UPPGIFTER TILL HT2021 – CM1000, DISKRET MATEMATIK

Fx-skrivning 1

1. Logik. Visa att följande slutledning är riktig genom att ange en detaljerad redogörelse för hur slutsatsen följer av premisserna med angivande av alla regler som behövs användas (*Modus Ponens*, *Modus Tollens* etc.)

1. $p \to (q \to r)$
2. $(p \to q) \to r$
3. $r \to \neg t$ (Uppgiften kan alltså *inte* lösas bara med hjälp av en sanningstabell.)
4. $\neg t \to \neg r$

$\therefore$ $\neg q$

Lösning: Vi börjar med att skriva om 3 enligt regeln för kontraposition och får

5. $t \to \neg r$ *Omskrivning av 3*

Vi tar 4,5 tillsammans och skriver om dessa som disjunktioner, det ger

6. $(t \vee \neg r) \wedge (\neg t \vee \neg r)$ *Omskrivningar av 4 och 5*

Detta skriver vi om med distributiva lagen och får

7. $(t \wedge \neg t) \vee \neg r$ *6, distributiva lagen*

Eftersom $t \wedge \neg t$ är en kontradiktion får 7 formen $\bot \vee \neg r$ vilket skrivs om till

8. $\neg r$ *7, omskrivning.*

Vi fortsätter och använder $\neg r$ i 2 och får via *Modus Tollens*

9. $\neg(p \to q)$ *2, 8, Modus Tollens.*

Vi skriver om detta till

10. $p \wedge \neg q$ *9, omskrivning.*

Och ur detta extraherar vi

11. p *10.*

som tillsammans med 1 ger

12. $q \to r$ *1, 11, Modus Ponens*

som slutligen tillsammans med 8 ger

13. $\neg q$ *12, 8, Modus Tollens*

vilket fullbordar beviset. (I en lösning på en tentamen behöver ni inte ha någon annan text än den som står på rader med nummer.)

2. Mängdlära. Låt A, B, C beteckna mängder vilka som helst. Betrakta nedanstående två påståenden. Det ena är sant och det andra är falskt. Ange vilket som är sant och vilket som är falskt och bevisa det sanna och motbevisa det falska.

$$A \subset B \cap C \wedge B \subset A \cap C \wedge C \subset A \cap B \Rightarrow A = B = C$$

$$A \subset B \cup C \wedge B \subset A \cup C \wedge C \subset A \cup B \Rightarrow A = B = C$$

Det är tillåtet att använda Venndiagram, men om du gör det *måste* de vara mycket tydliga, rita dem hellre för stora än för små. Du behvöver också motivera ordentligt med text, inte bara själva Venndiagrammet. För det påstående som ska motbevisas måste tre exempelmängder, A, B, C hittas som uppfyller förledet i implikationen men inte efterledet.

Lösning: Det första påståendet är sant och vi kan se det genom att observera att

$$A \subset B \cap C \wedge B \subset A \cap C \Rightarrow A \subset A \cap C \cap C = A \cap C \subset C$$

så tydligen gäller $A \subset C$. Men på samma sätt som vi ser att $A \subset C$ kan vi, genom att använda utsagorna i en annan ordning se att $C \subset B$ och även att $B \subset A$. Det betyder att

$$A \subset C \subset B \subset A \Rightarrow A = B = C$$

vilket fullbordar beviset av det första påståendet. Det betyder att det andra påståendet är falskt och vi kan se det genom att konstatera att om vi sätter

$$A = \emptyset \qquad B = \{1\} \qquad C = \{1\}$$

så uppfylls alla tre förutsättningarna, $A \subset B \cup C$, $B \subset A \cup C$ och $C \subset A \cup B$ men trots detta gäller inte $A = B = C$. Vi kan hitta dessa tre mängder genom att studera en sanningstabell hörande till utsagorna

$$p \to q \vee r \qquad q \to p \vee r \qquad r \to p \vee q$$

som är de satslogiska motsvarigheterna till mängdförhållandena $A \subset B \cup C$, $B \subset A \cup C$ och $C \subset A \cup B$. I sanningstabellen ser vi att om $p = falsk$, $q = sann$ och $r = sann$ så svarar det mot en rad där alla implikationer är uppfyllda, trots det gäller inte $p \leftrightarrow q \leftrightarrow r$.

