INF1080 – Logiske metoder for informatikk

Digital eksamen (med løsningsforslag)

Dette er et utkast til løsningsforslag til eksamen i INF1080, og feil kan forekomme. Hvis du finner noen feil, si ifra til Roger på `rantonse@ifi.uio.no`.

1 Små oppgaver [70 poeng]

1.1 Grunnleggende mengdelære [3 poeng]

Anta at $A = \{0, \{0\}, \{0, \{\}\}\}$.

- Hvor mange elementer har A? (**3** / 4)

Det er 3 elementer: 0 er et element. $\{0\}$ er et element. Og $\{0, \{0\}\}$ er et element.

- Er det slik at $\{\} \in A$? (Ja / **Nei**)

Den tomme mengden, $\{\}$, kan være et element i en mengde, men ikke i denne, hvor vi kun har de tre elementene nevnt før.

- Er det slik at $\{\} \subseteq A$? (**Ja** / Nei)

Den tomme mengden er en delmengde av alle mengder. Hvert element i den tomme mengden er med i A.

1.2 Utsagnslogikk [3 poeng]

Anta at P står for «det snør» og at Q står for utsagnet «toget går».

- Formelen $(P \to Q)$ representerer utsagnet «det snør bare hvis toget går». (**Sant** / Usant)

Utsagnet er en annen måte å si «hvis det snør, så går toget» på. Med andre ord, hvis «det snør», er det nødvendigvis også slik at «toget går».

- Formelen $\neg(P \to Q)$ representerer utsagnet «toget går ikke hvis det snør». (Sant / **Usant**)

Utsagnet sier «det er ikke tilfelle at hvis det snør så går toget». En korrekt formel hadde vært $(P \to \neg Q)$.

- Formelen $(P \to \neg Q)$ representerer utsagnet «toget går ikke fordi det snør». (Sant / **Usant**)

Formelen sier «hvis det snør så går ikke toget». Det er ikke mulig å uttrykke i utsagnslogikk at noe er tilfelle *fordi* noe annet er tilfelle, såkalt kausalitet.

1.3 Sannhetsverdier og valuasjoner [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Formelen $(P \lor Q \lor \neg P)$ er sann for alle valuasjoner. (**Sant** / Usant)

Enten P eller $\neg P$ er sann for enhver valuasjon. Da blir hele formelen sann.

- $(P \to \neg P)$ kan gjøres sann. (**Sant** / Usant)

I følge sannhetsverditabellen til $\to$ holder det at P kan gjøres usann.

- Hvis $(P \to Q)$ og $\neg Q$ er sanne, må $\neg P$ være sann. (**Sant** / Usant)

Formlene $(P \to Q)$ og $\neg Q$ er kun sanne samtidig dersom P og Q begge er usanne. Og da er $\neg P$ sann.

1.4 Utsagnslogiske begreper [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Alle utsagnslogiske tautologier er oppfyllbare. (**Sant** / Usant)

For at en formel skal være oppfyllbar må det finnes en valuasjon som gjør den sann. Tautologier blir til og med sanne under hver valuasjon.

- Det finnes en oppfyllbar formel som er kontradiktorisk. (Sant / **Usant**)

En formel er kontradiktorisk hvis det ikke finnes en valuasjon som oppfyller den. Det er altså det samme som å være ikke oppfyllbar.

- Formelen $((P \to Q) \lor (Q \to P))$ er en tautologi. (**Sant** / Usant)

Følgende sannhetsverditabell viser at formelen er sann for alle valuasjoner.

P	Q	$(P$	$\to$	$Q)$	$(Q$	$\to$	$P)$	$((P \to Q)$	$\lor$	$(Q \to P))$
1	1	1	1	1	1	1	1	1	1	1
1	0	1	0	0	0	1	1	0	1	1
0	1	0	1	1	1	0	0	1	1	0
0	0	0	1	0	0	1	0	1	1	1

1.5 Bevis og moteksempler [3 poeng]

Velg ett alternativ:

- Et moteksempel til påstanden «G er en logisk konsekvens av F»:
  - gjør G sann og F usann.
  - gjør G og F usanne.
  - **gjør F sann og G usann.**

«G er en logisk konsekvens av F» betyr at enhver valuasjon som gjør F sann, også gjør G sann. Da er et moteksempel til det en valusjon som ikke gjør det, det vil si at den gjør F sann, men ikke G.

- Er en påstand bevist, kan det ikke finnes et moteksempel til den: **Sant** / Usant

Det er sant. Et moteksempel viser at en påstand er usann, og da kan det ikke finnes et bevis for den.

- Hvilket av disse tallene er et moteksempel til påstanden «alle oddetall er primtall»: $6, 7, 8, \underline{9}$.

Her må vi finne et tall som er et oddetall, men ikke et primtall. Tallene 6 og 8 er ikke oddetall, så de er ikke brukbare som moteksempler. Tallet 7 er et primtall. Men, tallet 9 er altså et oddetall og ikke et primtall ($9 = 3 \cdot 3$).

1.6 Relasjoner [3 poeng]

La $R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,2\rangle\}$ være en relasjon på $A = \{1,2,3,4\}$.

- Er R refleksiv? (Ja / **Nei**)

Ikke refleksiv, fordi paret $\langle 3,3\rangle$ ikke er element i R.

