TMA4140- 5. forelesning

Utsagnslogiske begreper og bevis

Aslak Bakke Buan

September 19, 2023

Innhold

Utsagnslogiske begreper

Bevis

Husk!

Syntaks i utsagnlogikk: Utsagnsvariabler (som representerer atomære utsagn), konnektivene ($\neg, \wedge, \vee, \rightarrow$) og parenteser.

Eksempel: $\neg(P \vee Q)$.

Husk: $P \rightarrow Q$ har vi definert som $\neg(P \wedge \neg Q)$.

Semantikk, tolkning av utsagnslogiske formler. Vi har sett på $\iff$ (ekvivalens) og $\implies$ (konsekvens).

Eksempel: $\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$ og $(P \wedge Q) \implies (P \vee Q)$.

Konsekvens, ekvivalens og gyldige argumenter

Valuasjon: å tilordne sannhetsverdier (altså 0 eller 1) til utsagnsvariabler.

Husk: vi kaller to formler P og Q (som representerer sammensatte utsagn) ekvivalente, hvis alle valuasjoner av utsagnsvariablene som inngår i formelene, gir samme sannhetsverdi for P og Q.
Vi skriver $P \iff Q$.

Og, vi sier at Q er en logisk konsekvens av P, dersom alle valuasjoner av utsagnsvariablene som gjør P sann også gjør Q sann.
Vi skriver: $P \implies Q$

Definisjon: Vi sier at et resonnement er gyldig hvis konklusjonen er en logisk konsekvens av mengden av premisser.

Eksempel

Eksempel: Premisser $A \to B$ og $\neg B$. Konklusjon $\neg A$.

A	B	(A $\to$ B)	$\neg$ B	$(A \to B) \wedge \neg B$	$\neg A$
0	0	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	1
1	1	1	0	0	0

Dette er et gyldig argument (kalles modus tollens). Når (A $\to$ B) og $\neg$ B begge har sannhetsverdi 1, har også $\neg A$ sannhetsverdi 1.

Vi har tidligere sett at $(A \to C)$ er en logisk konsekvens av $(A \to B) \wedge (B \to C)$.
Altså premisser $(A \to B)$ og $(B \to C)$ og konklusjon $(A \to C)$, er et gyldig argument.

Fra Ludvig Holbergs Erasmus Montanus: «En sten kan ikke flyve. Mor Nille kan heller ikke flyve. Ergo er Mor Nille en sten.»
Dette er et eksempel på et argument som ikke er gyldig. Pauseoppgave: oversett til utsagnslogikk! Hint: "En sten kan ikke flyve", kan uttrykkes "Hvis du er en sten, så kan du ikke flyve."

Egenskaper ved formler

La F være en utsagnslogisk formel.
Definisjon: F er

- *oppfyllbar*, dersom det finnes minst en valuasjon som gjør F sann;
- *falsifiserbar*, dersom det finnes minst en valuasjon som gjør F usann;
- *en tautologi*, dersom alle valuasjoner gjør F sann;
- *en motsigelse*, dersom alle valuasjoner gjør F usann

Altså: en tautologi kan ikke være falsifiserbar, en motsigelse kan ikke være oppfyllbar.
Og: mange formler er både oppfyllbare og falsifiserbare

Oppfyllbare og falsifiserbare formler

For enkle formler er det ofte opplagt om de er oppyllbare og/eller falsifiserbare.

$P \to Q$, $P \to (Q \vee R)$, $((P \wedge Q) \wedge R)$ er alle både oppyllbare og falsifiserbare.

$P \wedge \neg P$ er ikke oppfyllbar, mens $P \vee \neg P$ og $P \to (P \vee Q)$ er ikke falisfiserbare.

For mer kompliserte formler, kan vi bruke en sannhetsverditabell.