3. Funktioner. Vi låter P vara funktion från $\mathbb{R}^n$ till $\mathbb{R}^n$ som uppfyller följande två krav:

1. P är *linjär*, det vill säga för alla $x, y \in \mathbb{R}^n$ och alla $a, b \in \mathbb{R}$ gäller $P(ax + by) = aP(x) + bP(y)$.
2. P är en *projektion*, det vill säga $P \circ P = P$.

Visa att om $P \neq \iota$ så är P inte injektiv.

Lösning: Eftersom $P \neq \iota$ så finns ett $x \in \mathbb{R}^n$ med $P(x_1) \neq x_1$. Om vi då kallar $x_2 = P(x_1)$ så har vi $x_1 \neq x_2$ men $P(x_2) = P(P(x_1)) = P(x_1)$ (eftersom $P \circ P = P$) vilket visar att P inte är injektiv.

Anmärkning: Vi använde aldrig att P var linjär.

4. Inledande talteori. I den mycket viktiga RSA-algoritmen används så kallade krypterings- och dekrypteringstal som vi kallar e respektive d. Dessa är positiva heltal som vi tar fram baserat på ett par av hemliga primtal p och q på följande sätt:

Steg 1. Välj två primtal p, q.
Steg 2. Bilda talet $\phi = (p-1)(q-1)$.
Steg 3. Välj e, d sådana att $ed \equiv 1 \pmod{\phi}$

Ange det minsta $d > 1$ som uppfyller kraven i de olika stegen ovan om $p = 5$, $q = 11$ och $e = 7$.

Lösning: Med $p = 5$, $q = 11$ får vi $\phi = (p-1)(q-1) = 4 \cdot 10 = 40$. Vi ska alltså hitta ett d med $7d \equiv 1 \pmod{40}$. Talet d ska alltså vara valt som en multiplikativ invers till 7 modulo 40. Vidare skulle $1 < d < 40$ (detta bestämmer d entydigt och då blir också d minimalt). Vi använder Euklides utvidgade algoritm och får

$$40 = 5 \cdot 7 + 5, 7 = 1 \cdot 5 + 2, 5 = 2 \cdot 2 + 1, 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 =$$

$$3 \cdot (40 - 7 \cdot 5) - 2 \cdot 7 = 3 \cdot 40 - 15 \cdot 7 - 2 \cdot 7 = 3 \cdot 40 - 17 \cdot 7 \Rightarrow -17 \cdot 7 \equiv 1 \pmod{40}$$

Om vi adderar 40 till -17 finner vi alltså

$$-17 \cdot 7 \equiv 1 \pmod{40} \Rightarrow (40 - 17) \cdot 7 \equiv 1 \pmod{40} \Leftrightarrow 23 \cdot 7 \equiv 1 \pmod{40}$$

vilket betyder att $d = 23$ är det minsta tal > 1 som uppfyller $de \equiv 1 \pmod{40}$.

5. Relationer. Beteckna med A mängden av alla positiva heltal ($\{1, 2, 3, \ldots\}$). Definiera relationen $\mathcal{R}$ på A genom

$$a \mathcal{R} b \Leftrightarrow a | b^2 \wedge b | a^2.$$

Bevisa att $\mathcal{R}$ *inte* är en ekvivalensrelation.

Lösning: Vi ska visa att relationen saknar någon av egenskaperna reflexivitet, symmetri eller transitivitet. Relationen är både reflexiv och symmetrisk så det är transitiviteten som måste falla. Det ser vi om vi betraktar följande val av heltal

$$a = 2 \qquad b = 4 \qquad c = 8$$

så har vi

$$a = 2 | 4^2 = b^2 \wedge b = 4 | 2^2 = a^2 \Leftrightarrow a \mathcal{R} b \quad \text{och} \quad b = 4 | 8^2 = c^2 \wedge c = 8 | 4^2 = b^2 \Leftrightarrow b \mathcal{R} c$$

och samtidigt gäller

$$a = 2 | 8^2 = c^2 \wedge c = 8 \nmid 2^2 = a^2 \Rightarrow \neg (a \mathcal{R} c)$$

vilket visar att relationen *inte* är transitiv. Eftersom relationen inte har alla egenskaper som en ekvivalensrelation måste ha är den inte en ekvivalensrelation vilket fullbordar beviset.

