MS-A0409 Grundkurs i diskret matematik I

G. Gripenberg

Aalto-universitetet

2 oktober 2014

Mängder (naiv, inte axiomatisk, mängdlära)

- $x \in A$ *om* x *är ett element i* **mängden** A*, dvs.* x *hör till* A *och* $x \notin A$ *om* x *inte gör det.*
- $\{2, 3, 5, 6\}$ *är mängden som innehåller talen* 2, 3, 5 *och* 5*, dvs.* $2 \in \{2, 3, 5, 6\}$, $3 \in \{2, 3, 5, 6\}$ *osv. men* $4 \notin \{2, 3, 5, 6\}$.
- *Mängderna* $\{2, 3, 5, 6\}$ *och* $\{6, 5, 3, 2, 2, 2\}$ *är desamma eftersom ordningen och upprepningar inte har någon betydelse för frågan om ett element hör till mängden eller inte och det är det enda som räknas.*
- *Istället för att räkna upp elementen i en mängd kan man definiera en mängd 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.* $\{ x \in \mathbb{R} : x \leq 4 \}$.

Russells paradox

Vad kan vi säga om $\{x : x \notin x\}$*?*

- *Ge ett namn åt detta:* $A = \{x : x \notin x\}$.
- *Antag att* $A \in A$*: Då uppfyller* A *villkoret* $x \notin x$ *dvs.* $A \notin A$*, och vi får en motsägelse.*
- *Antag att* $A \notin A$*: Då uppfyller* A *villkoret* $x \notin x$ *så enligt definitionen av* A *gäller* $A \in A$*, igen en motsägelse.*
- *Slutsats?*
- *Det går inte att definiera mängder hur som helst utan att få större problem än man hade!*

Mängder, forts.

- $\emptyset = \{\}$ *är den tomma mängden som inte har några element alls.*
- $A \subset B$ *om* $x \in B$ *för alla* $x \in A$ *och då är* A *är en* **delmängd** *av* B*.*
- $\mathcal{P}(A)$ *(potensmängden till* A*) är mängden av alla delmängder av* A*.*
- $A \cup B = \{\, x : x \in A \text{ eller } x \in B \,\}$ *är* **unionen** *av* A *och* B*.*
- $A \cap B = \{\, x : x \in A \text{ och } x \in B \,\}$ *är* **snittet** *av* A *och* B*.*
- $A \setminus B = \{\, x : x \in A \text{ och } x \notin B \,\}$ *är* **differensen** *mellan* A *och* B*.*
- $A^c = \Omega \setminus A$ *är* **komplementet** *till* 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.*
- *satsen* $a \leftrightarrow b$ *är sann då* $(a \to b)$ && $(b \to a)$ *är sann.*

I matematisk logik används vanligen $\wedge$ *istället för &&,* $\vee$ *istället för || och* $\neg$ *istället för !.*

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.*

Slutledningsregler och bevis

Antag att p och q är två satser. Vi skall nu bevisa att q är sant om vi antar att p && !p är sant, vilket alltså visar att om man antar en motsägelse kan man bevisa vad som helst.
Det finns många slutledningsregler men här skall vi bara använda följande:

(a) $\dfrac{x \mid\mid y \quad !x}{\therefore y}$

(b) $\dfrac{x \,\&\&\, y}{\therefore x}$

(c) $\dfrac{x}{\therefore x \mid\mid y}$

Det som gör att tex. (a) är en slutledningsregel är att satsen

$$(x \mid\mid y) \,\&\&\, !y \rightarrow x$$

är en tautologi, dvs. sann för alla sanningsvärden för x och y (vilket kan kontrolleras åtminstone så att man går genom alla möjligheter).

Slutledningsregler och bevis, forts.

Slutledningsregelerna var alltså följande:

(a) $\dfrac{x \;||\; y \qquad !x}{\therefore y}$

(b) $\dfrac{x \;\&\&\; y}{\therefore x}$

(c) $\dfrac{x}{\therefore x \;||\; y}$

Beviset ser nu ut på följande sätt:

(1) $p \;\&\&\; !p$: *Antagande*

(2) p: *(b) tillämpat på (1) med* $x = p$ *och* $y = !p$

(3) $p \;||\; q$: *(c) tillämpat på (2) med* $x = p$ *och* $y = q$

(4) $!p$: *(b) tillämpat på (1) med* $x = !p$ *och* $y = p$

(5) q: *(a) tillämpat på (3) och (4) med* $x = p$ *och* $y = q$.

Observera att vi i punkt (4) också använde det faktum att $x \;\&\&\; y = y \;\&\&\; x$.)

