Föreläsningsanteckningar till diskret matematik

Thore Husfeldt

Materialet på dessa sidor skall uppfylla två syften på introduktionskursen i diskret matematik, där det används.

För det första är kursen i diskret matematik för många studenter det första mötet med matematisk formalism. Jag anser det för viktigt, att den basala terminologiska apparaten etableras på svenska, så att matematikens språk inte blir ytterligare främmandegjort. Det är därför min ambition att erbjuda en introducerande text på svenska, mitt fjärde språk – i sakens natur en uppgift, som kräver samvetsgrann rapportering av språkliga fel, vartill läsaren härmed är uppmuntrad.

För det andra tillåter jag mig att avvika från kursboken på några punkter, varför dessa anteckningar innehåller kompletterande material: En rad problematiserande exempel, som jag anser som värdefulla, och alternativa presentationer av till exempel diskret sannolikhetsteori. Dessutom finns det en fördjupning av grafteori till Ramseyteori och slumpgrafer.

Framställningen är vald kort och koncis snarare än beskrivande och förväntas kompletterad med föreläsningar eller en mer omfattande kursbok, som till exempel 'Discrete mathematics with applications' (McGraw–Hill, 1999), med vars notation och ämnesortering jag försökt vara kompatibel.

Thore Husfeldt
Lund, 2001–2002

1. Två icke-triviala bevistekniker

1.1. Motsägelsebevis. *Heltalen* är mängden $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ (Z står för »Zahl«). Ett tal a är *jämnt* om det kan skrivas $a = 2c$ för något $c \in \mathbf{Z}$; annars är a udda.

LEMMA 1. *För alla $a \in \mathbf{Z}$ gäller att om a^2 är jämnt, så är a jämnt.*

Bevis. Om a är udda, så kan vi skriva $a = 2c + 1$ för något $c \in \mathbf{Z}$. Då fås

$$a^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1,$$

dvs a^2 är udda. ∎

De *rationella talen* är mängden $\mathbf{Q} = \{\, p/q \mid p, q \in \mathbf{Z}, q \neq 0 \,\}$ (Q för »Quotient«). *Roten* $\sqrt{y}$ av y är den positiva lösningen till $x^2 = y$.

PÅSTÅENDE 1 (Aristoteles). *$\sqrt{2} \notin Q$.*

Bevis. Antag att $\sqrt{2} \in Q$ för att nå en motsägelse. Vi kan välja $a, b \in \mathbf{Z}$ så att $\sqrt{2} = a/b$ och bråket är förkortat. Genom att kvadrera båda sidor fås $2 = a^2/b^2$, som kan skrivas

$$2b^2 = a^2. \tag{1}$$

Vi ser att a^2 är jämnt, och från lemmat ovan fås att även a är jämnt, dvs $a = 2c$ för något $c \in \mathbf{Z}$. Vi kan omskriva (1) till

$$2b^2 = (2c)^2 = 4c^2,$$

varav $b^2 = 2c^2$. Lemmat ovan ger att även b är jämnt. Men om båda a och b är jämna, så kan a/b förkortas. Detta strider mod att a/b är förkortat, vilket är absurt. Antagendet måste vara fel, dvs $\sqrt{2} \notin \mathbf{Q}$. ∎

1.2. Kåseri inför matematisk induktion. Låt $P(n)$ beteckna påståendet

$$n < n^2.$$

Exempel.

1. $P(5)$ är påståndet $5 < 5^2$, som är sant. Även $P(2)$, $P(-1)$ och $P(\pi)$ är sanna.
2. $P(0)$, $P(1)$ och $P(\frac{1}{2})$ är falska, så $P(n)$ gäller inte för alla $n \in \mathbf{Q}$ och inte ens för alla $n \in \mathbf{Z}$.
3. Matematisk analys tillåter följande resonemang: Låt $f(n) = n$ och $g(n) = n^2$. Vi har $f(2) < g(2)$. Derivatorna är $f'(n) = 1$ och $g'(n) = 2n$. Det är klart att $2n \geq 1$ för $n \geq 2$, så f växer långsammare än g for $n \geq 1$. Vi konkluderar att $n < n^2$ för alla reella tal $n \geq 2$.

Vi kan visa, att egenskapen $P(n)$ ärvs av ett tals »högre granne«, dvs att om det gäller för ett *konkret* tal n (till exempel 5422,7), så gäller det också för $n+1$ (till exempel 5423,7).

LEMMA 2. *Om $n \geq 0$ och $n < n^2$ så $n + 1 < (n+1)^2$.*

Bevis. Vi har

$$n + 1 < n^2 + 1 \leq n^2 + 2n + 1 = (n+1)^2.$$

Första olikheten gäller enligt hypotesen $n < n^2$. Andra olikheten gäller eftersom $2n > 0$, vilket följer av hypotesen $n > 0$. ∎

Vi kan nu använda lemmat som en sorts bevismaskin. Vi har set att $P(2)$ gäller. Enligt lemmat gäller det då också för $P(3)$. Men om det gäller för $n = 3$ så, enligt lemmat, gäller det för $n = 4$. *Et cetera ad infimum*; vi har implicit visat $P(n)$ för alla heltal $n \geq 2$. Observera att $P(n)$ gäller för många flera tal $(-1, \pi, \dots)$, vilket kräver andra bevis.

1.3. Exempel på matematisk induktion.

PÅSTÅENDE 2. *$n < n^2$ för varje heltal $n \geq 2$.*

Bevis. Låt $P(n)$ beteckna påståendet $n < n^2$.

Bas: P(2) är sann eftersom $2 < 2^2 = 4$.

Induktionssteg: Antag att $P(n)$ är sann, dvs $n < n^2$. Vi skall visa att $P(n+1)$ är sann, dvs $(n+1) < (n+1)^2$. Detta kan visas som följer:

$$n + 1 < n^2 + 1 \leq n^2 + 2n + 1 = (n+1)^2,$$

där den första olikheten använder induktionshypotesen $P(n)$, och den andra olikheten utnyttjar att $n \geq 0$. ∎

1.4. Kommentarer till notation. Följande alternativ till formuleringen av påståendet är ekvivalenta:

1. $n < n^2$ för alla heltal $n \geq 2$
2. $n < n^2$ $(n \in \mathbf{Z}, n \geq 2)$
3. Låt n vara ett heltal som uppfyller $n \geq 2$. Då gäller $n < n^2$.
4. Om $2 \leq n \in \mathbf{Z}$ så $n < n^2$.

Det finns också alternativ till bevisets formulering. Speciellt kan manipulationerna i induktionssteget dekoreras med deras förklaring:

$$\begin{aligned} n + 1 &< n^2 + 1 && \text{(med induktion)} \\ &\leq n^2 + 1 + 2n && \text{(eftersom } 2n \geq 0 \text{ för } n \geq 2) \\ &= (n+1)^2. \end{aligned}$$

Det sista är en enkel omskrivning och behöver ingen förklaring.

Uppgifter.

1. Visa $\sqrt[3]{2} \notin \mathbf{Q}$.
2. Visa per induktion $n < n^3$ för varje heltal $n \geq 2$.
3. På en ö lever k logiker, varav exakt b har blå ögon $(0 \leq b \leq k)$. Öns religion föreskriver att (1) hela befolkningen träffas varje kväll till gemensam bön och (2) om man får reda på att man har blå ögon, måste man begå självmord nästa morgon kl sju på offerplatsen. Eftersom det inte finns speglar och alla på ön är snälla (det är tabu att tala om för någon att de har blå ögon), vet ingen om att hon själv har blå ögon, och samhället fungerar utan problem. Tills en brunögd kristen missionär besöker ön. I frustration över sitt misslyckande att omvända befolkningen säger han till kvällsbönen, så alla kan höra det, »Det finns blåögda på ön, dvs $b \neq 0$.« Vad händer och när?

2. Informell logik

2.1. Logiska utsagor. En *utsaga* är ett påstående som har ett *sanningsvärde*, dvs är antingen *sant* eller *falskt*. Vi skriver **s** och **f** för dessa värden.

Om p är en utsaga definieras $(\neg p)$, kallad *negationen* av p, enligt följande:

p	$\neg p$
s	**f**
f	**s**

Om p och q är utsagor definieras deras *disjunktion* $(p \vee q)$, *konjunktion* $(p \wedge q)$, *exklusive disjunktion* $(p \oplus q)$, *implikation* $(p \to q)$ och *ekvivalens* $(p \leftrightarrow q)$ enligt följande:

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
f	**f**	**f**	**f**	**f**	**s**	**s**
s	**f**	**s**	**f**	**s**	**f**	**f**
f	**s**	**s**	**f**	**s**	**s**	**f**
s	**s**	**s**	**s**	**f**	**s**	**s**

För att reducera antalet parenteser antar vi konventionen att negation används först: $\neg p \vee q$ är det samma som $((\neg p) \vee q)$.

2.2. Logisk ekvivalens och sanningstabeller. En utsaga som alltid är sann kallas *tautologi*, och en som alltid är falsk kallas en *motsägelse*. Utsagorna p och q kallas *logiskt ekvivalenta* om $p \leftrightarrow q$ är tautologisk. Detta skrivs $p \Leftrightarrow q$.

Exempel.

1. $(p \vee \neg p)$ är en tautologi. För att inse detta kollar vi alla värden för p genom att betrakta sanningstabellen för $(p \vee \neg p)$:

p	$\neg p$	$(p \vee \neg p)$
s	**f**	**s**
f	**s**	**s**

   Vi har visat $(p \vee \neg p) \Leftrightarrow$ **s**.

2. $(p \wedge \neg p)$ är en motsägelse:

p	$\neg p$	$(p \wedge \neg p)$
s	**f**	**f**
f	**s**	**f**

3. $(p \to q)$ och $(\neg p \vee q)$ är logiskt ekvivalenta:

p	q	$\neg p$	$\neg p \vee q$
s	**s**	**f**	**s**
s	**f**	**f**	**f**
f	**s**	**s**	**s**
f	**f**	**s**	**s**

   Vi ser att kolumnen till höger är den samma som definitionen av $(p \to q)$. Vi har visat $(p \to q) \Leftrightarrow (\neg p \vee q)$.

2.3. Logisk algebra.

PÅSTÅENDE 3. *Låt p och q vara utsagor. Då gäller*

1. *Absorbering:*

$$p \wedge \mathbf{s} \Leftrightarrow p, \qquad p \vee \mathbf{f} \Leftrightarrow p.$$

2. *Dominans:*
$$p \vee \mathbf{s} \Leftrightarrow \mathbf{s}, \qquad p \wedge \mathbf{f} \Leftrightarrow \mathbf{f}$$
3. *Idempotens:*
$$p \vee p \Leftrightarrow p, \qquad p \wedge p \Leftrightarrow p$$
4. *Dubbel negation:*
$$\neg(\neg p) \Leftrightarrow p$$
5. *Kommutativa lagar:*
$$p \vee q \Leftrightarrow q \vee p, \qquad p \wedge q \Leftrightarrow q \wedge p.$$
6. *Associativa lagar:*
$$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r), \qquad (p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r).$$
7. *Distributiva lagar:*
$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r), \qquad p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r).$$
8. *De Morgans lagar:*
$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q, \qquad \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q.$$
9. *Logisk ekvivalens av kontraposition:*
$$p \to q \Leftrightarrow \neg q \to \neg p$$
10. *Ytterligare ekvivalenser:*
$$p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p), \qquad p \to q \Leftrightarrow (\neg p \vee q).$$

Bevis. Sanningstabeller. ∎

Associativitetslagen tillåter att vi skriver $p \vee q \vee r$ för båda $(p \vee q) \vee r$ och $p \vee (q \vee r)$.

Exempel.

1. Vi kan visa
$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg q.$$
genom att använda de algebraiska lagarna från påstående 3. [R: example 1.2.5]
2. Vi kan visa samma resultat med sanningstabeller.

Om $p_1, p_2, \ldots, p_n$ är utsagor skrivs
$$p_1 \vee p_2 \vee \cdots \vee p_n, \qquad \text{eller } \bigvee_{i=1}^{n} p_i,$$
för utsagan som är sann om och endast om minst en p_i är sann. Motsvarande skrivs
$$p_1 \wedge p_2 \wedge \cdots \wedge p_n, \qquad \text{eller } \bigwedge_{i=1}^{n} p_i,$$
för utsagan som är sann om och endast om alla p_i är sanna.

PÅSTÅENDE 4. *Låt $p_1, \ldots, p_n$ vara utsagor och $n \geq 2$. Då gäller De Morgans lagar,*
$$\neg \bigvee_{i=1}^{n} p_i \Leftrightarrow \bigwedge_{i=1}^{n} \neg p_i, \qquad \neg \bigwedge_{i=1}^{n} p_i \Leftrightarrow \bigvee_{i=1}^{n} \neg p_i.$$

Bevis. Vi visar första påstående med induktion efter n. Andra påståendet visas på samma sätt.

Bas: För $n = 2$ är påståendet $\neg(p_1 \vee p_2) \Leftrightarrow (\neg p_1 \wedge \neg p_2)$. Detta har visats i påstående 3.

Induktionssteg: Antag $n \geq 2$ och att påståendet gäller för $n-1$. Låt q beteckna utsagan $p_1 \vee \ldots \vee p_{n-1}$. Vi har

$$\neg \bigvee_{i=1}^{n} p_i \Leftrightarrow \neg(q \vee p_n) \Leftrightarrow \neg q \wedge \neg p_n,$$

från påstående 3. Per induktion har vi

$$\neg q \Leftrightarrow \bigwedge_{i=1}^{n-1} \neg p_i,$$

dvs att

$$\neg q \wedge \neg p_n \Leftrightarrow \left(\bigwedge_{i=1}^{n-1} \neg p_i\right) \wedge \neg p_n \Leftrightarrow \bigwedge_{i=1}^{n} \neg p_i.$$

∎

Uppgifter.

1. Visa hela påstående 3 med sanningstabeller.
2. Komplettera beviset för påstående 4.

2.4. Kvantorer. Ett påstående där det ingår (*fria*) variabler kallas ett *predikat* och har generellt inget sanningsvärde.