6. Fördjupad talteori. Studera följande identiteter

$$1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3,$$

$$1 \cdot 2 + 2 \cdot 3 = \frac{1}{3} \cdot 2 \cdot 3 \cdot 4,$$

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 = \frac{1}{3} \cdot 3 \cdot 4 \cdot 5.$$

Baserat på dessa likheter, formulera en hypotes (i form av en formel) med ett summatecken och bevisa sedan formeln med matematisk induktion.

Lösning: Hypotesen lyder

$$VL_n = \sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2) = HL_n, \quad n = 1, 2, 3 \ldots .$$

Vi visar nu att formeln gäller. Som vi ser har vi redan infört beteckningar för vänster respektive höger led i predikatet $A(n) \Leftrightarrow \sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$. Vi tar de tre stegen i ett induktionsbevis:

Steg 1. Det första steget är redan avklarat eftersom den första identiteten som angavs, alltså $1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3$, är precis $VL_1 = HL_1$ vilket visar att $A(1)(\Leftrightarrow VL_1 = HL_1)$ gäller. (Förstås kan vi även konstatera att $A(2)$ respektive $A(2)$ är precis de andra två identiteterna.)

Steg 2. Vi tar nu induktionssteget och vi ska därmed visa att implikationen $A(p) \rightarrow A(p+1)$ gäller för alla $p \geq 1$ så vi låter p vara ett sådant tal och antar att vi har

$$A(p) \Leftrightarrow VL_p = \sum_{k=1}^{p} k(k+1) = \frac{1}{3}p(p+1)(p+2) = HL_p.$$

Med kraft av detta ska vi visa att

$$A(p+1) \Leftrightarrow VL_{p+1} = \sum_{k=1}^{p+1} k(k+1) = \frac{1}{3}(p+1)(p+2)(p+3) = HL_{p+1}.$$

Vi arbetar därför med VL_{p+1}:

$$VL_{p+1} = \sum_{k=1}^{p+1} k(k+1) = \sum_{k=1}^{p} k(k+1) + (p+1)(p+2) = VL_p + (p+1)(p+2) =$$

$$HL_p + (p+1)(p+2) = \frac{1}{3}p(p+1)(p+2) + (p+1)(p+2).$$

Induktionsantagandet är ju $VL_p = HL_p$ och vi har använt det när vi ersatt VL_p med HL_p. Frågan är nu om det här uttrycket som vi kommit fram till verkligen är HL_{p+1}? Visst är det så vi fortsätter att behandla uttrycket och får

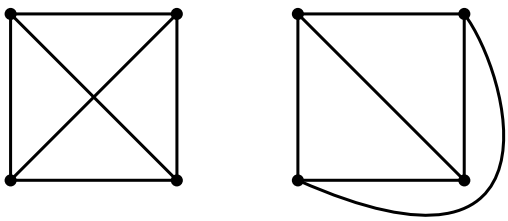
$$VL_{p+1} = \frac{1}{3}p(p+1)(p+2) + (p+1)(p+2) = \frac{1}{3}(p(p+1)(p+2) + 3(p+1)(p+2)) =$$

$$\frac{1}{3}((p+3)(p+1)(p+2)) = \frac{1}{3}(p+1)(p+2)(p+3) = HL_{p+1}.$$

Vi har alltså att $VL_{p+1} = HL_{p+1}$ det vill säga $A(p+1)$ gäller som följd av att induktionsantagandet $A(p)$ gäller.

Steg 3. Induktionsaxiomet och steg 1 och steg 2 fullbordar beviset.