Se på: $(P \to (Q \to R)) \wedge (Q \wedge \neg R)$

P	Q	R	$(Q \to R)$	$P \to (Q \to R)$	$\neg R$	$(Q \wedge \neg R)$	$(P \to (Q \to R)) \wedge (Q \wedge \neg R)$
0	0	0	1	1	1	0	0
1	0	0	1	1	1	0	0
0	1	0	0	1	1	1	1
0	0	1	1	1	0	0	0
				...			

Allerede etter å ha sjekket de tre første valuasjonene, kan vi se at formelen er oppfyllbar og falsifiserbar, og dermed ikke en tautologi og ikke en kontradiksjon.

Flere eksempler

Se på: $(P \to (Q \vee R)) \to (\neg Q \to P)$.
Dette er ikke en tautologi: Hvis P, Q, R alle er usanne, er F usann.
Det er heller ikke en kontradiksjon: Hvis P er sann, er F sann (uavhengig av Q, R.)

Noen tautologier er lette å kjenne igjen, e.eks. $P \vee \neg P$ eller $P \to P$.

Andre er mer kompliserte.
Se på $(P \wedge (Q \vee R)) \to (P \vee (Q \wedge R))$.

Dette er en tautologi.

P	Q	R	$(Q \vee R)$	$(Q \wedge R)$	$(P \wedge (Q \vee R))$	$(P \vee (Q \wedge R))$	$(P \wedge (Q \vee R)) \to (P \vee (Q \wedge R))$
0	0	0	0	0	0	0	1
1	0	0	0	0	0	1	1
0	1	0	1	0	0	0	1
0	0	1	1	0	0	0	1
1	1	0	1	0	1	1	1
1	0	1	1	0	1	1	1
0	1	1	1	1	0	0	1
1	1	1	1	1	1	1	1

Eksempel, forts.

Se på $(P \wedge (Q \vee R)) \rightarrow (P \vee (Q \wedge R))$.

Et direkte bevis for at dette er en tautologi:

Hvis implikasjonen $\rightarrow$ skal være usann, må $(P \vee (Q \wedge R))$ være usann. Dette er en egenskap ved $\rightarrow$.

Da må P være usann. Dette er en egenskap ved $\vee$.

Da er også premisset i hovedimplikasjonen $(P \wedge (Q \vee R))$ usant. Dette er en egenskap ved $\wedge$.

Så dermed er alltid $(P \wedge (Q \vee R))$ usann når $(P \vee (Q \wedge R))$ er usann.

Altså er formelen en tautologi.

Uavhengighet

La F og G være formler.

Vi sier at G er uavhengig av F, hvis hverken G eller $\neg G$ er en konsekvens av F.

Vi sier at F, G er uavhengige hvis G er uavhengig av F og F er uavhengig av G.

Eksempel: Formlene $P \to Q$ og $P \vee Q$ er uavhengige. Mens formlene $P \to Q$ og $P \wedge Q$ er ikke uavhengige.

Formlene $P \vee Q$ og $P \wedge Q$ er heller ikke uavhengige.

Oppgave: Hvorfor?

Eksempel: Formlene P og $P \to Q$ er uavhengige. Og formlene $P \to Q$ og $P \vee Q$ er uavhengige.

Oppgave: Kan vi da si at også P og $P \vee Q$ er uavhengige?

Bevis og formodninger

NB! Dette omhandler kapittel 5 i RB, men vi gjør det litt annerledes her.

Et bevis for en påstand, er en rekke av gyldige argumenter, som viser hvordan en samling av antagelser leder fram til påstanden.
I matematikken kaller vi ofte påstander som har et bevis for: Teoremer, Proposisjoner, Lemma.

Formodninger, er påstander, som vi *tror* er sanne, vanligvis basert på mange eksempler.

Goldbachs formodning (fra 1742), sier at ethvert partall > 2 kan uttrykkes som en sum av to primtall.