Exempel. Predikatet $(x + y = z) \vee (z > 5)$ har tre fria variabler, x, y och z. Vi kan beteckna det med $P(x, y, z)$. Påståendet $P(1, 2, 3)$ anger $(1 + 2 = 3) \vee (3 > 5)$ och är sant. Påståendet $P(1, 1, 0)$ är falskt. Påståendet $P(x, y, 6)$ är sant, även om det innehåller fria variabler.

Om $P(x)$ är ett predikat och U är en mängd anger *universalkvantifieringen*

$$\forall x \in U \colon P(x)$$

utsagan att $P(x)$ är sann för alla element x i U, och *existenskvantifieringen*

$$\exists x \in U \colon P(x)$$

utsagan att $P(x)$ är sann för något element x i U. Om mängden U (*universet*) är känd från kontexten skrivs ibland $\forall x P(x)$ och $\exists x P(x)$.

Exempel.

1. Den kommutativa lagen för de reella talen är

$$\forall x \in \mathbf{R}\, \forall y \in \mathbf{R} \colon x + y = y + x.$$

2. Om U är mängden av människor och $B(x, y)$ påståendet att y är x:s bästa vän, så säger

$$\forall x \in U\, \exists y \in U\, \forall z \in U \colon B(x, y) \wedge \big((z \neq y) \to \neg B(x, z)\big)$$

att alla människor har exakt en bästa vän.

3. Gränsvärdet $\lim_{x\to a} f(x) = L$ kan definieras som
$$\forall\epsilon > 0\, \exists\delta > 0\, \forall x \in \mathbf{R}\colon 0 < |x-a| < \delta \to |f(x) - L| < \epsilon.$$
Observera den kreativa notation $\forall\epsilon > 0$. Alternativet vore att definiera mängden av positiva heltal $\mathbf{R}_+$ och skriva $\forall\epsilon \in \mathbf{R}_+$.
4. Låt $Q(x,y)$ beteckna utsagan $x + y = 0$ om reella tal x och y. Påståendet
$$\exists y \forall x\, Q(x,y)$$
är falskt medan påståendet
$$\forall x \exists y\, Q(x,y)$$
är sant.

Vi formulerar ytterligare två påstående om predikatlogiken utan bevis.

PÅSTÅENDE 5. *Låt $[n]$ beteckna mängden $\{1, 2, \ldots, n\}$ och P ett predikat. Då gäller*

1. $\bigvee_{i=1}^{n} P(x_i) \Leftrightarrow \exists i \in [n]\colon P(x_i)$.
2. $\bigwedge_{i=1}^{n} P(x_i) \Leftrightarrow \forall i \in [n]\colon P(x_i)$.

PÅSTÅENDE 6. *Låt P vara en utsaga. Då gäller*

1. $\neg\forall x\, P(x) \Leftrightarrow \exists x\, \neg P(x)$.
2. $\neg\exists x\, P(x) \Leftrightarrow \forall x\, \neg P(x)$.

*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

3. Mängder

3.1. Sekvenser. En *sekvens* är en lista av element i en specifik *ordning*. Vi skriver en sekvens genom att lista dess medlemmar i denna ordning inom ( ):

$$(x_1, x_2, \dots, x_n),$$

för en sekvens av längd n. Två sekvenser är lika, $(x_1, \dots, x_n) = (y_1, \dots, y_m)$ om $n = m$ och $\forall i(x_i = y_i)$. En sekvens av längd 2 kallas en *tuppel* och en sekvens av längd n en n-tuppel.

Exempel.

1. Sekvensen av de första 6 primtalen är $(2, 3, 5, 7, 11, 13)$.
2. Observera att

$$(1,2) \neq (2,1), \qquad (1,2) \neq (1,2,2). \tag{2}$$

3.2. Mängder. En *mängd* är en oordnad samling av *element*. Om elementet a tillhör mängden M skrivs $a \in M$, i motsatt fall $a \notin M$. Vi skriver en mängd genom att lista dess medlemmar *minst en gång och i godtycklig ordning* inom { }:

$$\{x_1, x_2, \dots, x_n\}.$$

Exempel.

1. Observera att notationen inte är entydigt: mängden av de första 5 primtalen kan skrivas $\{2, 3, 5, 7, 11\}$ men också $\{5, 11, 7, 2, 3\}$ och även $\{2, 2, 2, 2, 2, 5, 11, 7, 3, 3\}$.
2. Varje typ eller klass i ett programspråk definierar en mängd bestånde av dess medlemmar (eller objekt). Till exempel kan vi betrakta **boolean** som mängden $\{\mathbf{s}, \mathbf{f}\}$ och **int**$=\{-2147483648, \dots, 2147483647\}$.

För att ange stora eller oändliga mängder används ofta tre prickar $\{e_1, e_2, \dots\}$ för att uppfordra läsaren till att använda sin fantasi till att utvidga listan, fast på ett konservativt sätt.

Ett annat viktigt sätt att ange mängder är mängdkonstruktören

$$A = \{x \mid P(x)\}, \tag{3}$$

där P är ett predikat, eller, om vi vill specificera en delmängd av en annan mängd,

$$B = \{\, x \in A \mid P(x) \,\}.$$

Exempel.

1. Mängden av tvåpotenser kan anges som $\{1, 2, 4, 8, 16, 32, \dots\}$ eller som $\{\, i \mid i = 2^j, j \in \mathbf{N} \,\}$ eller med en ytterligare flexibilisering av notationen som $\{\, 2^j \mid j \in \mathbf{N} \,\}$.
2. Om A är mängden av män anger

   $$\{\, x \in A \mid x \text{ är son till Adam} \,\}$$

   mängden $\{\, \text{Kain}, \text{Abel} \,\}$ och

   $$\{\, x \in A \mid x \text{ är Abels fader} \,\}$$

   är mängden $\{\text{Adam}\}$. En låda som innehåller en hatt är inte det samma som en hatt, och av samma andledning är $\{\text{Adam}\}$ inte det samma som Adam.

3. Välkända talmängder är:

$$\begin{aligned}
&\mathbf{N} = \{0, 1, 2, \dots\}, \text{naturliga tal,}\\
&\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2 \dots\}, \text{heltal,}\\
&\mathbf{R}, \text{reella tal,}\\
&\mathbf{Q} = \{\, a/b \mid a, b \in \mathbf{Z} \text{ och } b \neq 0 \,\}, \text{rationella tal}\\
&\mathbf{C} = \{\, a + bi \mid a, b \in \mathbf{R} \,\}, \text{komplexa tal}
\end{aligned}$$

4. Samma mängd kan anges på många sätt. Observera

$$\{3, 5\} = \{\, x \in \mathbf{N} \mid x \text{ är ett udda primtal mindre än } 6 \,\} = \{\, x \in \mathbf{R} \mid x^2 - 8x + 15 = 0 \,\}$$

   Detta kanske känns fel för en datalog (eftersom talen har olika »typer«) men matematiken gör inte denna skillnad.
5. Det finns en del friheter map vad man får skriva i mängdkonstruktören, och tyvärr en massa godtyckligheter. Speciellt är $\{\, x \in A \mid P(x) \,\}$ det samma som $\{\, x \mid P(x) \text{ och } x \in A \,\}$. Vi föredrar ofta den första varianten, eftersom den preciserar universet.
6. Betrakta mängden av alla mängder, som inte har sig själv som element:

$$R = \{\, x \mid x \notin x \,\}.$$

   För alla mängder y gäller nu $y \in R$ om och endast om $y \notin y$, speciellt gäller (med $y = R$), att

$$R \in R \text{ om och endast om } R \notin R,$$

   vilket är absurt. Detta exempel, Russels paradox, dyker upp i många variationer (till exempel barberaren som rakar alla på ön som inte rakar sig själva). Här är det menat som varning att mängdteorien kräver en ganska försiktig formalisering för att undvika inbyggda inkonsistenser. Läsaren får lita på, att en kraftfull och konsistent definition av vad (3) skall betyda, är möjlig.

Mängden utan element kallas den *tomma mängden* och betecknas $\emptyset$, vi har $\forall x(x \notin \emptyset)$. Vi säger att *$A$ är en delmängd av B* och skriver $A \subseteq B$ om varje element i A är ett element i B, dvs

$$\forall x(x \in A \to x \in B).$$

Observera notationsskillnaden: $x \in A$ om och endast om $\{x\} \subseteq A$.

PÅSTÅENDE 7. *För en godtycklig mängd B gäller $\emptyset \subseteq B$.*

Bevis. Givet elementet x. Vi vill visa implikationen $x \in \emptyset \to x \in B$. Men $x \in \emptyset$ är aldrig sant pga definitionen av $\emptyset$, så implikationen är sann. ∎

Två mängder är *lika*, $A = B$, om $A \subseteq B$ och $B \subseteq A$, som till exempel

$$\{1, 2\} = \{2, 1\}, \qquad \{1, 2\} = \{1, 2, 2\},$$

som bör jämföras med (2).

3.3. Mängdalgebra. Den *kartesiska produkten* av A och B är

$$A \times B = \{\, (a,b) \mid a \in A \wedge b \in B \,\},$$

unionen eller *föreningsmängden* av A och B är

$$A \cup B = \{\, a \mid a \in A \vee a \in B \,\},$$

snittet eller *skärningsmängden* av A och B är

$$A \cap B = \{\, a \mid a \in A \wedge a \in B \,\},$$

och *differensen* mellan A och B är

$$A - B = \{\, a \mid a \in A \wedge a \notin B \,\}.$$

Mängderna A och B är *disjunkta* om $A \cap B = \emptyset$. Om grundmängden U, som alla x tas från (*universet*) är entydigt, skrivs $U - A$ även $\overline{A}$.

PÅSTÅENDE 8. *Låt $A, B, C \subseteq U$ vara mängder. Då gäller*

1. *Absorbering:*
$$A \cap U = A, \qquad A \cup \emptyset = A.$$
2. *Dominans:*
$$A \cup U = U, \qquad A \cap \emptyset = \emptyset.$$
3. *Idempotens:*
$$A \cup A = A, \qquad A \cap A = A.$$
4. *Dubbelt komplement:*
$$\overline{(\overline{A})} = A.$$
5. *Kommutativa lagar:*
$$A \cup B = B \cup A, \qquad A \cap B = B \cap A.$$
6. *Associativa lagar:*
$$(A \cup B) \cup C = A \cup (B \cup C), \qquad (A \cap B) \cap C = A \cap (B \cap C).$$
7. *Distributiva lagar:*
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$
8. *De Morgans lagar:*
$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Bevis. Vi visar den ena av De Morgans lagar och lämnar resten till läsaren.

För att visa $\overline{A \cap B} = \overline{A} \cup \overline{B}$ visar vi inklusion åt båda hållen. Antag först att $x \in \overline{A \cap B}$, dvs $x \notin A \cap B$. Detta ger att $x \notin A$ eller $x \notin B$, dvs $x \in \overline{A}$ eller $x \in \overline{B}$, varav $x \in \overline{A} \cup \overline{B}$. Vi har visat att $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Antag nu att $x \in \overline{A} \cup \overline{B}$. Detta ger att $x \in \overline{A}$ eller $x \in \overline{B}$, dvs $x \notin A$ eller $x \notin B$. Därför har vi $x \notin A \cap B$, dvs $x \in \overline{A \cap B}$. Vi har visat att $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ och vilket färdiggör beviset. ∎

Exempel. Här är ett alternativt bevis för De Morgans lag, som använder logiska ekvivalenser: Eftersom

$$x \notin A \cap B \Leftrightarrow \neg\big(x \in (A \cap B)\big) \Leftrightarrow \neg(x \in A \wedge x \in B) \Leftrightarrow$$
$$\neg(x \in A) \vee \neg(x \in B) \Leftrightarrow (x \notin A) \vee (x \notin B) \Leftrightarrow (x \in \overline{A}) \vee (x \in \overline{B}) \Leftrightarrow (x \in \overline{A} \cup \overline{B})$$

genom att använda De Morgans lag för propositioner, kan vi skriva

$$\overline{A \cap B} = \{\, x \mid x \notin A \cap B \,\} = \{\, x \mid x \in \overline{A} \cup \overline{B} \,\} = \overline{A} \cup \overline{B}.$$

Om $A_1, \ldots, A_n$ är mängder skriver vi

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

för *föreningen* av alla A_i, dvs mängden som innehåller alla element som finns i något A_i. Vi skriver

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

för *snittet* av alla A_i, dvs mängden som innehåller alla element som finns i varje A_i.

PÅSTÅENDE 9. *Låt $A_1, \ldots, A_n \subseteq U$ vara mängder och $n \geq 1$. Då gäller*

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}, \qquad \overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} \overline{A_i}.$$

Bevis. Uppgift (induktion efter n). ∎

3.4. Kardinalitet av ändliga mängder. Om A har exakt n element kallas A *ändlig* och *kardinaliteten* $|A|$ är n. Potensmängden $P(S)$ är mängden av alla delmängder av S.

PÅSTÅENDE 10. *Om S är ändlig så gäller $|P(S)| = 2^{|S|}$.*

Bevis. Induktion efter $n = |S|$.

Bas: Om $n = 0$ då är $S = \emptyset$, som bara har en delmängd: $\emptyset \subseteq \emptyset$. Dvs $|P(S)| = |P(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|S|}$.

Induktionssteg: Antag som induktionshypotes att varje mängd med n element har 2^n delmängder. Vi skall visa, att varje mängd med $n+1$ element har $2^{n+1} = 2^n + 2^n$ delmängder. Låt härtill A vara en mängd med $|A| = n+1$ och fixera något $a \in A$. Vi kan skriva $A = B \cup \{a\}$ där $B = A - \{a\}$. Varje delmängd S av A antingen innehåller a eller inte, dvs

$$\begin{aligned} P(A) &= \{\, S \mid S \subseteq A, a \in S \,\} \cup \{\, S \mid S \subseteq A, a \notin S \,\} \\ &= \{\, T \cup \{a\} \mid T \subseteq B \,\} \cup \{\, T \mid T \subseteq B \,\}. \end{aligned}$$

Eftersom uppdelningen är disjunkt har vi $|P(A)| = |P(B)| + |P(B)| = 2^n + 2^n$ per induktion. ∎

En k-delmängd är en delmängd med k element. Vi låter $\binom{A}{k}$ beteckna mängden av k-delmängder av A.