Ett exempel

Antag att du befinner dig i en främmande stad och undrar om du kommer med buss 409 till ditt hotell. Du tänker fråga en invånare i staden men kommer ihåg att du hört att det finns två sorts människor i denhär staden, dels de som svarar sanningsenligt ja eller nej på varje fråga och dels de som svarar lögnaktigt ja eller nej.

Vad skall du fråga? Vi kan tex. resonera på följande sätt: Låt B vara påståendet att buss 409 för dig till ditt hotell och låt S vara påståendet att den person du frågar alltid talar sanning. Vi skall formulera ett påstående som vi frågar om är sant så att vi får svaret "ja" eller "påståendet är sant" i precis de fall då B är sant. Detta innebär att vi får följande tabell för sanningsvärdena:

B	T	T	F	F
S	T	F	T	F
P	T	F	F	T

Vi ser att P skall vara sant då B och S båda är sanna eller båda falska så påståendet eller frågan blir $(B \;\&\&\; S) \;||\; (!B \;\&\&\; !S)$.

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 $\rightarrow$.

Obs!

Oftast skriver man $\forall x \in A\,(P(x))$ *istället för det fullständiga* $\forall x((x \in A) \to P(x))$ *och* $\exists x \in A\,(P(x))$ *istället för* $\exists x((x \in A)\ \&\&\ P(x))$. *Kom också ihåg att*

$$!(\forall x\, P(x)) \leftrightarrow \exists x\, !P(x),$$

och (eftersom $!(!P) \leftrightarrow P$*)*

$$!(\exists x\, P(x)) \leftrightarrow \forall x\, !P(x).$$

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 $n \geq n_0$.

Induktion

Visa med hjälp av induktion att

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Lösning: Påståendet $P(n)$ *är alltså* $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ *och* $n_0 = 1$. *Då är påståendet* $P(1)$ *samma som att* $1 = \frac{1(1+1)}{2}$ *vilket är sant. Antag nu att* $P(k)$ *är sant och* $k \geq 1$. *Eftersom* $P(k)$ *är sant gäller* $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ *vilket innebär att*

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2},$$

vilket i sin tur innebär att $P(k+1)$ *är sant. Enligt induktionsprincipen följer nu påståendet. (Ofta, men kanske inte här, lönar det sig att formulera det man skall visa som att ett uttryck skall vara* 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 $[a, b]$ (eller (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 $X \times Y$.

Koordinaterna i ett ordnat par

Den första koordinaten i $[x, y]$ *(eller* (x, y)*) är (förstås)* x *och den andra* y*. Om man skriver paret med mängdbeteckningar som* $\{\{x\}, \{x, y\}\}$ *så hur skall man definiera predikaten* $F(p, x)$ *och* $A(p, y)$ *så att* $F(p, x)$ *är sann då* x *är första koordinaten i* p *och* $A(p, y)$ *är sann då* y *är andra koordinaten i* p*?*
Tex. på följande sätt:

$$F(p, x) \stackrel{\text{def}}{=} \forall z\,((z \in p) \to (x \in z))$$

(eller kortare $\forall z \in p(x \in z)$*) men den andra är besvärligare,*

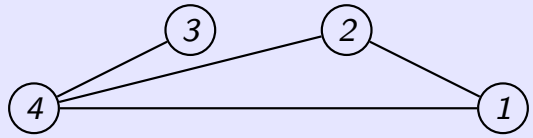
$$A(p, y) \stackrel{\text{def}}{=} \exists z((z \in p)\ \&\&\ (y \in z))\ \&\&$$
$$\forall u\,\forall v\,((u \in p)\ \&\&\ (v \in p)\ \&\&\ !(u == v) \to !(y \in u)\ ||\ !(y \in v)).$$

Man kan också skriva detta som

$$A(p, y) \stackrel{\text{def}}{=} \exists z \in p\,(y \in z)$$
$$\&\&\ \forall u \in p\,\forall v \in p\,(!(u == v) \to (y \notin u)\ ||\ (y \notin v)).$$

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 startnod och en slutnod, medan man i en icke riktad graf inte gör skillnad mellan start- och slutnoden.

- *En riktad graf kan beskrivas med 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 med 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* $[x, y] \in W \;||\; [y, x] \in W$ *för alla* x *och* $y \in X$.

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

Ekvivalensklasser

Om X är en mängd (som inte är tom) och $\sim$ är en ekvivalensrelation i X, dvs. $\sim$ är reflexiv, symmetrisk och transitiv så delar den in mängden X i delmängder $Y_j \neq \emptyset$, $j \in J$ som kallas ekvivalensklasser så att

- $\cup_{j \in J} Y_j = X$,
- $Y_j \cap Y_k = \emptyset$ *om* $j \neq k$,
- $a \sim b \leftrightarrow a$ *och* b *hör till samma mängd* Y_j.