Eks: $8 = 5 + 3 \quad 36 = 17 + 19 \quad \ldots$

Ingen har har kunnet bevise dette. Per 2013 var det verifisert for partall $< 10^{18}$.

(NB: det er bevist at seks primtall er tilstrekkelig, altså alle partall kan kunne skrives som en sum av maks 6 primtall.)

Hva skal bevises? To typer påstander

Det er to hovedtyper av påstander:

-Eksistenspåstander

-Universelle påstander

Eksempel: Det finnes en $x \in \mathbb{N}$ slik at $x^3 < 3x$.

Eksempel: For alle $x \in \mathbb{N}$ er $x^2 + 1 \geq 2x$.

Bevistyper, eksistensbevis

Eksistensbevis er enten konstruktive eller ikke-konstruktive.

I konstruktive bevis finner man eksplisitt et element/tall/objekt som beviser påstanden.

I ikke-konstruktive bevis, bevises kun at et slikt objekt finnes. Dette kan f.eks. gjøres ved et såkalt motsigelsebevis.

Ikke-konstruktivt eksistensbevis, eksempel

Husk: Alle naturlige tall > 1 kan skrives som et produkt av primtall.

Påstand: Det finnes et primtall med mer enn 1000 siffer.

Her er et ikke-konstruktivt bevis:

Hvis det ikke finnes et slikt primtall, må det bare være endelig mange primtall.

La da $p_1, p_2, p_3, \ldots, p_t$ være listen av alle forskjellige primtall.

Se på tallet $m = 1 + p_1 \cdot p_2 \cdot \cdots \cdot p_t$.

Hvis vi deler m på p_1 får vi rest 1, tilsvarende for alle p_i. Dermed, ingen av p_i-ene er divisor i m. Da har vi en motsigelse. Altså må det finnes et primtall med mer enn 1000 siffer.

NB! Vi finner altså ikke et primtall med 1000 siffer.

NB! Vi hevder ikke at m er et primtall.

Bevisteknikker

- Direkte bevis
- Kontrapositive bevis
- Motsigelsesbevis
- Induksjonsbevis
- Bevis ved tilfeller

NB: Ofte(st) kombineres disse. Et induksjonsbevis vil oftest også inkludere direkte bevis for delpåstander.

Direkte bevis - eksempel

Påstand: Hvis x er et positivt oddetall, så er x^2 også et oddetall.

Bevis: Siden x er et oddetall, kan vi skrive $x = 2y + 1$ for et heltall y. Da er $x^2 = (2y + 1)^2 = 4y^2 + 4y + 1$. Siden 4 er en divisor i $4y^2 + 4y = 4(y^2 + y)$, må $4y^2 + 4y$ være et partall. Da er $4y^2 + 4y + 1$ et oddetall, altså er x^2 et oddetall.

Påstand: $(P \wedge Q) \rightarrow (P \vee R)$ er en tautologi.

Bevis: Hvis $P \wedge Q$ er sann, må P være sann. Dette er en egenskap ved $\wedge$.

Da er $(P \vee R)$ også sann. Dette er en egenskap ved $\vee$.

Dermed er formelen en tautologi.

Kontrapositive bevis

Hvis man skal vise at G er en logisk konsekvens av F, er det nok å vise at $\neg F$ er en logisk konsekvens av $\neg G$.
Definisjon: et direkte bevis for at $\neg F$ er en logisk konsekvens av $\neg G$, er et *kontrapositivt* bevis for at G er en logisk konsekvens av F.

Hvis x og y er naturlige tall og xy er et partall, så er minst en av x og y et partall.

Altså G: x eller y partall er logisk konsekvens av F: xy partall.

Nok å vise at $\neg$ F: xy oddetall er logisk konsekvens av $\neg$ G: Både x og y er oddetall.

Dette kan vi gi et direkte bevis for. Det blir en oppgave til dere. Hint:Se på det direkte beviset for at x^2 er oddetall, når x er oddetall.

