Introduktion till diskret matematik

Niklas Brännström
Helsingfors Universitet

December 15, 2009

Abstract

Detta är ett utkast till föreläsningsanteckningar för kursen Introduktion till diskret matematik given under höstterminen 2009 vid Helsingfors Universitet. Frågor, synpunkter och utpekanden av fel eller språkmissar mottages tacksamt.

Contents

1 Kort om logiska operatorer

1.1 Satslogik

Inom satslogiken betraktar man resonemanget i påståenden och utsagor (dvs. vi är intresserade av resonemanget i sig, inte om invärdena (input) eller slutsatsen verkligen är sanna eller falska). Några standardoperatorer (satslogiska konnektiv) är

$\wedge$ och

$\vee$ eller

$\neg$ inte

$\Longrightarrow$ implikation - "om __, så __"

$\Longleftrightarrow$ ekvivalens - "__ om och endast om __"

1.1.1 Och (konjunktion)

Låt p och q vara två påståenden (som vardera kan anta värdet sant eller falsk - inget annat!), då är $p \wedge q$ ett sant påstående om om *både* p och q är sanna, och falskt i alla andra fall (dvs. det räcker inte med att antingen p eller q är sant). Detta kan sammanfattas i en sanningstabell:

p	q	$p \wedge q$
s	s	s
s	f	f
f	s	f
f	f	f

där s representerar sann och f falsk. Tabellen ska tolkas så att i den vänstra kolumnen finns alla möjliga sanningsutfall av påståendena p respektive q, och i den högra kolumnen finns sanningsvärdet som $p \wedge q$ antar givet sanningsvärdena för p och q på samma rad. Vi ser att $\wedge$ enligt definitionen är sann (endast) då p och q båda är sanna. Tex. är påståendet "boken är grön och skriven på engelska" sant bara om boken både är grön och skriven på engelska, men inte om boken är grön och skriven på svenska.

1.1.2 Eller (disjunktion)

Låt p och q vara två påståenden. Då är $p \vee q$ sann då åtminstonde en av de båda påståendena p,q är sanna. Enligt definitionen får $\vee$ följande sanningstabell:

p	q	$p \vee q$
s	s	s
s	f	s
f	s	s
f	f	f

Vi ser att ett påstående som "boken är grön eller skriven på engelska" är sant om tex: boken är grön och skriven på svenska, blå och skriven på engelska, grön och skriven på engelska, men påståendet är falskt om boken är blå och skriven på svenska.

1.1.3 Inte (Negation)

"Inte" växlar sanningsvärdet på ett påstående: om p är ett påstående som är sant så är $\neg p$ falskt, om p är falskt så är $\neg p$ sant. Sammanfattat i en sanningstabell får vi

p	$\neg p$
s	f
f	s

.

1.1.4 Implikation

Låt p och q vara två påståenden. Implikationen $p \implies q$ kan utläsas "om p (är uppfyllt) så (följer) q". Sanningstabellen för implikationen kan vid första anblicken (och kanske även den andra) te sig som icke-intuitiv, för implikationen, $p \implies q$, är en operation som bara är falsk i det fall då utsagan p är sann och utsagan q är falsk, vilket ges av sanningstabellen:

p	q	$p \implies q$
s	s	s
s	f	f
f	s	s
f	f	s

Vi accepterar detta som definitionen för implikationen (och noterar bara att om påståendet p är falskt så ger implikationen ingen information om q). Kanske följande exempel kan ge någon ledtråd bakom konstruktionen: Låt p vara "kör bil i en hastighet över 120km/h" och q vara "bryter mot Finlands lag". Om man kör bil i hastigheten 100 km/h så betraktar vi implikationen som sann eftersom dess villkor p är falskt (men vi kan för den skull inte dra slutsatsen att ett lagbrott har skett).

1.1.5 Ekvivalens

Låt p och q vara två påståenden. Ekvivalensen $p \iff q$ kan läsas som "p om och endast om q", och är sann om både p och q är sanna eller om både p och q är falska:

p	q	$p \iff q$
s	s	s
s	f	f
f	s	f
f	f	s

1.1.6 Tautologier

En sats är en tautologi om den är sann oberoende av sanningsvärdet på de olika utsagorna. Man kan använda sanningstabeller för att bevisa om något är en tautologi.

Exempel 1 *Det gäller att* $((p \implies q) \wedge (q \implies p)) \iff (p \iff q)$. *För att bevisa detta ska vi visa att ekvivalensen* $\iff$ *mellan höger och vänster led alltid är sann, och vi använder en sanningstabell för att göra detta*

p	q	$p \implies q$	$q \implies p$	$((p \implies q) \wedge (q \implies p))$	$(p \iff q)$	$\iff$
s	s	s	s	s	s	$\boldsymbol{s}$
s	f	f	s	f	f	$\boldsymbol{s}$
f	s	s	f	f	f	$\boldsymbol{s}$
f	f	s	s	s	s	$\boldsymbol{s}$

Den första kolumnen anger alla möjliga kombinationer av sanningsvärden för p *och* q, *de nästföljande två kolumnerna studerar komponenterna i vänsterledet och i kolumn 4 anges sanningsvärdena för hela vänsterledet. I kolumn 5 anges sanningsvärdet för högerledet och i den sista kolumnen jämförs sanningsvärdet för vänsterledet och högerledet och vi finner att oberoende av sanningsvärdena för* p *och* q *så är vänsterledet och högerledet ekvivalenta.*

Exempel 2 *Det gäller att* $(p \implies q) \iff (\neg q \implies \neg p)$. *Låt oss förvissa oss om detta genom att studera sanningstabellen*

p	q	$(p \implies q)$	$\iff$	$(\neg q$	$\implies$	$\neg p)$
s	s	s		f		f
s	f	f		s		f
f	s	s		f		s
f	f	s		s		s

p	q	$(p \implies q)$	$\iff$	$(\neg q$	$\implies$	$\neg p)$
s	s	s		f	s	f
s	f	f		s	f	f
f	s	s		f	s	s
f	f	s		s	s	s

p	q	$(p \implies q)$	$\iff$	$(\neg q$	$\implies$	$\neg p)$
s	s	s	$\boldsymbol{s}$	f	s	f
s	f	f	$\boldsymbol{s}$	s	f	f
f	s	s	$\boldsymbol{s}$	f	s	s
f	f	s	$\boldsymbol{s}$	s	s	s

I den första tabellen har vi infört sanningsvärdena för vänsterledet samt sanningsvärdena för $\neg q$ och $\neg p$, i den andra tabellen har vi använt sanningsvärdena för $\neg q$ och $\neg p$ för att bestämma sanningsvärdena för $(\neg q \implies \neg p)$, och slutligen i sista tabellen jämför vi sanningsvärdena för vänster och höger led och konstaterar att de är ekvivalenta.

Vi noterar att resultaten i båda exemplen kan vara användbara i bevisandet av olika satser.

1.2 Predikatslogik

I predikatslogiken kan vi införa variabler och betrakta sanningshalten i olika utsagor som innehåller dem. Två så kallade kvantorer är

$\forall$ för alla

$\exists$ för något, eller, det existerar.

Exempel 3 *Betrakta $\forall x(x \geq 0)$ "för alla x gäller att x är större eller lika med noll". Detta är sant för $x \in \mathbb{N}$ (de naturliga talen) men falskt för $x \in \mathbb{R}$.*

Exempel 4 *Betrakta $\exists x(x^2 = -2)$ "det existerar ett x så att x^2 är lika med -2". Detta är sant för $x \in \mathbb{C}$ (de komplexa talen) men falskt för $x \in \mathbb{R}$.*

2 En ofullständig icke-axiomatisk mängdlära

Mängder och mängdläran tillhör grunden inom matematiken, så det är otillfredställande att konstatera att vi i den här kursen inte har möjlighet att ge en definition av en mängd, eller de axiom (Zermelo-Fraenkels axiom + Urvalsaxiomet (**eng:** Axiom of Choice)) som krävs för att stringent kunna bygga upp mängdläran. Istället kommer vi att arbeta med följande "icke/nästandefinition" av en mängd (trots att vi vet att den leder till självmotsägande)

"Definition" 5 *En* mängd *består av ett antal element ur något universum $\mathcal{U}$.*

Vi säger att ett element x *tillhör* en mängd A, $x \in A$, om x finns med bland elementen i A. (och noterar som en parentes att begreppet "tillhör" är svårt att definera matematiskt, men vi förlitar oss i den här kursen på vår intuition (vilket är farligt!)). Vi säger vidare att två mängder A och B är lika, $A = B$, om (och endast om) de har samma element

$$A = B \iff (\forall x \in A)(x \in B) \wedge (\forall x \in B)(x \in A), \tag{Extensionalitetsaxiomet}$$

(vilket råkar vara ett av de axiom som mängdläran vilar på, **eng:** Axiom of Extension), där högerledet ska läsas: "för alla x som tillhör mängden A så tillhör x mängden B *och* för alla x som tillhör mängden B så tillhör x mängden A".

Vi kan skriva en mängd på två sätt:

1. Genom att räkna upp alla element som ingår i mängden, tex

   $$A = \{a, b, c\}$$

   eller

2. Använda den så kallade mängdbyggaren

   $$A = \{x \in \mathcal{U} : P(x)\},$$

   eller med ord "A är mängden av alla x tillhörande universum $\mathcal{U}$ så att villkoret $P(x)$ är uppfyllt"

Anmärkning 6 *Vi noterar att de två villkoren $P(x) : x \notin x$ eller $x = x$ inte definierar en mängd under Zermelo-Fraenkels axiom.*

Här följer några exempel på mängder.

Exempel 7

$$\begin{aligned} A &= \{1, 2, 3, 4\}, \\ B &= \{\textit{Pelle, Olle, Lisa}\}, \\ C &= \{x : x \textit{ är ett land vars namn börjar på } F\}, \\ D &= \{x \in \textit{Heltalen} : |x| < 5\}. \end{aligned}$$

Vi noterar att mängdbyggaren inte är en unik representation av en mängd, till exempel kan vi skriva mängden D i föregående exempel som

$$\begin{aligned} D &= \{-4, -3, -2, -1, 0, 1, 2, 3, 4\} = \{x \in \text{Heltalen} : |x| < 5\} \\ &= \left\{x \in \text{Heltalen} : x^2 \leq 16\right\}. \end{aligned}$$

Låt oss också notera att det följer från vår definition av lika mängder, Extensionalitetsaxiomet, att

$$\{1,2,1,2,1,3,5\} = \{1,2,3,5\} = \{3,2,5,1\},$$

dvs. elementen i en mängd har ingen ordning samt att det inte spelar någon roll hur många gånger samma element räknas upp inom mängdparenteserna, det är ändå samma element.

Vissa mängder förekommer oftare än andra inom matematiken, och till dessa hör

Mängden av de naturliga talen $\mathbb{N} = \{0,1,2,3,\ldots\}$,
Mängden av de reela talen $\mathbb{R}$,
Mängden av de hela talen $\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$,
Mängden av de rationella talen $\mathbb{Q} = \left\{\frac{n}{k} : (n,k \in \mathbb{Z}) \wedge (k \neq 0)\right\}$.

Anmärkning 8 *Om vi undlåter att specifiera ur vilket universum $\mathcal{U}$ vi väljer elementen x så uppstår lätt godtycke och missförståelser, betrakta till exempel $\{x : 0 \leq x \leq 1\}$. Om $\mathcal{U} = \mathbb{N}$ så har vi $\{x \in \mathbb{N} : 0 \leq x \leq 1\} = \{0,1\}$, men om $\mathcal{U} = \mathbb{R}$ så har vi $\{x \in \mathbb{R} : 0 \leq x \leq 1\} = [0,1]$ (dvs. hela intervallet från 0 till 1). Vi ser också att mängden C i det föregående exemplet är godtyckligt eftersom vi inte specifierat vilket språk ländernas namn ska skrivas på; om det är svenska ingår Finland och Frankrike medan om det är finska ingår varken Finland (Suomi) eller Frankrike (Ranska).*

2.1 Delmängd

Definition 9 *Om två mängder A och B är sådana att alla element i B också tillhör A så säger vi att B är en delmängd av A, vilket vi skriver $B \subset A$*

$$B \subset A \iff \forall x(x \in B \implies x \in A).$$

Tecknet $\subset$ kallas för inklusion och kan vändas "åt båda hållen": $B \subset A$ eller $A \supset B$ för att beteckna att B är en delmängd av A.

Exempel 10

$$\begin{array}{ll} a) & \{1,2,3\} \subset \mathbb{N}, \\ b) & \{2n : n \in \mathbb{N}\} \subset \mathbb{N}, \\ c) & \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}, \\ d) & \{x\} \subset A \iff x \in A. \end{array}$$

Definition 11 *Om $B \subset A$ och $B \neq A$ så säger vi att B är en* äkta delmängd *av A och skriver*

$$B \subsetneqq A.$$

Exempel 12 *I föregående exempel är a), b) och c) exempel på äkta delmängder.*

Sats 13 *Låt A, B och C vara mängder. Inklusionen $\subset$ har följande egenskaper*

(i)	$A \subset A$	*"Reflexivitet"*
(ii)	*Om $A \subset B$ och $B \subset A$, så är $A = B$*	*"Antisymmetri"*
(iii)	*Om $A \subset B$ och $B \subset C$, så $A \subset C$*	*"Transivitet"*

Bevis. (i) följer direkt ur definitionen av delmängd, nämligen

$$A \subset A \iff \forall x(x \in A \implies x \in A).$$

(ii) Antag att $A \subset B$ och $B \subset A$. Definitionen av delmängd ger att eftersom $A \subset B$ så har vi för varje $x \in A$ att det också tillhör B. På motsvararande sätt ger $B \subset A$ att för varje $x \in B$ så är det också i A. Detta är samma som: om $x \in A$ så $x \in B$ och om $x \in B$ så $x \in A$, med andra ord

$$\begin{aligned} \forall x(x &\in A \implies x \in B), \\ \forall x(x &\in B \implies x \in A), \end{aligned}$$

alltså (enligt det första exemplet i avnittet om satslogik)

$$\forall x(x \in A \iff x \in B),$$

dvs. $A = B$.

(iii) Antag att $A \subset B \subset C$. Per definition följer att om $x \in A$ så $x \in B$, och om $x \in B$ så $x \in C$. Av detta följer att om $x \in A$ och $x \in C$, dvs. $A \subset C$. ■

Ur denna sats följer denna mycket viktiga följdsats

Följdsats 14 *För alla mängder A och B gäller*

$$A = B \iff ((A \subset B) \wedge (B \subset A)).$$

Bevis. ($\implies$) ges av reflexiviteten. ($\impliedby$) ges av antisymmetrin. ■

Det här resultatet är väldigt användbart för att visa att två mängder är lika. Det är ofta lättare att visa att en mängd är en delmängd av en annan istället för att direkt visa att de två mängderna har samma element.

Övning 15 *Visa med hjälp av följdsatsen att*

$$\{2n + 1 : n \in \mathbb{N}\} = \left\{n \in \mathbb{N} : \frac{n}{2} \notin \mathbb{N}\right\}.$$

Istället för att bara studera en delmängd kan vi studera mängden av alla delmängder som går att skapa ur en given mängd A, men innan vi gör det måste vi stifta bekantskap med en annan speciell mängd.

Definition 16 *Om A är en mängd så är $\emptyset = \{x \in A : x \neq x\} \subset A$ den unika mängden utan element, den* tomma mängden*.*

Anmärkning 17 *Den tomma mängden är unik på grund av (Axiom of Extension). Antag att vi skulle ha en annan mängd $\emptyset_1$ som också saknar element. Då skulle $\emptyset = \emptyset_1$ eftersom de har samma (här inga) element. Vidare noterar vi att $\emptyset \neq \{\emptyset\}$ eftersom den tomma mängden $\emptyset$ inte innehåller något element, medan $\{\emptyset\}$ har ett element - den tomma mängden.*

Definition 18 *Potensmängden $\mathcal{P}(A) = \{B : B \subset A\}$ är mängden av alla delmängder ur A.*

Märk att både den tomma mängden $\emptyset$ och mängden A själv tillhör $\mathcal{P}(A)$.

Exempel 19 *Låt $A = \{a\}$. Då är potensmängden*

$$\mathcal{P}(A) = \{\emptyset, \{a\}\}.$$

Exempel 20 *Låt $A = \{a, b\}$. Då är potensmängden*

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Man kan visa att antalet element i $\mathcal{P}(A)$ är 2^n där n är antalet element i A, av den här anledningen skrivs ibland potensmängden som 2^A.

2.2 Unioner, Snitt och Mängddifferenser

Union, snitt och mängddifferens är tre sätt att skapa nya mängder utgående från redan existerande mängder (att detta är möjligt är ingen självklarhet utan vilar i den stringenta mängdläran på axiom).

Definition 21 *Unionen av två mängder A och B är mängden*

$$A \cup B = \{x : x \in A \text{ eller } x \in B\} = \{x : x \in A \vee x \in B\}.$$

Elementen i unionen $A \cup B$ tillhör alltså antingen A eller B eller både A och B. Om vi istället kräver att elementen i den nya mängden måste tillhöra både A och B så får vi snittet av dessa mängder.

Definition 22 *Snittet av två mängder A och B är mängden*

$$A \cap B = \{x : x \in A \text{ och } x \in B\} = \{x : x \in A \wedge x \in B\}\,.$$

Sedan kan vi kräva att den nya mängdens element bara ligger i, säg, A men inte i B. Detta ger mängddifferensen av A och B.

