MS-A0409 Grundkurs i diskret matematik
Sammanfattning, del I

G. Gripenberg

Aalto-universitetet

2 oktober 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.*
- $A \cup B = \{\, x : x \in A \text{ eller } x \in B \,\}$
- $A \cap B = \{\, x : x \in A \text{ och } x \in B \,\}$
- $A \setminus B = \{\, x : x \in A \text{ och } x \notin B \,\}$
- $A \subset B$ *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 $(!a) \mid b$ 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 $\rightarrow$) 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 $\rightarrow$.

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 $\forall x(\forall y((S(x) == S(y)) \rightarrow (x == y)))$ *(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 $(P(o)\ \&\ (\forall x(P(x) \rightarrow P(S(x))))) \rightarrow (\forall x P(x))$ *(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.

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

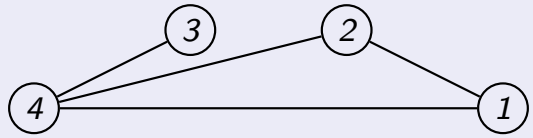
Det finns olika sätt att definiera paret $[a, b]$ endast med hjälp av mängdteoretiska beteckningar och ett ofta använt sätt är att säga att $[a, b]$ är mängden $\{\{a\}, \{a, b\}\}$.

Relationer

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

Vad är en graf?

En graf består av en mängd noder och en mängd bågar mellan noderna, tex. såhär:



I en riktad graf har varje båge en startpunkt och en slutpunkt, medan man i en icke riktad graf inte gör skillnad mellan start och slutpunkten.

- *En riktad graf kan enkelt beskrivas som ett ordnat par* $[V, E]$ *(*V *som "vertex",* E *som "edge") där* V *är en mängd (vanligtvis ändlig och inte tom) och* $E \subset V \times V$*, dvs.* E *är en relation i* V*.*
- *En icke riktad graf kan beskrivas som ett ordnat par* $[V, E]$ *där* V *är en mängd (igen vanligtvis ändlig och inte tom) och* $E \subset \{\, \{a, b\} : a \in V, b \in V \,\}$*.*

En icke riktad graf kan förstås (?) också beskrivas som en riktad graf där relationen E *är symmetrisk, dvs.* $[a, b] \in E \rightarrow [b, a] \in E$*. Observera att med ingendera av dessa definitioner kan man ha flera bågar mellan samma noder men nog en båge från en nod till samma nod.*

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

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

Funktioner

Om X och Y är mängder så är en funktion $f : X \to Y$ en relation mellan X och 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.
Mängden $\{ f : f$ är en funktion från X till $Y \}$ betecknas ofta med Y^X.

Injektioner, surjektioner och bijektioner

En funktion $f : X \to Y$ är en

- *injektion om $f(x_1) = f(x_2) \to x_1 = x_2$ för alla $x_1, x_2 \in X$.*
- *surjektion om det för varje $y \in Y$ finns ett $x \in X$ så att $f(x) = y$.*
- *bijektion om den är en injektion och en surjektion.*

Sammansatta och inversa funktioner

- *Om* $f : X \to Y$ *och* $g : Y \to Z$ *är två funktioner så är* $h = g \circ f : X \to Z$ *funktionen* $h(x) = g(f(x))$.
- *Om* $f : X \to Y$, $g : Y \to Z$ *och* $h : Z \to W$ *är funktioner så är* $(h \circ g) \circ f = h \circ (g \circ f)$ *så att denna funktion kan skrivas som* $h \circ g \circ f$.
- *Om* $f : X \to Y$ *är en funktion så att det finns en funktion* $g : Y \to X$ *så att* $(g \circ f)(x) = x$ *och* $(f \circ g)(y) = y$ *för alla* $x \in X$ *och* $y \in Y$ *så är* f *inverterbar,* g *är dess invers och man skriver ofta* $g = f^{-1}$.
- *En funktion* $f : X \to Y$ *är inverterbar om och endast om den är en bijektion.*
- *Om* $f : X \to Y$ *är inverterbar så är* $(f^{-1})^{-1} = f$.

Observera att f^{-1} *inte är samma sak som funktionen* $h(x) = f(x)^{-1}$ *som förutsätter att man i* Y *kan räkna inverser, vilket är fallet i* $\mathbb{R} \setminus \{0\}$ *men inte i* $\mathbb{Z}$.