Motsigelsesbevis

Idé: Anta at en påstand P ikke er sann. Gjør gyldige argument, og end opp med noe som er en motsigelse/kontradiksjon.
Da må den opprinnelige påstanden P være sann (altså siden det er umulig at den ikke er sann).

Eksempel: Skal vise at $(P \wedge Q) \rightarrow (P \vee R)$ er en tautologi.

Bevis: Anta at den ikke er det. Da finnes en valuasjon slik at $(P \vee R)$ er usann, og $(P \wedge Q)$ er sann.
Hvis $(P \vee R)$ er usann, så er P usann. Dette er en egenskap ved $\vee$.

Hvis $(P \wedge Q)$ er sann, så er P sann. Dette er en egenskap ved $\wedge$.
Dermed er P både sann og usann i denne valuasjonen. Dette er en motsigelse. Så formelen må være en tautologi.

NB: sammenlign dette med det tidligere direkte beviset for samme påstand.

Bevis ved tilfeller

I mange bevis må man diskutere flere forskjellige tilfeller.

Eksempel: Vis at $n^2 \geq n$ for alle heltall.

Bevis:

(i) Tilfellet $n \geq 1$. Da kan vi multiplisere med n på begge sider, og får $n^2 \geq n$.

(ii) Tilfellet $n = 0$. Ok, siden $n^2 = 0 \geq 0 = n$.

(iii) Tilfellet $n \leq -1$. Ok, siden $n^2 > 0 > n$.

Induksjonsbevis

Husk: induksjonsbevis brukes for å bevise universelle påstander om (induktivt definerte) uendelige mengder.

NB: kombineres med andre bevisteknikker.

Motbevise en universell påstand: finne eksempel

Hvis vi skal vi at at universell påstand P ikke holder, altså motbevise P, er det nok å finne et eksempel som viser at $\neg$ P kan være sann.
Altså: vi trenger et eksistensbevis for påstanden $\neg$ P.

Eksempel.
Påstand: Det er ikke slik at at $n! > n^3$ for alle naturlige tall n.

Det er da nok å finne en $n \in \mathbb{N}$ slik at $n! \leq n^3$.

La $n = 1$ (eller 2, eller 3...).

Å motbevise en påstand om eksistens: bevise en universell påstand

Anta at påstanden P er at det finnes et element med en viss egenskap.

Et motbevis vil da være å vise at ingen elementer har denne egenskapen.

Altså: et bevis for en universell påstand.

Eksempel.

Påstand: Det finnes et heltall n, slik at $n^2 < n$.

Vi motbeviser dette ved å vise at $n^2 \geq n$ for alle heltall n.

Det har vi gjort tidligere.

Oppsummering, utsagnslogikk

- Syntaks: Formler i utsagnslogikk er bygd opp av utsagnsvariabler, konnektiver ($\neg, \wedge, \vee, \rightarrow$) og parenteser.
- Utsagnsvariabler representerer "atomære utsagn" og kan ha sannhetsverdi 0/1 (= usann/sann).
- En valuasjon er et valg av sannhetsverdier for utsagnsvariablene i en formel.
- Semantiske begreper: Ekvivalens $P \iff Q$, konsekvens $P \implies Q$,
- tautologi (P alltid sann), motsigelse (P aldri sann), oppfyllbar (P kan være sann), falisfiserbar (P kan være usann).
- Vi kan bruke sannhetsverditabeller for å analysere formler og sammenheng mellom formler.
- Vi kan også bruke forskjellige bevisteknikker for å si noen om sammenhengen mellom formler.
- Vi har sett blant annet på direkte bevis, kontrapositive bevis, motsigelsesbevis.

Plenumsregningen og øving

- Den nye øvinga denne uka er kun skriftlig.
- På plenumsregninga og øvinga blir det blant annet sett på egenskaper ved reelle og rasjonale tall for å illustrere forskjellige bevisteknikker.