Ofta tolkar man ekvivalensrelationen $\sim$ så att två element som är ekvivalenta är "lika" så att man istället för mängden X tänker på mängden $\{ Y_j : j \in J \}$ med ekvivalensklasserna som element.

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 $y_1 = y_2$.*

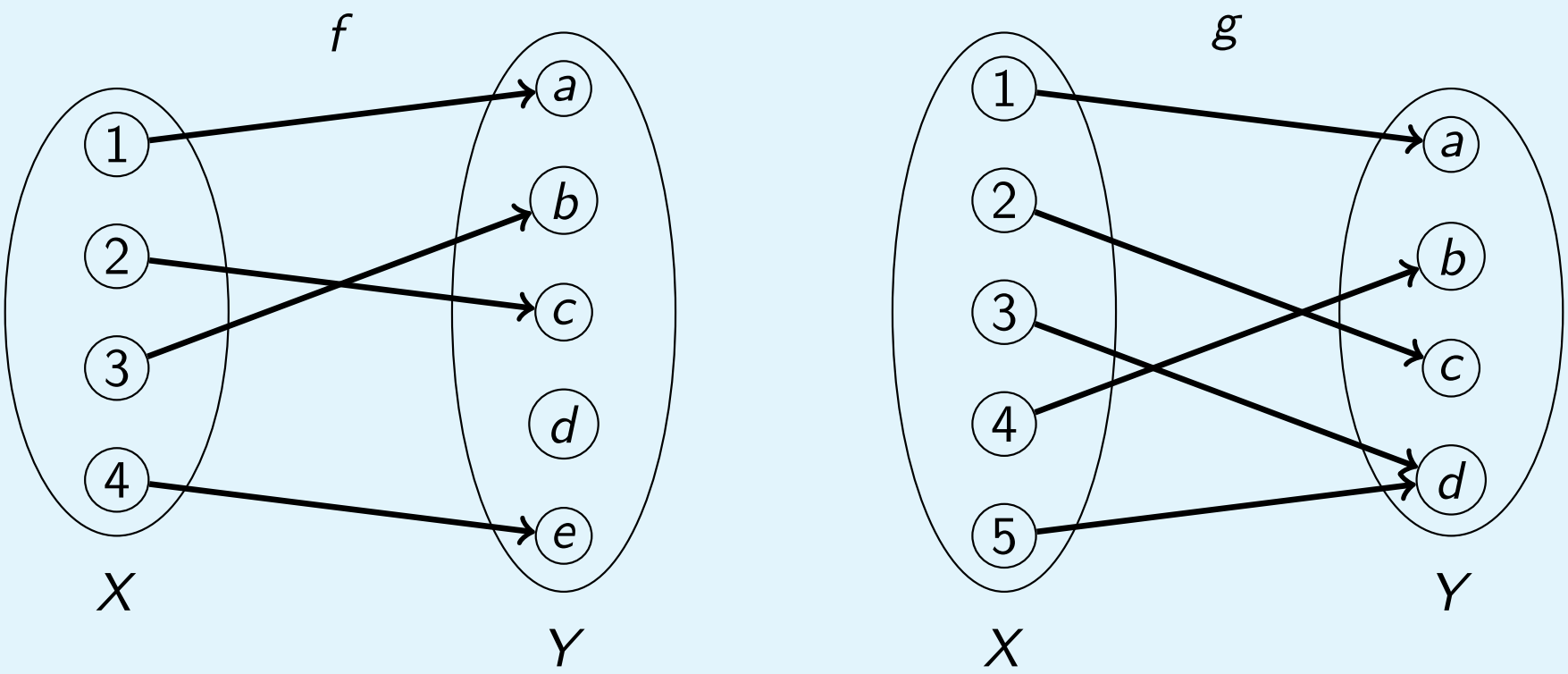
Här är X funktionens defintionsmängd och Y är dess målmängd.
Vanligtvis skriver man relationen så att $[x, y] \in f$ om och endast om $y = f(x)$, *även om $y = xf$ eller $y = x.f$ kunde vara bättre om man läser från vänster till höger.*
Med andra ord, en funktion f från X till Y är en "regel" som för **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.*

Injektioner och surjektioner



Funktionen $f : X \to Y$ är en injektion ("till varje element i Y kommer **högst** *en pil") men inte en surjektion eftersom det inte finns något element i X så att $f(x) = d$.*
Funktionen $g : X \to Y$ är en surjektion ("till varje element i Y kommer **minst** *en pil") men inte en injektion, eftersom $g(3) = g(5)$.*