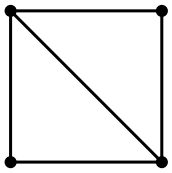
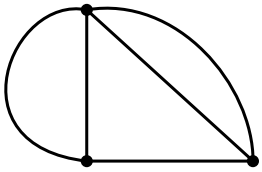
7. Grafteori. En graf kallas *plan* om den kan ritas utan överkorsande kanter. Det är inte alltid lätt att se om en graf är plan eller inte. K_5 respektive $K_{3,3}$ är inte plana. K_4 är dock plan. Nedan visas en figur där vi kan se varför K_4 är plan.



K_4 K_4 *ritad plant*

Till vänster är K_4 ritad, inte plant, en kant korsar en annan. Till höger ges en framställning av K_4 som är ritad plant, inga kanter korsar någon annan. Med detta har vi visat att K_4 är plan. Läsaren uppmuntras att försöka rita K_5 respektive $K_{3,3}$ plant för att få en känsla för vad en plan graf är.

En plan graf delar upp den plana yta som den är ritad på i ett antal delytor. Om dessa är F till antalet så har en plan graf tre tal: V = antalet hörn, E = antalet kanter och F = antalet delytor som grafen delar upp planet i. Nedan illustreras detta begrepp för två plana grafer:

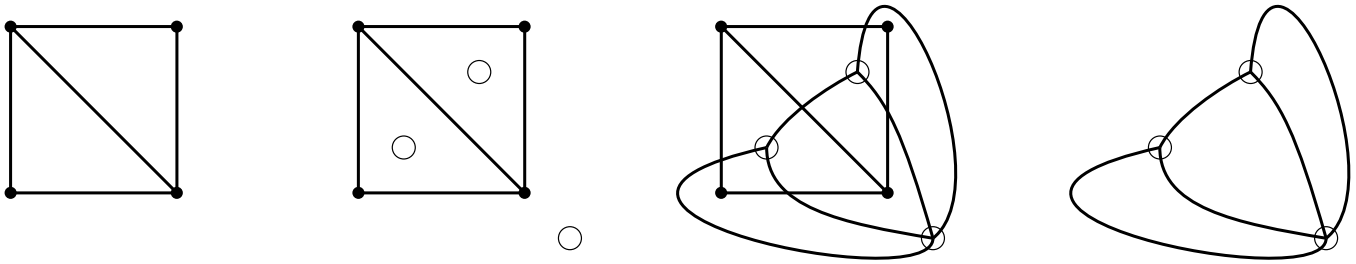



Till vänster ser vi en plan graf med $V_1 = 4$, $E_1 = 5$ och $F_1 = 3$, till höger ser vi en graf med $V_2 = 3$, $E_2 = 5$ och $F_2 = 4$.

Vi låter nu $G = (\mathcal{V}_1, \mathcal{E}_1)$ vara en plan graf med $V_1 = |\mathcal{V}_1|$ hörn, $E_1 = |\mathcal{E}_1|$ kanter och f delytor. Vi skapar nu en ny graf G' genom följande procedur:

Steg 1. Placera ett nytt hörn i varje delyta.
Steg 2. För varje kant e i G inför en kant e' i G' på följande sätt: förbind de två isolerade noderna som ligger i delytorna som avgränsas av e så att e' korsar e.

Dessa steg finns illustrerade i nedanstående figur:



Längst till vänster ser vi ursprungsgrafen, G, i mitten till vänster ser vi de införda nya hörnen som ska höra till den nya grafen. Vi illustrerar de nya hörnen med större prickar som inteär ifyllda. I mitten till höger har dessa nya hörn förbundits med de nya kanterna. Längst till höger ser vi den nya grafen G'.

Vi kallar en graf G' som är skapad på detta sätt utgående från en given plan graf G för *den duala grafen till G*.

Visa att summan av gradtalen av alla hörn i G' och summan av alla gradtalen av alla hörn i G alltid är lika.

Lösning: Eulers sats säger att summan av alla gradtal i en graf alltid är lika med dubbla antalet kanter. Eftersom en graf G och dess duala graf G' alltid har exakt lika antal kanter (enligt konstruktionen) överenstämmer båda gradtalssummorna med det gemensamma antalet kanter gånger 2.