3.5. Strängar. Ett *alfabet* Σ är en mängd vars element kallas *tecken*. En *sträng över* Σ är en ändlig sekvens av tecken från Σ. Mängden av strängar över Σ betecknas Σ^*. En typisk sträng i Σ^* skrivs $w = (w_1, \dots, w_n)$ eller $w_1 w_2 \cdots w_n$, där $w_i \in \Sigma$ $(1 \le i \le n)$. Strängens *längd* är $l(w) = n$. Strängen av längd noll betecknas λ (*lambda*, för tyska »leer«). Mängden av strängar av längd n över Σ betecknas Σ^n, dvs

$$\Sigma^* = \bigcup_{n \ge 0} \Sigma^n.$$

Sammanfogningen av två strängar $u = (u_1, \dots, u_n)$ och $v = (v_1, \dots, v_m)$ betecknas

$$uv = (u_1, \dots, u_n, v_1, \dots, v_m).$$

Den m-faldiga *repitionen* av en sträng u är sammanfogningen

$$u^m = \underbrace{uu \cdots u}_{m \text{ termer}}.$$

Speciellt definierar vi $u^0 = \lambda$.

Exempel.

1. Mängden av *bitsträngar* är
$$\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, \dots\}.$$
2. $\{a\}^* = \{\lambda, a, aa, aaa, \dots, a^n, \dots\}$.
3. $\emptyset^* = \{\lambda\}$. För alla andra $\Sigma \ne \emptyset$ har Σ^* oändligt många element.
4. Om C är en javaklass så anger $C[\,]$ klassen av strängar över C. Till exempel är **boolean**[ ] klassen av bitsträngar. Metoden length är längdfunktionen l.

PÅSTÅENDE 11. *Låt u, v, w vara strängar och $m, n \ge 0$. Då gäller*

1. *Absorbering:* $u\lambda = \lambda u = u$.
2. *Konkatenering är associativ:* $u(vw) = (uv)w$
3. $u^m u^n = u^{m+n}$.
4. $l(uv) = l(u) + l(v)$.
5. $l(u^m) = ml(u)$

Det finns ett närt samband mellan sekvenser och strängar, så närt att vi ofta blandar ihop notation och begrepp.

Låt $U = \{u_1, \dots, u_n\}$ vara ett ändligt univers. För en delmängd $A \subseteq U$ definierar vi dess *bitsträngsrepresentation* som strängen $a \in \{0,1\}^n$ där

$$a_i = \begin{cases} 1, & u_i \in A, \\ 0, & u_i \notin A. \end{cases}$$

Uppgifter.

1. Hitta en mängd A som är disjunkt med sig själv.
2. Visa $|A \cap B| \le |A \cup B|$. När gäller $|A \cap B| = |A \cup B|$?
3. Hitta ett nödvändigt och tillräckligt villkor för att $(A \cap B) \cup C = A \cap (B \cup C)$. Villkoret får inte innehålla B. Bevisa ditt svar.
4. Ange ett element från varje av de följande mängder: $\mathbf{N} \times \mathbf{Z} \times \mathbf{R}$, $P(\mathbf{N} \times \mathbf{N})$, $P(\emptyset) \times \mathbf{N}$, $(\mathbf{N} \times \mathbf{N}) - ((\mathbf{N} - \{0,1\}) \times \mathbf{N})$, $P(P(P(\emptyset)))$.
5. Definiera tuppeln (,) som $(x, y) = \{x, \{x, y\}\}$. Visa att denna definition är ekvivalent med den urspungliga genom att visa att

$$(x_1, y_1) = (x_2, y_2) \quad \text{medför} \quad x_1 = x_2 \text{ och } y_1 = y_2. \tag{4}$$

6. Definiera tuppeln $(\,,\,)$ som $(x, y) = \{\{x, 0\}, \{y, 1\}\}$. Är egenskapen (4) fortvarande uppfylld? Bevisa ditt svar.
7. Ge motexempel som visar att följande definition av $(\,,\,)$ inte uppfyller (4): $(x, y) = \{x, y\}$.
8. Här är några försök på att definiera 3-tuppeln $(\,,\,,\,)$. Diskutera.
   (a) $(x, y, z) = \big\{\{x\}, \{x, y\}, \{x, y, z\}\big\}$.
   (b) $(x, y, z) = \big(x, (y, z)\big)$.
   (c) $(x, y, z) = \big\{\{x, 0\}, \{y, 1\}, \{z, 3\}\big\}$.

*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

4. Funktioner

Låt A och B vara mängder. En *funktion* f från A till B, skrivit $f\colon A \to B$ är en tilldelning av exakt ett element från B till varje element i A. Vi kan skriva $a \mapsto b$ eller $b = f(a)$ för att ange att b är detta element. Vi säger att b är a:s *bild.* Mängderna A och B heter f:s *domän* och *kodomän.* Funktionens *värdemängd* är

$$f(A) = \bigcup_{a\in A} f(a).$$

Mängden av funktioner från A till B betecknas B^A.

Exempel.

1. Låt A vara en mängd. Identitetsfunktionen är
$$\iota_A\colon A \to A, \qquad a \mapsto a$$
2. Låt A, U vara mängder med $A \subset U$. Den karakteristiska funktionen $\chi_A\colon S \to \{\mathbf{s}, \mathbf{f}\}$ är
$$\chi_A(a) = \begin{cases} \mathbf{s} & x \in A \\ \mathbf{f} & x \notin A \end{cases}.$$
3. För varje tal $n \in \mathbf{Z}$ definieras den konstanta funktionen
$$n\colon A \to \mathbf{Z}, \qquad x \mapsto n.$$
Till exempel är $6(x) = 6$ för alla x.
4. *Golvfunktionen* $\mathbf{R} \to \mathbf{Z}$ definieras av
$$\lfloor x \rfloor = \max\{\, n \in \mathbf{N} \mid n \le x \,\}$$
och *takfunktionen* $\mathbf{R} \to \mathbf{Z}$ definieras av
$$\lceil x \rceil = \min\{\, n \in \mathbf{N} \mid n \ge x \,\}.$$
Det gäller
   (a) $x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$
   (b) $\lceil -x \rceil = -\lfloor x \rfloor$, $\lfloor -x \rfloor = -\lceil x \rceil$
   (c) $\lceil x + n \rceil = \lceil x \rceil + n$, $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, om $n \in \mathbf{N}$.
5. I det funktionella programspråket *Lisp* definieras funktionen
$$f\colon Z \to Z, \quad x \mapsto x^2$$
som
```
(define (f x) (* x x))
```
Språket *Haskell* är ett *typad* funktionellt språk, och här skrivs samma funktion på följande sätt:
```
f   :: Integer → Integer
f x = x * x
```
6. Även en statisk metod i et objektorienterad språk som Java,
```
static B f(A x)
```
kan betraktas som en funktion
$$f\colon A \to B, \qquad x \mapsto f(x).$$
Till exempel är följande funktion precis identitetsfunktionen på mängden **int**.
```
static int f(int x) { return x; }
```
7. En icke-statisk metod i Java är *ingen* funktion. Betrakta följande klass:
```
class C
{ int i= 0;
  int f(int x) { return i++; }
}
```

Första anrop av f returnerar 0, men nästa returnerar 1. Metoden tilldelar *inte* exakt ett element från kodomänet till varje element i domänet. Vi säger att icke-statiska metoder har *tillstånd* (eller *minne*); funktioner är därimot tillståndslösa.

8. Modelleringen av programspråkskonstruktioner vha matematiken är icke-trivial och föremål för datalogisk forskning på särdelas hög nivå. För att antyda problemen kan vi nämna terminering. Icke alla metoder, även de statiska, terminerar, som till exempel

   static int $f()$ { **while**(**true**) ; }

   eller

   static float f(**int** x) { **return** $5/x$; }

   I detta exempel går det ändå att beskriva

   $$f\colon \mathbf{int} - \{0\} \to \mathbf{float}$$

   men generellt är metoders beteende för komplext till att restringera domänet. I stället kan man betrakta metoden som som

   $$f\colon A \to B \cup \{\text{abort}\},$$

   där »abort« är ett speciellt värde (som inte är i B), som tar hand om icke-terminering.

4.1. Egenskaper. En funktion $f\colon A \to B$ är *injektiv* om

$$f(x) = f(y) \Rightarrow x = y \qquad (x, y \in A);$$

En ekvivalent och möjligen mera naturlig formulering är att f ger olika bilder på olika variabler:

$$x \neq y \Rightarrow f(x) \neq f(y) \qquad (x, y \in A).$$

Funktionen är *surjektiv* om $f(A) = B$. Funktionen är *bijektiv* om den är både injektiv och surjektiv.

Exempel. Identitetsfunktionen är bijektiv.

SATS 1. *Givet två ändliga mängder A och B. Vi har $|A| = |B|$ om och endast om det finns en bijektion $A \to B$.*

Bevis. Antag först att det finns en bijektion $f\colon A \to B$. Sätt $n = |A|$ och skriv $A = \{a_1, \dots, a_n\}$. Betrakta nu mängden

$$f(A) = \{f(a_1), \dots, f(a_n)\}.$$

Eftersom alla element är olika (f är ju injektiv) har vi $|f(A)| = n$. Surjektivitet ger $f(A) = B$. Därför fås $|B| = |f(A)| = n$.

Skriv mängderna som $A = \{a_1, \dots, a_n\}$ och $B = \{b_1, \dots, b_m\}$ och antag nu $n = m$. Betrakta funktionen

$$f\colon A \to B, \qquad a_i \mapsto b_i.$$

Denna är väldefinierad eftersom $n \leq m$. Funktionen är klart injektiv. Den är surjektiv eftersom $m \leq n$. ∎

För en injektiv funktion $f\colon A \to B$ definieras dess *invers* som

$$f^{-1}\colon f(A) \to A, \qquad f(a) \mapsto a.$$

Dvs att $f^{-1}(b) = a$ när $f(a) = b$, vi kallar a för b:s *urbild*. Observera att f^{-1} inte är definierad för $B - f(A)$.

Funktionens *graf* är en delmängd av $A \times B$ definierad med

$$\operatorname{graf}(f) = \{\, (a,b) \mid b = f(a), a \in A \,\}.$$

Låt $g\colon A \to B$ och $f\colon B \to C$. Då definieras den *sammansatta* funktionen $h = f \circ g$ som

$$h\colon A \to C, \qquad a \mapsto f(g(a)).$$

4.2. Uppräkneliga mängder. Vi återvänder till mängders kardinalitetsbegrepp. En mängd M är *ändlig* om $|M| < \infty$. En mängd är *uppräknelig* om den är ändlig eller det finns en bijektion $M \to \mathbf{N}$. Kardinaliteten av en oändlig, uppräknelig mängd skrivs $|\mathbf{N}| = \aleph_0$ (alef-null). En mängd som inte är uppräknelig är *överuppräknelig*.

Exempel.

1. $\mathbf{Z}$ är uppräknelig; observera att detta strider mot intuitionen om att den är drygt dubbelt så stor som $\mathbf{N}$. För att se detta, betrakta

   $$f\colon \mathbf{N} \to \mathbf{Z}, \qquad z \mapsto \begin{cases} \frac{1}{2}z, & \text{om } z \text{ är jämnt;} \\ -\frac{1}{2}(z+1), & \text{om } z \text{ är udda.} \end{cases}$$

   några värden kan ses här:

$f(z)$	0	1	2	3	4	5	6	$\cdots$
z	0	-1	1	-2	2	-3	3	$\cdots$

   Det är klart att alla heltal finns någonstans och exakt en gång på denna lista. Funktionen f är alltså en bijektion mellan $\mathbf{N}$ och $\mathbf{Z}$.

   Det är möjligen instruktivt att se ett felaktigt försök på en uppräkning, t ex först alla positiva tal, och sen alla negativa, som i

   $$0, 1, 2, \ldots, -1, -2, \ldots.$$

   Detta fungerar inte, vilket blir klart så fort man försöker att formalisera denna lista som en bijektion till $\mathbf{N}$ – vilket »nummer« får -1?
2. $\mathbf{N} \times \mathbf{N}$ är uppräknelig. Cantors argument för detta är som följer: Vi räknar $\mathbf{N}^2$ i varv. I varv 1 räknas bara $(0,0)$. I varv 2 räknas $(1,0)$ och $(0,1)$. Generellt räknas alla tuppler (i,j) i varv $i+j+1$ i någon ordning. Varje varv är ändligt, så alla tuppler räknas (exakt en gång) förr eller senare. Bijektionen är t ex

   $$f\colon \mathbf{N}^2 \to \mathbf{N}, \qquad f(i,j) = i + \sum_{k=1}^{i+j} k.$$
3. Σ^* är uppräknelig om $\Sigma = \{\sigma_1, \ldots, \sigma_k\}$ är ändligt. Vi listar först λ, sen hela Σ, sen hela Σ^2, etc. i någon ordning, till exempel den lexikografiska. För $\Sigma = \{a, b\}$ är avbildningen till exempel

z	0	1	2	3	4	5	6	7	$\cdots$
$f(z)$	λ	a	b	aa	ab	ba	bb	aaa	$\cdots$

   Bijektionen är

   $$f\colon \Sigma^* \to \mathbf{N}, \qquad f(\sigma_{i_1} \cdots \sigma_{i_n}) = \left| \bigcup_{r=0}^{n-1} \Sigma^r \right| + \sum_{r=1}^{n} i_r |\Sigma|^r,$$

   och $f(\lambda) = 0$.

