Bevisteknikker

I matematikk kan vi si at et bevis er en logisk forklaring på hvorfor noe er sant.

Når man fører bevis kan man legge seg på ulike nivåer av grundighet, eller formalitet.
Den minst formelle formen for bevis er gjerne muntlige forklaringer hvor man hopper over mange steg.
I skriftlig språk kan vi ofte velge hvor mange detaljer vi tar med.

Den mest formelle formen for bevis kan sies å være den som i prinsippet kan leses av en datamaskin.

Eksempler:

La P og Q være to påstander. Si at vi har bevist ~~P~~ $(P \to Q)$

~~Q~~ Viser vi da senere P, kan vi bevise Q:

$$\frac{\begin{array}{c} P \to Q \\ P \end{array}}{Q}$$

Denne form for logisk deduksjon kan sjekkes på en datamaskin; teorien vår om logisk implikasjon og sannhetsverditabeller er tilstrekkelig til å implementere en algoritme som sjekker om det "under streken" faktisk er en konsekvens.

Bevis ved moteksempel

Eksempel: "fire heltall addert sammen blir alltid et ~~oddetall~~ partall"

Kan motbevises ved å finne ét moteksempel.

Vi kan for eksempel ta de fire heltallene 1, 1, 1, 2. Da får vi $1+1+1+2=5$, som er et oddetall. OK.

Vi har sett denne teknikken for å vise at relasjoner ikke er, for eksempel, symmetriske: Da må vi finne et par (x, y) slik at x er relatert til y, men y ikke er relatert til x.

Oppsumert kan vi si at en påstand $\forall x \, P(x)$ kan motbevises ved å bevise negasjonen, $\neg \forall x \, P(x) \Leftrightarrow \exists x \neg P(x)$, som igjen ofte kan bevises direkte, altså ved å finne en passende "x".

Indirekte bevis

Si at vi ønsker å vise en påstand $\exists x\, P(x)$.
En mulighet er å identifisere/finne en passende X.

En annen strategi er å indirekte vise at det <u>må</u> eksistere en passende X.

Eksempel:

La $U = \{1, 2, \dots, 15\}$, og la A, B, C være delmengder av U, alle med 11 elementer, altså $|A| = |B| = |C| = 11$.

Påstand: $\exists x \in U\,(x \in A \land x \in B \land x \in C)$

$(A \cap B \cap C \neq \emptyset)$

Bevis:

La oss undersøke $\overline{A \cap B \cap C}$. Vi har

$\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$. Hvor mange elementer er det i mengden til høyre? $|\overline{A}| = |\overline{B}| = |\overline{C}| = 4$.
<u>Maksimalt</u> $4 \cdot 3 = 12$ elementer. Altså,

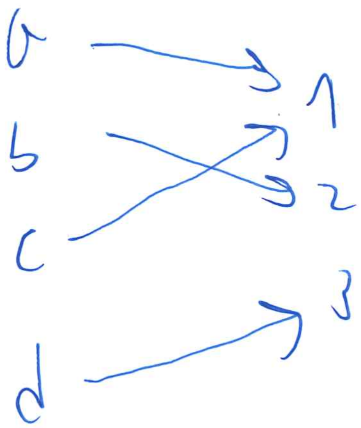
$\overline{A \cap B \cap C} = U \setminus A \cap B \cap C$ har maks 12 elementer, så $A \cap B \cap C$ har minst 3 elementer.

Altså: Det <u>må</u> eksistere en x i $A \cap B \cap C$.

Dette beviset kan kalles et bevis ved telling. Et nyttig prinsipp i slike bevis er det som på engelsk kalles "Pigeonhole principle", altså "Due-hull-prinsippet":

Har du 10 duer som skal plasseres i 9 hull, må det ende opp minst to duer i minst ett av hullene.

Generelt: Skal $n+1$ objekter/elementer fordeles i n deler/grupper, vil det eksistere en gruppe med minst to elementer.