Definition 23 *Mängddifferensen av två mängder A och B är mängden*

$$A \backslash B = \{x : x \in A \text{ och } x \notin B\} = \{x \in A : x \notin B\}\,.$$

Låt oss bekanta oss med dessa nya mängder i ett exempel.

Exempel 24 *Låt* $A = \{1, 3, 5, 5, 6\}$ *och* $B = \{2, 3, 6, 7\}$. *Då har vi*

$$\begin{aligned} A \cup B &= \{1, 2, 3, 5, 6, 7\}\,, \\ A \cap B &= \{3, 6\}\,, \\ A \backslash B &= \{1, 5\}\,, \\ B \backslash A &= \{2, 7\}\,. \end{aligned}$$

Fråga 25 *Låt* $\mathcal{U}$ *vara mängden av alla människor,* A *vara mängden av alla kvinnor, och* B *mängen av alla läkare. Vad är följande mängder:* $A \cup B$, $A \cap B$, $A \backslash B$, $B \backslash A$*?*

2.2.1 Räkneregler

För snitt, union och mängddifferens kan man härleda ett stort antal räkneregler, till exempel gäller

$$\begin{aligned} A \cup B &= B \cup A, \\ A \cap B &= B \cap A, \\ A \cup (B \cup C) &= (A \cup B) \cup C, \\ A \cap (B \cap C) &= (A \cap B) \cap C, \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \end{aligned}$$

och de följande två har fått namnet *De Morgans lagar*

$$\begin{aligned} A \backslash (B \cup C) &= (A \backslash B) \cap (A \backslash C), \\ A \backslash (B \cap C) &= (A \backslash B) \cup (A \backslash C). \end{aligned}$$

För att bevisa att någon av dessa räkneregler gäller måste vi visa att mängderna i höger led och vänster led har exakt samma element. För att göra detta är ofta Följsats 14 användbar. Låt oss som exempel bevisa den första av De Morgans lagar.

Sats 26 *För alla mängder* A, B *och* C *gäller*

$$A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C).$$

Bevis. Vi visar först att $A\backslash(B \cup C) \subset (A\backslash B) \cap (A\backslash C)$. Låt $x \in A\backslash(B \cup C)$. Enligt definitionen av mängddifferens följer att $x \in A \wedge x \notin (B \cup C)$. Att $x \notin (B \cup C)$ är samma som att $x \notin B \wedge x \notin C$ enligt definitionen för union. Vi har alltså att $x \in A \wedge x \notin B \wedge x \notin C$, vilket vi skriver som $(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$. Vi använder definitionen för mängddifferens för uttrycken inne i parenteserna och definitionen för snitt för hela uttrycket för att skriva om det som $x \in (A\backslash B) \cap (A\backslash C)$.

Låt oss nu visa att $A\backslash(B \cup C) \supset (A\backslash B) \cap (A\backslash C)$. Antag att $x \in (A\backslash B) \cap (A\backslash C)$. Då följer att $(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$. Det är samma som $x \in A \wedge x \notin B \wedge x \notin C$, dvs. $x \in A \wedge (x \notin B \cup C)$ alltså $x \in A\backslash(B \cap C)$.

Enligt Följsats 14 följer nu satsen. ■

Prova gärna att härleda någon av de andra räknereglerna enligt samma principer.

Låt oss modifiera vårt förra exempel.

Exempel 27 *Låt* $A = \{2, a, \{f\}\}$ *och* $B = \{1, 2, a, b, \{f\}, 10\}$. *Då har vi*

$$\begin{aligned} A \cup B &= \{1, 2, a, b, \{f\}, 10\} = B, \\ A \cap B &= \{2, a, \{f\}\} = A, \\ A\backslash B &= \emptyset, \\ A &\subset B. \end{aligned}$$

Vi sammanfattar vår observation i följande sats.

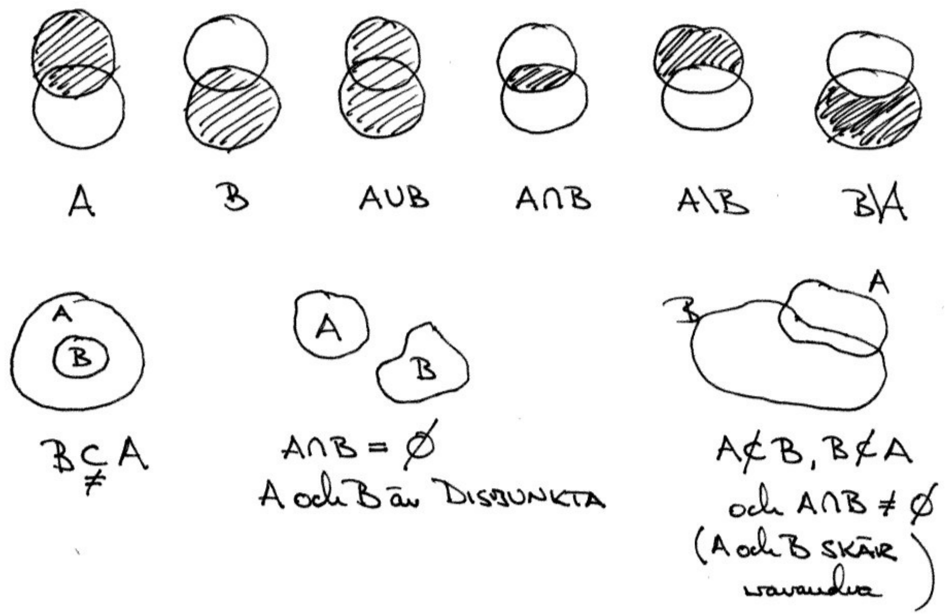
Sats 28 *Följande villkor är ekvivalenta för alla mängder* A *och* B *(dvs. om ett är uppfyllt så är alla uppfyllda)*

$$\begin{array}{rl} (i) & A \subset B \\ (ii) & A \cap B = A \\ (iii) & A \cup B = B \\ (iv) & A\backslash B = \emptyset. \end{array}$$

Bevis. Att $(iii) \iff (iv)$ finns som övning på Övningsblad 1. För att bevisa hela satsen kan man visa $(i) \iff (ii) \iff (iii) \iff (iv)$, men det räcker med att visa $(i) \implies (ii) \implies (iii) \implies (iv) \implies (i)$. ■

2.2.2 Venndiagram

Venndiagram (John Venn 1880-talet) infördes som en metod för att visualisera mängder så att man lättare skulle förstå vilka mängder man talade om. Det är mycket användbart som hjälpmedel, men man ska ha i åtanke att bilder kan vara missvisande och att de inte duger som bevis.



Figuren visar några exempel på Venndiagram. Under de övre bilderna finns angivet vilken mängd den skuggade delen representerar. De tre undre bilderna visar; från vänster till höger: en äkta delmängd, två disjunkta mängder och två mängder som skär varandra.

Fråga 29 *Låt $\mathcal{U}$ vara mängden av alla språk, S_P alla språk som Pelle talar, S_O alla språk som Olle talar, S_L alla språk som Lisa talar. Vad är innebörden av $S_P \cup S_O \cup S_L$? Vad är innebörden av $S_P \cap S_O \cap S_L$? Om Lisa vill berätta en hemlighet för Olle så att Pelle inte kan förstå (även om han hör vad hon säger), vilket villkor måste då vara uppfyllt för språket $s \in \mathcal{U}$ som hon väljer?*

Fråga 30 *Om vi vill visa att $A = B$, varför räcker det då inte med att visa att $A \subset B$? (varför måste vi också visa att $B \subset A$?)*

Svar 31 *Om vi har visat att $A \subset B$ så vet vi att alla $x \in A$ också tillhör B, men nu kan det vara så att B innehåller fler element än de i A (B är "större" än A). Om så är fallet så finns det element i B som inte finns i*

A, och då gäller inte vårt påstående att mängderna är lika. Rita gärna ett Venndiagram över situationen och förvissa er om att detta verkar stämma.

Övning 32 *Rita Venndiagram för De Morgans lagar.*

2.2.3 Mängdfamiljer

Om $\mathcal{A}$ är en familj av mängder, dvs. varje element i $\mathcal{A}$ är en mängd så definerar vi

$$\begin{aligned} \cup\mathcal{A} &= \{x : x \in A \text{ för något } A \in \mathcal{A}\}, \\ \cap\mathcal{A} &= \{x : x \in A \text{ för alla } A \in \mathcal{A}\}. \end{aligned}$$

(eftersom variationerna på mina "svarta-tavlanfonter" inte var stor nog skrev jag $\boxed{\mathcal{A}}$ istället för $\mathcal{A}$ på svarta tavlan). Om vi har något sätt att indexera ("numrera") elementen i $\mathcal{A}$ kan vi skriva $\mathcal{A} = \{A_i : i \in I\}$ där A_i är mängder och I är en indexmängd ("alla nummer som används för att numrera elementen i $\mathcal{A}$"). Då blir ovanstående uttryck

$$\begin{aligned} \cup\mathcal{A} &= \cup_{i\in I} A_i = \cup \{A_i : i \in I\}, \\ \cap\mathcal{A} &= \cap_{i\in I} A_i = \cap \{A_i : i \in I\}. \end{aligned}$$

Exempel 33 *Låt $A_1 = \{a\}$, $A_2 = \{a, b\}$, $A_3 = \{a, b, c\}$,..., $A_{28} = \{a, b, \ldots, ö\}$, och $I = \{1, \ldots, 28\}$, och $\mathcal{A} = \{A_i : i \in I\}$. Då är*

$$\begin{aligned} \cup\mathcal{A} &= \cup_{i\in I} A_i = \cup_{i=1}^{i=28} A_i = \{a, b, c, d \ldots, ö\}, \\ \cap\mathcal{A} &= \cap_{i\in I} A_i = \cap_{i=1}^{i=28} A_i = \{a\}. \end{aligned}$$

3 Kardinalitet

I kursboken behandlas kardinalitet tämligen kortfattat så därför samlar vi information om detta i dessa föreläsningsanteckningar.

Definition 34 *Antalet element i mängden A skrivs $|A|$ och kallas för mängden A's* kardinalitet.

Vi börjar med att titta på ett enkelt exempel för att bekanta oss med konceptet.

Exempel 35 *Låt* $A = \{1, 2, 5\}$, $B = \{c, f\}$, $C = \{2\}$, $D = \{1, c, f\}$. *Kardinaliteten för dessa mängder är*

$$|A| = 3, \ \ |B| = 2, \ \ |C| = 1, \ \ |D| = 3,$$

vilket nog ligger i linje med vår intuition gällande begreppet "antal". Vidare har vi

$$\begin{aligned} |A \cup B| &= |\{1, 2, 5, c, f\}| = 5 = |A| + |B| , \\ |A \backslash C| &= |\{1, 5\}| = 2 = |A| - |C| , \end{aligned}$$

där A *och* B *är disjunkta och där* C *är en äkta delmängd av* A. *För unionen av mängderna* A *och* D *är kardinaliteten*

$$|A \cup D| = |\{1, 2, 5, c, f\}| = 5 = |A| + |D| - |A \cap D| ,$$

dvs. antalet element i unionen är summan av antalet element i de ingående mängderna minus antalet element som ligger i snittet av de båda - detta för att motverka "överräkning" av dessa.

Att basera begreppet kardinalitet på vår intuition är dock inte tillfredställande. Att definera begreppet kardinalitet är snarlikt problemet att mäta längd inom fysiken; "hur lång är en meter?". När vi bestämmer kardinaliteten av en mängd så kommer vi att jämföra den med en standardmängd. Vi börjar med att definera standardmängden (eller snarare en familj av standardmängder) och sedan bestämmer vi oss för hur jämförelsen med andra mängder ska ske.

Definition 36 *För varje* $n \in \mathbb{N}$ *låter vi* $[n] = \{x \in \mathbb{N} : 1 \leq x \leq n\} = \{1, \ldots, n\}$.

Sedan bestämmer vi att kardinaliteten av $[n]$ är just n.

Definition 37 *För varje* $n \in \mathbb{N}$ *låter antalet element i mängden* $[n]$ *vara* n, *dvs.* $|[n]| = n$.

Tillsammans ger de här två definitionerna oss vår "måttstock", precis som meterstaven i Paris ger oss en möjlighet att mäta längden av olika objekt. Följande definition preciserar hur man använder standardmängden för att bestämma kardinaliteten av en mängd A (om möjligt).

Definition 38 *Låt* A *vara en godtycklig mängd. Vi säger att* $|A| = n$ *om det finns en bijektion* $\varphi : [n] \to A$. *Vi säger då att* A *är* ändlig. *Om* A *är icketom och det inte finns något* n *för vilket det existerar en bijektion* $\varphi : [n] \to A$ *säger vi att antalet element i* A *är* oändligt.

Märk att antalet element i $[n]$ är ändligt då identitetsfunktionen

$$Id_{[n]}x = x$$

är en bijektion från $[n]$ till $[n]$.

Definition 39 $|\emptyset| = 0$ *och* $\emptyset$ *är ändlig.*

Följande sats försäkrar oss om att kardinaliteten är väldefinierad, det finns alltså ingen möjlighet att kardinaliteten av en ändlig mängd A är både k och n där $k \neq n$.

Sats 40 *Om A är en ändlig mängd så existerar endast ett $n \in \mathbb{N}$ för vilket det finns en bijektion $[n] \to A$.*

(Den här satsen kan härledas ur följande hjälpsats

Lemma 41 *Låt $n, k \in \mathbb{N}$ där $k < n$. Då finns det ingen bijektion $[n] \to [k]$.*

som i sin tur vilar på *välordningsprincipen* (som vi sin tur stiftat bekantskap med i samband med matematisk induktion))

Låt oss fortsätta att jämföra kardinalitet med att mäta längd med hjälp av en måttstock. I den här liknelsen är måttstocken vår familj av standardmängder $[n]$ och sättet att "läsa av" längden på måttstocken är att hitta en bijektion från standardmängden till den mängden vi är intresserade av. På samma sätt som det är möjligt att säga att två brädor är lika långa utan att använda en måttstock kan man säga att två mängder har samma kardinalitet utan att hänvisa till standardmängden $[n]$ (liknelsen med måttstocken håller inte fullt ut eftersom vi använder standardmängden i beviset).

Sats 42 *Låt A och B vara sådana mängder att finns en bijektion från A till B. Om mängden A eller B är ändliga så är både A och B ändliga samt*

$$|A| = |B|.$$

Bevis. Låt $f : A \to B$ vara en bijektion. Antag att A är ändlig så att $A = \{a_1, \ldots, a_n\}$ för något n. Definiera sedan $\varphi(i) := a_i$ för varje $i \in [n]$, då är $\varphi : [n] \to A$ en bijektion. Om vi bildar sammansättning av dessa funktioner får vi $h(k) := f(\varphi(k)) = f \circ \varphi(k)$ där

$$h : [n] \to B$$

är en bijektion[1]. Eftersom det existerar en bijektion mellan $[n]$ och B så är B ändlig och $|B| = n = |A|$.

Låt oss nu istället anta att B är ändlig (istället för A). Eftersom $f : A \to B$ är en bijektion så existerar dess invers $f^{-1} : B \to A$ som även den är en bijektion. Resten av beviset är analogt med föregående konstruktion. ■

Det är inte bara ändliga mängder som har intresserat matematiker genom tiderna, tvärtom har de oändliga mängderna fått större uppmärksamhet och rönt större kontroverser (hjälten i den här historien är George Cantor). Vi nöjer oss med att göra ett par observationer.

Definition 44 *Det finns* numrerbart oändligt *många element i mängden av de naturliga talen* $\mathbb{N}$*, vi skriver detta som* $|\mathbb{N}| = \aleph_0$*.*

Bokstaven $\aleph$ är hebreisk och heter Alef. Det finns olika typer av oändligheter, $\aleph_0$ är den numrerbara oändligheten, medan $\aleph_1$ är den onumrerbara oändligheten (tex $|\mathbb{R}| = \aleph_1$). När de gäller oändliga mängder är vår intuition sällan till någon större nytta som vi ska se. Vi börjar med att generalisera föregående sats till oändliga mängder.

Sats 45 *Låt A och B vara sådana mängder att finns en bijektion från A till B. Då är $|A| = |B|$.*

(Vi ger inget bevis, men noterar att eftersom det finns en bijektion från A till B så avbildas varje element i A på ett unikt element i B och det finns inga element i B som inte är en bild av ett element i A, därför är antalet element lika stort.)

Detta leder till följande fenomen.

Exempel 46 *Låt* $2\mathbb{N} = \{2n : n \in \mathbb{N}\} = \{0, 2, 4, 6, \ldots\}$ *vara mängden av alla jämna naturliga tal.* $2\mathbb{N}$ *är en äkta delmängd av* $\mathbb{N}$, $2\mathbb{N} \subsetneq \mathbb{N}$*. Men funktionen* $f : \mathbb{N} \to 2\mathbb{N}$ *given av* $f(n) = 2n$ *är en bijektion. Föregående sats implicerar då att*

$$|\mathbb{N}| = |2\mathbb{N}|,$$

alltså antalet naturliga tal är samma som antalet jämna naturliga tal!

---

[1]

Sats 43 *Låt $f : A \to B$ och $g : B \to C$. Om f är en injektion och g är en injektion så är $g \circ f : A \to C$ en injektion. Om f är en surjektion och g är en surjektion så är $g \circ f : A \to C$ en surjektion.*

För oändliga mängder kan det alltså hända att äkta delmängder har lika många element som mängden den är en delmängd av! Detta kan aldrig hända för ändliga mängder, vilket vi kommer att visa senare i kapitlet.