Listor, talföljder och kartesiska produkter som funktioner

- *En lista* $[a, b, c, d]$ *kan tolkas som en funktion* f *definierad i mängden* $\{1, 2, 3, 4\}$ *(eller* $\{0, 1, 2, 3\}$*) så att* $f(1) = a$, $f(2) = b$, $f(3) = c$ *och* $f(4) = d$.
- *En oändlig talföljd* $(a_n)_{n=0}^{\infty} = (a_0, a_1, a_2, \ldots)$ *kan tolkas som en funktion* f *definierad i* $\mathbb{N}_0$ *så att* $f(n) = a_n$ *för alla* $n \in \mathbb{N}_0$.
- *Om* X_j *är en mängd för varje* $j \in J$ *där* J *är en (annan) mängd så kan man definiera den kartesiska produkten* $\prod_{j \in J} X_j$ *som mängden av alla funktioner* $f : J \to \bigcup_{j \in J} X_j$ *så att* $f(j) \in X_j$.

$f(A)$ och $f^{\leftarrow}(B)$

Om $f : X \to Y$ är en funktion, $A \subset X$ och $B \subset Y$ så är

$$f(A) = \{ f(x) : x \in A \} \quad \text{och} \quad f^{\leftarrow}(B) = \{ x \in X : f(x) \in B \}.$$

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 $x \to 0$.

Hur många jämförelser behövs för att sortera n tal i storleksordning?

Vi skall visa att det räcker med högst $n \log_2(n)$ jämförelser och använda en variant av induktionsprincipen.

- *Då $n = 1$ (eller $n = 2$) är det klart att detta är sant.*
- *Antag nu att det stämmer för alla $n \leq k$ och att vi har $k + 1$ tal som vi skall ordna.*
- *Antag först att $k + 1 = 2m$ och dela upp talen i två mängder med m tal som vi ordnar (genom att använda sammanlagt högst $2m \log_2(m)$ jämförelser och sedan kombinerar vi dehär ordnade listorna till en lista.*
- *Om vi skall kombinera två ordnade listor med j_1 och j_2 element kan detta göras med högst $j_1 + j_2 - 1$ jämförelser eftersom det stämmer då j_1 ellr $j_2 = 1$ och annars behövs det en jämförelse för att hitta det största talet och sedan återstår det att kombinera två listor med antingen $j_1 - 1$ och j_2 eller j_1 och $j_2 - 1$ tal.*

Hur många jämförelser behövs för att sortera n tal i storleksordning? Forts.

- *Det sammanlagda antalet jämförelser då $k+1=2m$ blir alltså högst*

$$\begin{aligned} 2m\log_2(m)+m+m-1 &= 2m\big(\log_2(2m)-1\big)+2m-1 \\ &\leq 2m\log_2(2m) = (k+1)\log_2(k+1). \end{aligned}$$

- *Om $k+1=2m+1$ så delar vi upp mängden i två mängder med m och $m+1$ element och får på samma sätt att antalet jämförelser blir högst*

$$\begin{aligned} & m\log_2(m)+(m+1)\log_2(m+1)+m+1+m-1 \\ &= m\log_2(m(m+1))+\log_2(m+1)+2m \\ &\leq m(\log_2(2m+1)^2)-\log_2(4))+\log_2(m+1)+2m \\ &\leq m(2\log_2(2m+1)-2)+\log_2(2m+1)+2m \\ &\leq 2m\log_2(2m+1))+\log_2(2m+1) = (k+1)\log_2(k+1). \end{aligned}$$

- *Induktionssteget fungerar och högst $n\log_2(n)$ jämförelser behövs!*

Hur många jämförelser behövs för att hitta talet med storleksordningsnummer p i en mängd med n tal?

Det är klart att om $p = 1$ (det minsta talet) eller $p = n$ (det största talet) så räcker det med (men behövs också) $n - 1$ jämförelser men hur är det i det allmänna fallet?

Vi skall nu visa att då $1 \leq p \leq n$ så hör maximimantalet jämförelser till $O(n)$, dvs. det finns en konstant C så att antalet jämförelser är högst Cn och vi bryr oss här inte så mycket om hur stor konstanten C blir:

- *Dela in talen i grupper om tex. 5: Inga jämförelser.*
- *Bestäm medianerna i dessa gupper: Behövs $O(n)$ jämförelser.*
- *Bestäm medianen av medianerna: Behövs $C(\frac{1}{5}n + 1)$ jämförelser om vi kan använda ett induktionsantagande.*
- *Dela in talen i två grupper, de som är större än medianernas median och de som är mindre: Behövs $O(n)$ jämförelser.*
- *Den större av dessa grupper kommer att innehålla högst $(1 - \frac{1}{5} \cdot \frac{1}{2} \cdot 3)n + O(1) = \frac{7}{10}n + O(1)$ tal!*

Hur många jämförelser behövs för att hitta talet med storleksordningsnummer p i en mängd med n tal? Forts.