PÅSTÅENDE 12. *Om B är uppräknelig och $A \subseteq B$ så är A uppräknelig.*

Bevis. Om A är ändlig är vi klara. Antag alltså att A är oändlig. Uppräkningen av elementen i A är den samma som uppräkningen av B, där $B-A$ har tagits bort. Formellt (men inte mycket klarare), om vi låter $b_1, b_2, \dots$ ange uppräkningen av B:s element, är

$$f\colon A \to \mathbf{N}, \qquad f(b_i) = |\{b_1, \dots, b_{i-1}\} \cap A|.$$

Detta är väldefinierat eftersom varje element i A kan skrivas som b_i för något i. Surjektiviteten följer av att A är oändlig. ∎

Exempel. $\mathbf{Q}$ är uppräknelig, vilket är minst lika kontraintuitivt som att $\mathbf{Z}$ är det (det finns ju oändligt många rationella tal mellan 3 och 4, och – mera skrämmande – oändligt många mellan varje par av rationella tal). Vi visar detta bara för de positiva rationella talen, $\mathbf{Q}_+$. För att inse påståendet kan vi betrakta $\mathbf{Q}_+$ som delmängd av $\mathbf{N}^2$. Helt formellt betraktar vi funktionen

$$\mathbf{Q}_+ \to \mathbf{N}^2, \qquad a/b \mapsto (a,b),$$

som är en bijektion mellan $\mathbf{Q}_+$ och en delmängd av $\mathbf{N}^2$. Denna är uppräknelig enligt påst. 12.

4.3. En datavetenskaplig tillämpning. En funktion $f\colon \mathbf{N} \to \{\mathbf{s}, \mathbf{f}\}$ kan *javaberäknas* om det finns ett metod **static boolean** m(**Integer** i) skriven i Java så att $m(i) = f(i)$ för alla $i \in \mathbf{N}$.

PÅSTÅENDE 13. *Det finns funktioner* $\mathbf{N} \to \{\mathbf{s}, \mathbf{f}\}$ *som inte kan javaberäknas.*

Bevis. Låt J ange mängden av javaprogram. Om Σ anger mängden av Unicodetecken har vi $J \subseteq \Sigma^*$. Eftersom Σ^* kan räknas, kan J också det.

Vi visar nu att $\mathbf{boolan}^{\mathbf{N}}$ inte kan räknas. Antag motsatsen, att en uppräkning $f_0, f_1, \dots$ finns. Konstruera funktionen

$$d\colon \mathbf{N} \to \mathbf{boolean}, \qquad d(i) = \neg f_i(i).$$

Enligt antagandet måste d finnas någonstans i listan, dvs $d = f_j$ för något j. Vi har $d(i) = f_j(i)$ för alla i, speciellt gäller

$$d(j) = f_j(j),$$

i motstrid med definitionen av d.

Vi konkluderar med påst. 12 att $\mathbf{boolean}^{\mathbf{N}}$ inte kan vara en delmängd av J. ∎

Uppgifter.

1. En funktion $g\colon B \to A$ är *vänsterinvers* till $f\colon A \to B$ om $g \circ f = \iota_A$. En funktion $g\colon B \to A$ är *högerinvers* till $f\colon A \to B$ om $f \circ g = \iota_B$.
   (a) Visa att om f är injektiv, så har f en vänsterinvers.
   (b) Visa att om f är surjektiv, så har f en högerinvers.

4.4. Summor. Om $l \leq r$ skriver vi

$$\sum_{i=l}^{r} a_i$$

för summan $a_l + a_{l+1} + \cdots + a_r$.

PÅSTÅENDE 14. *För $n \geq 1$ gäller*

$$\sum_{i=1}^{n} i = \tfrac{1}{2}n(n+1).$$

Bevis. Induktion efter n.

Bas: För $n = 1$ är påståendet $1 = \frac{1}{2}1(1+1) = 1$, vilket är sant.

Induktionssteg: Antag påståendet för något $n \geq 1$. Då fås

$$\sum_{i=1}^{n+1} i = n + 1 + \sum_{i=1}^{n} i = n + 1 + \tfrac{1}{2}n(n+1) = \tfrac{1}{2}(n+2)(n+1),$$

där induktionshypotesen används för att omskriva summan. ∎

PÅSTÅENDE 15. *Om $r \neq 1$ och $n \geq 0$ gäller*

$$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}.$$

Bevis. Per induktion efter n.

Bas: För $n = 0$ är påståendet

$$a = \frac{ar - a}{r - 1} = \frac{a(r-1)}{r-1},$$

vilket är sant.

Induktionssteg: Antag påståendet för något $n \geq 1$. Vi har

$$\sum_{j=0}^{n+1} ar^j = ar^{n+1} + \sum_{j=0}^{n} ar^j = ar^{n+1} + \frac{ar^{n+1} - a}{r - 1} = \frac{ar^{n+2} - a}{r - 1},$$

där induktionshypotesen används för att omskriva summan. ∎

Som ett nyttigt specialfall av resultatet ovan har vi

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Definiera de *harmoniska talen* H_k enligt

$$H_k = \sum_{i=1}^{k} \frac{1}{i}.$$

Vi har

k	1	2	3	4	5	6	$\cdots$	10000	$\cdots$
H_k	1	$\frac{3}{2}$	$\frac{11}{6}$	$\frac{25}{12}$	$\frac{137}{60}$	$\frac{49}{20}$	$\cdots$	14,39272...	$\cdots$

PÅSTÅENDE 16. *För $n \geq 0$ gäller*

$$H_{2^n} \geq 1 + \tfrac{1}{2}n.$$

Bevis. Per induktion efter n.

Bas: För $n = 0$ är påståendet $H_1 = 1$, vilket är sant.

Induktionssteg: Antag påståendet för något $n \geq 1$. Vi har

$$H_{2^{n+1}} = \sum_{i=1}^{2^{n+1}} \frac{1}{i} = \sum_{i=1}^{2^n} \frac{1}{i} + \sum_{i=2^n+1}^{2^{n+1}} \frac{1}{i} = H_{2^n} + \sum_{i=2^n+1}^{2^{n+1}} \frac{1}{i} \geq$$
$$H_{2^n} + 2^n \cdot \frac{1}{2^{n+1}} = H_{2^n} + \frac{1}{2}.$$

Enligt induktionshypotesen är detta högst $(1 + \frac{1}{2}n) + \frac{1}{2} = 1 + \frac{1}{2}(n+1)$, som önskat.
∎

Sätter vi $k = 2^n$ i detta resultat fås

$$H_k \geq 1 + \tfrac{1}{2} \log k, \qquad k = 1, 2, 4, 8, 16, \cdots,$$

så vi kan uppskatta H_k (det *harmoniska talet*) för alla tvåpotenser. Det kan visas att

$$\lim_{n \to \infty} (H_n - \ln n) = \gamma,$$

där $\gamma = 0{,}57727156649\ldots$ är Eulers konstant.

Exempel.

1. Det är instruktivt att försöka att bevisa $H_k \geq 1 + \frac{1}{2} \log k$ per induktion efter k (i stället för efter 2^k som vi gjorde).
2. En långsam men envis mask M startar i ena ändan av ett meterlångt gummiband och kryper 1 cm per minut mot andra ändan. En lika envis gummibandsansvarig G, vars enda uppgift i livet är att frustrera M, drar vid slutet av varje minut ut bandet ytterligare en meter. Alltså är M efter en minuts krypande 1 cm från starten och 99 cm från slutet, och sen drar G ut bandet 1 m. När bandet dras ut behåller M sin relativa position: 1% från start och 99% från mål; dvs M är nu 2 cm från start och 198 cm från mål. När M har krupit ytterligare en minut, är han 3 cm från start och 197 cm från mål; när G drar blir avstånden 4,5 och 295,5.

   När G drar i bandet är M:s relativa avstånd det samma. Han kryper alltså 1/100 av bandet i första minut, 1/200 i andra, etc. Efter n minut har han krupit

   $$\frac{1}{100}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) = \frac{H_n}{100}.$$

   Han är klar när $H_n \geq 100$. Efter $287 \cdot 10^{33}$ sekler når han bandets slut, som nu är 10^{27} ljusår långt. Triumf!

4.5. Funktioners tillväxt. I detta avsnitt är

$$f, g \colon \mathbf{N} \to \mathbf{R}$$

eller

$$f, g \colon \mathbf{R} \to \mathbf{R}.$$

En funktion f är *mindre än* g (vi skriver $f \leq g$) om

$$f(n) \leq g(n), \qquad \forall n.$$

En funktion f är *försumbar i jämförelse med* g eller *lilla ordo av* g (vi skriver $f(n)$ är $o\big(g(n)\big)$ eller $f(n) = o(g(n)))$ om

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 0.$$

En funktion f är *högst g:s ordning* eller *stora ordo av g* (vi skriver $f(n)$ är $O\big(g(n)\big)$ eller $f(n) = \mathrm{O}(g(n))$) om

$$\exists C, k > 0\colon n \geq k \rightarrow |f(n)| \leq C|g(n)|.$$

En funktion f är *stora omega av g* (vi skriver $f(n)$ är $\Omega\big(g(n)\big)$ eller $f(n) = \Omega(g(n))$) om

$$\exists C, k > 0\colon n \geq k \rightarrow |f(n)| \geq C|g(n)|.$$

En funktion f är *stora theta av g* (vi skriver $f(n)$ är $\Theta\big(g(n)\big)$ eller $f(n) = \Theta(g(n))$) om

$$f(n) = \mathrm{O}\big(g(n)\big) \text{ och } f(n) = \Omega\big(g(n)\big).$$

PÅSTÅENDE 17. 1. *$f \leq g$ medför $f(n) = \mathrm{O}(g(n))$.*
2. *$f(n) = o(g(n))$ medför $f(n) = \mathrm{O}(g(n))$.*
3. *$f(n) = \Omega(g(n))$ då och endast då $g(n) = \mathrm{O}(f(n))$*
4. *$f(n) = \Theta(g(n))$ då och endast då*

$$\exists C_1, C_2, k > 0\colon C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|.$$

Exempel.

1. Låt $f(n) = n$ och $g(n) = n + 1$. Vi har $f \leq g$. Men $\lim_{n\to\infty} n/(n+1) = 1$, så f är inte lilla ordo av g.
2. Låt $f(n) = n$ och $g(n) = n^2$. Vi har $f(\frac{1}{2}) > g(\frac{1}{2})$ så f är inte mindre än g. Men $\lim_{n\to\infty} n/n^2 = \lim_{n\to\infty} n^{-1} = 0$, så f är lilla ordo av g.
3. $$\sum_{i=1}^{n} i \leq \sum_{i=1}^{n} n = n^2 = \mathrm{O}(n^2),$$
med $C = 1$ och $k = 1$ i definitionen av stora ordo.
4. $$\sum_{i=1}^{n} i \geq \sum_{i=\lceil n/2\rceil}^{n} i \geq \sum_{i=\lceil n/2\rceil}^{n} \lceil n/2\rceil = (n - \lceil n/2\rceil + 1)\lceil n/2\rceil \geq (n/2)(n/2) = n^2/4 = \Omega(n^2)$$
med $C = \frac{1}{4}$ och $k = 1$ i definitionen av stora omega. Med föregående exempel har vi alltså $\sum_{i=1}^{n} i = \Theta(n^2)$. Jämnför påst. 14.
5. $$\log(n!) = \sum_{i=1}^{n} \log i \leq \sum_{i=1}^{n} \log n \leq n \log n = \mathrm{O}(n \log n)$$
med $C = 1$ och $k = 1$ i definitionen av stora ordo.

LEMMA 3 (Generaliserad triangelolikhet). *Om $b_1, \ldots, b_n \in \mathbf{R}$, så*

$$\left|\sum_{i=1}^{n} b_i\right| \leq \sum_{i=1}^{n} |b_i|$$

Bevis. Induktion efter n.

Bas: För $n = 1$ är påståendet $|b_1| = |b_1|$, vilket är sant.

Induktionssteg: Vi vill först visa olikheten (»triangelolikheten«)

$$|a + b| \leq |a| + |b|, \qquad a, b \in \mathbf{R}. \tag{5}$$

För att inse detta observeras först

$$\begin{aligned} a+b &\leq |a|+|b|, \text{ eftersom } \quad a \leq |a|, \quad b \leq |b|, \\ -(a+b) &\leq |a|+|b|, \text{ eftersom } \quad -a \leq |a|, -b \leq |b|. \end{aligned}$$

Eftersom $|a+b|$ är antingen $a+b$ eller $-(a+b)$ följer (5) i alla fall.

Antag nu påståendet för något $n \geq 1$ och betrakta

$$\left|\sum_{i=1}^{n+1} b_i\right| = \left|b_{n+1} + \sum_{i=1}^{n} b_i\right| \leq |b_{n+1}| + \left|\sum_{i=1}^{n} b_i\right| \leq |b_{n+1}| + \sum_{i=1}^{n} |b_i| = \sum_{i=1}^{n+1} |b_i|,$$

där olikheterna använder respektive triangelolikheten och induktionshypotesen. ∎

PÅSTÅENDE 18. *Om* $a_0, \ldots, a_n \in \mathbf{R}$, *så*

$$\sum_{i=0}^{n} a_i x^i = \mathrm{O}(x^n).$$

Bevis. För $x > 1$ har vi

$$\left|\sum_{i=0}^{n} a_i x^i\right| \leq \sum_{i=0}^{n} |a_i| x^i = x^n \sum_{i=0}^{n} |a_i| x^{i-n} \leq x^n \sum_{i=0}^{n} |a_i|.$$

Detta visar påståendet med $C = \sum_{i=0}^{n} |a_i|$ och $k = 1$ i definitionen av stora ordo. ∎

Om $f, g\colon A \to \mathbf{R}$ definieras funktionerna $f+g$ och fg som

$$\begin{aligned} (f+g)\colon A \to \mathbf{R}, &\qquad (f+g)(x) = f(x) + g(x), \\ (f \cdot g)\colon A \to \mathbf{R}, &\qquad (f \cdot g)(x) = f(x) \cdot g(x). \end{aligned}$$

PÅSTÅENDE 19. *Om* $f_1(n) = \mathrm{O}(g_1(n))$ *och* $f_2(n) = \mathrm{O}(g_2(n))$, *så gäller*

1. $(f_1 + f_2)(n) = \mathrm{O}(g_1(n) + g_2(n)) = \mathrm{O}(\max\{g_1(n), g_2(n)\})$
2. $(f_1 \cdot f_2)(n) = \mathrm{O}(g_1(n) \cdot g_2(n))$

Bevis. [Rosen, Thm. 1.8.1, 1.8.2]. ∎

Uppgifter.

1. Om man kastar Kenny ut ur fönstret dör eller överlever han beroende på vilken våning han kastas från. Upp till och inklusive våning K (ett för oss okänd men fast tal, som vi kaller *kennytalet*), mår han fint; kastas kan från våning $K+1$ eller högre, då dör han. Vi försöker att fastställa kennytalet.