Cantor visade även att de rationella talen har samma kardinalitet som de naturliga talen! (även om Cantor som sagt är hjälten i den historien så betyder det inte att han ansågs vara en hjälte då det begav sig; tvärtom hade han inflytelserika motståndare som häcklade hans forskning).

Sats 47 *De rationella talen* $\mathbb{Q}$ *och de naturliga talen* $\mathbb{N}$ *har samma kardinalitet.*

Vi ger bara en inblick i hur man gör för att visa att de rationella talen är numrerbara. Vi skriver alla de rationella talen i en matris

$$
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \frac{6}{2} & \frac{7}{2} & \dots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \frac{6}{3} & \frac{7}{3} & \dots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \frac{6}{4} & \frac{7}{4} & \dots \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \frac{6}{5} & \frac{7}{5} & \dots \\
\frac{1}{6} & \frac{2}{6} & \frac{3}{6} & \frac{4}{6} & \frac{5}{6} & \frac{6}{6} & \frac{7}{6} & \dots \\
\frac{1}{7} & \frac{2}{7} & \frac{3}{7} & \frac{4}{7} & \frac{5}{7} & \frac{6}{7} & \frac{7}{7} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

och räknar sedan elementen längs diagonalerna genom att följa pilarna:

$$
\begin{array}{cccccccccc}
1 & \rightarrow & 2 & & 3 & \rightarrow & 4 & & 5 & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \dots \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \dots \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \dots \\
\frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \frac{4}{4} & & \frac{5}{4} & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \dots \\
\frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & & \frac{5}{5} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

Vi ser att man kan räkna de rationella talen på samma sätt som de naturliga talen. Så vi har igen exempel där en äkta delmängd $\mathbb{N} \subsetneqq \mathbb{Q}$ har samma kardinalitet som mängden den är en delmängd av. Vi avslutar diskutionen kring oändliga mängder med att notera att de reella talen är "oändligare" än de naturliga talen.

Sats 48 $|\mathbb{R}| = \aleph_1 > \aleph_0 = |\mathbb{N}|$.

(Cantor förmodade att det inte existerar någon mängd A sådan att $\aleph_0 < |A| < \aleph_1$ (strikta olikheter!), men kunde inte bevisa det. Problemet har nu namnet "kontiniumhypotesen". Det har visats (Gödel, Cohen) att Cantors påstående varken går att bevisa eller motbevisa under Zermelo-Fraenkels axiom + urvalsaxiomet.)

Låt oss nu återvända till de ändliga mängderna och visa att situationen är annorlunda här (nu i linje med vår intuition).

Sats 49 *Låt A vara en ändlig mängd och låt B vara en äkta delmängd till A. Då är B ändlig och $|B| < |A|$.*

Låt oss avsluta det här kapitlet med att återvända till de räknelagar vi intuitivt utnyttjade i kapitlets början.

Sats 50 *Låt A och B vara två disjunkta ($A \cap B \neq \emptyset$) ändliga mängder. Då är mängden $A \cup B$ ändlig och*

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

Idén i beviset är följande: Om vi använder liknelsen med måttstockar så vet vi att brädan A har en längd (vi har en måttstock som mäter dess längd) och brädan B har en längd (vi har en annan måttstock som mäter dess längd). Det vi nu vill göra är att mäta längden av brädorna A och B tillsammans; så vi lägger dem efter varandra och sedan klistrar vi ihop deras måttstockar och mäter den totala längden. Vi måste dock verifiera att två ihopklistrade måttstockar fortfarande är en måttstock.

Bevis. Låt $|A| = n$ och $|B| = k$ och låt $\phi : [n] \to A$ och $\psi : [k] \to B$ vara bijektioner (vi vet att dessa existerar ty A och B är ändliga). Vi definerar en ny funktion $\theta : [n+k] \to A \cup B$ som

$$\theta(i) = \begin{cases} \phi(i) & \text{om } i \leq n, \\ \psi(i-n) & \text{om } n < i \leq n+k. \end{cases}$$

Då är θ en bijektion $[n+k] \to A \cup B$. ■

Följdsats 51 *Låt A vara en ändlig mängd och $B \subset A$. Då gäller att*

$$|A \backslash B| = |A| - |B|\,.$$

Bevis. B är en delmängd till den ändliga mängden A alltså är B ändlig (vilket förljer av Sats 49 om B är en äkta delmängd, och om B råkar vara hela A är mängderna samma mängd och följdaktligen är B ändlig). $A \backslash B$ är en delmängd till A, alltså är $A \backslash B$ ändlig. $A \backslash B$ och B är två disjunkta ändliga mängder, alltså ger föregående sats att

$$|(A \backslash B) \cup B| = |A \backslash B| + |B| \, ,$$

men $(A \backslash B) \cup B = A$ alltså får vi (efter omordning av termerna)

$$|A \backslash B| = |A| - |B| \, .$$

■

Följdsats 52 *Låt A och B vara två ändliga mängder. Då är $A \cup B$ ändlig och*

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

Bevis. Notera att $A \cup B = A \cup (B \backslash A)$. Enligt antagandet är A en ändlig mängd. Vi visar härnäst att mängden $B \backslash A$ är också ändlig. Vi skriver

$$B \backslash A = B \backslash (A \cap B) \tag{1}$$

och noterar att B är en ändlig mängd enligt satsens antagande och mängden

$$A \cap B \subset B \tag{2}$$

alltså är $A \cap B$ en ändlig mängd. Enligt Följdsats 51 följer nu att $B \backslash A$ är ändlig. Eftersom nu A och $A \backslash B$ är ändliga mängder och $A \cap (B \backslash A) = \emptyset$ så ger Sats 50 att

$$|A \cup B| = |A \cup (B \backslash A)| = |A| + |B \backslash A| \, . \tag{3}$$

Men (1) och (2) ger

$$|B \backslash A| = |B \backslash (A \cap B)| = |B| - |A \cap B| \, .$$

Insättning av detta uttryck i (3) ger resultatet. ■

Vi kan även bestämma kardinaliteten av den kartesiska produkten av två mängder.

Sats 53 *Låt A och B vara två ändliga mängder. Då är $A \times B$ ändlig och*

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

4 Rekursivt definierade funktioner

Vår kursbok behandlar rekursion tämligen snabbt, men det ger en idé av det är för något. Det finska kurskompendiet (och den finskspråkiga parallellkursen) väljer fokusera på lite mer mängdteoretiska resultat som följer av rekursiva definitioner. Vi väljer istället att fokusera på rekursionsekvationer som är den diskreta motsvarigheten till differentialekvationer[2]. Låt oss dock börja med att definiera rekursion.

Definition 54 *Vi säger att talföljden $f(1), f(2), f(3), \ldots$ är* rekursivt definierad *om det för något heltal $a \geq 1$ gäller att*

1. *Talen $f(1), f(2), \ldots, f(a)$ är givna (begynnelsevärdena)*
2. *För varje heltal $n \geq a+1$ gäller att $f(n)$ är en funktion av $f(1), f(2), \ldots, f(n-1)$. (rekursionen).*

Det vill säga, utgående från de givna begynnelsevärdena kan vi generera hela talföljden genom att använda någon given regel (funktion). Ett exempel på detta är fakulteten.

Exempel 55 *Låt $f(0) = 1$ och för $n \geq 1$ låter vi*

$$f(n) = nf(n-1).$$

Då är talföljden $f(n)$ rekursivt definierad och

$$\begin{aligned}
f(0) &= 1, \\
f(1) &= 1 \cdot f(0) = 1, \\
f(2) &= 2 \cdot f(1) = 2 \cdot 1 = 2, \\
f(3) &= 3 \cdot f(2) = 3 \cdot 2 \cdot 1 = 6, \\
f(4) &= 4 \cdot f(3) = 4 \cdot 3 \cdot 2 \cdot 1 = 24, \\
f(5) &= 5 \cdot f(4) = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120, \\
& \quad \textit{och så vidare.}
\end{aligned}$$

Talet $f(n)$ är fakulteten *av n, och den normala notationen är $n! := f(n)$.*

Exempel 56 *Fibonaccitalen. Låt $F(0) = 0$ och $F(1) = 1$ så genererar rekursionen*

$$F_n = F_{n-1} + F_{n-2}$$

resten av Fibonaccitalen för $n \geq 2$. Början av serien ges av: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$.

[2] Bekantskap med differentialekvationer förutsätts dock ej av texten!

Vi gissar från det sätt definitionen av rekursion är skriven (samt det faktum att de behandlas nästan samtidigt i kursen!) att det finns likheter med matematisk induktion. Induktionen passar ofta som hand i handske när det gäller att bevisa egenskaper hos rekursivt definierade objekt. Som exempel tar vi en likhet som involverar Fibonaccitalen.

Exempel 57 *Visa att för alla positiva heltal*

$$\sum_{i=1}^{n} \frac{F_{i-1}}{2^i} = 1 - \frac{F_{n+2}}{2^n}. \tag{4}$$

Bassteg: *Visa att (4) gäller för $n = 1$.*

$$\begin{aligned} V.L. &= \sum_{i=1}^{1} \frac{F_{i-1}}{2^i} = \frac{F_0}{2} = 0, \\ H.L. &= 1 - \frac{F_3}{2^1} = 1 - \frac{2}{2} = 0, \end{aligned}$$

så V.L.=H.L.
Induktionshypotes: *Antag att (4) håller för $n = k$, det vill säga*

$$\sum_{i=1}^{k} \frac{F_{i-1}}{2^i} = 1 - \frac{F_{k+2}}{2^k}. \tag{Ind. hyp.}$$

Induktionssteg: *Låt oss visa att formeln gäller för $n = k + 1$, dvs. att*

$$\sum_{i=1}^{k+1} \frac{F_{i-1}}{2^i} = 1 - \frac{F_{k+3}}{2^{k+1}}.$$

$$\begin{aligned} V.L. &= \sum_{i=1}^{k+1} \frac{F_{i-1}}{2^i} = \sum_{i=1}^{k} \frac{F_{i-1}}{2^i} + \frac{F_k}{2^{k+1}} \\ &\overset{(Ind.hyp.)}{=} 1 - \frac{F_{k+2}}{2^k} + \frac{F_k}{2^{k+1}} = 1 - \frac{2F_{k+2} - F_k}{2^{k+1}} \\ &= 1 - \frac{F_{k+2} + F_{k+2} - F_k}{2^{k+1}} \overset{(*)}{=} 1 - \frac{F_{k+2} + (F_{k+1} + F_k) - F_k}{2^{k+1}} \\ &= 1 - \frac{F_{k+2} + F_{k+1}}{2^{k+1}} \overset{(*)}{=} 1 - \frac{F_{k+3}}{2^{k+1}} = H.L., \end{aligned}$$

där $(*)$ i det här beviset markerar att vi använder definitionen av Fibonaccitalen.
Slutsats: *Enligt induktionsprincipen gäller (4) för alla $n \in \mathbb{Z}^+$.*

5 Lösning av rekursionsekvationer

Kärt barn har många namn, därför går rekursionsekvationer även under namnen rekurrensekvationer och differensekvationer. Dessa är synonymer. Som sagts tidigare är rekursionsekvationer den diskreta motsvarigheten till differentialekvationer (i differentialekvationer är "tiden" kontinuerlig medan i rekursionsekvationer är "tiden" (ofta) given av de naturliga talen). Rekursionsekvationer klassificeras på ett sätt liknande differentialekvationer, klassificeringen ger oss möligheten att välja rätt metod för att lösa dem. Vi noterar också att rekursionsekvationer generellt sett inte är lösbara, dvs. det är inte möjligt att ange någon formel för det n:te elementet, utan man får vackert beräkna alla föregående $n-1$ tal innan man kan bestämma värdet på det n:te talet.

Not: Efter att ha undervisat det här materialet har det framgått att differentialekvationer inte vanligtvis påträffas i de finska gymnasiera, materialet i detta kapitel kan dels tolkas som en "kokbok" för hur man löser rekursionsekvationer, men framförallt som en källa till exempel där den diskreta matematiken kommer till använding.

5.1 Första ordningens linjära homogena rekursionsekvationer med konstanta koefficienter

En första ordningens linjär homogen rekursionsekvation med konstanta koefficienter ges allmänt av

$$a_{n+1} - da_n = 0$$

och har lösningen

$$a_n = A \cdot d^n,\ n \geq 0.$$

För att bestämma konstanten A måste ett begynnelsevillkor för rekursionsekvationen specificeras; tex. lös $a_{n+1} - da_n = 0$ om $a_0 = C$. Då ser vi att $A = C$, och lösning ges av

$$a_n = C \cdot d^n.$$

Exempel 58 *Rekursionsekvationen* $a_{n+1} = 3a_n$ *där* $a_0 = 2$ *har den allmänna lösningen* $a_n = A \cdot 3^n$. *För* $n = 0$ *får* $A \cdot 3^0 = A = 2 = a_0$, *alltså är*

$$a_{n+1} = 2 \cdot 3^n.$$

Ett mer konkret exempel är hur besparingar på banken utvecklas med konstant ränta.

Exempel 59 *Med 1% inlåningsränta hur mycket pengar finns på ett bankkonto efter 50 år om €1000 sätts in år 0? Ekvationen vi ska lösa är*

$$\begin{aligned} a_{n+1} &= 1.01 \cdot a_n, \\ a_0 &= 1000. \end{aligned}$$

Lösningen till rekursionsekvationen är $a_n = 1000 \cdot 1.01^n$*, och svaret på ges av*

$$a_n = 1000 \cdot 1.01^{50} \approx 1650.$$

5.2 Andra ordningens linjära homogena rekursionsekvationer med konstanta koefficienter

En andra ordningens linjär homogen rekursionsekvation med konstanta koefficienter kan skrivas allmänt på formen

$$a_{n+2} + c \cdot a_{n+1} + d \cdot a_n = 0. \tag{5}$$

Vi löser denna på samma sätt som en motsvarande differentialekvation ($y'' + cy' + y = 0$), nämnligen med hjälp av en karakteristisk ekvation

$$r^2 + cr + d = 0. \qquad \text{(Karakteristisk ekv.)}$$

Och precis som i fallet för differentialekvationer har vi tre fall att studera separat: den karakteristiska ekvationen kan ha två distinkta (olika) reella rötter, två lika reella rötter eller två komplexa rötter.

5.2.1 Distinkta reella rötter

Låt r_1 och r_2 vara reella rötter till (Karakteristisk ekv.) där $r_1 \neq r_2$. Då ges den allmänna lösningen till (5) av

$$a_n = Ar_1^n + Br_2^n, \text{ där } A, B \in \mathbb{R}.$$

Bevis. Testa helt enkelt om den föreslagna lösningen verkligen är en lösning genom att sätta in den i ekvationen (5) den påstås lösa.

$$\begin{aligned} a_{n+2} + ca_{n+1} + da_n &= Ar_1^{n+2} + Br_2^{n+2} + c(Ar_1^{n+1} + Br_2^{n+1}) + d(Ar_1^n + Br_2^n) \\ &= Ar_1^n(r_1^2 + cr_1 + d) + Br_2^n(r_2^2 + cr_2 + d) \\ &\overset{(Karakteristiskekv.)}{=} Ar_1^n(0) + Br_2^n(0) = 0. \end{aligned}$$

■

Exempel 60 *Fibonaccitalen ges av en rekursionsekvation av andra ordningen som är linjär, homogen och har konstanta koefficienter*

$$F_{n+2} - F_{n+1} - F_n = 0,$$
$$F_0 = 0, \ F_1 = 1.$$

Låt oss lösa den rekursionsekvationen. Vi börjar med att lösa den karakteristiska ekvation som motsvarar den givna rekursionsekvationen

$$r^2 - r - 1 = 0,$$

alltså

$$r = \frac{1}{2} \pm \sqrt{\left(\frac{1}{2}\right)^2 + 1},$$

dvs. rötterna är

$$\begin{aligned} r_1 &= \frac{1+\sqrt{5}}{2}, \\ r_2 &= \frac{1-\sqrt{5}}{2}. \end{aligned}$$

Så lösningen är

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

där A och B måste bestämmas ur begynnelsevärdena, dvs. vi ska lösa ekvationssystemet

$$\begin{aligned} F_0 &= A + B = 0, \\ F_1 &= A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 1, \end{aligned}$$

vilket ger

$$A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}.$$

Så $F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$. *Talet* $\left(\frac{1+\sqrt{5}}{2}\right)$ *kallas för övrigt för det gyllene snittet.*

5.2.2 Komplexa rötter

Antag att vi får två rötter på formen

$$r_{1,2} = x \pm iy,$$

då är den allmänna lösningen

$$a_n = Ar_1^n + Br_2^n$$

eller för att slippa de komplexa talen

$$a_n = \rho^n \left(C \cos n\theta + D \sin n\theta\right),$$

där $\rho = |r_1| = |r_2|$ och $\theta = \arg r_1 = -\arg r_2$.