- *Det tal vi söker finns i någondera gruppen* *eller är medianernas median* *så vi kan hitta det med* $C\frac{7}{10}n + CO(1)$ *jämförelser.*
- *Vi har använt*

$$O(n) + \frac{1}{5}Cn + C + O(n) + \frac{7}{10}Cn + CO(1) = \frac{9}{10}Cn + CO(1) + O(n)$$
$$= \frac{9}{10}Cn + Ck_1 + k_2 n$$

jämförelser där k_1 *och* k_2 *är några konstanter*

- *Eftersom vi för* $n \leq 20k_1$ *kan först sätta alla talen i storleksordning och sedan välja det med storleksordningsnummer* p *så ser vi att om vi väljer*

$$C > \max\{20k_1 \log_2(20k_1), 20k_2\}$$

så är

$$\frac{9}{10}Cn + Ck_1 + k_2 n \leq \frac{9}{10}Cn + \frac{1}{20}Cn + \frac{1}{20}Cn = Cn$$

och induktionsresonemanget fungerar.

Antalet element i en mängd

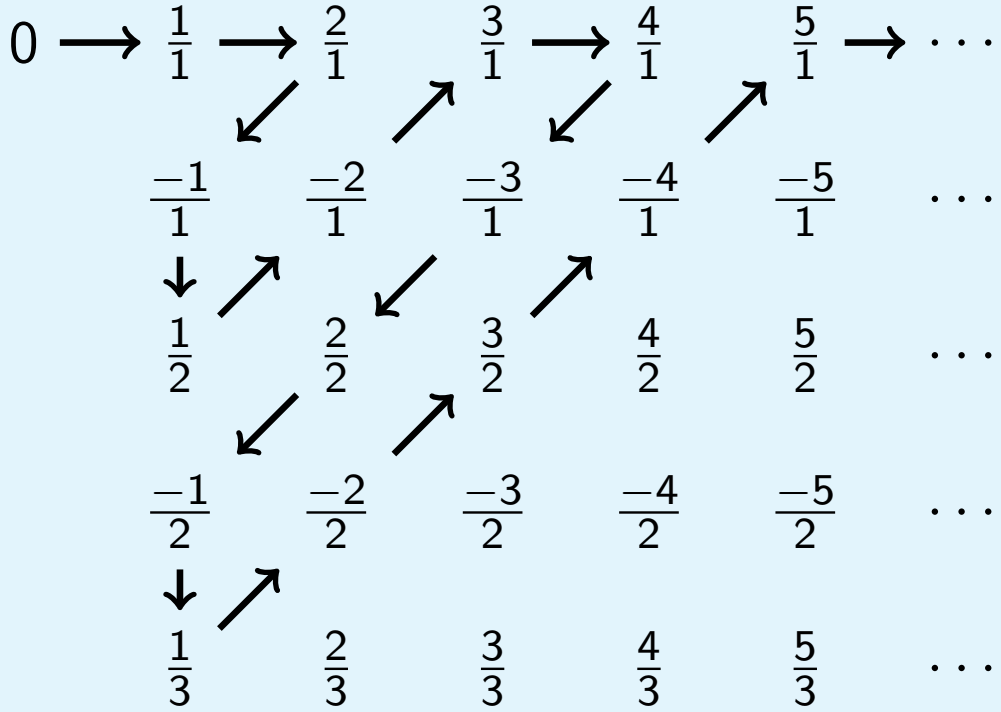
- *Två mängder A och B har samma antal element (eller kardinaliteter), dvs. $|A| = |B|$ om det finns en bijektion $A \to B$.*
- *Mängden A har färre än eller lika många element som mängden B, dvs., $|A| \leq |B|$, om det finns en injektion $A \to B$.*
- *Mängden A har färre element än mängden B, dvs., $|A| < |B|$, 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 $A \to B$.

