MEETING 11 - REPETITION

Idag repeterar vi allt som hittills gåtts igenom. Kontrollskrivningen är på fredag denna vecka så det är värt att stödja studierna inför den särskilt. (Nästa möte handlar om ett helt nytt område (grafer) som inte kommer på kontrollskrivningen.)

Vi har hittills gått igenom följande områden:

1. Logik
2. Mängdlära
3. Talteori
4. Bevisföring

Och bevisföring spänner förstås över alla områdena. Det betyder att vi kan repetera alla områden genom att studera bevis av påståenden som involverar logik, mängdlära och talteori.

1. Bevisföring inom logiken

Logiken studerar utsagor och kombinationer av dessa, vi använder konnektiv som $\wedge, \vee, \oplus, \rightarrow, \leftrightarrow$ och negationen, $\neg$, för att forma nya utsagor. (Vi skriver ibland $\oplus$ för xor). Den enklaste formen av bevis inom logiken är då man använder en sanningstabell.

Exempel. Visa att utsagorna $p \rightarrow (q \rightarrow r)$ och $(p \rightarrow q) \rightarrow r$ inte är ekvivalenta genom att ange en kombination av tilldelningar av sanningsvärden till p, q, r för vilka dessa utsagor har olika sanningsvärden.

Lösning. Vi sätter upp en sanningstabell och studerar kolumnerna med sanningsvärdena för allting:

p	q	r	$q \rightarrow r$	$p \rightarrow (q \rightarrow r)$	$p \rightarrow q$	$(p \rightarrow q) \rightarrow r$
s	s	s	s	s	s	s
s	s	f	f	f	s	f
s	f	s	s	s	f	s
s	f	f	s	s	f	s
f	s	s	s	s	s	s
f	s	f	f	s	s	f
f	f	s	s	s	s	s
f	f	f	s	s	s	f

Vi ser att kolumnerna för $p \rightarrow (q \rightarrow r)$ och $(p \rightarrow q) \rightarrow r$ skiljer sig åt (på den sista och den näst-näst sista raden) - alltså har $p \rightarrow (q \rightarrow r)$ och $(p \rightarrow q) \rightarrow r$ inte alltid precis samma sanningsvärde - att konstatera det (med hjälp av en sanningstabell) utgör ett fullt acceptabelt bevis för att de givna utsagorna inte är ekvivalenta. Men vi skulle också ange en tilldelning av sanningsvärden på p, q, r för vilken $p \rightarrow (q \rightarrow r)$ och $(p \rightarrow q) \rightarrow r$ har olika sanningsvärden, vi kan då till exempel välja den sista raden som anger att alla p, q, r ska vara falska och konstatera att om det är på det viset så blir $p \rightarrow (q \rightarrow r)$ sann och $(p \rightarrow q) \rightarrow r$ blir falsk. (Detta är en gammal tentafråga.)

Exempel. Är följande logiska härledning korrekt?:

1. $p \vee q \vee r$
2. $p \rightarrow r$
3. $\neg r$

$\therefore$ q

Lösning. Slutledningen är korrekt, vi kan se det på följande sätt:

4. $\neg p$ (Motivering: 2, 3 och *Modus Tollens*)
5. $q \vee r$ (Motivering: 4, 1 och *Disjunktiv Syllogism (egentligen också med hänvisning till* $p \vee q \vee r \Leftrightarrow p \vee (q \vee r)$)
6. q (Motivering: 5, 3 och *Disjunktiv Syllogism*)

2. Bevisföring inom mängdläran

Vi repeterar nu hur vi gör bevis med utsagor om mängder. Observera att utsagor om mängder föstå kan ses som vanliga utsagor så allt som gäller logik och bevis inom logik, gäller också mängder och bevisen som vi konstruerar angående mängder. Vi börjar med att titta på två gamla tentafrågor från sista tentan.

Exempel. (Från A-delen.) Är följande sant eller falskt: För alla mängder A, B, C, D gäller

$$A \times B \cap C \times D \neq \emptyset \Rightarrow A \cap C \neq \emptyset \wedge B \cap D \neq \emptyset.$$

Vad säger vi?