Exempel 61 *Lös rekursionsekvationen*

$$\begin{aligned} &a_{n+2} - a_{n+1} + a_n = 0, \\ &a_0 = 2, \ a_1 = 1. \end{aligned}$$

Karakteristiska ekvationen är

$$r^2 - r + 1 = 0,$$

vilken har rötterna

$$r = \frac{1}{2} \pm \sqrt{\left(\frac{1}{2}\right)^2 - 1} = \frac{1}{2} \pm i\frac{\sqrt{3}}{2},$$

så

$$\begin{aligned} \rho &= |r| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1, \\ \theta &= \arg r_1 = \tan \frac{\sqrt{3}/2}{1/2} = \tan \sqrt{3} = \frac{\pi}{3}, \end{aligned}$$

så

$$a_n = 1^n \left(C \cos \frac{n\pi}{3} + D \sin \frac{n\pi}{3}\right).$$

Vi fastställer C och D genom att använda begynnelsevillkoren

$$\begin{aligned} 2 &= a_0 = C, \\ 1 &= a_1 = 2\cos\frac{\pi}{3} + D\sin\frac{\pi}{3} = 2 \cdot \frac{1}{2} + D\frac{\sqrt{3}}{2} \implies D = 0, \end{aligned}$$

så lösningen är

$$a_n = 2\cos\frac{n\pi}{3}.$$

5.2.3 Reell dubbelrot

Om $r_1 = r_2 = r$ och r är reell så ges lösningen av rekursionsekvationen av

$$a_n = Ar^n + Bnr^n,$$

där A och B som vanligt fås från begynnelsevillkoren.

5.3 Första och andra ordningens linjära inhomogena rekursionsekvationer med konstanta koefficienter

En första ordningens linjär inhomogen rekursionsekvation med konstanta koefficienter ges av

$$a_{n+1} + ca_n = f(n),$$

och en andra ordningens linjär inhomogen rekursionsekvation med konstanta koefficienter ges av

$$a_{n+2} + ca_{n+1} + da_n = f(n),$$

där $f(n)$ är en funktion av n.

Återigen finns paralleller till differentialekvationer. Man löser dessa rekursionsekvationer genom att 1) sätta $f(n) = 0$ och lösa den resulterande rekursionsekvationen, vilket ger en "homogenlösning", och sedan 2) ansätta (gissa) en partikulärlösning och visa att det är en lösning, för att 3) få den allmänna lösningen genom att addera homogen- och partikulärlösningen. Slutligen 4) bestäms konstanterna i den allmänna lösningen genom användning av begynnelsevillkoren.

Att hitta en partikulärlösning är ofta ingen lek, men om $f(n)$ är ett polynom i n kan följande "regel" användas: Om $f(n)$ är ett polynom i n ansätter vi ett allmänt polynom i n av samma grad som $f(n)$, om inte 1 är en rot till den karakteristiska ekvationen för då skall ansatsen multipliceras med n^m där m är multipliciteten till nollstället.

Exempel 62 *Antag att vi löser $a_{n+2}+ca_{n+1}+da_n = 3n^3+2n+4$ och att den karakteristiska ekvationen har rötterna $r_1 = 4$ och $r_2 = 3$. Eftersom $r \neq 1$ så ansätter vi som partikulärlösning ett polynom av grad 3 (samma som $f(n)$), dvs.*

$$a_n^{part} = An^3 + Bn^2 + Cn + D,$$

och insättning i V.L. av rekursionsekvationen låter oss bestämma A, B, C, D (om möjligt!).

Exempel 63 *Antag istället att* $a_{n+2} + ca_{n+1} + da_n = 0$ *har en dubbelrot som är* 1. *Dubbelrot är samma som multiplicitet* 2. *Om* $f(n)$ *är som i föregående exempel så ansätter vi nu* $a_n = n^2(An^3+Bn^2+Cn+D)$, *och igen ger instättning i V.L. av rekursionsekvationen oss möjligheten att bestämma* A, B, C, D *(om möjligt).*

Exempel 64 ***Hanoi Tower.*** *Rekursionsekvationen för detta spel är*

$$\begin{aligned} a_{n+1} &= 2a_n + 1, \\ a_1 &= 1. \end{aligned}$$

Den karakteristiska ekvationen för den homogena rekursionsekvationen är $a_{n+1} - 2a_n = 0$ *är*

$$\begin{aligned} r - 2 &= 0, \\ r &= 2, \end{aligned}$$

så den homogena lösningen är

$$a_n^{(h)} = A \cdot 2^n.$$

Partikulärlösning: Eftersom 1 *inte är en rot till den karakteristiska ekvationen och* $f(n) = 1$ *så ansätter vi ett polynom av grad* 0 *som partikulärlösning. Ansats:* $a_n^{(p)} = C$. *Insättning ger*

$$\begin{aligned} C &= 2C + 1, \\ C &= -1. \end{aligned}$$

Så den totala lösningen är

$$a_n = a_n^{(h)} + a_n^{(p)} = A \cdot 2^n - 1.$$

Vi använder begynnelsevärdet för att bestämma A

$$a_1 = A \cdot 2 - 1 = 1,$$

alltså

$$A = 1.$$

Så rekursionsekvationen har lösningen

$$a_n = 2^n - 1, \quad n \geq 1.$$

6 De naturliga talen

Under föreläsningen måndag vecka 48 ägnades en timme åt att diskutera hur man konstruerar de naturliga talen utgående från vad vi lärt oss i mängdläran. Detta är kursivt material och skall snarast ses som en orientering. Vår kursbok behandlar ämnet tämligen utförligt i Kapitel 4, men jag valde att börja "lite tidigare i historien" än vad boken gör - som börjar med Peanoaxiomen. Vår framställning följer den i [P.R. Halmos, *Naive Set Theory*, New York: Van Nostrand, 1960].

OBS: I kursboken definieras de naturliga talen så att 1 är det första naturliga talet, medan vi har definierat det som 0.

Att definiera de naturliga talen är av samma natur som att definiera en meter eller som vi tidigare sett definiera kardinaliteten av en mängd. Vi börjar helt enkelt med att definiera vad 0 är och bygger sedan upp de naturliga talen med en induktiv definition. Enligt mängdlärans axiom existerar den tomma mängden, så låt oss definiera noll på följande sätt.

Definition 65 *Låt*

$$0 := \emptyset.$$

Sedan skapar vi med hjälp av mängdoperationen $\cup$ en ny mängd från den tomma mängden (mängdlärans axiom ger att unionen av två mängder är en ny mängd) enligt följande definition.

Definition 66 *Om x är en mängd så är dess* efterföljare

$$s(x) = x \cup \{x\}.$$

Så efterföljaren till 0 blir

$$s(0) = 0 \cup \{0\} = \emptyset \cup \{\emptyset\}.$$

För att inte skapa problem för oss själva väljer vi att kalla efterföljaren till 0 för 1 (kanske detta är ett *naturligt* val??)

$$1 := s(0),$$

och vi fortsätter genom att definiera efterföljaren till 1 som 2

$$2 := s(1) = 1 \cup \{1\} = (\emptyset \cup \{\emptyset\}) \cup \{\emptyset \cup \{\emptyset\}\},$$

och

$$3 := s(2),$$

och så vidare.

Intuitivt ser vi att vi kan skapa alla de naturliga talen på det här sättet, men slutklämmen "och så vidare" är inte tillräckligt för att tillfredställa alla. Vad som krävs är ett axiom:

Oändlighetsaxiomet: Det finns en mängd som innehåller 0 och alla dess efterföljare.

Definition 67 *En mängd A är en* efterföljarmängd *om* $0 \in A$ *och om* $s(x) \in A$ *då* $x \in A$.

(Uppgift 4 på Övningsblad 1 efterfrågade ett exempel på en efterfjöljarmängd!)

Oändlighetsaxiomet garanterar att det existerar en efterföljarmängd A. De naturliga talen $\mathbb{N}$ definierar vi som snittet av alla efterföljarmängder (de naturliga talen är den minsta efterföljarmängden).

Vi har nu konstruerat, via en induktiv definition, mängden av de naturliga talen $\mathbb{N}$. Den här mängden saknar dock ännu de egenskaper vi förväntar oss att de naturliga talen har, framförallt finns här ännu ingen aritmetik (addition, multiplikation, subtraktion och division (de två sistnämnda är lite svårare att definiera)). Definitionen av addition och multiplikation är också induktivt (eller rekursivt) definierad och vilar på Peanoaxiomen. Axiomen samt addition och multiplikation med dess tillhörande räkneregler finns beskrivna på ett bra sätt i inledningen av Kapitel 4 i kursboken.

7 Kombinatorik

Kombintorik är konsten att räkna hur många möjligheter man har att göra ett val av något slag. Den baserar sig på två enkla principer: summationsprincipen och multiplikationsprincipen. Vi har nog redan en känsla för resultaten av de här två principerna, men nu ska vi även se kopplingen till mängdläran. Vi börjar med summationsprincipen.

7.1 Summationsprincipen

Låt oss börja med ett exempel.

Exempel 68 *Antag att Helsingfors universitet under en termin ger 2 matematikkurser på svenska och 3 kurser inom datavetenskap på svenska. Vi konstaterar att det finns 5 svenskspråkiga kurser att välja bland. Med andra ord om Kalle ska läsa en kurs, kan han välja vilken som helst av de fem kurserna. Detta är kontentan av summationsprincipen.*

Summationsprincipen säger att om ett val kan göras på m sätt och ett annat val kan göras på n sätt, och om dessa val inte kan göras samtidigt, så finns det totalt $m+n$ möjliga val. I termer av mängder så säger summationsprincipen, som vi formulerat den, att om A och B är två mängder sådana att $|A| = m$ och $|B| = n$ och $A \cap B = \emptyset$ så är

$$|A \cup B| = |A| + |B| = n + m,$$

så om vi ska välja ett element ur $A \cup B$ så kan vi välja bland $n + m$ element (valet kan göras på $n + m$ sätt).

Om mängderna A och B helt eller delvis innehåller samma element så är antalet element vi kan välja ur $A \cup B$ inte lika stort, vi har tidigare bevisat att

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

Jämför med

Exempel 69 *Kalle vill köpa en dagstidning. Han kan köpa den från Tidningsbyrån eller Tidningskiosken. På Tidningsbyrån har de Helsingin Sanomat och Hufvudstadsbladet. På Tidningskiosken säljer de Hufvudstadsbladet och Borgåbladet. Kalle kan alltså välja bland tre dagstidningar (inte fyra).*

7.2 Multiplikationsprincipen

Vi börjar igen med ett exempel.

Exempel 70 *Vi fortsätter att följa Kalle från Helsingfors universitet i det tidigare exemplet. Han får veta att hans studieplan förutsätter att han under den innevarande terminen läser en matematikkurs och en kurs i datavetenskap. På hur många sätt kan han välja dessa två kurser? Matematikkursen kan väljas på 2 sätt och datakursen på 3 sätt. Det finns alltså*

$$2 \cdot 3 = 6$$

olika kombinationer av kurser att välja bland. Om vi kallar mattekurserna M1,M2, och datakurserna för D1,D2,D3, så är de sex möjligheterna till kursval som Kalle har: M1 och D1, eller M1 och D2, eller M1 och D3, eller M2 och D1, eller M2 och D2, eller M2 och D3.

Om vi ska göra två val i tur och ordning, och det första valet kan göras på m sätt och det andra valet på n sätt så finns det $m \cdot n$ sätt att göra valen i tur och ordning. Precis som för summationsprincipen så har detta sin motsvarighet inom mängdläran. Om A och B är två mängder sådana att $|A| = m$ och $|B| = n$ så är

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

vilket vi såg i Sats 53.

Den här satsen, dvs. multiplikationsprincipen kan generaliseras till ett ändligt antal mängder.

Sats 71 *Låt $k \in \mathbb{N}$, och låt $A_1, \ldots, A_k$ vara k stycken ändliga mängder. Då är antalet element i den kartesiska produkten av dessa*

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1| |A_2| \cdots |A_k| = \prod_{i=1}^{k} |A_i|. \tag{6}$$

Den här satsen bygger på en rekursiv definition av kartesisk produkt och induktion, vi ger beviset för fullständighetens skull.

Bevis. Innan vi påbörjar induktionsbeviset måste vi generalisera begreppet *ordnat par* som vi nyttjat för att beskriva elementet i en kartesisk produkt av två mängder. Vi kallar ett element i den kartesiska produkten av n mängder för en ordnad *n-tett* (jämför kvartett, kvintett osv.). Dessa definieras också rekursivt utgående från de ordnade paren

$$(x_1, x_2, \ldots, x_{n+1}) := ((x_1, x_2, \ldots, x_n), x_{n+1}).$$

Med hjälp av induktion kan man visa att n-tetten är väldefinierad och att

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$$

om och endast om

$$x_i = y_i \quad \forall i = 1, \ldots n.$$

Vi lämnar denna del av beviset som övning och bevisar nu satsen med hjälp av induktion.

Bassteg: För $n = 1$ är (6) sann ty $|A_1| = |A_1|$.

Induktionsantagande: Antag att (6) gäller för $n = k$.

Induktionssteg: Vi visar att (6) gäller för $n = k + 1$. Per definition

$$\begin{aligned} &|A_1 \times A_2 \times \cdots \times A_k \times A_{k+1}| = \\ &|\{(a_1, a_2 \ldots, a_k, a_{k+1}) : a_i \in A_i \quad \forall i = 1, \ldots k+1\}|, \end{aligned}$$

och via den rekursiva definitionen av n-tett finner vi

$$\begin{aligned} & |A_1 \times A_2 \times \cdots \times A_k \times A_{k+1}| = \\ = \; & |\{((a_1, a_2 \ldots, a_k), a_{k+1}) : a_i \in A_i \quad \forall i = 1, \ldots k \ \text{ och } a_{k+1} \in A_{k+1}\}| \\ = \; & |\{((a_1, a_2 \ldots, a_k), a_{k+1}) : (a_1, a_2 \ldots, a_k) \in A_1 \times \ldots \times A_k \ \wedge a_{k+1} \in A_{k+1}\}|. \end{aligned}$$

Vi kallar $(a_1, a_2 \ldots, a_k) = b$ och $A_1 \times \ldots \times A_k = B$ så att

$$|A_1 \times A_2 \times \cdots \times A_k \times A_{k+1}| = |B \times A_{k+1}|.$$

Sats 53 ger oss då att

$$\begin{aligned} |A_1 \times A_2 \times \cdots \times A_k \times A_{k+1}| &= |B \times A_{k+1}| = |B| \cdot |A_{k+1}| \\ &= |A_1 \times \ldots \times A_k| \cdot |A_{k+1}|, \end{aligned}$$

och induktionshypotesen ger oss då

$$|A_1 \times A_2 \times \cdots \times A_k \times A_{k+1}| = |A_1| |A_2| \cdots |A_{k+1}|$$

vilket bevisar induktionssteget.

Det följer av induktionsprincipen att (6) gäller för alla $n \geq 1$. ■

Låt oss se ett exempel på hur vi kan använda multiplikationsprincipen.

Exempel 72 *En finsk registreringsskylt för bilar ges på formen ABC·123 (förutom om det är en veteranbil, men vi bortser från dessa). Hur många bilar kan registreras i Finland (dvs. hur många olika registreringsskyltar finns det)?. Alfabetet har 29 bokstäver, men å,ä och ö används inte i registreringsskyltar, och sedan finns 10 siffror. Vi väljer de tre bokstäverna och de tre siffrorna i tur och ordning, och multiplikationsprincipen ger att det finns*

$$26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17576000$$

stycken möjliga registreringsskyltar.

Av multiplikationsprincipen följer detta resultat.

Följdsats 73 *Låt A vara en mängd med $|A| = k$. Då är kardinaliteten av dess potensmängd $|P(A)| = 2^k$.*

Bevis. Låt $A = \{a_1, a_2, \ldots, a_k\}$. Vi söker $|P(A)|$, vilket är samma som antalet delmängder i mängden A. För att skapa en godtycklig delmängd till mängden A bestämmer vi i tur och ordning om elementet a_1 ska finnas med i delmängden eller inte, om elementet a_2 ska finnas med i delmängden eller inte, … , om elementet a_k ska finnas med i delmängden eller inte. Vi måste alltså fatta k stycken val av typen Ja/Nej. Enligt multiplikationsprincipen finns det

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{k \text{ termer}} = 2^k$$

sätt att göra dessa val. Det går alltså att skapa 2^k olika delmängder till A, och följdaktligen

$$|P(A)| = 2^k.$$

■

7.2.1 Mer om oändliga mängder

Låt oss ta en liten avstickare från kombinatoriken av ändliga mängder och konstatera att

Sats 74 *Föregående sats gäller även för numrerbart oändliga mängder,*

$$|P(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}.$$

Anmärkning 75 *Det finns övernumrerbart oändligt många delmängder till de naturliga talen:* $|P(\mathbb{N})| > |\mathbb{N}|$.

Cantor gav ett argument (diagonal argumentet) för att $|P(\mathbb{N})| > |\mathbb{N}|$. I korthet går det ut på följande. Vi såg tidigare att vi skapar delmängder av en mängd genom att fatta ett Ja/Nej beslut om vart och ett av dess element ska finnas med i delmängden. Stringent betyder det här att det finns en bijektion

$$P(A) \to \{0,1\}^k\,,$$

där $Ja = 0$ och $Nej = 1$. Så en delmängd i A kan representeras som en ordnad k-tett (0,1,1,...,1) av ettor och nollor. Om $A = \mathbb{N}$ så finns det numrerbart oändligt många element i A och därför blir $k-$ tetten av ettor och nollor en oändligt lång sträng av nollor och ettor.