   Om vi bara har en Kenny till förfogande kastar vi honom från våning 1,2,3, etc. tills han dör. Vi behöver $\mathrm{O}(K)$ kast för detta. Har vi två Kennyr kan vi kasta den första från våning $1, 3, 5$ etc. tills han dör och därefter bestämma det exakta kennytal med ett extra kast. Det tar bara $\lceil (K+1)/2 \rceil + 1$ kast vilket dock fortfarande är $\mathrm{O}(K)$. Det känns som om vi har slösat bort den andra Kennyn.

   Hitta en metod för att bestämma kennytalet med två Kennyr och asymptotisk färre kast än $\mathrm{O}(K)$. Ledning: det går att göra i $\mathrm{O}(\sqrt{K})$.
2. Ordna följande funktioner efter deras tillväxt, dvs skriv dem på en lista $f_1(n)$, $f_2(n)$, ..., så att $f_i(n) = \mathrm{O}(f_{i+1}(n))$:

$$10^{10}, n^2, \log n, \log\log n, (\log n)^2, \sqrt{\log n}, n!, n^n,$$
$$n^2 \log n, n \log n \log\log n, n^{3/2}, 2^n, 2^{n^2}, 3^n, \log(n^2+1)$$

---

*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

5. Kombinatorik

5.1. Summa- och produktprincipen. *Produktprincipen* säger att två oberoende händelser kan uppträda på lika många sätt som produkten av varje. I mängdnotation: $|A \times B| = |A| \cdot |B|$.

En annan, och mera generell, formulering är följande. Låt $U_1, \dots, U_m$ vara en sekvens av uppgifter och antag att U_i kan göras på n_i sätt efter att $U_1, \dots, U_{i-1}$ har gjorts. Då kan hela sekvensen av uppgifter göras på $n_1 \cdots n_m$ sätt.

Exempel.

1. Om A är en ändlig mängd, så är $|P(A)| = 2^{|A|}$. För att räkna antal delmängder räknar vi antal olika sätt att välja en delmängd. En delmängd B av A kan väljas på följande sätt: för varje element $x \in A$ väljer vi, om x skal tillhöra B eller ej. Vi har $|A|$ val, varje val kan göras på två sätt. Produktprincipen ger att det finns $2^{|A|}$ sätt att välja B på.
2. $|\Sigma^k| = |\Sigma|^k$. En sträng $\sigma_1 \cdots \sigma_k \in \Sigma^k$ kan skapas genom att välja först σ_1, sen σ_2, etc. Varje tecken kan väljas på $|\Sigma|$ sätt.
3. $|A^k| = |A|^k$. En tuppel i A^k kan skapas genom att välja k värden från A.
4. $|B^A| = |B|^{|A|}$. En funktion $f\colon A \to B$ kan skapas på följande sätt: för varje element i definitionsmängden $a \in A$ väljer vi värdet $f(a) \in B$. Det finns $|A|$ val mellan $|B|$ möjligheter.
5. Vi räknar de injektiva funktionerna från A till B. Om $|A| > |B|$ finns det inga injektiva funktioner från A till B, så vi betraktar det intressantare fallet $|A| \leq |B|$. Låt $A = \{a_1, \dots, a_m\}$. Vi vill välja $f(a_1), f(a_2), \dots$ i tur och ordning. Det finns $|B|$ möjligheter för att välja $f(a_1)$. Eftersom f är injektiv finns måste $f(a_2)$ väljas från $B - f(a_1)$, det finns $|B| - 1$ möjligheter för detta. Generellt kan vi välja $f(a_k)$ på $|B| - k + 1$ sätt. Enligt produktprincipen finns det $|B|(|B|-1)\cdots(|B|-|A|+1)$ injektiva funktioner.

Två händelser är *ömsesidigt uteslutande* om de inte kan uppträda samtidigt. *Summaprincipen* säger att någon av två ömsesidigt uteslutande händelser kan uppträda på lika många sätt som summan av varje. I mängdnotation: om $A \cap B = \emptyset$ så $|A \cup B| = |A| + |B|$.

En annan, och mera generell, formulering är följande: Låt $U_1, \dots, U_m$ vara en sekvens av uppgifter och antag att U_i kan göras på n_i sätt. Då kan uppgiften »antingen U_1 eller U_2 eller $\cdots$ eller U_m« göras på $n_1 + \cdots + n_m$ sätt.

Inkludering-exkluderingsprincipen är en utvidgning av summaprincipen. I mängdnotation: $|A \cup B| = |A| + |B| - |A \cap B|$.

Exempel.

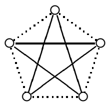
1. Låt $\Sigma^{\leq m}$ ange mängden av strängar över Σ av längd högst m, dvs
$$\Sigma^{\leq m} = \bigcup_{i=0}^{m} \Sigma^i.$$
Vi vill visa att $|\Sigma^{\leq m}| = \sum_{i=0}^{m} |\Sigma|^i$. En sträng i $\Sigma^{\leq m}$ har antingen längd 0 eller 1 eller $\cdots$ eller m. Vi kan välja en sträng av längd i på $|\Sigma|^i$ sätt, som vi såg enligt produktregeln i exemplet ovan.
2. Låt S vara mängden av bitsträngar av längd 6 som börjar på 1 eller slutar på 00. För att beräkna $|S|$ betraktar vi två relaterade mängder: A är mängden av längd-6-bitsträngar som börjar på 1, och B är mängden av längd-6-bitsträngar som slutar på 00. Produktprincipen ger $|A| = 2^5$ och $|B| = 2^4$. Dessa mängder är inte disjunkta, och produktprincipen ger $|A \cap B| = 2^3$. Inkludering-exkluderingsprincipen ger $|S| = 2^5 + 2^4 - 2^3 = 40$.

5.2. Duvhålsprincipen. Om $n+1$ duvor fördelas på n hål måste ett hål innehålla minst två duvor.

Exempel.

1. I en grupp på 367 människor måste två ha samma födelsedag (*födelsedagssatsen*).
2. Om $n+1$ tal väljes ur $\{1,2,3,\ldots,2n\}$ så dividerar ett av talen ett annat. (Observera först att om vi bara väljer n tal, t ex $\{n+1,n+2,\ldots,2n\}$, behöver de inte dividera varann.) För att bevisa påståendet skriver vi varje tal som produkten av en tvåpotens och ett udda tal, t ex $40 = 2^3 \cdot 5$, $1 = 2^0 \cdot 1$, $14 = 2^1 \cdot 7$, etc. Vi placerar talen i n lådor $1,3,5,\ldots,2n-1$ så att talet $2^i \cdot l$ hamnar i låda l. Det finns $n+1$ tal och bara n lådor, så en av lådorna måste innehålla två tal, kalla dem $2^i \cdot l$ och $2^j \cdot l$ $(i < j)$. Vi har $2^j \cdot l/(2^i \cdot l) = 2^{j-i}$.
3. Vi vill visa *vänskapssatsen*: i varje grupp av sex personer finns tre vänner (dvs varje par har redan träffats tidigare) eller tre främlingar (dvs ingen av de tre har träffats tidigare). Kalla personen Ett, Två, ..., Sex. Vi kan indela Två till Sex i två mängder, V (Etts vänner) och F (främlingar för Ett). Enligt den utvidgade lådprincipen har en av mängderna minst $\lfloor (5-1)/2 \rfloor + 1 = 3$ element. Det finns två fall. Om V har 3 element är de antingen främlingar för varann (då har vi en trio främlingar) eller minst två av dem är vänner och skapar därmed en trio vänner med Ett. Om F har 3 element är de antingen en trio vänner eller minst två av dem är främlingar (då har vi en trio främlingar med Ett). Vänskapssatsen är bevisad.

   Observera att en grupp på 5 personer inte är nog. Om vi ritar vänner som ○—○ och främlingar som ○···○ då kan vi rita gruppen



5.3. Permutationer och kombinationer. En *r-permutation* av en mängd S är ett ordnat arrangemang av r element från S. Om $r = |S|$ kallas arrangemanget en *permutation av S.*

Sats 2. *Antalet r-permutationer av en mängd med n element är*

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

En *r-kombination* av en mängd S är en r-delmängd av S.

Sats 3. *Antalet r-kombinationer av en mängd med n element är*

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

Sats 4. *För positivt heltal n gäller*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Påstående 20. *Låt $0 \le r \le n$ och $r \le m$. Då gäller*

1.

$$\binom{n}{r} = \binom{n}{n-r}$$

2.
$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

3.
$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

4.
$$\binom{n+m}{r} = \sum_{i=0}^{r} \binom{m}{r-i}\binom{n}{i}$$

5.4. Några uppskattningar. Binomialkoefficienterna är notoriskt svårtberäknade. Det är klart att $0 \leq \binom{n}{k} < 2^n$, och detta avsnitt etablerar några mer försiktiga uppskattningar, som är tillräckligt precisa i många fall.

För $n \geq k > 2$ gäller

$$\frac{n}{k} \leq \frac{n-1}{k-1} \leq \frac{n}{2}.$$

Genom att upprepa detta argument fås

$$\frac{n}{k} \cdot \frac{n}{k} \cdots \frac{n}{k} \leq \frac{n}{k} \cdot \frac{n-1}{k-1} \cdots \frac{n-k+1}{1} \leq \frac{n}{2} \cdot \frac{n}{2} \cdots \frac{n}{2},$$

vilket etablerar

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{n}{2}\right)^k, \quad (2 < k \leq n). \tag{6}$$

Man kan uppnå en något bättre övre gräns:

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k, \quad (1 \leq k \leq n), \tag{7}$$

där $e \approx 22/7$ är den naturliga logaritmens bas. Detta kräver ett lite längre argument.

PÅSTÅENDE 21. $\binom{n}{k} < \left(\frac{en}{k}\right)^k$.

Bevis. För alla $t \in \mathbf{R}$, $t \neq 0$ gäller $1 + t < e^t$. Detta inses antingen genom derivation eller genom att betrakta exponentialfunktionens Taylorutveckling. Från Binomialsatsen 4 får vi

$$e^{nt} = (e^t)^n > (1+t)^n = \sum_{i=0}^{n} \binom{n}{i} t^i > \binom{n}{k} t^k, \quad 0 \leq k \leq n.$$

Låt $t = k/n$ i ovanstående uttryck. Då fås

$$e^k > \binom{n}{k}\left(\frac{k}{n}\right)^k,$$

som önskat. ∎

Uppgifter.

1. Låt $S = \{1, 2, 3, 4\}$. Lista följande mängder:
   (a) alla 2-tuppler av element från S (dvs mängden $S \times S$)
   (b) alla 2-permutationer av S
   (c) alla 2-kombinationer av S.

Skissa svaret på samma fråga med 5-tuppler, -permutationer och -kombinationer.

*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

6. Ändlig sannolikhetsteori

Ett (ändligt) *utfallsrum* är en (ändlig) mängd S av *elementarhändelser*. Ett sannolikhetsmått är en funktion

$$p\colon S \to \mathbf{R}$$

som uppfyller följande villkor:

1. $0 \leq p(s) \leq 1$ för alla $s \in S$
2. $\sum_{s\in S} p(s) = 1$.

Exempel.

1. Låt $T = \{\text{⚀},\text{⚁},\text{⚂},\text{⚃},\text{⚄},\text{⚅}\}$ vara utfallsrummet av kast med en tärning. Vi definierar ett sannolikhetsmått p_1 på T genom att ange värdet på varje utfall:
$$p_1(\text{⚀}) = p_1(\text{⚁}) = \cdots = p_1(\text{⚅}) = \tfrac{1}{6},$$
vilket vi kan uppfatta som kast med en symmetrisk tärning. Ett annat sannolikhetsmått är
$$p_2(\text{⚀}) = p_2(\text{⚁}) = \cdots = p_2(\text{⚄}) = \tfrac{1}{7}, \quad p_2(\text{⚅}) = \tfrac{2}{7}$$
vilket vi kan uppfatta som kast med en tärning som favoriserar ⚅.
2. Låt T^2 ange utfallsrummet av kast med två tärningar,
$$T^2 = \{\text{⚀⚀},\text{⚀⚁},\ldots,\text{⚅⚅}\}.$$
Vi uppfattar dessa tärningar som olika, dvs att utfallen ⚁⚂ och ⚂⚁ är olika. Ett sannolikhetsmått på T^2 är
$$p_3(t_1t_2) = \tfrac{1}{36} \qquad \text{för alla } t_1t_2 \in T^2.$$
Ett annat mått är
$$p_4(\text{⚀⚀}) = p_4(\text{⚁⚁}) = \cdots = p_4(\text{⚅⚅}) = \tfrac{1}{6}, \qquad p_4(t_1t_2) = 0 \text{ annars.}$$

6.1. Händelser. En *händelse* är en delmängd $E \subseteq S$. *Sannolikheten av en händelse* är

$$p(E) = \sum_{s\in E} p(s).$$

Exempel.

1. Händelsen »antal ögon udda« är delmängden $U = \{\text{⚀},\text{⚂},\text{⚄}\}$. Under måttet p_1 (symmetrisk tärning) är dess sannolikhet
$$p_1(U) = p_1(\text{⚀}) + p_1(\text{⚂}) + p_1(\text{⚄}) = \tfrac{1}{6} + \tfrac{1}{6} + \tfrac{1}{6} = \tfrac{1}{2}.$$
Under måttet p_2 (osymmetrisk tärning) är sannolikheten
$$p_2(U) = p_2(\text{⚀}) + p_2(\text{⚂}) + p_2(\text{⚄}) = \tfrac{1}{7} + \tfrac{1}{7} + \tfrac{1}{7} = \tfrac{3}{7}.$$
2. Om alla elementarhändelser är lika sannolika, dvs
$$p(s) = \frac{1}{|S|}, \qquad \text{för alla } s \in S,$$
så fås för godtycklig händelse $E \subseteq S$
$$p(E) = \sum_{s\in E} p(s) = \sum_{s\in E} \frac{1}{|S|} = \frac{|E|}{|S|}.$$
I exemplet ovan är förvisso
$$p_1(U) = \frac{|U|}{|T|} = \frac{|\{\text{⚀},\text{⚂},\text{⚄}\}|}{|\{\text{⚀},\text{⚁},\text{⚂},\text{⚃},\text{⚄},\text{⚅}\}|} = \frac{1}{2},$$

men detta gäller inte för p_2.