Ordo eller Stora O: $f \in O(g)$

Om g är en funktion som är definierad för alla "tillräckligt stora" heltal så betyder $f \in O(g)$ att f också är definierad för alla "tillräckligt stora" heltal och att det finns en konstant C och ett heltal n_0 så att

$$|f(n)| \leq C|g(n)|, \quad n \geq n_0,$$

Användningen av denna beteckning betyder också att man inte är speciellt intresserad av, eller inte exakt vet, vad C och n_0 är.
Ofta skriver man $f(n) = O(g(n))$ istället för $f \in O(g)$, men om man då istället för $O(n) + O(n^2) \in O(n^2)$ skriver $O(n) + O(n^2) = O(n^2)$ så måste man inse att man inte kan förkorta bort $O(n^2)$!
Det är inget speciellt med att funktionerna här antas vara definierade bara för (endel) heltal och att man ser vad som händer då $n \to \infty$. Tex. gäller också $\frac{x^4 - x^3}{x^3 + x^2} \in O(x)$ då $x \to 0$.

Antalet element i en mängd

- *Två mängder A och B har samma antal element (eller kardinaliteter) $|A|$ och $|B|$ om det finns en bijektion $A \to B$.*
- *Mängden A har färre än eller lika många element som mängden B, dvs., $|A| \leq |B|$, om det finns en injektion $A \to B$.*
- *Mängden A har färre element än mängden B, dvs., $|A| < |B|$, om det finns en injektion $A \to B$ men ingen bijektion $A \to B$.*
- *Ifall $A = \{0, 1, 2, \ldots, n-1\}$ så är $|A| = n$.*
- *En mängd A sägs vara ändlig om det finns en bijektion $A \to \{0, 1, 2, \ldots, n-1\}$ för något heltal $n \geq 0$, dvs., om $|A| = n$.*

Obs!

För att dessa definitioner skall vara förnuftiga måste man visa att det finns en bijektion $\{0, 1, 2, \ldots, n-1\} \to \{0, 1, 2, \ldots, m-1\}$ om och endast om $m = n$ och att ifall det finns injektioner $A \to B$ och $B \to A$ så finns det en bijektion $A \to B$.

Summeringsregeln, enkel form

Om A och B är två (ändliga) mängder så att $A \cap B = \emptyset$ så är

$$|A \cup B| = |A| + |B|.$$

Av detta följer att om $B \subset A$ så är $|A \setminus B| = |A| - |B|$.

Produktregeln, enkel form

Om A och B är två (ändliga) mängder så är

$$|A \times B| = |A| \cdot |B|.$$

Lådprincipen: Enkel men nyttig!

Ifall $m \geq 1$ föremål placeras i $n \geq 1$ lådor så måste en låda innehålla minst $\left\lceil \frac{m}{n} \right\rceil$ föremål!
Varför? Om det största antalet föremål som finns i någon av lådorna är k så är $k \cdot n \geq m$ så att $k \geq \frac{m}{n}$ och eftersom $\lceil \frac{m}{n} \rceil$ definieras som det minsta heltal som är $\geq \frac{m}{n}$ så måste vi ha $k \geq \lceil \frac{m}{n} \rceil$.

Summerings eller inklusions-exklusionsprincipen

Om A och B är två (ändliga) mängder så är

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

och mera allmänt (förutsatt att alla mängder A_j nedan är ändliga)

$$\left|\bigcup_{j=1}^{k} A_j\right| = \sum_{r=1}^{k} (-1)^{r+1} \sum_{1 \le j_1 < j_2 < \ldots < j_r \le k} \left|\bigcap_{i=1}^{r} A_{j_i}\right|.$$

En allmän form av produktregeln

Ifall

$$C = \{\, (x_1, x_2, \ldots, x_k) : x_1 \in A_1,\ x_2 \in A_{2,x_1},\ \ldots, x_k \in A_{k,x_1,\ldots,x_{k-1}} \,\},$$

där $|A_1| = n_1$, for varje $x_1 \in A_1$ gäller $|A_{2,x_1}| = n_2$ och så vidare så att för alla $x_1 \in A_1$, $x_2 \in A_{2,x_1}, \ldots, x_{k-1} \in A_{k-1,x_1,\ldots,x_{k-2}}$ gäller $|A_{j,x_1,x_2,\ldots,x_{j-1}}| = n_j$, $1 \le j \le k$, så är

$$|C| = n_1 \cdot n_2 \cdot \ldots \cdot n_k.$$

Välj r föremål ur en mängd med n föremål eller element

Det finns (åtminstone) två sätt skilja på olika situationer:

- *Ordnat val: Det har betydelse vid vilket val föremålet väljs — Inte ordnat val: Det har inte någon betydelse vid vilket val föremålet väljs.*
- *Ingen upprepning: ett föremål kan väljas bara en gång — Upprepning möjlig: samma föremål kan väljas många gånger.*

Antalet olika sätt på vilket detta kan göras blir därför:

	Ingen upprepning	*Upprepning möjlig*
Ordnat	$n(n-1)\cdot\ldots\cdot(n-r+1)$	n^r
Inte ordnat	$\binom{n}{r}$	$\binom{n+r-1}{r}$

Här är $\binom{m}{j} = \dfrac{m!}{j!\cdot(m-j)!}$.

Upprepning kan både tolkas så att man väljer ett föremål, noterar vilket det är, och sätter tillbaka det, och så att elementen i mängden är de olika slag av föremål som man kan välja.

Plocka bollar ur en låda eller sätta bollar in en låda?

Ett annat sätt att se på situationen där man väljer r föremål ur en mängd med n föremål (med ett ordnat eller inte ordnat val, med upprepningar eller utan) är att tänka på föremålen i mängden, inte som bollar i en låda, utan som lådor i vilka man väljer att placera ett föremål, tex. en boll, som i det ordnade fallet kan vara numrerade eller på annat sätt identifierbara och i det inte ordnade fallet identiska.
Ett val utan upprepningar innebär då att i varje låda kan sättas högst en boll och ett val med upprepningar att flera bollar kan sättas i samma låda. I ett ordnat val är det alltså inte ordningen som är det viktiga, det avgörande att valen är olika på något annat sätt än bland vilka föremål det görs, dvs. bollarna som sätts i lådor är inte identiska. Om man sedan på någon sätt ordnar de valda föremålen eller lådorna i det inte ordnade fallet har ingen betydelse.

Antalet funktioner $A \to B$

Antag $|A| = m$ *och* $|B| = n$.

- *Antalet funktioner:* $A \to B$ *is är* n^m *(och därför är det förnuftigt att beteckna mängden av funktioner* $A \to B$ *med* B^A*).*
  Observera att en funktion är ett ordnat val med upprepningar av m *element ur en mängd med* n *element.*
- *Antalet injektioner* $A \to B$ *är* $n \cdot (n-1) \cdot \ldots \cdot (n-m+1) = \dfrac{n!}{(n-m)!}$
  $m \leq n$.
  Varför? Ordna elementen i A *och gör sedan ett ordnat val utan upprepningar av* m *element ur mängden* B *(som har* n *element) så att de blir värdena av funktionen.*
- *Antalet surjektioner* $A \to B$ *är* $\displaystyle\sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r} r^m$.
  Varför? Antalet surjektioner är antalet funktioner minus antalet funktioner till en strikt delmängd av B *och detta senare antal kan man räkna med hjälp av inklusions-exklusionsprincipen* *vilket efter diverse räkningar ger formeln ovan.*

Multinomialtal

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!} \qquad n = n_1 + n_2 + \ldots + n_k.$$

- *Om man har valt n föremål med upprepningar från en mängd med k element så att man har tagit n_1 av typ y_1, n_2 av typ y_2 och så vidare, då är $\binom{n}{n_1, n_2, \ldots, n_k}$ antalet sätt på vilka dessa föremål kan ordnas så att föremål av samma typ inte kan skiljas åt.*
- *Om A är en mängd med n element och $B = \{y_1, \ldots, y_k\}$ är en mängd med k element och $n_1, n_2, \ldots, n_k$ är icke-negativa tal så att $n_1 + n_2 + \ldots n_k = n$ så då är $\binom{n}{n_1, n_2, \ldots, n_k}$ antalet funktioner $f : A \to B$ så att $|\{ x \in A : f(x) = y_j \}| = n_j$.*
- *Om $n \geq 0$ och $k \geq 1$ så är*

$$(x_1 + \ldots + x_k)^n = \sum_{\substack{n_1 + \ldots + n_k = n \\ n_j \geq 0}} \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1} \cdot \ldots \cdot x_k^{n_k}.$$