Låt oss nu anta att $P(\mathbb{N})$ är numrerbart oändlig. Det betyder att vi kan skriva en lista med dess delmängder uppradade en efter en [varje rad i matrisen motsvarar en delmängd] (det blir så klart numrerbart många rader av dessa strängar eftersom vi antagit att $P(\mathbb{N})$ är numrerbart oändlig), tex. (varje rad är en delmängd, där 0 resp 1 avgör om motsvarande tal i $\mathbb{N}$ ska vara med i delmängden)

$$\begin{array}{cccccccc}
\mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
1 & \mathbf{1} & 1 & 1 & 1 & 1 & 1 & \ldots \\
0 & 1 & \mathbf{0} & 1 & 0 & 1 & 0 & \ldots \\
1 & 0 & 1 & \mathbf{0} & 1 & 0 & 1 & \ldots \\
1 & 1 & 1 & 0 & \mathbf{1} & 1 & 1 & \ldots \\
0 & 0 & 0 & 1 & 0 & \mathbf{0} & 0 & \ldots \\
1 & 1 & 0 & 0 & 1 & 1 & \mathbf{0} & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

där den ordning vi valt att lista delmängderna inte spelar någon roll. Om $P(\mathbb{N})$ är numrerbar så finns alla delmängder med i listan. Men Cantor visade att om vi väljer en sträng $\xi = (1,0,1,1,0,1,1,\ldots)$ sådan dess element är negationen av de fetmarkerade diagonalelementen i matrisen (första diagonalelementet i matrisen är 0 alltså väljer vi att börja vår sträng med 1, andra diagonalelementet i strängen är 1 alltså väljer vi att sätta 0 som andra elementet i vår sträng, osv.) så finns den här strängen inte med i listan! ξ har minst ett element som är olika med strängarna på varje rad (nämnligen diagonalelementet). Alltså är är listan inte komplett och antagandet att $P(\mathbb{N})$ är numrerbart oändlig är alltså falsk.

Låt oss återvända till kombinatoriken av ändliga mängder.

7.3 Permutationer

En permutation är *val utan återläggning med hänsyn till ordning.*

Exempel 76 *Antag att du har en kruka med 5 bollar numrerade från 1 till 5. Först ska en boll dras för att utse vinnaren i ett lotteri och sedan ska en till boll dras för att utse vem som får tröstpriset. Ordningen spelar alltså roll. Multiplikationsprincipen ger att antalet permutationer är* $5 \cdot 4 = 20$*, det finns 5 möjligheter att dra första bollen och sedan finns det fyra bollar kvar i krukan när nästa boll dras, alltså är antalet möjligheter 4. Det finns totalt 20 sätt (permutationer!) att utse en vinnare och tröstpristagare.*

Återigen finns en koppling till mängdläran, antalet permutationer av r element ur n möjliga är antalet ordnade r-tetter där alla element är distinkta. Se diskutionen i boken. Antalet permutationer av r element ur n möjliga ges av

$$n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!},$$

och om vi ska permutera alla n element, dvs. $r = n$ får vi att antalet permutationer är $n!$ ty $0! = 1$ per definition. Boken har några bra exempel på när permutationer kommer till använding. Läs dem!

Boken nämner dock inte permutationer av bokstäver i ord (utom flyktigt bland övningarna).

Exempel 77 *Antalet permutationer av bokstäverna i SENAPTUB är* $8!$ *eftersom vi permuterar alla 8 bokstäverna S,E,N,A,P,T,U,B.*

Exempel 78 *Hur många "ord" på fyra bokstäver kan vi skapa med bokstäverna i SENAPTUB? Här är det en permutation av 4 element ur 8, så svaret ges av*

$$\frac{8!}{(8-4)!} = 1680 \text{ stycken.}$$

Låt oss nu titta på ett exempel av permutationer av ord där vissa bokstäver förkommer flera gånger.

Exempel 79 *Hur många permutationer finns det av bokstäverna i APA? Vi vet från exemplet ovan att om bokstäverna hade varit olika, säg att vi skriver* A_1PA_2 *så finns det* $3! = 6$ *permutationer, dessa är*

$$A_1PA_2,\ A_1A_2P,\ A_2PA_1,\ A_2A_1P,\ PA_1A_2,\ PA_2A_1,$$

men eftersom vi betraktar $A_1 = A_2 = A$ *som samma bokstav så är inte alla dessa permutationer distinkta, utan de som är distinkta är*

$$APA,\ AAP \text{ och } PAA.$$

Vi ser att det för vart och ett av dessa finns två motsvarande permutationer om vi betraktar $A_1 \neq A_2$. *Detta är ingen slump! Det vi har upptäckt är att för att få antalet permutationer av ett ord som* APA *så betraktar vi först alla bokstäver som distinkta men sedan måste vi dividera med antalet* inbördes *permutationer av de bokstäver som är lika. Alltså i det här exemplet är antalet permutationer av* APA

$$\frac{3!}{2!} = 3,$$

där $3!$ *är antalet permutationer av* A_1, A_2, P *och* $2!$ *är antalet inbördes permutationer av de två A:na.*

Låt oss titta på ytterligare exempel av den här typen.

Exempel 80 *Hur många permutationer finns det av ordet PAPP? Från förra uppgiften vet vi att antalet permutationer är*

$$\frac{4!}{3!} = 4,$$

där $4!$ *är antalet permutationer av 4 olika bokstäver, och divisionen med* $3!$ *kommer från att det finns* $3!$ *många inbördes permutationer av* P *:na.*

Vårt generalexempel hämtar vi från seriernas värld.

Exempel 81 *Hur många permutationer finns det av ordet BARBAPAPPA? Här har vi 2 B, 1 R, 4 A, 3P alltså totalt 10 bokstäver. Antalet permutationer blir*

$$\frac{10!}{2!1!4!3!},$$

där fakulterna i nämnaren är antalet inbördes permutationer av de respektive bokstäverna av samma typ.

7.4 Kombinationer

Fråga 82 *Antag att det finns 11 cricketspelare i Helsingfors, på hur många sätt kan man välja ett cricketlag bestående av 11 spelare från dessa?*

Svar 83 *På ett sätt! Man måste välja alla 11 spelare!*

Nu kommer vi till kombinationer som är *val utan återläggning och utan hänsyn till ordning.*

I boken visas att antalet kombinationer av r element av totalt n möjliga är samma sak som att beräkna hur många delmängder med just r element som kan bildas ur en mängd med kardinalitet n. Se boken för diskution, se särskilt hur man härleder formeln för antalet kombinationer av r element ur n med hjälp av multiplikationsprincipen och antalet permutationer av r element ur n.

Antalet kombinationer av r element ur n ges av formeln

$$\frac{n!}{r!(n-r)!}.$$

För att förenkla notationen definierar vi

$$\binom{n}{r} := \frac{n!}{r!(n-r)!}$$

vilket utläses "n över r". $\binom{n}{r}$ kallas även för binomialkoefficient. Boken har bra exempel på situationer där kombinationer används. En av de viktigaste tillämpningarna av kombinationer är binomialsatsen. Kontrollera att du förstår hur beviset fungerar! Än viktigare är att kunna tillämpa satsen.

Låt oss tillföra två exempel till kapitlet om kombinationer.

Exempel 84 *Bridge är ett kortspel som spelas med en vanlig kortlek (som har 52 kort). En bridgehand består av 13 kort.*
a) Hur många bridgehänder finns det? Här spelar ordningen man får korten i ingen roll, huvudsaken är att man får 13 kort, så antalet bridgehänder är

$$\binom{52}{13} = \frac{52!}{13!(52-13)!}.$$

b) Hur många av dessa bridgehänder innehåller exakt 2 kungar (det finns 4 kungar i en kortlek). Vi löser problemet genom att först bestämma på hur *många sätt vi kan välja 2 kungar bland 4 möjliga, antalet sätt att göra detta är*

$$\binom{4}{2}$$

sedan kan vi välja de resterande 11 korten till bridgehanden nästan fritt - vi måste bara plocka bort de två kvarvarande kungarna (så att bridgehanden inte får mer än 2 kungar), så de resterande 11 korten väljs bland 48 möjliga, alltså

$$\binom{48}{11}.$$

Multiplikationsprincipen ger slutligen att antalet bridgehänder med exakt två kungar är

$$\binom{4}{2} \cdot \binom{48}{11}.$$

Exempel 85 *Hur många omordningar av ordet KALAS är sådana att inga A står bredvid varandra? Vi börjar med att plocka bort båda A:na och se hur många permutationer av de kvarvarande bokstäverna K,L,S vi har, det finns* 3! *sådana. Ett exempel på en sådan permutation är*

$$_\wedge L_\wedge K_\wedge S_\wedge$$

där vi också markerat de positioner där bokstäverna A kan stå. För den givna permutationen finns $\binom{4}{2}$ *val av platser där de två A:na inte står bredvid varandra (vi väljer två platser bland 4, och de ges av en kombination eftersom ordningen av A:na inte spelar någon roll). Multiplikationsprincipen ger att antalet "ord" som kan bildas av KALAS utan att två A står bredvid varandra är*

$$3!\binom{4}{2} = 3!\frac{4!}{2!(4-2)!} = 36.$$

7.5 Antal funktioner mellan två mängder

Exempel 86 *Hur många funktioner* $f : A \to B$ *finns det? Definitionen av funktion säger att till varje* $a \in A$ *ska det finnas ett entydigt funktionsvärde* $f(a) \in B$. *Antag att* $A = \{a_1, a_2, \ldots, a_k\}$. *Vi börjar med att välja funktionsvärdet av* a_1, *dvs. vi kan välja värdet av* $f(a_1)$ *på* $|B|$ *sätt (vi kan välja vilket värde i värdemängden B som helst). Sedan väljer vi funktionsvärdet av* a_2, *detta kan också väljas på* $|B|$ *sätt eftersom inget hindrar att vi avbildar* a_2 *på samma element som* a_1 *avbildades på. Vi finner att funktionsvärdet* *på vart och ett av elementen i definitionsmängden A kan väljas på $|B|$ sätt, därför ges antalet funktioner $f : A \to B$ av*

$$|B|^{|A|},$$

enligt multiplikationsprincipen.

Exempel 87 *Hur många injektioner $f : A \to B$ finns det? Detta kräver att $|A| \leq |B|$. Enligt definitionen är f en injektion om $f(x) = f(y) \Rightarrow x = y$. Detta betyder att för varje $a_i \in A$ (för varje värde i definitionsmängden) ska vi välja ett* unikt *värde i värdemängden (detta är alltså ett val utan återläggning men med hänsyn till ordning!). Antalet injektioner är alltså samma sak som antalet permutationer av $|A|$ element bland $|B|$, dvs.*

$$\frac{|B|!}{(|B| - |A|)!}.$$

Exempel 88 *Det är betydligt svårare att räkna antalet surjektioner $f : A \to B$ och därför ger vi för fullständighetens skull bara svaret. Om $|A| = m$ och $|B| = n$, med $m \geq n$, så ges antalet surjektioner $f : A \to B$ av*

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

Exempel 89 *Hur många bijektioner $f : A \to B$ finns det? Först och främst måste $|A| = |B|$ för att en bijektion ska kunna existera. För det andra så är varje injektion från A till B också en bijektion om $|A| = |B|$. Av detta följer att vi kan sätta in värdet $|A| = |B|$ i formeln för antalet injektioner från A till B för att få antalet bijektioner $f : A \to B$, dvs.*

$$|A|!.$$

7.6 Stirlings formel

När vi beräknar antalet kombinationer eller permutationer i exempel hämtade från verkligheten så slutar det ofta med att man måste handskas med fakulteter av stora tal. Och om ett tal är stor så är dess fakultet JÄTTESTOR! Så stor att de flesta miniräknare ofta kroknar innan man nått fakulteten av 200. För att kunna hantera fakulteten av stora tal finns Stirlings formel som beskriver hur fakulteten beter sig *asymptotiskt* när $n \to \infty$. Stirlings formel är

$$\lim_{n \to \infty} \frac{n!}{(2\pi n)^{1/2} e^{-n} n^n} = 1.$$

Vi kan nyttja den här formeln för att approximera $n!$ för stora n

$$n! \simeq (2\pi n)^{1/2} e^{-n} n^n.$$

8 Grafer

Grafteorin sägs ha börjat med Leonard Eulers studie av broarna i Königsberg 1736. Euler löste då gåtan som hade gäckat invånarna i Königsberg under en längre tid - kunde man göra en vandring runt stadskärnan och bara gå en gång över varje av de sju broarna och ändå komma hem igen? Euler bevisade att detta är omöjligt.

Vår kursbok behandlar grafer på ett tämligen koncist sätt (hoppa över stycket som handlar om grannmatriser). Inom grafteorin finns mycket notation och nomenklatur för att beskriva grafer eller dess egenskaper. Studera bokens definitioner, tex. definitionerna av väg, enkel väg, cykel, enkel cykel, grad, sammanhängande graf, delgraf, inducerad delgraf, maximalt sammanhängande, komponent, de speciella delgraferna: n-vägen, den fullständiga grafen K_n, bipartita grafer, fullständiga bipartita grafer $K_{m,n}$, multigraf.

Fråga 90 *Finns det någon graf som har en delgraf som är maximalt sammanhängande och inte inducerad?*

Svar 91 *I figuren finns ett exempel på den sökta delmängden.*

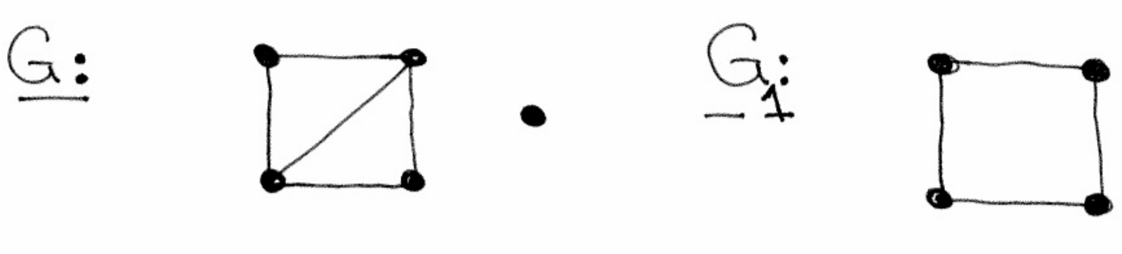


Figure 1: I figuren visas en graf G som har en delgraf G_1 som är maximalt sammanhängande och inte inducerad.

Vi noterar att den fullständiga grafen K_n i någon mån kan anses vara universum till en graf med n noder. Vi kan nämnligen definiera komplementet (detta gäller inte multigrafer) av en graf G på följande sätt.

Definition 92 *Komplementet av en oriktad graf $G = (V, E)$ är*

$$G^c = (V, \{(x, y) : (x, y) \notin E \wedge x \neq y\}).$$

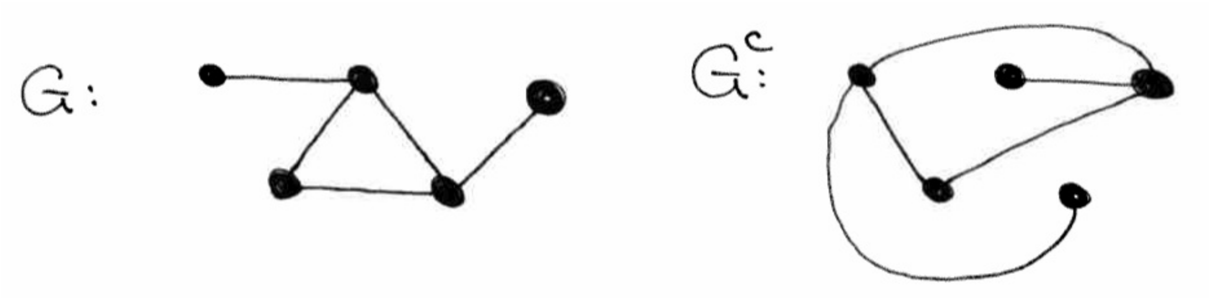


Figure 2: I figuren visas ett exempel på en graf G med 5 noder och dess komplement G^c (i K_5).

Komplementet till grafen $G = (V, E)$, där $|V| = n$, består alltså av alla kanter i K_n som inte finns i grafen G.

I Figur 2 finns ett exempel på en graf och dess komplement.

Sats 93 *Låt $G = (V, E)$ vara en graf. Om G inte är sammanhängande så är G^c sammanhängande.*

Bevis. Om $G = (V, E)$ inte är sammanhängande så består G av ett antal komponenter, $G_1, \ldots, G_k$. Låt oss för enkelhetens skull anta att $k = 2$. Då har vi två komponenter $G_1 = (V_1, E_1)$ och $G_2 = (V_2, E_2)$ där $V_1 \cap V_2 = \emptyset$ och $V_1 \cup V_2 = V$ och $E_1 \cup E_2 = E$ och $E_1 \cap E_2 = \emptyset$. Det finns alltså inga kanter som sammanbinder någon nod i G_1 med någon nod i G_2. Betrakta nu komplementet $G^c = (V, E')$ där E' innehåller alla kanter som inte finns i E. Detta betyder att i komplementet G^c är *varje* nod i nodmängden V_1 är sammanbunden med kanter till *alla* noder i nodmängden V_2. Detta medför att grafen G^c är sammanhängande. ■

8.1 Isomorfa grafer

Isomorfi betyder "likhet upp till omdöpning", så två isomorfa grafer är i strikt mening inte identiskt lika, men i allt väsentligt är det "samma graf". Isomorfi är ett viktigt koncept inom matematiken. Formellt definieras en isomorfi på följande sätt.

Definition 94 *Låt $G_1 = (V_1, E_1)$ och $G_2 = (V_2, E_2)$ vara två grafer. Om det existerar en bijektion $f : V_1 \to V_2$ sådan att $\forall x, y \in V_1$ gäller att $(x, y) \in E_1$ om och endast om $(f(x), f(y)) \in E_2$ så sägs G_1 och G_2 vara* isomorfa grafer *och f är en* isomorfi.

I boken finns ett lätt exempel på tre grafer som alla är isomorfa med varandra och två grafer som inte är isomorfa med varandra. Börja med att titta på dessa exempel.