Antalet element i några oändliga mängder

- $|\mathbb{N}_0| = |\mathbb{Z}|$ *eftersom* $f : \mathbb{N}_0 \to \mathbb{Z}$ *där* $f(0) = 0$, $f(2k-1) = k$ *och* $f(2k) = -k$ *för* $k \geq 1$ *är en bijektion.*
- $|\mathbb{N}_0| = |\mathbb{Q}|$ *eftersom vi kan konstruera en bijektion på följande sätt:*



Om vi sedan hoppar över de tal vi redan gått genom får vi följande bijektion: $f(0) = 0$, $f(1) = 1$, $f(2) = 2$, $f(3) = -1$, $f(4) = \frac{1}{2}$, $f(5) = -2$, $f(6) = 3$, $f(7) = 4$, $f(8) = -3$, $f(9) = -\frac{1}{2}$ *(och inte* $\frac{2}{2} = 1$*)*, $f(10) = \frac{1}{3}$, $f(11) = \frac{3}{2}$ *(och inte* $\frac{-2}{2} = -1$*)*, $f(12) = -4$, *osv.*

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 $\binom{m}{j} = \frac{m!}{j!\cdot(m-j)!}$. *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.
I det ordnade fallet kan dessa bollar vara numrerade eller på annat sätt identifierbara och i det inte ordnade fallet är de identiska och kan inte skiljas åt.
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.

Ordnat val av r föremål från en mängd med n föremål

- *Om varje föremål kan väljas bara en gång kan det första väljas på n olika sätt, det andra på $n-1$ olika sätt och så vidare så att föremål nummer r kan väljas på $n-r+1$ olika sätt. Genom att använda produktregeln ser vi att antalet olika möjligheter är*
  $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-r+1)$ *eller* $\dfrac{n!}{(n-r)!}$.
- *Om varje föremål kan väljas flera gånger (dvs. de tas inte bort ur mängden eller så är mängdens element typer av föremål som tas från något annat ställe) då finns det n alternativ vid varje val så att det följer av produktregeln att antalet möjligheter är n^r.*

Icke-ordnat val av r föremål från en mängd med n föremål utan upprepningar

Låt $b(n, r)$ vara detta antal av icke-ordnade val av r föremål från en mängd med n föremål utan upprepningar. När vi har gjort ett sådant val får vi ett ordnat val genom att ordna de valda r föremålen. Detta kan göras på $r!$ olika sätt så det följer av produktprincipen att antalet sätt göra att ett ordnat val av r föremål från en mängd med n föremål utan upprepningar är $b(n, r) \cdot r!$. Eftersom vi vet att detta antal är $n \cdot (n-1) \cdot \ldots \cdot (n-r+1) = \frac{n!}{(n-r)!}$ så får vi

$$b(n, r) = \frac{n!}{r! \cdot (n-r)!} = \binom{n}{r}.$$

Icke-ordnat val av r föremål från en mängd med n föremål **med** upprepningar, I

Tänk på situationen så att vi har ett obegränsat antal av n olika slags föremål och vi skall välja r stycken. Om vi har gjort ett val kan situationen beskrivas tex. såhär:

$$**|*||***|**|***$$

vilket skall tolkas som att vi valt 2 *stycken av typ* 1, 1 *av typ* 2, 0 *av typ* 3, 3 *av typ* 4, 2 *av typ* 5 *och* 3 *av typ* 6 *så att i detta fall är* $n = 6$ *och* $r = 2 + 1 + 0 + 3 + 2 + 3 = 11$.
Varje val motsvaras alltså att vi placerar r stycken föremål $*$ *och* $n - 1$ *stycken skiljetecken* $|$ *i en rad vilket alltså betyder att väljer de r positioner där vi placerar föremålen* $*$ *(så att resten får skiljetecken* $|$*), eller tvärtom. Eftersom detta är ett oordnat val utan upprepningar blir antalet alternativ*

$$\binom{n-1+r}{n-1} = \binom{n+r-1}{r}.$$

Icke-ordnat val av r föremål från en mängd med n föremål **med** upprepningar, II

Låt $f(r,n)$ vara antalet sätt på vilka man kan göra ett icke-ordnat val av r föremål från en mängd med n föremål **med** *upprepningar. Ett sådant val är detsamma som att placera r föremål i n ordnade (dvs. inte identiska) lådor. Om $n = 1$, så kan detta göras på bara ett sätt så att $f(r,1) = 1$ för alla $r \geq 0$. Om $n > 1$ kan vi sätta $j = 0, 1, \ldots, r$ föremål i den första lådan och de återstående $r - j$ föremålen i de återstående $n - 1$ lådorna. Eftersom vi får olika resultat för varje val värde på j så får vi rekursionsekvationen*

$$f(r,n) = \sum_{j=0}^{r} f(r-j, n-1) \overset{k=r-j}{=} \sum_{k=0}^{r} f(k, n-1).$$

I synnerhet betyder detta att $f(r,2) = r+1$ och med hjälp av formeln för summan av en aritmetisk serie får vi $f(r,3) = \frac{(r+2)(r+1)}{2}$. Nu gissar vi att $f(r,n) = \binom{r+n-1}{n-1} = \binom{r+n-1}{r}$ så vi skall visa att

$$\binom{r+n-1}{n-1} = \sum_{k=0}^{r} \binom{k+n-2}{n-2}, \quad r \geq 0, \quad n \geq 2.$$

Icke-ordnat val av r föremål från en mängd med n föremål **med** upprepningar, II, forts.