8. Kombinatorik. Låt $n > 0$ vara ett godtyckligt heltal. Visa att för alla heltal $0 \leq k < n$ gäller olikheten

$$\binom{2n}{k} < \binom{2n}{n}.$$

Ledning: Du kan försöka visa att $\binom{2n}{k} < \binom{2n}{k+1}$ för alla $k = 0, 1, \ldots, n-1$. Då följer $\binom{2n}{k} < \binom{2n}{n}$ om $k < n$.

Lösning: Vi visar att olikheten

$$\binom{2n}{k} < \binom{2n}{k+1} \Leftrightarrow$$

gäller för alla $0 \leq k < n$. Vi studerar en följd av ekvivalenser:

$$\binom{2n}{k} < \binom{2n}{k+1} \Leftrightarrow$$

$$\frac{(2n)!}{(2n-k)!k!} < \frac{(2n)!}{(2n-(k+1))!(k+1)!} \Leftrightarrow$$

$$\frac{1}{(2n-k)!k!} < \frac{1}{(2n-(k+1))!(k+1)!} \Leftrightarrow$$

$$\frac{(2n-(k+1))!(k+1)!}{(2n-k)!k!} < 1 \Leftrightarrow$$

$$\frac{k+1}{2n-k} < 1 \Leftrightarrow$$

$$k+1 < 2n-k \Leftrightarrow 2k+1 < 2n \Leftrightarrow k+1/2 < n \Leftrightarrow k < n$$

där den sista ekvivalensen håller eftersom både k och n är heltal. Eftersom vi kan gå baklänges i ekvivalenskedjan har vi visat att för heltal ≥ 0 har vi

$$k < n \Rightarrow \binom{2n}{k} < \binom{2n}{k+1}$$

så talföljden $\binom{2n}{k}$ växer alltså så länge $k < n$, det betyder att

$$\binom{2n}{k} < \binom{2n}{n}$$

för alla k med $0 \leq k < n$ vilket fullbordar beviset.

9. Sannolikhetslära. Antag att A, B, C är tre händelser som uppfyller följande krav:

1. $P(A \cap (B \cup C)^c) = P(B \cap (A \cup C)^c) = P(C \cap (A \cup B)^c) = 0.3$
2. De kan inte inträffa samtidigt men någon av dem inträffar säkert.

Beräkna sannolikheten av att precis två av dem inträffar.

Ledning: Du får motivera med ett Venndiagram hur den sökta sannolikheten är fördelad.

Lösning: Vi betecknar händelsen att två av A, B, C inträffar med X. Om inte alla tre kan inträffa samtidigt så sammanfaller sannolikheten av att precis två av dem inträffar med sannolikheten av att minst två av dem inträffar så händelsen X beskriver alltså precis detta: "två av A, B, C inträffar" = "precis två av A, B, C inträffar". Med ett Venndiagram kan vi se följande formel:

$$P(X) = P(A \cap B) + P(B \cap C) + P(A \cap C) - 2 \cdot P(A \cap B \cap C) = P(A \cap B) + P(B \cap C) + P(A \cap C).$$

Med ett Venndiagram kan vi även härleda följande formel:

$$P(A \cup B \cup C) = P(A \cap (B \cup C)^c) + P(B \cap (A \cup C)^c) + P(C \cap (A \cup B)^c) + P(A \cap B) + P(B \cap C) + P(A \cap C) - 2 \cdot P(A \cap B \cap C).$$

som kan skrivas

$$P(A \cup B \cup C) = P(A \cap (B \cup C)^c) + P(B \cap (A \cup C)^c) + P(C \cap (A \cup B)^c) + P(X).$$

Att någon av de tre händelserna alltid inträffar innebär att $P(A \cup B \cup C) = 1$ och om vi även sätter krav 1 i ekvationen ovan får vi

$$1 = 0.3 + 0.3 + 0.3 + P(X) \Leftrightarrow P(X) = 0.1.$$