Anmärkning 95 *En graf G är isomorf med sig själv. Isomorfin ges då av identitetsavbildningen.*

Här följer några fler exempel på grafer som inte är isomorfa respektive isomorfa, se Figur 3, Figur 4 och Figur 5.

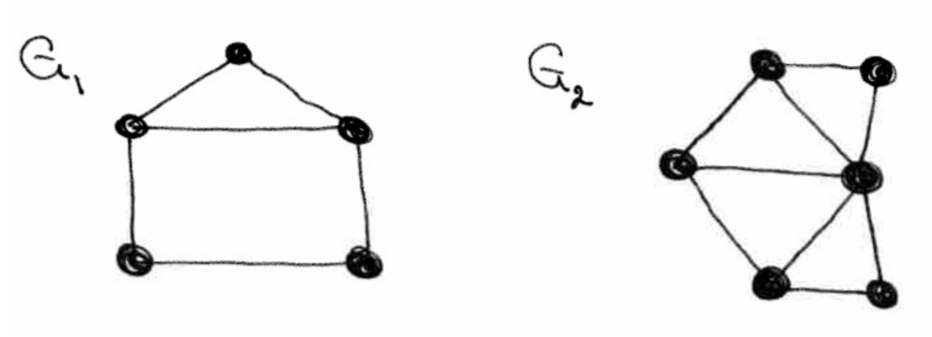


Figure 3: Graferna G_1 och G_2 är inte isomorfa eftersom de inte har samma antal noder (eller kanter).

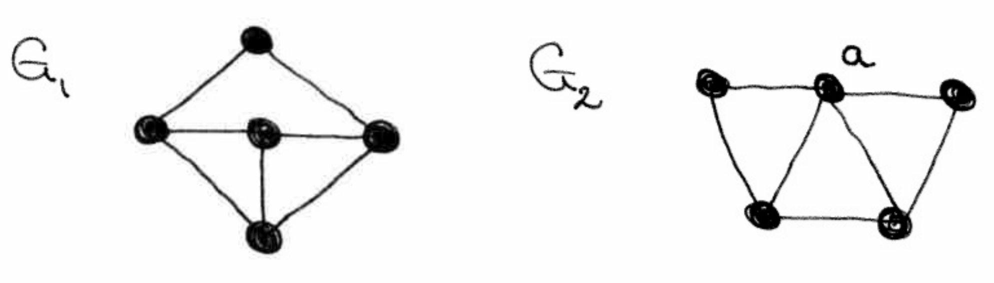


Figure 4: Graferna G_1 och G_2 är inte isomorfa efterom grafen G_2 har en nod, kallad a, som har fyra anslutande kanter (grad 4). Det finns ingen motsvarande grad i G_1 alltså är de inte isomorfa.

8.2 Eulercykler, Eulervägar och Hamiltonvägar.

Eulercykler och Eulervägar finns beskrivna i boken tillsammans med lösningen på Königbergs broar. Det är lätt att karakterisera grafer som har Eulercykler och Eulervägar med hjälp av graden på grafens noder.

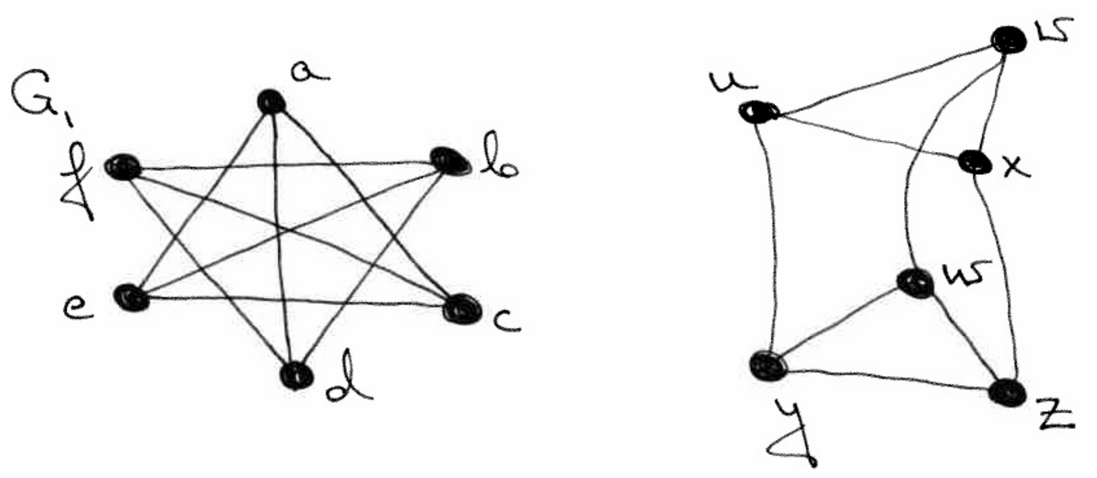


Figure 5: Graferna är isomorfa. En Isomorfi ges av: $a \mapsto v, c \mapsto x, e \mapsto u, d \mapsto w, b \mapsto y, f \mapsto z$. (notera att isomorfierna inte behöver vara unika, i det här exemplet finns flera alternativ)

Sats 96 *Låt $G = (V, E)$ vara en oriktad graf utan isolerade noder. Då har G en Eulercykel om och endast om G är sammanhängande och varje nod i G har jämnt gradtal.*

Den här satsen har ett trevligt bevis som går via induktion, läs gärna versionen som finns i kursboken (rita en bild av en graf med en Eulercykel så att du kan följa med i induktionssteget!).

Följdsats 97 *Om G är en oriktad graf utan isolerade noder så existerar en Eulerväg i G om och endast om G är en sammanhängande graf och har exakt två noder med udda grad.*

Anmärkning 98 *Eulervägen börjar och slutar i de två noderna som har udda grad. Förklara varför! (Rita en bild av en graf med en Eulerväg så klarnar kanske argumentet fortare.)*

Fråga 99 *I Figur 6 finns en schematisk bild av Gamla stan och Helgeandsholmen i Strömmen i Stockholm.*
a) Kan kungen ta en promenad under sin lunchpaus sådan att den börjar och slutar på slottet och passerar alla broar på bilden exakt en gång? Om inte, ge ett förslag på brobygge som skulle hjälpa kungen!
b) I själva verket finns två ytterligare broar utöver dem på bilden, men dessa

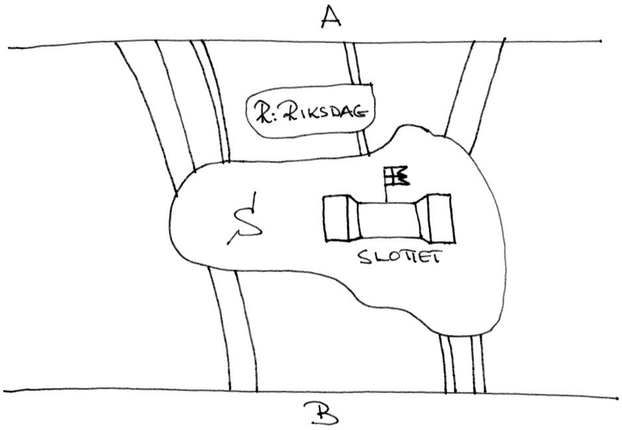


Figure 6: I figuren visas en schematisk bild av broarna runt Gamla stan i Stockholm.

får bara användas av riksdag och regering. Den ena går från riksdagen söderut till Gamla stan (där slottet ligger) och den andra går norrut från riksdagen till stranden. Antag nu att riksdagens talman har en känslig fråga att diskutera med kungen. Han vill fundera över saken och vill därför ta en lång promenad från riksdagen till slottet: kan han passera alla broar exakt en gång på vägen från riksdagen till slottet?

Svar 100 *I fråga a) efterfrågas en Eulercykel som börjar i slottet. Om man ritar en graf som motsvarar situationen i bilden, se Figur 7 a), så ser vi att noden S och noden B båda har udda grad. Ingen Eulercykel existerar alltså. Detta kan lösas genom att bygga ytterligare en bro från Gamla Stan till Södra stranden. Då får alla noder jämn grad och då existerar en Eulercykel.*
I fråga b) inför vi de två extra broarna, och motsvarande graf blir enligt Figur 7 b). Vi ser att noden R fortfarande har jämn grad, alltså finns ingen Eulerväg som börjar vid riksdagen. (Däremot finns en Eulerväg från Norra Stranden till den Södra stranden).

Anmärkning 101 *Det följer av definitionen på Eulerväg och Eulercykel att om en sådan finns i grafen så kan grafen ritas utan att man lyfter pennan från papperet.*

Vi ger några exempel på grafer som har respektive inte har Eulercykler/vägar, se Figur 8.

Utöver frågan om man kan vandra genom en graf genom att besöka dess kanter högst en gång kan man fråga sig om det går att vandra genom en

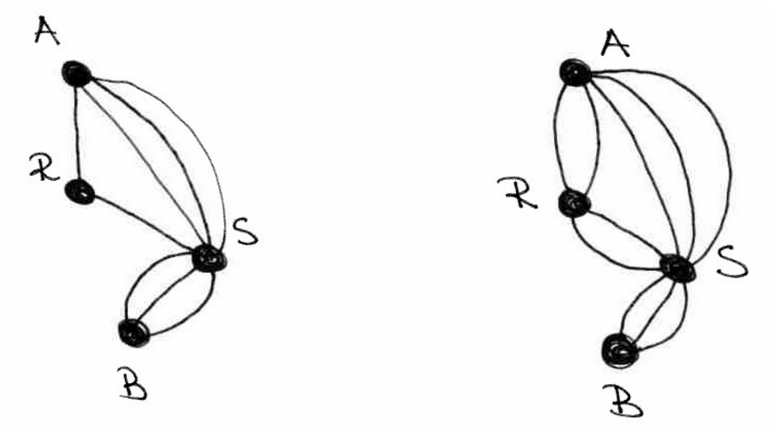


Figure 7: I a) visas en grafrepresentation av broarna i Stockholm. I b) finns riksdagshusets egna broar inkluderade i grafen.

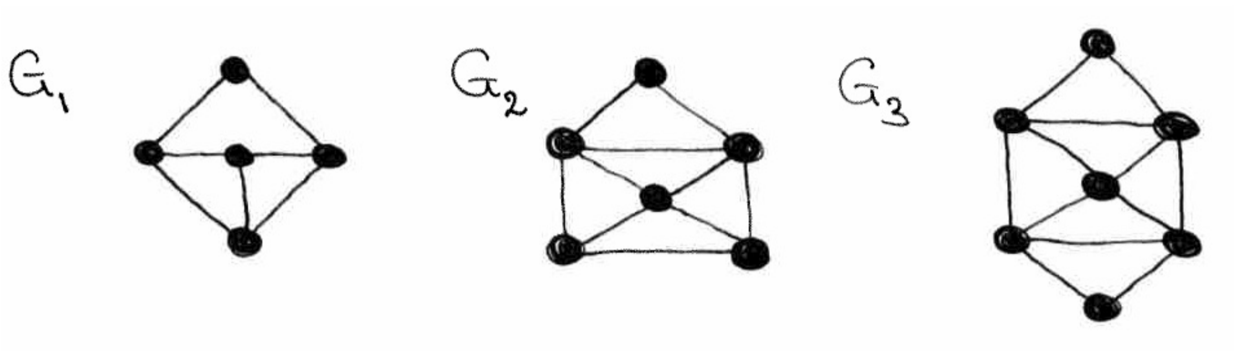


Figure 8: Grafen G_1 har ingen Eulercykel eller Eulerväg eftersom bara en av de fem noderna har jämn grad. I grafen G_2 finns det däremot en Eulerväg eftersom de två nedersta noderna har udda graf men alla övriga noder jämn. Eulervägen måste börja och sluta i noderna med udda grad. I grafen G_3 finns det en Eulercykel eftersom alla noderna har jämnt gradtal.

graf och besöka alla dess noder exakt en gång. En sådan väg kallas för en Hamiltonväg, eller om den är sluten en Hamiltoncykel.

Definition 102 *Om $G = (V, E)$ är en graf med $|V| \geq 3$ så har G en* Hamiltoncykel *om det finns en enkel cykel som innehåller alla noder i G. En* Hamiltonväg *är en enkel väg i G som innehåller alla noder.*

Exempel 103 *Alla graferna i Figur 8 har en Hamiltoncykel.*

Vi noterar att det inte finns någon känd karakterisering av grafer som innehåller Hamiltoncykler. Så medan det är lätt att bestämma om en graf har en Eulercykel så är det ett svårt problem att bestämma om en given graf har en Hamiltoncykel.

8.3 Graffärgning

Det mest kända graffärgningsproblemet är det så kallade fyrfärgsproblemet. Här är frågan om det går att färga länderna på en karta (plan karta) med enbart fyra färger, om inget land får ha samma färg som sitt grannland. Frågan ställdes redan på 1850-talet men det skulle dröja fram till 1976 innan frågan fick sitt svar med hjälp av ett så kallat datorstött bevis. Svaret är att det räcker med fyra färger.

Materialet i det stycket följer framställningen i [R. P. Grimaldi, Discrete and Combinatorial Mathematics An applied introduction, Pearson Addison Wesley, 5th ed.].

Definition 104 *Om $G = (V, E)$ är en oriktad graf så är en* äkta färgning *av G sådan att om alla noder i G har någon färg så måste två noder a och b som är sammanbundna av en kant $\{a, b\}$ ha olika färg.*

Definitionen säger att två noder som är grannar (delar en kant) måste ha olika färg. Som fyrfärgsproblemet indikerar är vi främst intresserade av det minsta antalet färger som krävs för att färga en graf. Detta leder till definitionen av en grafs kromatiska tal.

Definition 105 *Det minsta antalet färger som krävs för att åstadkomma en äkta färgning av en graf G kallas för grafen G's* kromatiska tal *och skrivs $\chi(G)$.*

Anmärkning 106 *Den här typen av färgning skiljer sig åt från det problemet som beskrevs som fyrfärgsproblemet. Här färgas inte fält som på kartan utan noder. Man kan dock använda sig av så kallade duala grafer för att skriva om färgningsproblemet av en karta som ett färgningsproblem av noderna i en graf.*

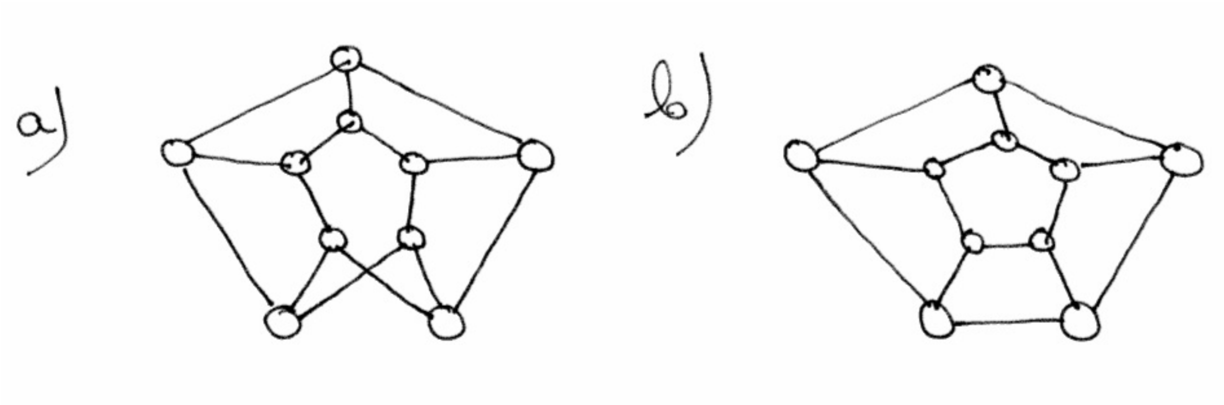


Figure 9: Grafen a) har kromatiskt tal 2 och grafen b) har det kromatiska talet 3.

Generellt sett är det ett svårt problem att bestämma det kromatiska polynomet för en graf, dvs. om G är godtycklig är det svårt att hitta $\chi(G)$. I vissa fall kan vi dock bestämma det kromatiska talet - ibland genom trial and error (fungerar om $\chi(G)$ är 2 eller kanske om det är 3, men sedan blir det snabbt svårt) och ibland genom att reducera grafer till några specialfall.

Fråga 107 *Kan du genom att testa färga graferna i Figur 9 sluta dig till att grafen i a) har* $\chi(G) = 2$ *och bilden i b) har* $\chi(G) = 3$*?*

Anmärkning 108 *Det kromatiska talet kan användas för att säga att två grafer med olika kromatiskt tal* inte *är isomorfa med varandra (som för graferna i Figur 9). Om två grafer har samma kromatiska tal kan man dock inte dra slutsatsen att graferna är isomorfa, vilket framgår av Figur 10.*

Ett verktyg vi kan använda för att bestämma en grafs kromatiska tal är ett *kromatiskt polynom.* Låt λ vara det antal färger vi kan använda för att färga en graf, och låt $P(G, \lambda)$ vara ett polynom i λ som beskriver hur många olika äkta färgningar av G som vi kan skapa med λ färger. $P(G, \lambda)$ ger alltså svaret på ett kombinatoriskt problem. Vi kallar $P(G, \lambda)$ för grafen G's kromatiska polynom. Låt oss nu titta på några exempel där vi relativt lätt kan bestämma grafens kromatiska polynom.