Denna likhet gäller säkert för $r = 0$ och varje $n \geq 2$. Antag att den gäller för $r = s$ och $n \geq 2$. Då får vi när $r = s + 1$ och $n \geq 2$

$$\sum_{k=0}^{s+1} \binom{k+n-2}{n-2} = \binom{s+1+n-2}{n-2} + \sum_{k=0}^{s} \binom{k+n-2}{n-2}$$

$$= \binom{s+1+n-2}{n-2} + \binom{s+n-1}{n-1}$$

$$= \frac{(s+n-1)\cdot\ldots\cdot(s+2)}{(n-2)!} + \frac{(s+n-1)\cdot\ldots\cdot(s+1)}{(n-1)!}$$

$$= \frac{(s+n-1)\cdot\ldots\cdot(s+2)\cdot(n-1+s+1)}{(n-1)!}$$

$$= \frac{(s+n)\cdot(s+n-1)\cdot\ldots\cdot(s+n-(n-1)+1)}{(n-1)!} = \binom{s+1+n-1}{n-1}.$$

Induktionssteget fungerar och påståendet följer med induktionsprincipen.

Antalet funktioner $A \to B$

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

- *En funktion* $f : A \to B$ *är ett ordnat val* **med** *upprepningar av* m *element (funktionens värden) ur mängden* B *som har* n *element. Antalet funktioner:* $A \to B$ *är därför* n^m *(och därför är det förnuftigt att beteckna mängden av funktioner* $A \to B$ *med* B^A*).*
- *En injektion:* $A \to B$ *är ett ordnat val* **utan** *upprepningar av* m *element (funktionens värden) ur mängden* B *som har* n *element. Antalet injektioner* $A \to B$ *är därför*

  $$n \cdot (n-1) \cdot \ldots \cdot (n-m+1) = \frac{n!}{(n-m)!} \text{ då } m \leq n.$$

- *Antalet surjektioner* $A \to B$ *är* $\displaystyle\sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r} r^m$.

  Varför? Antalet surjektioner är totala 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*.

Antalet surjektioner $A \to B$ då $|A| = m$ och $|B| = n$

Antag att $B = \{y_1, y_2, \ldots, y_m\}$. *Låt* $F = B^A$ *vara mängden av alla funktioner* $A \to B$. *Låt* $F_j = (B \setminus \{y_j\})^A \subset F$ *vara mängden av alla funktioner* $A :\to B \setminus \{y_j\}$, *dvs. alla funktioner* $f \in F$ *så att* $f(x) \neq y_j$ *för alla* $x \in A$. *Detta innebär att mängden av surjektioner är* $F \setminus \cup_{j=1}^{n} F_j$. *Nu är* $F_{j_1} \cap F_{j_2} \cap \ldots \cap F_{j_k}$ *mängden* $(B \setminus \{y_{j_1}, y_{j_2}, \ldots y_{j_k}\})^A$ *av alla funktioner* $A \to B$ *som inte får något av värdena* $y_{j_1}, \ldots, y_{j_k}$. *Om* $1 \leq j_1 < \ldots < j_k \leq n$ *så är* $|F_{j_1} \cap F_{j_2} \cap \ldots \cap F_{j_k}| = (n-k)^m$. *Eftersom indexen* $1 \leq j_1 < \ldots < j_k \leq n$ *kan väljas på* $\binom{n}{k}$ *olika sätt så kan vi med hjälp av inklusions-exklusionsprincipen dra slutsatsen att antalet surjektioner:* $A \to B$ *är*

$$n^m - \left(\sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)^m \right) = \sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r} r^m.$$

Observera att då $m < n$ *så finns det inga surjektioner:* $A \to B$ *så att* $\sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r} r^m = 0$ *då* $n < m$, *vilket kanske inte är helt uppenbart.*

Hur många delmängder av en mängd med m element finns det?

Ett sätt att besvara denna fråga är följande:
Om A är en mängd med m element så bestämmer varje delmängd $B \subset A$ en funktion $f_B : A \to \{0,1\}$ så att $f_B(x) = 1$ då $x \in B$ och $f_B(x) = 0$ då $x \notin B$. På motsvarande sätt bestämmer vare funktion $f : A \to \{0,1\}$ en delmängd $B_f \subset A$ genom definitionen $B_f = \{\, x \in A : f(x) = 1 \,\}$. Def finns alltså en bijektion från potensmängden $\mathcal{P}(A)$ till mängden $\{0,1\}^A$ av alla funktioner: $A \to \{0,1\}$. Därför är antalet delmängder i A

$$|\mathcal{P}(A)| = |\{0,1\}^A| = 2^{|A|} = 2^m,$$

om A innehåller m element.