Prinsippet gir for eksempel at en funksjon fra $\{a, b, c, d\}$ til $\{1, 2, 3\}$ umulig kan være <u>injektiv</u>, illustrert over.

Kontrapositivt bevis

Fra utsagnslogikk: $P \to Q \equiv \neg Q \to \neg P$

$(P \to Q \equiv \neg P \vee Q \equiv Q \vee \neg P \equiv \neg(\neg Q) \vee \neg P \equiv \neg Q \to \neg P)$

Noen ganger er det enklere å bevise "$\neg Q \to \neg P$" enn $P \to Q$. Kalles kontrapositivt bevis.

Eksempel: Vi sier at to heltall har lik paritet hvis begge er oddetall eller begge er partall.

~~Si at vi ønsker å vise at "Summen av to tall med samme paritet er et partall"~~

~~La P: "x og y har samme paritet"~~

og ~~Q: "x+y er partall"~~

Si nå at vi ønsker å vise at

"Hvis summen av to heltall er et partall, har de to tallene samme paritet".

Den ekvivalente, kontrapositive påstanden er: Hvis to heltall har ulik paritet, er summen av dem et oddetall.

La $P(x,y) \equiv$ "$x+y$ er partall"

og $Q(x,y) \equiv$ "x og y har samme paritet"

Over universet $\mathbb{Z}$ kan vi skrive

$$\forall x \forall y (P(x,y) \Rightarrow Q(x,y))$$

Dette er den originale påstanden. Da

$$~~R(S)~~\ P(x,y) \Rightarrow Q(x,y) \equiv \neg Q(x,y) \Rightarrow \neg P(x,y)$$

Kan vi like gjerne bevise

$$\forall x \forall y (\neg Q(x,y) \Rightarrow \neg P(x,y))$$

Altså, la x og y være to tall med ulik paritet. Da har vi ett partall og ett oddetall. Skriv partallet på formen 2a og oddetallet som 2b+1. Summen blir da

$$2a+2b+1 = 2(a+b)+1$$

som er et oddetall

Vi kan nå undersøke hvordan et direkte bevis $\forall x \forall y (P(x,y) \rightarrow Q(x,y))$ kan se ut.

La x, y være heltall slik at summen er et partall.

Vi betrakter to scenario:

* X er partall: La $x = 2a$.

$$2a + y = 2k$$

$$y = 2k - 2a = 2(k-a)\text{, partall}$$

Altså x og y har samme paritet.

* X oddetall; $x = 2a + 1$

$$2a + 1 + y = 2k$$

$$y = 2k - 2a - 1$$

$$y = 2(k-a) - 1 = 2(k-a-1) + 1$$

y oddetall og har samme paritet som x.

Bevis ved motsigelse

Si at vi ønsker å bevise P.

Hvis negasjonen til P fører til en motsigelse, altså noe som aldri er sant, kan vi konkludere at P må være sant:

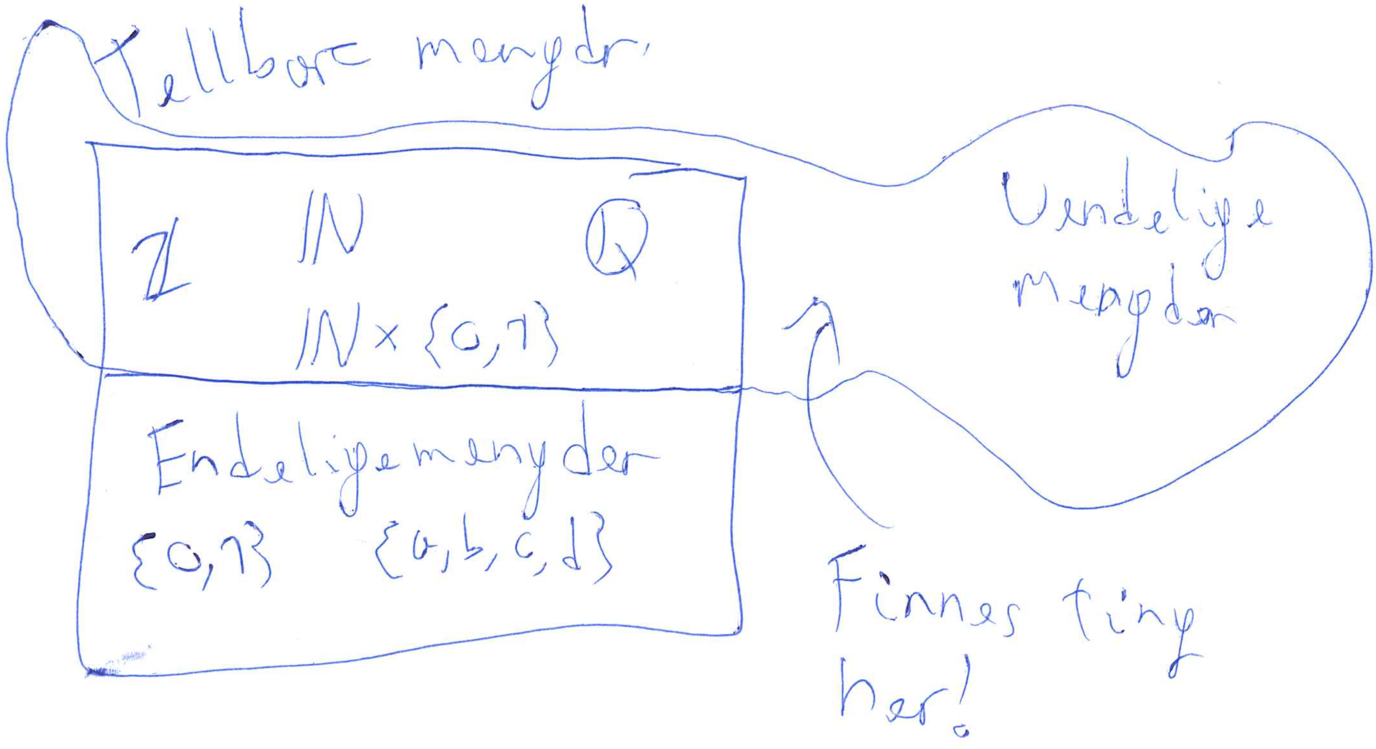
$$\neg P \to \bot \equiv \neg\neg P \vee \bot \equiv P$$

Altså: Hvis vi fra $\neg P$ kan ~~å~~ finne et paradoks eller dedusere oss frem til en motsigelse, må $\neg\neg P \equiv P$ være sann.

Eksempel: $(P \to Q) \vee (Q \to P)$ er en tautologi.

Bevis: Anta $(P \to Q) \vee (Q \to P)$ ikke er en tautologi. Velg en valuasjon slik at påstanden blir usann. Da har vi at både $P \to Q$ og $Q \to P$ er usann. Det første gir oss at P er sann, og Q usann. Det andre gir oss derimot at Q er sann. Q kan ikke både være sann og usann, ~~[illegible]~~ gitt en spesifikk valuasjon. Vi har derfor en motsigelse.

(Over) Tellbarhet



Vi kan bruke bevis ved motsigelse til å vise at det finnes mengder som <u>ikke</u> er tellbare.

~~I øvingen som publiseres onsdag denne uken vil det være en~~

Husk, $|A| = |B|$ hvis

finnes surjektiv og injektiv funksjon

$A \to B$.

$|A| \leq |B|$ betyr finnes injektiv funksjon

$A \to B$.

$|X| \leq |P(X)|$ for alle mengder X:

~~Anta for enkelhets~~

Anta $X \neq \emptyset$.