Exempel 109 *En* $n-$*väg kan färgas på*

$$P(G, \lambda) = \lambda\underbrace{(\lambda - 1)(\lambda - 1)\cdots(\lambda - 1)}_{n-1 \ termer} = \lambda(\lambda - 1)^n$$

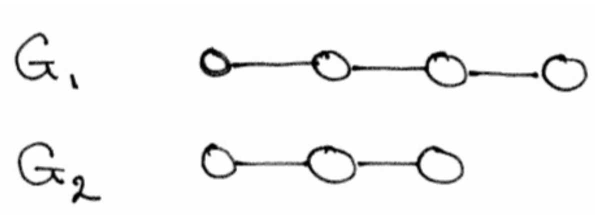


Figure 10: Dessa två grafer har samma kromatiska tal (nämnligen 2) men det är inte isomorfa. (Det kromatiska talet mäter bara en egenskap hos grafen, så bara för att två grafer har samma kromatiska tal är de inte isomorfa.)

sätt med λ färger. Vi hittar polynomet genom att konstatera att vi till den första noden kan välja vilken som helst av de λ färgerna, och sedan på nästa nod kan vi välja vilken färg som helst utom den vi valde till den första noden, alltså finns det $\lambda - 1$ färger att välja bland. På samma sätt finns det $\lambda - 1$ färger tillgängliga för varje nästkommande nod. Multiplikationsprincipen ger oss då det kromatiska polynomet. Så vad är $n-$vägens kromatiska tal? Vi testar vad det minsta antal färger är som kan åstadkomma en äkta färgning

$$\begin{aligned} P(G,0) &= 0, \\ P(G,1) &= 0, \\ P(G,2) &= 2, \end{aligned}$$

så $\lambda = 2$ är det minsta antal färger med vilka vi kan åstadkomma någon äkta färgning (i det här fallet 2 olika äkta färgningar).

Exempel 110 *n isolerade noder. Här blir det kromatiska polynomet*

$$P(G,\lambda) = \lambda^n$$

eftersom vi kan använda vilken av de λ färgerna vi vill på varje nod (eftersom de inte sammanbinds av någon kant påverkar färgvalet av en nod inte färgvalet på någon annan nod). Vad är det kromatiska talet för den här grafen? Vi använder det kromatiska polynomet som tidigare för att avgöra frågan

$$\begin{aligned} P(G,0) &= 0, \\ P(G,1) &= 1, \end{aligned}$$

så det kromatiska talet är 1 (och med denna enda färg kan vi bara åstadkomma en unik äkta färgning av grafen).

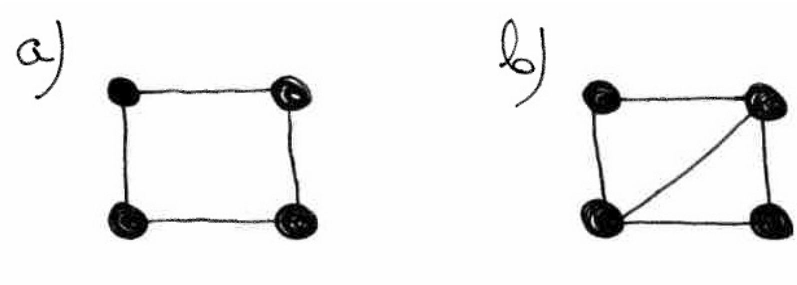


Figure 11: Både grafen i a) coh i b) är plana!

Exempel 111 *Den fullständiga grafen K_n. Att bestämma det kromatiska polynomet till det här problemet är ett permutationsproblem. Eftersom alla noder är sammanbunda med kanter med alla andra noder så måste vi välja en ny färg för varje nod som vi färglägger. Vi ska alltså bland λ färger välja n färger* utan återläggning men med hänsyn till ordning*. Detta ges av*

$$P(G, \lambda) = \frac{\lambda!}{(\lambda - n)!}.$$

Vi ser att om $\lambda < n$ så finns det inga äkta färgningar av grafen, men om $\lambda = n$ så finns det

$$P(G, n) = n!$$

stycken äkta färgningar! Så det kromatiska talet för K_n är n (och med n färger kan man åstadkomma $n!$ olika äkta färgningar).

Med dessa specialfall kan man komma ganska långt eftersom det finns tekniker för att reducera en given graf till dessa specialfall och därigenom bestämma dess kromatiska tal. Detta är ligger dock utanför vår kurs.

8.4 Plana grafer

Plana grafer är en delmängd av mängden av alla grafer.

Definition 112 *En graf G är* plan *om den kan ritas på ett plan utan att någon av dess kanter skär varandra.*

Med andra ord är alltså en plan graf en graf vars kanter enbart möts i noderna. Låt oss titta på några exempel på plana grafer, Figur 11 och Figur 12.

Som ett exempel på en graf som inte är plan studerar vi K_5, se Figur 13.

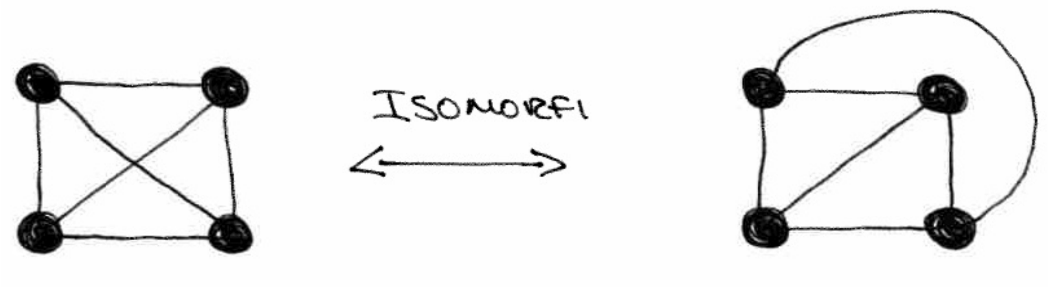


Figure 12: Även grafen till vänster är plan eftersom den är isomorf med grafen till höger vilken uppenbarligen är plan.

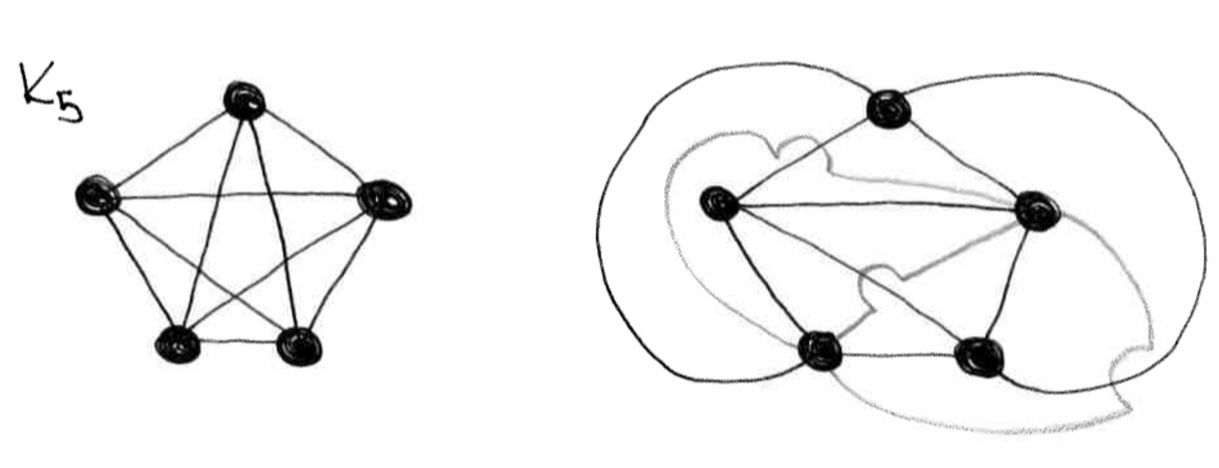


Figure 13: Grafen K_5 är inte plan. Till vänster visas ett vanligt sätt att rita grafen, och till höger har vi försökt rita grafen som en plan graf. När vi försöker dra den sista kanten (de tre försöken i ljusare färg) märker vi att det inte går att nå den andra noden utan att skära någon av de andra kanterna.

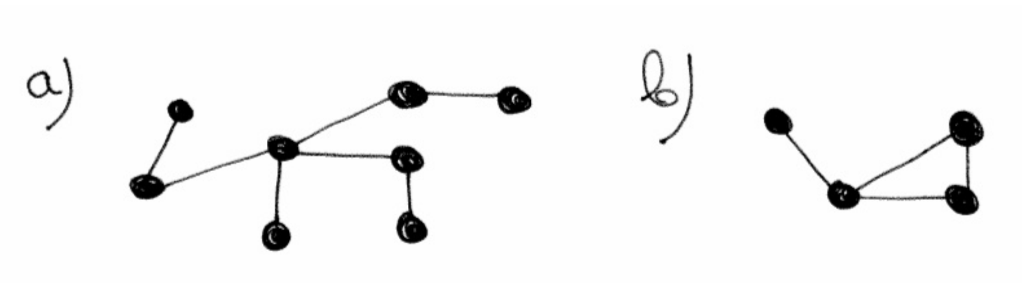


Figure 14: I figur a) finns ett exempel på ett träd, medan figuren i b) inte är ett träd.

Vi påstår att den fullständiga grafen K_5 och den fullständiga bipartita grafen $K_{3,3}$ inte är plana. Prova rita dem! En vanlig frågeställning kring $K_{3,3}$ är: Om det finns tre hushåll A, B, C och tre leverantörer av gas, vatten resp. elektricitet går det att leda dessa varor direkt från varje leverantör till varje hushåll (alla tre hushåll behöver alla tre varorna) utan att någon ledning korsar varandra? Eftersom $K_{3,3}$ inte är plan så går det inte!

Enligt följande sats av Kuratowski är graferna K_5 eller $K_{3,3}$ alltid en delgraf till en icke-plan graf.

Sats 113 (Kuratowski) *En graf G är icke-plan om (och endast om) den har en delgraf som är isomorf (homeomorf) med antingen K_5 eller $K_{3,3}$.*

En kommentar till satsen: sättet parenteserna är använda betyder att för att få "och endast om" biten så måste isomorf ersättas med "homeomorf". Vi har inte talat om begreppet homeomorfi i den här kursen och kommer inte att göra det här i anteckningarna heller, vi nöjer oss bara med att konstatera att graferna K_5 eller $K_{3,3}$ på något sätt är inblandade i alla icke-plana grafer.

8.5 Träd

I det här stycket ska vi titta på en speciell delgraf av mängden av alla grafer som har särskild relevans inom datavetenskapen; binära rotade träd. Låt oss börja med att införa sammanhängande grafer som saknar cykler.

Definition 114 *Ett* träd *är en sammanhängande graf som saknar cykler.*

I Figur 14 finns två enkla exempel på grafer där det ena är ett träd och det andra inte.

Definitionen av träd leder direkt till det här resultatet.

Sats 115 *I ett träd finns en unik enkel väg mellan varje par av noder.*

Den här satsen är bevisad i kursboken. Kortfattat kan man säga att det faktum att grafen är sammanhängande medför att det existerar en väg mellan alla par av noder, och avsaknaden av cykler medför att vägen är entydig.

Det finns flera egenskaper/karakteriseringar av träd, vi sammanfattar några av dem i en sats.

Sats 116 *För en graf G utan öglor är följande påståenden ekvivalenta*
a) G är en graf.
b) Om en kant tas bort sönderfaller G i två komponenter.
c) G saknar cykler och $|V| = |E| + 1$.
d) G är sammanhängande och $|V| = |E| + 1$.
e) G saknar cykler men om vi lägger till en kant mellan två godtyckliga noder i grafen bildas en cykel.

Det vi vill göra härnäst är att införa en hierarki i trädet, eller rättare sagt vi vill representera en hierakisk struktur med hjälp av ett träd. För att lyckas med det inför vi begreppet rotade träd. Vanligtvis är det här ett begrepp som införs för riktade träd, men vi tar en genväg och definierar rotade träd som följer.

Definition 117 *Ett träd $T = (V, E)$ med en nod $r \in V$,* roten*, är ett* rotat träd*.*

Definitionen är inte bra eftersom det enda vi egentligen har gjort är att namnge en av noderna i grafen. Vår tolkning (som inte följer av vår "light"-definition av rotat träd) är dock att ett rotat träd börjar i roten, och resten av noderna är underordnade roten. Se Figur 15.

Låt oss införa några till begrepp som finns in anslutning till träd genom Figur 16.

Om ett träd är *ordnat* så har ordningen på löven betydelse, som exempel kan vi ta ett släktträd: om man har som princip att ordna barnen till en förfader så att det äldsta barnet alltid skrivs längst till vänster och det yngsta längst till höger så har man ett ordnat träd. Om man inte följer någon sådan princip har man ett oordnat träd.

Definition 118 *Ett rotat träd $T = (V, E)$ är* binärt *om varje nod har högst två barn.*

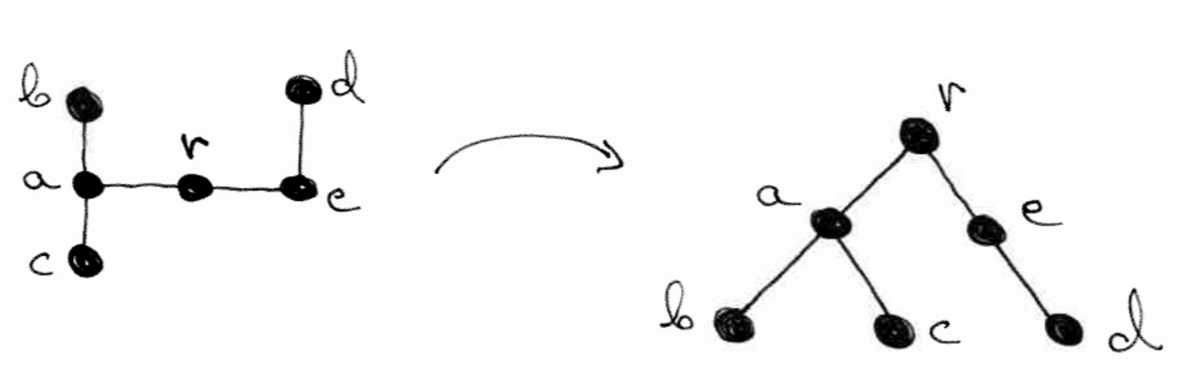


Figure 15: Till vänster visas ett träd där vi namngivit roten med r. Till höger visas samma träd men efter att vi "tagit tag i roten och lyft grafen i roten" - detta visar trädets hierarki.

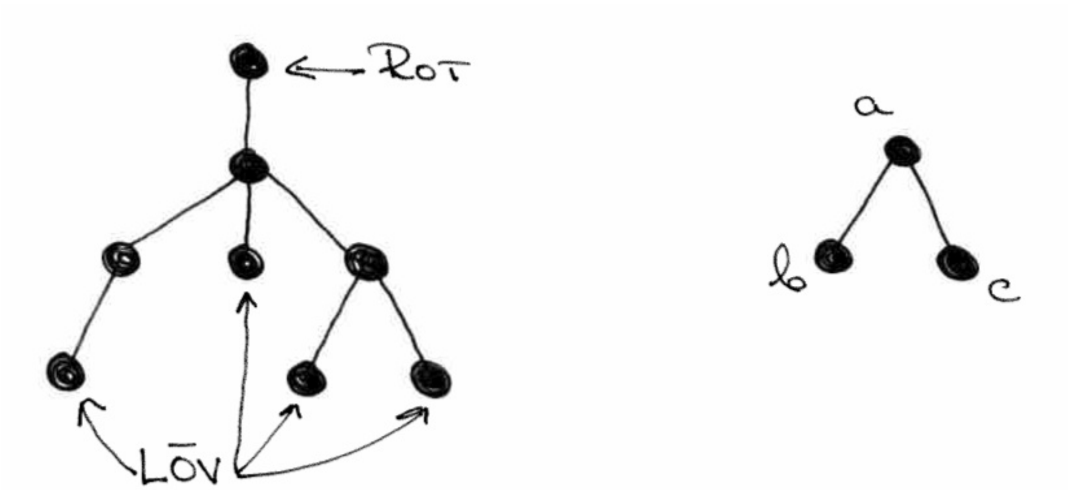


Figure 16: I figuren till vänster visas ett rotat träd med roten r placerad högst upp. De nedersta markerade noderna ("ändpunkterna") kallas för löv. De övriga noderna kallas för interna noder. I figuren till vänster visas tre noder. Benämningen intern nod är ofta för grov så då kallar man a för bs förälder, b för as barn och b och c kallas för syskon.

Trädet i Figur 16 är ett binärt träd.

Varför denna hype kring allt som är binärt? Den enkla anledningen är att våra datorer representerar all sin data binärt. (Det finns exempel på datorer som räknat i andra baser än 2 men de har varit mindre lyckade.) Låt oss titta på två tillämpningar av binära träd, först hur man representerar aritmetiska uttryck som ett binärt träd, och sedan hur man konstruerar en kodning av alfabetet.

8.6 Aritmetiska uttryck representerade som binära träd

Den notationen som vi är mest vana med när det gäller aritmetiska uttryck kallas för *infixnotation*, dvs. de aritmetiska operatorerna skrivs mellan de två operanderna, tex.

$$z(4w-3)-(7z+2), \tag{7}$$

vilket i själva verket borde skrivas

$$z \times (4 \times w - 3) - (7 \times z + 2).$$

En nackdel med infixnotationen är att den kräver parenteser för att uttrycken ska beräknas i rätt ordning. En annan nackdel är den bara fungerar för binära operationer, hur skulle man skriva en operator $\circ$ som kräver tre argument mellan argumenten? Låt oss dock hålla oss till binära operatorer.