3. Händelsen »dubblett« $D =$ {⚀⚀, …, ⚅⚅} $\subseteq T^2$ har sannolikheterna $p_3(D) = 6 \cdot \frac{1}{36} = \frac{1}{6}$ och $p_4(D) = 1$ under olika sannolikhetsmått.

PÅSTÅENDE 22. *Låt $E, F \subseteq S$ vara händelser i ett ändligt utfallsrum. Då gäller*

1. $p(\overline{E}) = 1 - p(E)$
2. $p(E \cup F) = p(E) + p(F) - p(E \cap F)$

Bevis. Vi har enligt definitionen av sannolighetsmåttet

$$1 = \sum_{s \in S} p(s) = \sum_{s \in E} p(s) + \sum_{s \in \overline{E}} p(s) = p(E) + p(\overline{E}),$$

vilket ger första påståendet.

För det andra påståendet har vi

$$p(E \cup F) = \sum_{s \in E \cup F} p(S) = \sum_{s \in E} p(S) + \sum_{s \in F} p(S) - \sum_{s \in E \cap F} p(S) = p(E) + p(F) - p(E \cap F),$$

som önskat. ∎

6.2. Betingad sannolikhet. Den *betingade sannolikheten för E givet F* är

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)},$$

om $p(F) > 0$ (annars är $p(E \mid F)$ odefinierad). Händelserna E och F är *oberoende* om

$$p(E \cap F) = p(E)p(F).$$

Observera att om E och F är oberoende och $p(F) > 0$, så gäller

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)} = \frac{p(E)p(F)}{p(F)} = p(E).$$

Exempel.

1. Betrakta utfallsrummet T_2 och händelserna

   $A =$ {⚀⚀, ⚀⚁, …, ⚀⚅} och $B =$ {⚀⚀, ⚁⚀, …, ⚅⚀},

   dvs första (resp andra) tärningen ger ⚀. Observera att händelsen $A \cap B$ är {⚀⚀}.

   Vi studerar först måttet p_3. Vi har $p_3(A) = p_3(B) = 6 \cdot \frac{1}{36} = \frac{1}{6}$, så

   $$p_3(A) \cdot p_3(B) = \tfrac{1}{6} \cdot \tfrac{1}{6} = \tfrac{1}{36} = p_3(A \cap B),$$

   dvs A och B är oberoende.

   Betrakta nu p_4. Vi har $p_4(A) = \frac{1}{6}$ och $p_4(B) = \frac{1}{6}$ men också $p_4(A \cap B) = \frac{1}{6}$, så A och B är *inte* oberoende. Observera speciellt at

   $$p_4(A \mid B) = p_4(B \mid A) = 1.$$

6.3. Slumpvariabler och förväntning. En *slumpvariabel* är en funktion

$$X\colon S \to \mathbf{R}.$$

Förväntningen av en slumpvariabel är

$$E(X) = \sum_{s\in S} p(s)X(s).$$

Exempel.

1. Definiera

$$S\colon T^2 \to \mathbf{R}$$

så att $S(t_1t_2)$ är antal ögon, t ex $S(\text{⚂⚃}) = 7$.

Under sannolikhetsmåttet p_5 fås

$$E(S) = \tfrac{1}{6}S(\text{⚀⚀}) + \tfrac{1}{6}S(\text{⚁⚁}) + \cdots + \tfrac{1}{6}S(\text{⚅⚅}) + 0\cdot S(\text{⚀⚁}) + \cdots = \tfrac{1}{6}(2+4+6+8+10+12) = 7,$$

en summa av 36 termer, varav 30 har koefficient 0.

Under sannolikhetsmåttet p_3 är förväntningen

$$E(S) = \sum_{t_1t_2\in T^2} p_3(s)S(t_1t_2) = \frac{1}{36}\big((1+1)+(1+2)+\cdots+(6+6)\big) = \frac{1}{36}\cdot 282 = 7,$$

en summa av 36 termer.

Låt U vara ett utfallsrum, p en sannolikhet, och X en slumpvariabel. Slumpvariabler ger upphov till ett nytt utfallsrum där elementarhändelsen är av typen »$X(s) = r$« för alla $r \in X(S)$ och sannolikheten är

$$p\big(X(s) = r\big) = \sum_{s\in S\wedge X(s)=r} p(s)$$

Oftast skrivs $X = r$ för $X(s) = r$.

PÅSTÅENDE 23.

$$E(X) = \sum_{r\in X(S)} p(X=r)r.$$

Bevis.

$$E(X) = \sum_{s\in S} X(s)p(s) = \sum_{r\in X(S)}\ \sum_{s\in S\wedge X(s)=r} X(s)p(s) = \sum_{r\in X(S)}\ \sum_{s\in S\wedge X(s)=r} rp(s) = \sum_{r\in X(S)} r \sum_{s\in S\wedge X(s)=r} p(s) = \sum_{r\in X(S)} rp(X=r).$$

∎

Exempel.

1. För S som i exemplet ovan är utfallsrummet

$$\{S=2, S=3, \ldots, S=12\}.$$

När vi väljer en sannolikhet (för T^2) har vi också en sannolikhet för detta rum. T ex för p_3:

$$p_3(S=4) = p_3(\text{⚀⚂}) + p_3(\text{⚁⚁}) + p_3(\text{⚂⚀}) = \tfrac{3}{36} = \tfrac{1}{12}$$

Vi beräknar $E(S)$ med påståendet ovan:

$$E(S) = 2 \cdot p_3(S = 2) + 3 \cdot p_3(S = 3) + 4 \cdot p_3(S = 4) + \cdots + 12 \cdot p_3(S = 12) = \tfrac{2}{36} + \tfrac{3}{18} + \tfrac{4}{12} + \cdots + \tfrac{12}{12} = 7,$$

en summa av bara 11 termer.

Observera att $E(S)$ under p_4 är även enklare:

$$E(S) = \frac{2}{6} + \frac{4}{6} + \frac{6}{6} + \frac{8}{6} + \frac{10}{6} + \frac{42}{6} = 7.$$

Påstående 24. *Om X och Y är slumpvariabler på samma utfallsrum, så gäller*

1. $E(X + Y) = E(X) + E(Y)$
2. $E(aX + b) = aE(X) + b$, *där* $a, b \in \mathbf{R}$.

Exempel. Låt de slumpvariablerna S_1 och S_2 ange antal ögon på första och andra tärningen, dvs $S_1(\text{⚀⚄}) = 1$. Betraka sannolikheten p_4 och observera

$$E(S_1) = E(S_2) = \frac{1}{6}(1 + 2 + 3 + 4 + 5 + 6) = \frac{7}{2}.$$

Vi har med resultatet ovan

$$E(S) = E(S_1 + S_2) = \frac{14}{2} = 7.$$

Två slumpvariabler X och Y är *oberoende* om

$$p(X = x \wedge Y = y) = p(X = x)p(Y = y), \qquad \text{för alla } r \in \mathbf{R}.$$

Exempel.

1. Betrakta S_1 och S_2 under sannolikheten p_4. Vi har t ex

$$p_4(S_1 = 3 \wedge S_2 = 2) = p_4(\text{⚂⚁}) = 0,$$

men också

$$p_4(S_1 = 3) = p_4(\text{⚂⚂}) = \tfrac{1}{6}, \quad \text{och} \quad p_4(S_2 = 2) = p_4(\text{⚁⚁}) = \tfrac{1}{6}.$$

så $p_4(S_1 = 3)p_4(S_2 = 2) = \frac{1}{36}$. Därför är S_1 och S_2 inte oberoende under p_4.

2. Betrakta nu S_1 och S_2 under p_3. Vi vill visa oberoendehet, dvs

$$p_3(S_1 = i \wedge S_2 = j) = p_3(S_1 = i)p_3(S_2 = j)$$

för alla reella i, j. Om $i, j \notin \{1, 2, 3, \cdots, 6\}$ är sannolikheterna på båda sidorna 0. Annars är

$$p_3(S_1 = i \wedge S_2 = j) = \frac{1}{36},$$

eftersom det bara finns en händelse med detta resultat (nämligen där första tärning har i ögon och andra tärning j ögon), och denna händelse inträffar med sannolikhet $\frac{1}{36}$ under p_3. Motsvarende är

$$p_3(S_1 = i) = \frac{1}{36} + \frac{1}{36} + \cdots + \frac{1}{36} = \frac{1}{6}$$

eftersom det finns 6 händelser som ger värdet i till S_1.

Sats 5. *Om X och Y är oberoende slumpvariabler gäller*

$$E(XY) = E(X)E(Y).$$

Exempel. Vi definierar slumpvariabeln P på T^2 som produkten av ögonen; $P($⚂⚄$) = 15$. Betrakta p_4 och observera

$$E(P) = \tfrac{1}{6}(1\cdot 1 + 2\cdot 2 + 3\cdot 3 + 4\cdot 4 + 5\cdot 5 + 6\cdot 6) = \tfrac{91}{6}.$$

Detta är inte det samma som

$$E(S_1)E(S_2) = \tfrac{7}{2}\cdots\tfrac{7}{2} = \tfrac{49}{4}.$$

Under p_3 är S_1 och S_2 oberoende, så vi kan skriva

$$E(P) = E(S_1S_2) = E(S_1)E(S_2) = \tfrac{49}{4},$$

vilket kan verifieras – och uppskattas! – genom att beräkna $E(P)$ utifrån definitionen.

6.4. Bernoulliförsök. Betrakta ett experiment med två utfall, det *lyckas* med sannolikhet p, eller *misslyckas* med sannolikhet $q = 1 - p$.

Ett experiment med två utfall, succe och misslyckande kallas ett bernoulliförsök.

PÅSTÅENDE 25. *Sannolikheten för att exakt k utav n oberoende bernoulliförsök lyckas är*

$$b(k; n, p) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Exempel.

1. En (symmetrisk) mynt kastas n gånger. Sannolikheten för exakt k utfall »krona« är $b(k; n, \frac{1}{2})$. Det är överraskande hur skarpt detta är koncentrerat kring hälften. För $n = 1000$ kan man beräkna
$$b(500; 1000, \tfrac{1}{2}) = 0{,}025225\ldots$$
och
$$b(900; 1000, \tfrac{1}{2}) < 0{,}59 \cdot 10^{-161}.$$
2. Låt X ange slumpvariabeln som räknar antal lyckade av n bernoulliförsök.

   Observera att elementarhändelserna i utfallsrummet nu är resultaten av alla n försök, dvs tuppler med n element där varje element kan vara »lyckades« eller »misslyckades«. Här är några elementarhändelser för $n = 3$: $\{(l,l,m), (l,m,l), (m,m,l), \ldots\}$, och $X(l,l,m) = 2$.

   Förväntningen av X kan beräknas som i exempel [R: 4.5.14]. Alternativt kan X_i definieras och beräknas som i exempel [R: 4.5.16]

*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

7. Rekursionsekvationer och genererande funktioner (supplement)

Det kan visas att om C och D är olika, så gäller

$$\frac{Ax+B}{(1-Cx)(1-Dx)} = \frac{a}{1-Cx} + \frac{b}{1-Dx}$$

för konstanter a och b. Om D, E och F är olika, gäller

$$\frac{Ax^2+Bx+C}{(1-Dx)(1-Ex)(1-Fx)} = \frac{a}{1-Dx} + \frac{b}{1-Ex} + \frac{c}{1-Fx}$$

för konstanter a, b och c.

Exempel.

1. Betrakta rekursionsekvationen

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 4, \\ a_k &= a_{k-1} + 6a_{k-2}. \end{aligned}$$

Låt $G(x) = \sum_{k=0}^{\infty} a_k x^k$ och observera

$$\begin{aligned} xG(x) &= \sum_{k=0}^{\infty} a_k x^{k+1}, \\ 6x^2G(x) &= \sum_{k=0}^{\infty} 6a_k x^{k+2}, \end{aligned}$$

vilket vi behöver i följande beräkning:

$$G(x) - xG(x) - 6x^2G(x) = \sum_{k=0}^{\infty} a_k x^k - \sum_{k=0}^{\infty} a_k x^{k+1} - \sum_{k=0}^{\infty} 6a_k x^{k+2} =$$

$$a_0 + (a_1 - a_1)x + \sum_{k=2}^{\infty} (a_k - a_{k-1} - 6a_{k-2})x^k = a_0 + (a_1 - a_0)x = 1 + 3x.$$

Vi får

$$G(x) = \frac{1+3x}{1-x-6x^2} = \frac{1+3x}{(1-3x)(1+2x)} = \frac{1}{5}\left(\frac{6}{1-3x} - \frac{1}{1+2x}\right) =$$

$$\frac{1}{5}\left(\sum_{k=0}^{\infty} 3^i x^i - \sum_{k=0}^{\infty} (-2)^k x^k\right),$$

varav $a_k = \frac{6}{5}3^k - \frac{1}{5}(-2)^k$.

2. I stället för att *gissa* de rätta funktionerna som $xG(x)$ och $6x^2G(x)$ i exemplet ovan kan man tillämpa följande strategi: (i) Multiplicera båda sidorna i rekursionsekvationen med x^k, (ii) summera över alla k där ekvationen är sann, i vårt fall från 2 till ∞. I exemplet fås

$$\begin{aligned} a_k &= a_{k-1} + 6a_{k-2}, \\ a_k x^k &= a_{k-1} x^k + 6a_{k-2} x^k, \\ \sum_{k=2}^{\infty} a_k x^k &= \sum_{k=2}^{\infty} a_{k-1} x^k + \sum_{k=2}^{\infty} 6a_{k-2} x^k. \end{aligned}$$

Nu gäller det att rekonstruera summor av formen $\sum_{k=0}^{\infty} a_k x^k$ i detta uttryck. Vänsterledet är nästan klart:

$$\sum_{k=2}^{\infty} a_k x^k = \sum_{k=0}^{\infty} a_k x^k - a_0 - a_1 x = \sum_{k=0}^{\infty} a_k x^k - 1 - 4x.$$

Högerledet kräver flera manipulationer,

$$\sum_{k=2}^{\infty} a_{k-1} x^k + \sum_{k=2}^{\infty} 6a_{k-2} x^k = x \sum_{k=2}^{\infty} a_{k-1} x^{k-1} + 6x^2 \sum_{k=2}^{\infty} a_{k-2} x^{k-2} =$$

$$x \sum_{k=1}^{\infty} a_k x^k + 6x^2 \sum_{k=0}^{\infty} a_k x^k = x(\sum_{k=0}^{\infty} a_k x^k - a_0) + 6x^2 \sum_{k=0}^{\infty} a_k x^k = x \sum_{k=0}^{\infty} a_k x^k - 6x^2 \sum_{k=0}^{\infty} a_k x^k - x.$$

Om vi skriver $G(x)$ för $\sum_{k=0}^{\infty} a_k x^k$ har vi igen

$$G(x) - 1 - 4x = xG(x) - 6x^2 G(x) - x$$

som i exempel 1.