Exempel. (Från B-delen.) För vilka tre mängder som helst, A, B, C, bevisa att

$$A \subset B \wedge B \subset C \Rightarrow A \times B \subset B \times C.$$

Lösning. Vi ska visa en inklusion (typ $E \subseteq F$), att en mängd finns inuti en annan (E finns i F), då väljer vi ett element i E och visar att det också finns i F. Vi visar alltså implikationen

$$x \in E \Rightarrow x \in F$$

och detta betyder precis $E \subseteq F$. Här är förstås $E = A \times B$ och $F = B \times C$. Vi ska visa inklusionen $A \times B \subset B \times C$ så vi väljer ett element, vilket som helst, $x \in A \times B$ $(= E)$. Då gäller att $x = (a, b)$ för några $a \in A$, $b \in B$. Men enligt förutsättningarna gäller $A \subset B$ och $B \subset C$ och alltså har vi $a \in A \subseteq B \Rightarrow a \in B$ och $b \in B \subseteq C \Rightarrow b \in C$ som sammantaget betyder att $x = (a, b) \in B \times C$ $(= F)$ och vi har visat den implikation som vi behövde visa och alltså gläller inklusionen som var det vi skulle bevisa.

Princip: Om man vill visa en mängdinklusion så visar man alltså en implikation (enligt ovan). Om man vill visa likhet mellan två mängder, E och F, så kan man göra det genom att visa två inklusioner, dels $E \subseteq F$ men också $F \subseteq E$. Vi ser på ett exempel.

Exempel: För alla mängder A, B, C visa att $A \times (B - C) = A \times B - A \times C$.

Lösning: Vi visar inklusion åt båda hållen:

1. Välj $x \in A \times (B - C)$. Då gäller att $x = (a, b)$, där $a \in A$, $b \in B$ men $b \notin C$. Det betyder att $x = (a, b) \in A \times B$ och $x \in A \times C^c$, det vill säga $x \in A \times B \cap A \times C^c$. Men eftersom $A \times C^c \subseteq (A \times C)^c$ får vi alltså $x \in A \times B \cap A \times C^c \subseteq A \times B \cap (A \times C)^c$ så vi alltså har $x \in A \times B \cap (A \times C)^c$ vilket visar ena inklusionen. (Eftersom $A \times B \cap (A \times C)^c = A \times B - A \times C$.
2. Välj nu $x \in A \times B - A \times C = A \times B \cap (A \times C)^c$. Då kan vi återigen skriva x som (a, b) där $(a, b) \in A \times B$ men $(a, b) \notin A \times C$. Men $(a, b) \notin A \times C$ innebär att antingen gäller $a \notin A$ eller $b \notin C$. Eftersom $a \in A$ måste vi således ha $b \notin C$. Men då har vi sammantaget att $a \in A$, $b \in B$ och $b \notin C$, det betyder precis att $x = (a, b) \in A \times (B - C)$ vilket är den andra inklusionen.

Eftersom inklusionerna gäller åt båda hållen är mängderna lika. Beviset är klart.

Man kan också visa likhet mellan två mängder genom att använda räknereglerna för mängder. Vi ser på ytterligare ett exempel:

Exempel: Visa att för alla mängder A, B gäller

$$A \cap B = A - (A - B).$$

Lösning: Mängddifferensen, $E - F$, är ett annat sätt att skriva $E \cap F^c$, alltså har vi

$$A - (A - B) = A \cap (A - B)^c = A \cap (A \cap B^c)^c = A \cap (A^c \cup B) = (A \cap A^c) \cup (A \cap B) = \emptyset \cup (A \cap B) = A \cap B$$

och beviset är klart.

Man kan också föra resonemang om vad mängderna är och vad de innehåller:

Exempel: Visa att, för alla mängder, A, B gäller $A - (B - A) = A$.

Lösning: Eftersom det inte finns några element från A i mängden $B - A$ (det är ju precis de vi tar bort) så tas inga element ur A bort från A då vi bildar mängddifferensen $A - (B - A)$, det innebär att mängden $A - (B - A)$ måste vara A själv och beviset är klart.

In-class problem: Visa att $A \times B - C \times D = A \times (B - D) \cup (A - C) \times B \cap D$.

3. Bevisföring inom talteorin

Eftersom talteorin bygger mycket på mängdlära och logik kommer som sagt mycket av bevisteknikerna för mängder och logik att vara direkt användbart då skapar bevis som rör heltal och de begrepp som vi infört för heltalen. Dock är ju *matematisk induktion* något som specifikt förutsätter en heltalsstruktur på det matematiska begrepp man studerar.

Vi repeterar bevistekniker för talteori genom att studera kongruenser.

Repetition: Om $a \equiv b \pmod{n}$ och $c \equiv d \pmod{n}$ så gäller $a + c \equiv b + d \pmod{n}$ och $ac \equiv bd \pmod{n}$.
Den här egenskapen gör att vi kan lösa problem med delbarhet väldigt smidigt.

Exempel: Visa att $17|18^m - 1$ för alla värden på m.