Definer $f: X \to P(X)$ ved

$$f(a) = \{a\}$$

Eks: $X = \{1, 2\}$

$\emptyset$

$1 \to \{1\}$

$2 \to \{2\}$

$\{1, 2\}$

Kan bevise at

$|X| \neq |P(X)|$, sammen med $|X| \leq |P(X)|$ får

vi $|X| < |P(X)|$.

<u>Eks:</u> $|\mathbb{N}| < |P(\mathbb{N})|$, så $P(\mathbb{N})$ er ikke

tellbar.

$P(P(\mathbb{N}))$ er enda større.

Kan bevise: $|\mathbb{R}| = |P(\mathbb{N})|$

Altså, $\mathbb{R}$ er ikke tellbar!

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ er tellbar

$\mathbb{R}$, $P(\mathbb{N})$, $\mathbb{C}$ <u>ikke</u> tellbar.

I øving: Stjernemarket oppgave om å

vise at $|X| \neq |P(X)|$, ~~g~~

$\mathbb{Q}$ er tellbar

Strategi: Vis at $\mathbb{N} \times \mathbb{N}$ er tellbar, altså

$$|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$$

Vis så $|\mathbb{Q}| \leq |\mathbb{N} \times \mathbb{N}|$

Da har vi

$$|\mathbb{Q}| \leq |\mathbb{N}|$$

Som ønsket: Å sammenligne størrelser /kardinalitet er transitivt. (Vi har ikke bevist dette)

$\mathbb{N} \times \mathbb{N}$ er tellbar. For å vise dette må vi tilordne et naturlig tall til hvert punkt $(a, b) \in \mathbb{N} \times \mathbb{N}$ på en slik måte at ulike punkter får ulike tall.
Hvordan kan vi gjøre dette?

	0	1	2	3	4
0					
1			(1,2)		
2		(2,1)			
3					
4					

(4, 1)

Vi kan fylle ut øverste rad med tallene 0, 1, 2, 3, 4, ... Da gir vi ikke noe tall til for eksempel (2, 0), men kun til punktene (0,1), (0,2), (0,3), ...

I stedet kan vi fylle ut diagonalene fra høyre og ned mot venstre.

	0	1	2	3	4		
0	0	1	3	6	10	15	21
1	2	4	7	11	16	22	
2	5	8	12	17	23		
3	9	13	18	24			
4	14	19	25				
	20	26					

Nå får alle punktene en unik "id"!

~~AF~~

Kan vise at denne funksjonen kan defineres ved $(a, b) \longmapsto \frac{(a+b)^2 + (a+b)}{2} + a$

Vi leter nå etter en injektiv funksjon

$\mathbb{Q} \to \mathbb{N} \times \mathbb{N}$.

Obs: fristende å definere $\frac{a}{b} \mapsto (a, b)$

to problemer: * brøker kan representeres på forskjellige måter.

* Hva om a eller b er negativ?

Første problem løser vi med forenkling av brøker.

$\frac{15}{10}$ skriver vi som $\frac{3}{2}$, og vi setter minustegn på telleren. Så

$\frac{15}{-10}$ skriver vi som $\frac{-3}{2}$. $\frac{-3}{-6}$ skriver vi $\frac{1}{2}$.

Dette gir oss en unik måte å skrive brøker på.

La oss nå definere en funksjon

$f: \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$

$$f\left(\frac{a}{b}\right) = \begin{cases} ((-2a), b) & \text{hvis } a \leq 0 \\ (2a+1, b) & \text{hvis } a > 0 \end{cases}$$

Hvor $\frac{a}{b}$ er ~~så~~ antatt å være forenklet

Som over.

Eks: $\frac{4}{-12} = \frac{1}{-3} = \frac{-1}{3} \mapsto (2,3)$

Injektiv: $f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right) = (x,y)$

Hvis x partall: Da er $a = \frac{-x}{2} = c$

Hvis x oddetall: $a = \frac{x-1}{2} = c$

Vinsett: $b = y = d$.