3. Betrakta

$$a_0 = 9$$
$$a_k = 8a_{k-1} + 10^{k-1}, \quad (k \geq 1).$$

(Rosens exempel [R:5.4.17] är liknande men hans sekvens börjar i a_1 i stället, vilket behöver ytterligare ett trick.)

Vi multiplicerar båda sidorna med x^k och summerar från 1:

$$\sum_{k=1}^{\infty} a_k x^k = 8 \sum_{k=1}^{\infty} a_{k-1} x^k + \sum_{k=1}^{\infty} 10^{k-1} x^k$$

Sätts $G(x) = \sum_{k=0}^{\infty} a_k x^k$, blir vänsterledet $G(x) - a_0$, och högerledet blir

$$8 \sum_{k=0}^{\infty} a_k x^{k+1} + \sum_{k=0}^{\infty} 10^k x^{k+1} = 8xG(x) + \frac{x}{1 - 10x}$$

enligt tabel [R:5.4.1]. Härav fås

$$G(x) = \frac{9 - 89x}{(1 - 10x)(1 - 8x)} = \frac{1}{2}\frac{1}{1 - 10x} + \frac{17}{2}\frac{1}{1 - 8x} = \frac{1}{2}\sum_{k=0}^{\infty} 10^k x^k + \frac{17}{2}\sum_{k=0}^{\infty} 8^k x^k.$$

Vi konkluderar att $a_k = \frac{1}{2}10^k + \frac{17}{2}8^k$.

4. Om rekursionsekvationen inte definierar a_0, som ju behövs för över huvud taget att kunne skriva $\sum_{k=0}^{\infty} a_k x^k$, måste man konstruera ett värde för a_0. Exempel [R:5.4.17] betraktar

$$a_1 = 9$$
$$a_k = 8a_{k-1} + 10^{k-1}, \quad (k \geq 2),$$

vars sekvens börjar som

a_1	a_2	a_3	$\cdots$
9	82	756	$\cdots$

Rosen sätter nu $a_0 = 1$. Detta är konsistent med ekvationen, och i princip betraktar han

$$a_0 = 1$$
$$a_k = 8a_{k-1} + 10^{k-1}, \quad (k \geq 1),$$

vars sekvens börjar

a_0	a_1	a_2	a_3	$\cdots$
1	9	82	756	$\cdots$

Alternativet är att betrakta samma sekvens, men upfatta den som börjande i a_0:

a'_0	a'_1	a'_2	$\cdots$
9	82	756	$\cdots$

Rekursionsekvationen för denna är

$$a'_0 = 9,$$
$$a'_k = 8a'_{k-1} + 10^k,$$

som kan lösas som vanligt. Helt formellt har vi introducerat en ny sekvens a'_k där $a'_k = a_{k-1}$.

8. Grafer

En (oriktad, enkel) *graf* är en tuppel $G = (V, E)$ där $E \subseteq \binom{V}{2}$. Mängden V kallas grafens *hörn*, mängden E kallas grafens *kanter*. Ibland skrivs kanten $\{u, v\}$ som uv eller vu.

En *riktad graf* är en tuppel $G = (V, E)$ där $E \subseteq V^2$. Mängden V kallas grafens *noder*, mängden E kallas grafens *bågar*. Ibland skrivs bågen (u, v) som uv. Observera att $uv \neq uv$ i motsättning til (oriktade) grafer.

En (oriktad) *multigraf* är en tuppel $G = (V, E)$ och en funktion

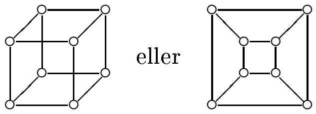
$$f\colon E \to \binom{V}{2},$$

dvs grafen har *multipla kanter*: två kanter $e_1, e_2 \in E$ med $f(e_1) = f(e_2)$. En (oriktad) *pseudograf* är en multigraf där

$$f\colon E \to \binom{V}{2} \cup V,$$

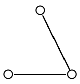
dvs grafen har multipla kanter och *öglor* $f(e) = \{v, v\}$.

Exempel. Terminologien antyder att vi inte brukar uppfatta en graf som en tuppel av delmängder. Till exempel kan grafen $(\{1, 2, 3, 4, 5, 6, 7, 8\},\ \{12, 23, 34, 41, 56, 67, 78, 85, 15, 26, 37, 48\})$ ritas som

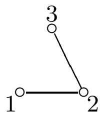


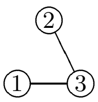
figuren till vänster motiverar även begreppen »hörn« och »kant«. Observera att det finns många sätt att rita samma graf.

Ibland är hörnens namn vigtiga. Till exempel är $G_1 = (\{1, 2, 3\}, \{12, 23\})$ och $G_1 = \{1, 2, 3\}, \{13, 23\})$ inte samma graf, även om både kan ritas som

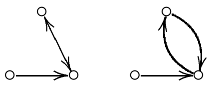


Man kan då ytterligare dekorera sina ritningar med hörnnamn

$G_1 =$ 

$G_2 =$ 

Bågarna i en riktad graf ritas som pilar. Här är två ritningar av $(\{1, 2, 3\}, (1, 2), (2, 3), (3, 2)\})$:



Om kanten uv finns i grafen kallas u och v för *grannar*. Hörnen u och v är *endpunkter* för kanten uv, och kallas *incidenta* till u och v. Ett hörns *grad*

$$\deg(w) = |\{\, w \in W \mid \{v, w\} \in W \}|$$

är dess antal grannar. I en riktad graf definieras *ingrad* och *utgrad* som

$$\deg^-(v) = |\{\, w \in W \mid (v, w) \in E \,\}|$$
$$\deg^+(v) = |\{\, w \in W \mid (w, v) \in E \,\}|.$$

Exempel.

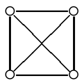
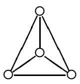
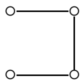
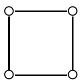
1. Betrakta en oriktad graf. För varje hörn, räkna kanterna incidenta till hörnet. Härmed räknas varje kant i grafen exakt två gånger (en gång från varje endpunkt), dvs
$$\sum_{v \in V} \deg(v) = 2|E|.$$
Speciellt är gradsummen jämn. Denna observation kallas *handskakningslemmat*, och visar att det ved varje fest finns ett jämnt antal handskakningar.
2. Finns det en graf med 5 noder med udda grad? Vi kan indela hörnmängden i $V = U \cup J$, hörnen med udda och jämn grad. Vi har
$$\sum_{v \in V} \deg(v) = \sum_{v \in U} \deg(v) + \sum_{v \in J} \deg(v),$$
dvs att $\sum_{v \in J} \deg(v)$ kan skrivas som differensen av två jämna tal och är då själv jämn. Eftersom summen av ett udda antal udda tal är udda måste $|J|$ vara jämn. Konklusionen är att en graf alltid har en jämnt antal noder med udda grad.

En graf (V, E) är en *väg* om
$$V = \{x_0, x_1, \dots, x_k\}, \quad E = \{x_0x_1, x_1x_2, \dots, x_{k-1}x_k\},$$
där alla x_i är olika. Vägens *längd* är k, antalet av kanter. Vi låter P_k beteckna vägen av längd k. Vi kan ange en väg genom att ange dess hörn i ordning.

Om (V, E) med $V = \{x_0, \dots, x_{k-1}\}$ och $k \geq 3$ är en väg så kallas grafen $(V, E \cup \{x_kx_0\})$ en *cykel* av längd k och betecknas C_k. Ofta kallas C_3 även för *triangeln* och C_5 *pentagonen*. En *cyklisk* graf är en graf som innehåller en cykel.

En graf är en *klick* om $E = \binom{V}{2}$; vi låter K_n beteckna klicken med n hörn. En graf är *oberoende* om $E = \emptyset$; vi låter I_n beteckna n oberoende hörn ('I' för *independent*).

Exempel.

$K_4 =$  $=$  $P_3 =$  $C_4 =$ 

Om $G = (V, E)$ och $G' = (V', E')$ med $V' \subseteq V$ och $E' \subseteq E$ säjer vi att G är en *delgraf* av G' och att G' *innehåller* G.

En graf är *sammanhängande* om varje par av noder har en väg mellan sig.

8.1. Träd. En *skog* är en graf utan cykler, och ett (fritt) *träd* är en sammanhängande skog.

PÅSTÅENDE 26. *En graf $G = (V, E)$ är ett träd om och endast om det finns en unik väg mellan varje par av hörn.*

Bevis. Antag G är ett träd och betrakta $u, v \in V$. Eftersom G är sammanhängande finns det en väg från u till v. Antag nu att det finns två väger från u till v, kallad $x_1, \dots, x_k$ och $y_1, \dots y_r$ (där $x_1 = y_1 = u$ och $x_k = y_r = v$). Betrakta det minsta i så att $x_i \neq y_i$ och de minsta $j > i, k > i$ så att $x_j = y_k$. Då är $x_ix_{i+1} \dots x_jy_{k-1}y_{k-2}y_{i+1}$ en cykel, i motstrid med att G är ett träd.

Antag nu att G har en unik väk mellan varje par av hörn. Speciellt är G sammanhängande. För att inse att G är utan cykler observera att hörnen på en cykel är förbundna med minst två vägar. ∎

LEMMA 4. *Ett träd* $G = (V, E)$ *med* $|V| > 1$ *har ett hörn* $v \in V$ *med* $\deg(v) = 1$, *kallad ett* löv.

Bevis. Antag i stället att alla hörn har grad minst 2. Vi vill visa att då måste G innehålla en cykel.

Låt v_1 vara att hörn i G. Eftersom $\deg(v_1) \geq 1$ har den en granne v_2 av grad minst 2, som därför själv måste ha en ny granne $v_3 \neq v_1$. Vi har konstruerat en väg $v_1v_2v_3$. Generellt, efter $k \geq 3$ steg, har vi konstruerat en väg $v_1v_2 \cdots v_k$. Eftersom $\deg(v_k) \geq 2$ har v_k en granne $v_{k+1} \neq v_{k-1}$. Om $v_{k+1} \in \{v_1, \ldots, v_{k-1}\}$ har vi hittat en cykel (och är färdiga), annars är $v_1v_2 \cdots v_{k+1}$ en väg. När $k = n$ kan processen inte fortsätta (vägen innehåller då alla hörn), så vi måste hitta en cykel. ∎

PÅSTÅENDE 27. *En graf* $G = (V, E)$ *är ett träd om och endast om* G *är sammanhängande och* $|V| = |E| + 1$.

Bevis. (*rightarrow*) Antag att G är ett träd. Det är klart att G är sammanhängande. Vi användar induktion efter $n = |V|$ till att visa att $|V| = |E| + 1$. För $n = 1$ består G av bara ett hörn och inga kanter, så $|V| = 1 = 0 + 1 = |E| + 1$. Betrakta ett träd med $n+1$ hörn. Välg ett löv v med $\deg(v) = 1$, detta finns enligt lemmat ovan. Ta bort v och dess incidenta kant e. Grafen G' som är kvar är ett träd: den är klart acyklisk (G var acyklisk, och borttagningen av v kan inte skapa en cykel), och den är sammanhängande, eftersom två hörn u, w som var förbundna i G inte kan ha användt v på vägen (v var ett löv). Eftersom G' är ett träd med n hörn måste den ha $n - 1$ kanter per induktion, så G har $n - 1 + 1$ kanter.

($\leftarrow$) Antag att G är en sammanhängande graf med n hörn och $n - 1$ kanter. Vi vill visa att den är acyklisk. .... ∎

Ett *m-ärt träd* är antingen

1. tomt eller
2. ett hörn (kallad *roten*) med som är förbunden till roten i d disjunkta m-ära träd ($0 \leq d \leq m$), kallad *underträd.*

Om $d = m$ i definitionen fås ett *fullt* m-ärt träd. Fallet $m = 2$ kallas ibland binärt träd. *Varning:* I många böcker är *binärt träd* det samma som *fullt* binärt träd.

PÅSTÅENDE 28. *Ett* m*-ärt träd är ett träd.*

Bevis. Vi vill visa att ett m-ärt träd T (enligt den rekursiva definitionen) är minimalt sammanhängande, vilket etablerar påståendet med Påst. 26. Detta göras ved induktion efter antalet hörn i det m-ära trädet.

Bas: Det tomma trädet är sammanhängande (trivialt) och minimalt.

Steg: (Sammanhang:) Underträden är sammanhängande per induktion, och eftersom roten är kopplad till varje underträd blir T sammanhängande. (Minimalitet:) Ta bort en kant från T. Tas den från något underträd blir detta osammanhängande per induktion. Annars måste kanten ha kopplat ett underträd till roten, så borttagningen gör T osammanhängande. ∎

8.2. Ramseyteori. Vi säger att en graf $G = (V, E)$ *innehåller* I_k om det finns en oberoende k-delmängd $U \subseteq V$, dvs

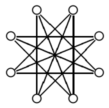
$$\{\, uv \mid u \in U, v \in U \,\} \cap E = \emptyset.$$

(Detta brukar kallas 'innehåller I_k som *inducerad* delgraf'.)

Låt $R(s, t)$ ange det minsta n så att en graf på n hörn måste innehålla antingen K_s eller I_t.

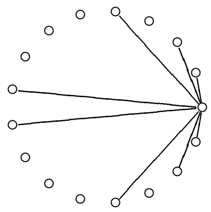
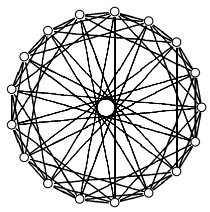
Exempel.