Lösning: Vi räknar modulo 17 och eftersom $18 \equiv 1 \pmod{17}$ så kan vi skriva $18^m = (17+1)^m \equiv 1^m = 1$ och detta gäller oberoende av m, alltså har vi $18^m - 1 \equiv 1^m - 1 \equiv 1 - 1 \equiv 0 \pmod{17}$, men om $18^m - 1 \equiv 0 \pmod{17}$ så betyder detta precis att $17|18^m - 1$ och det var det vi ville visa.

Vi tittar på ett annat liknande problem.

Exempel: Visa att $13|4^{2n+1} + 3^{n+2}$. Eftersom vi ska visa att något är delbart med 13 så räknar vi modulo 13. Då har vi

$$4^{2n+1} + 3^{n+2} = 4 \cdot (4^2)^n + 9 \cdot 3^n = 4 \cdot 16^n + 9 \cdot 3^n \equiv 4 \cdot 3^n + 9 \cdot 3^n = 13 \cdot 3^n \equiv 0 \pmod{13}$$

och eftersom alltså $4^{2n+1} + 3^{n+2} \equiv 0 \pmod{13}$ så måste $13|4^{2n+1} + 3^{n+2}$.

Vi studerar det klassiska beviset med heltal: induktionsbeviset:

Exempel: För varje positivt heltal n, bevisa att $\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$.

Lösning: Vi konstaterar först att eftersom $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ så kan det som vi ska visa skrivas så här

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

så vi kallar detta påstående för $A(n)$ och vi visar med matematisk induktion att $\forall n \geq 1 : A(n)$. Nu tar vi de tre stegen som en alltid tar i induktionsbevis:

1. Kolla att $A(1)$ är sann: vi sätter $n = 1$ och studerar om höger och vänster led i $A(1)$ är samma. $VL_1 = \sum_{k=1}^{1} k^3 = 1^3 = 1$. $HL_1 = \frac{1^2(1+1)^2}{4} = 4/4 = 1$, ja de är lika (båda är 1) alltså är $A(1)$ sann.
2. För varje $p \geq 1$, visa att implikationen $A(p) \Rightarrow A(p+1)$ är sann. Vi visar som vanligt en implikation genom att visa att om förledet är sant blir också efterledet sant, vi gör alltså det så kallade *induktionsantagandet*, låt därför p vara ett godtyckligt heltal ≥ 1 och antag

   $$A(p) \Leftrightarrow VL_p = \sum_{k=1}^{p} k^3 = \frac{p^2(p+1)^2}{4} = HL_p.$$

   Vi ska visa att $A(p+1)$ blir sant tack vare detta antagande, så nu visar vi alltså att $VL_{p+1} = HL_{p+1}$ med hjälp av att $VL_p = HL_p$:

   $$VL_{p+1} = \sum_{k=1}^{p+1} k^3 = \sum_{k=1}^{p} k^3 + (p+1)^3 = VL_p + (p+1)^3 = /\text{induktionsantagandet används}/ =$$

   $$= HL_p + (p+1)^3 = \frac{p^2(p+1)^2}{4} + p^3 + 3p^2 + 3p + 1 = \frac{p^4 + 2p^3 + p^2}{4} + \frac{4p^3 + 12p^2 + 12p + 4}{4} =$$

   $$\frac{p^4 + 6p^3 + 13p^2 + 12p + 4}{4}$$

   och det är alltså nu vår uppgift att visa att detta också är lika med HL_{p+1}. Men för att slippa skriva en massa 4:or överallt så studerar vi $4 \cdot HL_{p+1}$ och försöker visa att det är lika med täljaren i $\frac{p^4+6p^3+13p^2+12p+4}{4}$, alltså $p^4 + 6p^3 + 13p^2 + 12p + 4$. Studera därför $4 \cdot HL_{p+1}$, det är $(p+1)^2(p+1+1)^2$ som vi skriver som $(p^2 + 2p + 1)(p^2 + 4p + 4)$ vars utveckling är

   $$p^4 + 2p^3 + p^2 + 4p^3 + 8p^2 + 4p + 4p^2 + 8p + 4 = p^4 + 6p^3 + 13p^2 + 12p + 4$$

   och detta uttryck är precis det vi ville att det skulle vara. Alltså är efterledet i implikationen, $A(p+1)$ sant och det följde av antagandet att $A(p)$ var sann, vi har alltså visat att implikationen $A(p) \Rightarrow A(p+1)$ är sann. Detta fullbordar det andra steget av induktionsbeviset.
3. Vi konstaterar att eftersom $A(1)$ är sann och implikationen $A(p) \Rightarrow A(p+1)$ alltid gäller så måste vi ha

   $$A(1) \text{ är sann} \Rightarrow A(2) \text{ är sann} \Rightarrow A(3) \text{ är sann} \ldots$$

   och det innebär att $A(n)$ är sann för alla $n \geq 1$ enligt induktionsprincipen och det fullbordar beviset.