Det finns sätt att representera samma uttryck utan parenteser, dessa är *prefixnotation* och *postfixnotation.* Andra namn på som används är polsk notation för prefixnotationen och omvänd polsk notation för postfixnotationen. Den omvända polska notationen (postfixnotationen) skrivs ofta RPN (reverse polish notation) och är det poluläraste alternativet. Om vi skriver (7) med prefixnotation blir det

$$- \times z - \times 4w3 + \times 7z2,$$

vilket vi läser från vänster till höger, och den senast lästa operationen utförs när man har läst in två argument: låt oss se hur det fungerar; vi läser först in minus, sedan gånger, sedan z (nu har vi ett argument, z, och vår senast inlästa operator är minus, så vi är beredda att subtrahera om nästa sak vi läser in är ett argument), men nu är nästa sak vi läser in ett till minustecken, vi fortsätter alltså med att läsa in gånger, och sedan 4 (nu har vi ett argument, 4, och vår senast inlästa operator är gånger, så vi är beredda att multiplicera om nästa sak vi läser in är ett argument), och nästa sak vi läser in är ett argument, nämligen w. Vi utför multiplikationen och får $4w$. Vårt minne innehåller nu $- \times z - (4w)$ där jag använt parentesen för att visa att $4w$

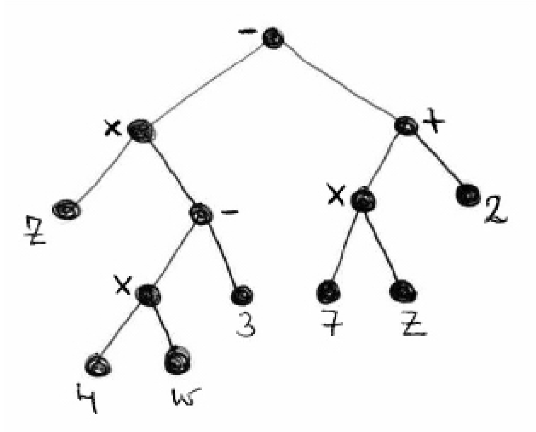


Figure 17: Figuren visar trädrepresentationen av uttrycket (7).

är *ett* argument, vi fortsätter att läsa in fler tecken från vårt uttryck på prefixnotation - nästa sak vi läser in är 3, så nu har vi igen två argument i (närminnet) $(4w)$ och 3 så vi kan utföra den senaste operationen vi läste in, nämligen minus. Uttrycket i vårt minne är nu $- \times z(4w-3)$ och vi ser att vi direkt kan utföra nästa operation som är multiplikation. Strängen i vårt minne blir $-(z(4w-3))$. Sedan fortsätter vi att läsa in tecken från prefixnotationen. Kontrollera att du får samma uttryck som vi började med!

I postfixnotationen blir samma uttryck

$$z4w \times 3 - \times 7z \times 2 + -,$$

och återigen läser vi från vänster till höger. Det fina med postfixnotationen är att vi bara behåller argument (variabler) i minnet och inga operatorer, direkt vi läser in en operator så kan vi utföra den på de två senast inlästa argumenten: låt oss se hur det går med ovanstående uttryck, vi läser in $z, 4, w$ och sedan multiplikation - den utför vi direkt och i minnet har vi $z, (4w)$ sedan läser vi in 3 så att minnet innehåller $z, (4w), 3$. När sedan minustecknet läses in utför vi operationen direkt så att listan i minnet blir $z, (4w-3)$ och när nästa tecken läses in, vilket är multiplikation så utför vi den direkt och minnet innehåller nu bara ett argument $z(4w-3)$. Fortsätt den här processen och se att du får tillbaka samma uttryck som vi började med!

Vad har nu detta med träd att göra? Uttrycket (7) kan representeras som trädet i Figur 17.

För att få prefixnotationen så börjar vi från roten och besöker noden först, sedan besöker vi barnen i tur och ordning (detta betyder att vi besöker alla

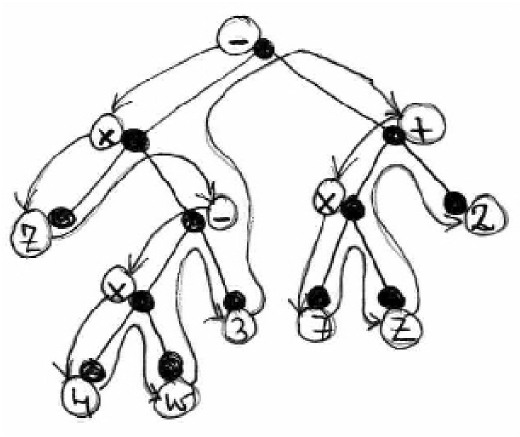


Figure 18: I figuren visas i vilken ordning noderna och löven besöks för att åstadkomma en prefixnotation.

avkommor till vänster före vi besöker någon avkomma som ligger till höger). Se Figur 18.

Postfixnotationen fås genom att först besöka barnet längst ner till vänster i hierarkin och sedan besöka barnen under varje nod före operatorn vid noden skrivs till uttrycket. Se Figur 19.

8.7 Kodning av bokstäver

I vårt alfabete finns 29 bokstäver. För att representera dessa digitalt, dvs. att koda bokstäverna digital, krävs att vi använder strängar med 5 bitar. En bit kan ta värdet 1 eller 0. Varför krävs det just 5 bitar? Antalet strängar som vi kan få genom att kombinera fem tecken där varje kan vara 0 eller 1 är $2^5 = 32$ enligt multiplikationsprincipen. Detta ger ju fler strängar än vi har bokstäver, men å andra sidan är $2^4 = 16$ så fyra bitar skulle inte vara tillräckligt. Vi kan nu koda de 29 bokstäverna på exempelvis följande sätt

$$\begin{aligned} A &= 00000, \\ B &= 00001, \\ C &= 00010, \\ D &= 00011, \end{aligned}$$

och så vidare. Frågan är nu om detta är det effektivaste sättet att koda bokstäverna? Eftersom vi ägnat ett stycke åt det här problemet är nog svaret Nej. Låt oss undersöka.

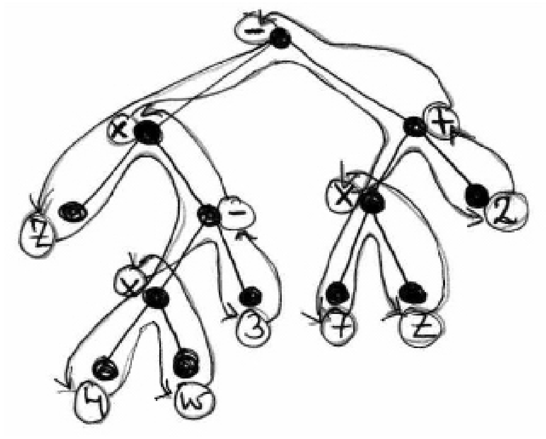


Figure 19: I figuren visas i vilken ordning noderna och löven besöks för att åstadkomma en postfixnotation.

Låt oss ta ett exempel med färre bokstäver än hela alfabetet. Antag att vårt alfabete är $\{A, B, N, P, R\}$. Då räcker det med 3 bitar för att koda de här tecknen, tex skulle vi kunna koda bokstäverna som

$$\begin{aligned} A &= 000, \\ B &= 001, \\ N &= 010, \\ P &= 011, \\ R &= 100. \end{aligned}$$

Låt oss se testa om det går att använda något annat antal bitar, tex.

$$\begin{aligned} A &= 01, \\ B &= 0, \\ N &= 101, \\ P &= 10, \\ T &= 1. \end{aligned}$$

Om vi nu vill koda ordet ABBA och skicka det till vår mottagare så använder vi kodningsschemat och får strängen 010001 och skickar iväg den. Mottagaren får strängen och börjar avkoda den, första 0:an avkodar han som B, sedan 10 som P och sedan 0 igen som B, och nästa 0 som B och sista 1:an som T, så ordet blir BPBBT. Något gick fel! Mottagaren hade kunnat koda av ordet till ABBA, men eftersom det finns godtycke så håller inte detta som kodningsschema. Problemet är att N,P,T alla börjar med varandras kod och att A,B lider av samma problem. Hur fungerar följande kod?

$$\begin{aligned} A &= 1, \\ B &= 001, \\ N &= 0000, \\ P &= 01, \\ R &= 0001. \end{aligned}$$

Här kodas ABBA som 10010011. När sedan mottagaren tar emot strängen finns inga alternativ, det avkodas entydigt som ABBA. Kodningen vi använde saknar de problemen som den tidigare kodningen hade, dvs. ingen kod är ett prefix till någon annan kod. Det senare kallas för en prefixkod.

Definition 119 *En mängd P av binära strängar är en* prefixkod *om ingen sträng i P är ett prefix till någon annan.*

I den felaktiga kodningen ovan så är $B = 0$ ett prefix till strängen $A = 01$ (och strängen T är ett prefix till strängen P som är ett prefix till strängen N). Det var alltså ingen prefixkod.

Hur hittar man då en prefixkod? Vi kan hitta dessa koder genom att använda en algoritm av Huffmann och skapa kodningen genom att bygga ett binärt träd. Den resulterande kodningen kallas för Huffmannkod och är en optimal prefixkod. Låt oss lära oss algoritmen genom att titta på ett exempel.

Exempel 120 *Antag att vi vill koda ordet BARBAPAPPAN. Det finns 5 olika bokstäver i det här ordet och de förekommer med frekvensen B:2, A:4, R:1, P:3, N:1 (detta är samma alfabete vi använde tidigare). För att skicka ordet BARBAPAPPAN med den "vanliga" trebitarskoden kräver att vi skickar* $11 \times 3 = 33$ *tecken. Låt oss nu skapa en Huffmannkod och se om den är effektivare.*
Steg1. Vi börjar med att välja de två bokstäverna med lägst frekvens, R och N och sammanfoga dem i ett träd. R och N utgör löven i trädet, och noden ger vi värdet 2 vilket är summan av deras frekvenser, se Figur 20.
Steg2. Ta den bokstaven med lägst frekvens som är kvar i listan, detta är B med frekvensen 2. Vi ska nu avgöra om det ska bindas till trädet som innehåller R och N eller inte. För att göra detta jämför vi frekvenssumman av noden i RN trädet och B med frekvenssumman av B och P (som är den bokstaven med näst lägst frekvens som är kvar i listan). RN+B ger 4 medan

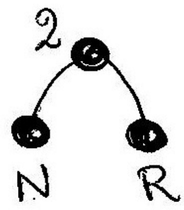


Figure 20: I figuren ser vi första steget i konstruktionen av Huffmannkoden. Bokstäverna N och R har sammanfogats i ett träd och roten har värdet 2 vilket är summan av lövens frekvenser.

B+P ger 5. Vi väljer alternativet med lägst summa. Bokstaven B binds nu till trädet med R och N genom att hamna på samma nivå som noden som håller ihop R och N och sammanbinds med en ny nod ovanför de båda (se bild). Till den nya noden ger vi värdet $2 + 2 = 4$ *vilket är summan av frekvensvärdet av den gamla noden och Bs frekvensvärde, se Figur 21.*

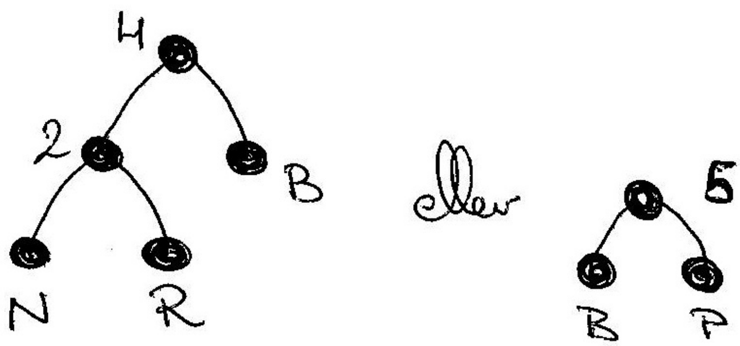


Figure 21: I figuren visas det andra steget i konstruktionen av Huffmannkoden. Vi ska i detta steg avgöra om vi ska binda bokstaven B (som har lägst frekvens av de kvarvarande bokstäverna) till vårt gamla träd eller skapa ett nytt träd med P (som har den näst lägsta frekvensen av de kvarvarande bokstäverna). Vi väljer det vänstra alternativet eftersom dess rot har det lägsta värdet (rotens värde är summan av frekvenserna av dess barn).

Steg3. Vi forsätter. Den bokstaven med lägst frekvens i listan är P med frekvensen 3. Om den läggs till trädet som nu innehåller RNB så få får den nya noden värdet $4 + 3 = 7$, *medan alternativet är att bilda ett nytt träd med P och A - denna kombination får också frekvensvärdet 7! Nu kan vi välja hur*

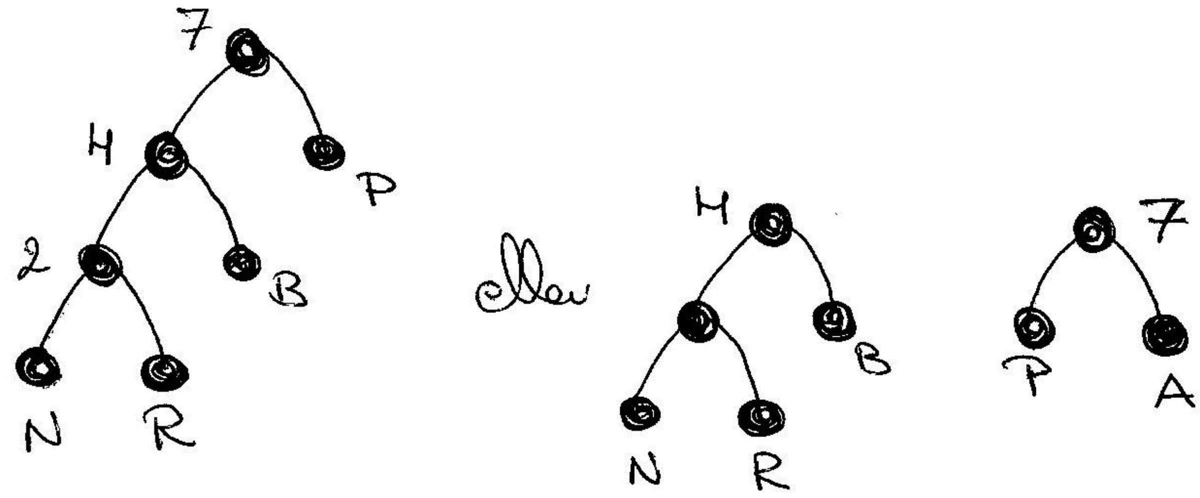


Figure 22: Det tredje steget i konstruktionen är analogt med det andra. Vi ska avgöra om vi ska binda bokstaven P (som har lägst frekvens av de kvarvarande bokstäverna) till vårt gamla träd eller om vi ska bilda ett nytt träd med bokstaven A (som har den näst lägsta frekvensen av de kvarvarande bokstäverna). När vi jämför värdet på roten i de två tänkbara alternativen ser vi att det är samma! I det här läget kan vi fritt välja endera av de två alternativen. Vi väljer det högra alternativet med två träd.

vi binder samman bokstäverna, låt oss göra ett nytt träd med P och A som binds samman med en nod med värdet 7, se Figur 22.
Steg4. Eftersom det nu inte finns kvar några fler bokstäver binder vi samman våra två träd, se Figur 23.
Steg5. Ge bokstäverna dess kod utifrån dess positioner i trädet. Se Figur 23. Den kodningen som vi fick är

$$\begin{aligned} N &= 000, \\ R &= 001, \\ B &= 01, \\ A &= 11, \\ P &= 10. \end{aligned}$$

Så att koda ordet BARBAPAPPAN tar $2+2+3+2+2+2+2+2+2+2+3 = 24$ *tecken. Detta är en förbättring jämfört med den "vanliga" kodningen som kostade oss 33 bitar.*

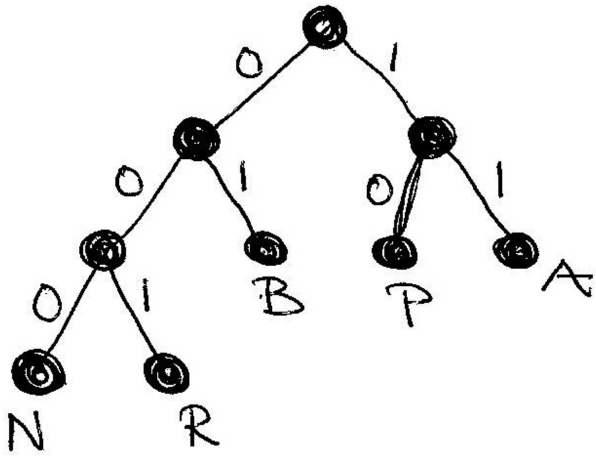


Figure 23: I figuren visas resultatet av vår konstruktion. Eftersom vi inte hade några fler bokstäver sammanbinder vi de träden från föregående steg. Bokstäverna ges sedan en kod som motsvarar deras position i trädet.

Slutsatsen som vi drar är att prefixkodning är effektivare än den "vanliga" kodningen om det finns en skillnad i frekvensen av bokstäverna. Om alla bokstäverna har samma frekvens är det inte lönt att ta fram en prefixkod. I alla språk förekommer bokstäver med olika frekvens, tex. är bokstäverna a,e och s vanligare än de andra i svenska och bokstäver som q och w används väldigt sällan. Det finns skillnader mellan olika språk, tex. används inte bokstaven å särskilt ofta i finskan, alltså bör Huffmannkoderna för svenska och finska skilja sig åt.