1. $R(s, 2) = R(2, s) = s$ för alla $s \geq 2$.
2. $R(s, t) = R(t, s)$: Betrakta $G = (V, \overline{E})$.
3. Vi har redan sett att $R(3, 3) = 6$, vänskapssatsen.
4. $R(3, 4) \leq 10$: Betrakta hörn v. Antag först att v har minst 4 grannar, kalla dem N. Om N innehåller en kant uw, så är uvw en triangel (färdig). Annars är R en oberoende 4-mängd (färdig). Antag nu att v har 6 icke-grannar; kalla dem M. Vi vet att $R(3, 3) = 6$, så antingen har M en triangel (färdig) eller en oberoende mängd $\{u, w, x\}$, som skapar en oberoende 4-mängd med v.
5. $R(3, 4) \leq 9$: Vi försöker använda samma argument som ovan. Nu är det möjligt att v har precis 3 grannar och 5 icke-grannar (i alla andra fall kan vi återanvända beviset ovan). Om detta vore sant för alla val av v hade vi ett problem. Men så kan det inte vara pga handskakningslemmat.
6. $R(3, 4) = 9$: Det kvarstår att etablera existensen av en graf med 8 hörn som varken innehåller K_3 eller I_4:



7. $R(4, 4) = 18$: Välj v i en graf med 18 hörn. Antag att v har 9 grannar N. Vi vet att $R(3, 4) = 9$, så N innehåller antingen K_3 (som ger K_4 med v) eller I_4. Andra fallet är symmetrisk, eftersom $R(s, t) = R(t, s)$: om v har 9 icke-grannar M, så måste M innehålla K_4 eller I_3, som ger I_4 med v. Vi har visat $R(4, 4) \leq 18$.

   Läsaren är välkommen att inspicera följande 17-noders graf utan varken K_4 eller I_4 för att inse $K(4, 4) > 17$. Varje nod har 8 grannar, placerat som på ritningen med avstånd 1, 2, 4, 8, 9, 13, 15, och 16 runt cirkeln. Vi ritar grannarna till endast en nod i bilden till vänster, och hela grafen till höger.

Sats 6. *Antag $s, t \geq 2$. $R(s, t)$ är ändligt, och*

$$R(s, t) \leq R(s-1, t) + R(s, t-1), \quad \text{för } s, t > 2.$$

Bevis. Antag att $R(s-1, t)$ och $R(s, t-1)$ är ändliga och låt $n = R(s-1, t) + R(s, t-1)$. Betrakta en graf med n hörn och låt v vara ett av dessa. Det finns $n-1$ andra hörn, så antingen har v minst $R(s-1, t)$ grannar eller $R(s, t-1)$ icke-grannar (duvhålsprincipen). I första fall innehåller grannarna antingen K_{s-1} (som skapar K_s med v) eller I_t, som önskat. I andra fallet innehåller icke-grannarna antingen K_s eller I_{t-1} (som skapar I_t med v), som önskat. ∎

Påstående 29. *För $s, t > 2$,*

$$R(s, t) \leq \binom{s+t-2}{s-1}.$$

Bevis. Induktion över $s+t$. För $s=2$ och $t=2$ gäller uttrycket (med likhet), se exempel 1. Antag nu att uttrycket gäller för varje s', t' med $2 \leq s'+t' \leq s+t$. Teoremet ovan ger

$$R(s,t) \leq R(s-1,t) + R(s,t-1) \leq \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1}.$$

∎

Av speciellt intresse är de diagonala Ramseytalen $R(s) = (s,s)$. Vi har beräknat $R(3,3)$ och $R(4,4)$ i exemplen ovan, och det är anmärkningsvärt, att ingen känner $R(5,5)$ bättre än $43 \leq R(5,5) \leq 49$. Vi ser från resultatet ovan att

$$R(s) \leq \binom{2(s-1)}{s-1} \leq \frac{2^{2s-2}}{\sqrt{s}}.$$

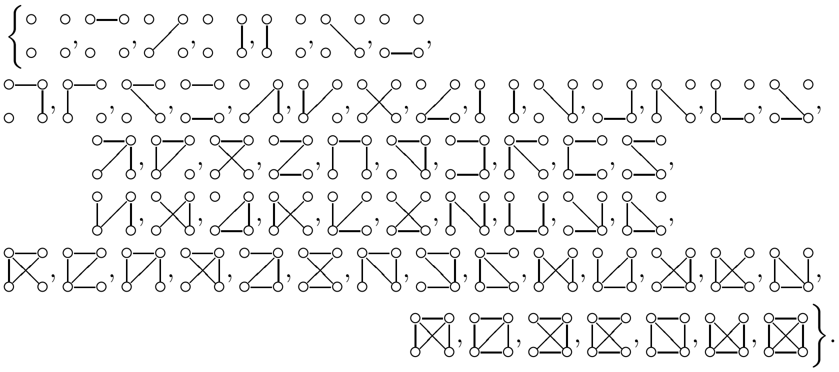
*LU datavetenskap, dat 401 DM, VT 2002. Thore Husfeldt. 19 september 2002.

9. Slumpgrafer

En *p-slumpgraf* med n noder är resultatet av följande proces: Börja med en tom graf med n noder. För varje nodpar $\{u,v\}$, inkludera kanten uv med sannolikhet p, oberoende av tidigare val. Resultatet av denna process skrivs ofta $G(n,p)$. Ett viktikt specialfall är $p=\frac{1}{2}$, där varje kant in- eller exkluderas med samma sannolikhet.

Vi låter $\mathbf{G}_n$ beteckna mängden av grafer med n hörn. Till exempel

$\mathbf{G}_4 =$



Exempel.

1. För $p=0$ är resultatet av processen ovan alltid den tomma grafen. Dvs att $G(n,0)$ är $(\{1,\dots,n\},\emptyset)$ med sannolikhet 1:

$$p\big(G(n,0)=(\{1,\dots,n\},\emptyset)\big)=1$$

2. För $p=1$ är resultatet av processen ovan alltid den fullständiga grafen.

Betrakta $p=\frac{1}{2}$. För godtycklig graf $G\in\mathbf{G}_n$ gäller

$$p\big(G(n,\tfrac{1}{2})=G\big)=2^{-n(n-1)/2}$$

Detta är samma sannolikhet som resultatet av följande process: Välj slumpmässigt en av de $2^{n(n-1)/2}$ grafer i $\mathbf{G}_n$, alla med samma sannolikhet $2^{-n(n-1)}$. Ibland är det mera naturligt att betrakta denna konstruktion är definitionen.

PÅSTÅENDE 30. *Sannolikheten för att $G(n,p)$ innehåller en k-klick är högst*

$$\binom{n}{k}p^{\binom{k}{2}}=\binom{n}{k}p^{k(k-1)/2}$$

Bevis. Betrakta en konkret k-delmängd U av V. Denna är en klick precis när alla $\binom{k}{2}$ kanter i U finns, vilket händer med sannolikhet $p^{\binom{k}{2}}$. Det finns $\binom{n}{k}$ möjliga k-delmängder. ∎

Bevis (lång version). Låt K beteckna händelsen 'det finns en k-klick i $G(n,p)$'. Vi vill beräkna $p(K)$. Låt U vara en k-delmängd av V och låt K_U beteckna händelsen 'U är en k-klick'. Observera att K är unionen av K_U över alla k-delmängder U, i symboler

$$K=\bigcup_U K_U,$$

och därför

$$p(K) = p\Big(\bigcup_U K_U\Big) \leq \sum_U p(K_U),$$

där summationen är över alla k-delmängder U av V, total $\binom{n}{k}$ termer.

Det återstår att beräckna $p(K_U)$. För att U skal vara en klick måste alla $\binom{k}{2}$ kanter mellan Us hörn finns, vilket händer med sannolikhet

$$p(K_U) = p^{\binom{k}{2}}.$$

Vi konkluderar

$$p(K) \leq \sum_U p^{\binom{k}{2}} = \binom{n}{k} p^{\binom{k}{2}},$$

som önskat. ∎

9.1. Några slumpvariabler. Slumpgrafer är en rik källa för interessanta slumpvariabler.

Antal kanter. Den första är *antalet av kanter* M. Det är klart att M är minst 0 och högst $\binom{n}{2}$. Förväntningen är

$$E[M] = \sum_{i=0}^{\binom{n}{2}} i \cdot p(M = i).$$

För att beräkna $p(M = i)$ betraktar vi slumpgrafsprocessen som $r = \binom{n}{2}$ Bernoulliförsök, så sannolikheten för precis i kanter är

$$p(M = i) = \binom{r}{i} p^i (1-p)^{r-i}.$$

Vi har nu

$$E[M] = \sum_{i=0}^{r} \left[i \cdot \binom{r}{i} p^i (1-p)^{r-i} \right], \quad \text{där } r = \binom{n}{2},$$

som inte omedelbart kan förenklas.

Vi kan däremot begagna förväntningens linearitet (påst. 24) till et mycket enklare argument. Introducera m nya slumpvariabler M_{uv}, en för varje nodpar. M_{uv} skall räkna antalet kanter mellan u och v; det ses lätt att $M_{uv} \in \{0, 1\}$ och att

$$E[M_{uv}] = 0 \cdot p(M_{uv} = 0) + 1 \cdot p(M_{uv} = 1) = p(M_{uv} = 1) = p.$$

M_{uv} är ett exempel på en *indikatorvariabel* (vars värde alltid är 0 eller 1), deras förväntning är alltid precis sannoliketen för utfallet '1', som ofta är lättberäknelig.

Det är också klart att

$$M = \sum_{u,v \in V} M_{uv},$$

så

$$E(M) = \sum_{u,v \in V} E(M_{uv}) = \sum_{u,v \in V} p = p\binom{n}{2}.$$

Antal triangler. Låt T ange antalet av triangler i grafen. För varje 3-mängd av noder $\{u, v, w\}$ introduceras indikatorvariabeln T_{uvw} som är 1 när $\{u, v, w\}$ är en triangel och 0 annars. Sannolikheten för triangeln T_{uvw} är p^3. T är summan av alla dessa, så

$$E(T) = \sum_{\{u,v,w\}\in V} E[T_{uvw}] = \sum_{\{u,v,w\}\in V} p^3 = \binom{n}{3} p^3.$$

Det är viktikt att observera att variabel T_{uvw} inte är oberoende, men att detta heller inte är nödvändigt för att kunna använda påst. 24. Betrakta till exempel $G(4, \frac{1}{2})$ med hörn 1, 2, 3 och 4. Sannolikheten för T_{123} är $\frac{1}{8}$, och det samma gäller för T_{234}. Sannolikheten för T_{123} *givet* T_{123} är däremot

$$p(T_{123} \mid T_{234}) = \frac{1}{4},$$

så de är *inte* oberoende.

Slumpmetoden. Slumpmetoden är en bevismetod för att etablera existensen av konstruktioner *utan att konstruera dem.* Metoden är överraskande enkel. Här är en av dess första tillämpningar, av Erdös (1947):

SATS 7. $R(k) > 2^{k/2}$.

Bevis. Antag att $n \leq 2^{k/2}$. Låt K beteckna händelsen '$G(n, \frac{1}{2})$ innehåller er k-klick' och låt I beteckna händelsen '$G(n, \frac{1}{2})$ innehåller en oberoende k-mängd'. Vi visade i påst. 30 att

$$p(K) \leq \binom{n}{k} 2^{-\binom{k}{2}}$$

På samma sätt kan vi beräkna

$$p(I) \leq \binom{n}{k} 2^{-\binom{k}{2}}.$$

Vi har

$$p(I \vee K) \leq 2\binom{n}{k} 2^{-\binom{k}{2}}.$$

Eftersom $\binom{n}{k} \leq n^k/2^k$ (se (6) på s. 25), kan vi skriva

$$p(I \vee K) \leq 2\frac{\left(2^{k/2}\right)^k}{2^k} 2^{-k(k-1)/2} = 2^{-k/2+1} < 1.$$

Speciellt,

$$p(\overline{I} \wedge \overline{K}) = p(\overline{I \vee K}) = 1 - p(I \vee K) > 0.$$

Konklusionen är att sådana grafer finns. ∎

Uppgifter.

1. Givet $G \in \mathbf{G}_n$ med m kanter. Beräckna $p\big(G(n,p) = G\big)$.
2. Beräckna det förväntade antal 4-cykler i $G(n,p)$.
3. Beräckna det förväntade antal k-klickar i $G(n,p)$.

APPENDIX A

Notation

Notationen i dessa anteckningar är konsistent med [Rosen]. Vill man läsa ytterligare litteratur måste man känna till alternativer.

1. Symboler

Symbol	betydelse	alternativ
$\neg p$	negationen av p	$\overline{p}$
$p \to q$	p medför q	$p \Rightarrow q$
$p \leftrightarrow q$	biimplikation mellan p och q	$p \Leftrightarrow q$
$p \Leftrightarrow q$	p är ekvivalent med q	$p \equiv q$, $p = q$
$\{\, x \mid P(x) \,\}$	mängdkonstruktion	$\{\, x \colon P(x) \,\}$
$\emptyset$	tomma mängden	$\{\,\}$, $\varnothing$
$A - B$	mängddifferens	$A \setminus B$
$\lvert A \rvert$	kardinalitet	$\# A$
$P(S)$	potensmängd	2^A, $\mathcal{P}A$
uv	sammanfogning	$u \cdot v$, $u \circ v$
λ	tomma strängen	Λ, ϵ, 1

Applikationen av funktioner har så många olika notationer att det fortjäner ett eget avsnitt. Här är fyra vanliga sätt att ange den funktionen, som kvadrerer ett tal

$$
\begin{aligned}
x &\mapsto x^2, \\
x &\curvearrowright x^2, \\
f(x) &= x^2, \\
y &= x^2,
\end{aligned}
$$

men *inte* $x \to x^2$.

2. Alternativ svensk terminologi

domän	definitionsmängd
kodomän	målmängd
funktion	avbildning
hörn	nod
kant	båge
klik	fullständig graf
slumpvariabel	stokastisk variabel
förväntning	väntevärde