Multinomialtal

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

- $\binom{n}{n_1, n_2, \ldots, n_k}$ *är antalet sätt på vilka en mängd med* n *element kan delas i* k *disjunkta delmängder med* n_1, n_2, $\ldots$ *och* n_k *element.*
- $\binom{n}{n_1, n_2, \ldots, n_k}$ *är antalet sätt på vilka man kan ordna* n_1 *föremål av typ* y_1, n_2 *av typ* y_2 *och så vidare, då* $n = n_1 + n_2 + \ldots + n_k$ *och 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*

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

Ett exempel

(a) *Fyra kort ur en normal kortlek med 52 kort placeras i en rad. På hur många sätt kan detta göras om alla kort i raden skall ha samma färg?*

(b) *Fyra kort ur en normal kortlek med 52 kort placeras i en rad. På hur många sätt kan detta göras om raden skall innehålla exakt en knekt?*

(a) Färgen kan väljas på 4 *olika sätt och sedan skall man göra ett ordnat val av* 4 *kort bland* 13 *och detta kan göras på* $13 \cdot 12 \cdot 11 \cdot 10$ *olika sätt så antalet alternativ blir sammanlagt*

$$4 \cdot 13 \cdot 12 \cdot 11 \cdot 10 = 68640.$$

(b) Det finns 4 *olika knektar att välja på och den kan placeras på* 4 *olika ställen, så sammanlagt ger detta* 16 *olika alternativ. Sedan skall man göra ett ordnat val av de* 3 *återstående* 48 *korten och detta kan göras på* $48 \cdot 47 \cdot 46$ *olika sätt så det sammanlagda antalet alternativ blir*

$$4 \cdot 4 \cdot 48 \cdot 47 \cdot 46 = 1660416.$$

Ett ordningsproblem

18 personer har delats in i tre lika stora grupper. Alla 18 personer skall nu i tur och ordning utföra ett uppdrag (tex. lösa en uppgift i diskret matematik) och villkoret är att vid varje tidpunkt skall skillnaderna mellan antalen personer i varje grupp som redan utfört uppdraget till sina absolutbelopp vara högst 1. På hur många sätt kan ordningsföljden då väljas (när gruppindelning är given)?

Ett annat sätt att formulera problemet är att man bildar 6 grupper, som alla innehåller exakt en medlem från var och en av de ursprungliga grupperna, och sedan sätter man dessa mindre grupper och medlemmarna i dem i ordningsföljd. Eller så att medlemmarna i de ursprunliga grupperna sätts i ordningsföljd och personerna med samma ordningsnummer bildar en grupp som sedan i sin tur ordnas.

Medlemmarna i de tre ursprungliga grupperna kan ordnas på $6! \cdot 6! \cdot 6!$ *olika sätt och med hjälp av dessa ordningar utses medlemmar till de mindre grupperna som i sin tur kan ordnas var och en på* $3!$ *olika sätt så att det sammanlagd antalet alternativ blir*

$$6! \cdot 6! \cdot 6! \cdot (3!)^6 = 17414258688000.$$

På hur många sätt kan man placera m identiska bollar i n identiska lådor?

Låt $A(m,n)$ vara detta antal. Eftersom vi kan placera $m \geq 0$ bollar i 1 låda på bara ett sätt så har vi $A(m,1) = 1$ då $m \geq 0$. Om $m = 0$ förblir alla lådor tomma och det ger bara ett alternativ, dvs. $A(0,n) = 1$ för alla $n \geq 1$.

Antag nu att $m \geq 1$ och $n \geq 2$. Låt k vara antalet bollar i den låda (eller de lådor) som innehåller minst bollar. Olika värden på k ger upphov till olika fördelningar på bollarna i lådorna. Fördelningen av bollarna i lådorna kan nu göras så att vi först sätter k bollar i varje låda och sedan sätter de återstående $m - n \cdot k$ bollarna i de $n-1$ lådor som kan innehålla flera än k bollar. Detta kan göras på $A(m - n \cdot k, n-1)$ olika sätt. Eftersom vi måste ha $m - n \cdot k \geq 0$, dvs. $k \leq \frac{m}{n}$, så får vi

$$A(m,n) = \sum_{k=0}^{\lfloor \frac{m}{n} \rfloor} A(m - n \cdot k, n-1).$$