det här frågan om andra ordningens predikatkalkyl.
Observera också att P3 säger att de naturliga talen är precis $\{o, S(o)), S(S(o)), \ldots\}$ och inte något mera.

Induktionsprincipen

Om $P(n)$ är ett påstående (som för alla $n \geq n_0$ antingen är sant eller falskt) så att

- *$P(n_0)$ är sant*
- *$P(k+1)$ är sant ifall $P(k)$ är sant (dvs. $P(k) \to P(k+1)$) då $k \geq n_0$*

så är $P(n)$ sant för alla $n \geq n_0$.

Kartesisk produkt

Den kartesiska produkten $X \times Y$ av två mängder X och Y består av alla ordnade par (a, b) eller $[a, b]$ där $a \in X$ och $b \in Y$, dvs.

$$X \times Y = \{\, [a, b] : a \in X \text{ och } b \in Y \,\}.$$

Det finns olika sätt att definiera paret $[a, b]$ endast med hjälp av mängdteoretiska beteckningar och ett ofta använt sätt är att säga att $[a, b]$ är mängden $\{\{a\}, \{a, b\}\}$.

Relationer

En relation i mängderna X och Y (eller i X om $Y = X$) är en delmängd av den kartesiska produkten $X \times Y$.

Olika slag av relationer i en mängd X

En relation W i mängden X är

- *reflexiv ifall $[x, x] \in W$ för alla $x \in X$.*
- *symmetrisk ifall $[x, y] \in W \to [y, x] \in W$ för alla x och $y \in X$.*
- *transitiv ifall $[x, y] \in W \;\&\; [y, z] \in W \to [x, z] \in W$ för alla x, y och $z \in X$.*
- *en ekvivalensrelation om W är reflexiv, symmetrisk och transitiv.*
- *antisymmetrisk om $[x, y] \in W \;\&\; x \neq y \to [y, x] \notin W$ för alla x och $y \in X$.*
- *partiell ordning om den är reflexiv, antisymmetrisk och transitiv.*

Ofta skrivar man xWy istället för $[x, y] \in W$, tex. $x < y$ (istället för idiotiska $[x, y] \in <$).

Funktioner

Om X *och* Y *är mängder så är en funktion* $f : X \to Y$ *en relation i* $X \times Y$ *dvs. en delmängd i* $X \times Y$ *så att*

- *för varje* $x \in X$ *finns det ett* $y \in Y$ *så att* $[x, y] \in f$.
- *om* $[x, y_1] \in f$ *och* $[x, y_2] \in f$ *så är* $y_1 = y_2$.

Vanligtvis skriver man relationen så att $[x, y] \in f$ *om och endast om* $y = f(x)$, *även om* $y = xf$ *eller* $y = x.f$ *kunde vara bättre om man läser från vänster till höger.*
Med andra ord, en funktion f *från* X *till* Y *är en "regel" som för varje* $x \in X$ *ger som svar ett entydigt element* $y = f(x)$ *i* Y.