- Er R symmetrisk? (**Ja** / Nei)

For hvert par $\langle x,y\rangle$ er også paret $\langle y,x\rangle$ med.

- Er R transitiv? (Ja / **Nei**)

Ikke transitiv, fordi $\langle 1,2\rangle$ og $\langle 2,3\rangle$ er med i R men ikke $\langle 1,3\rangle$.

1.7 Funksjoner [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- En «funksjon» er definert som en injektiv relasjon. (Sant / **Usant**)

En relasjon R (fra A til B) er en funksjon hvis den er slik at for hvert $x \in A$, så finnes det nøyaktig ett element $y \in B$ med $\langle x, y \rangle$. Denne egenskapen er noe annet enn å være injektiv.

- Enhver bijektiv funksjon $f : a, b, c \to a, b, c$ er en symmetrisk relasjon. (Sant / **Usant**)

Funksjonen definert ved $f(a) = b$, $f(b) = c$, $f(c) = a$ er bijektiv. Men, siden $f(a) = b$ og ikke $f(b) = a$, er den ikke en symmetrisk relasjon.

- Det finnes en bijektiv funksjon $f : a, b, c \to a, b, c$ som er en symmetrisk relasjon. (**Sant** / Usant)

Funksjonen definert ved $f(a) = b$, $f(b) = a$, $f(c) = c$ er bijektiv og en symmetrisk relasjon. Det samme er identitetsfunksjonen.

1.8 Litt mer mengdelære [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Den tomme mengden har ikke en potensmengde. (Sant / **Usant**)

Alle mengder har en potensmengde. Den tomme mengden har nøyaktig én delmengde, som er den tomme mengden selv: $\{\} \subseteq \{\}$. Dermed er potensmengden av den tomme mengden, $\{\{\}\}$, mengden som inneholder den tomme mengden som eneste element.

- Alle uendelige mengder har lik kardinalitet. (Sant / **Usant**)

Mengden av reelle tall er overtellbar, det vil si at den har en høyre kardinalitet enn mengden av de naturlige tallene.

- Mengden av primtall, $\{2, 3, 5, 7, 11, \ldots\}$, har kardinalitet mindre eller lik mengden av de naturlige tallene, $\{0, 1, 2, 3, \ldots\}$. (**Sant** / Usant)

Funksjonen $f : P \to \mathbb{N}$, definert ved at $f(n) = n$, som sender ethvert primtall til seg selv, er injektiv. Dermed har P kardinalitet mindre eller lik $\mathbb{N}$. I det hele tatt har en delmengde alltid kardinalitet mindre eller lik den hele mengden.

1.9 Tillukning [3 poeng]

La $P = \{q \in Q \mid q > 0\}$ være mengden av positive rasjonale tall.

- P er lukket under divisjon («delt med»). (**Sant** / Usant)

Ethvert positivt brøktall x kan deles med ethvert positivt brøktall y. Resultatet er igjen et positivt brøktall. Dermed er mengden lukket under divisjon.

- P er lukket under subtraksjon («minus»). (Sant / **Usant**)

Vi har at $\frac{1}{1} - \frac{2}{1} = -\frac{1}{1}$. Resultatet er altså ikke i P.

- Den refleksive tillukningen av relasjonen $<$ på P er relasjonen $\leqslant$ på P. (**Sant** / Usant)

Vi får den refleksive tillukningen ved å legge til $\langle x, x\rangle$ for alle $x \in P$. Da får vi følgende relasjon:

$$
\begin{aligned}
&\{\langle x, y\rangle \mid x < y \text{ for alle } x, y \in P\} \cup \{\langle x, x\rangle \text{ for alle } x \in P\} \\
= &\{\langle x, y\rangle \mid x < y \text{ eller } x = y \text{ for alle } x, y \in P\} \\
= &\{\langle x, y\rangle \mid x \leqslant y \text{ for alle } x, y \in P\}
\end{aligned}
$$

1.10 Rekursive funksjoner [3 poeng]

La f være en funksjon fra naturlige tall til strenger over alfabetet $\{\mathtt{a}, \mathtt{b}\}$ definert rekursivt på følgende måte:

(1) $f(0) = \mathtt{a}$

(2) $f(n + 1) = f(n)\mathtt{b}f(n)$

Avgjør om følgende påstander er sanne eller usanne.

- Det er slik at $f(2) = \mathtt{ababa}$. (Sant / **Usant**)

$$
\begin{aligned}
f(0) &= \mathtt{a} \\
f(1) &= f(0)\mathtt{b}f(0) = \mathtt{aba} \\
f(2) &= f(1)\mathtt{b}f(1) = \mathtt{abababa}
\end{aligned}
$$

- Det første tegnet i $f(23)$ er en $\mathtt{a}$. (**Sant** / Usant)

Strengen $f(0)$ begynner på en $\mathtt{a}$. Men for alle n begynner $f(n + 1)$ på samme tegn som $f(n)$, siden $f(n)$ åpenbart aldri er den tomme strengen. Da er mulig å gjøre et enkelt induksjonsbevis for at $f(n)$ begynner på en $\mathtt{a}$ for alle n, også for $n = 23$.

- Lengden (antall tegn) av $f(n)$ er et oddetall for alle naturlige tall n. (**Sant** / Usant)

Vi har at $|f(0)| = |a| = 1$ er et oddetall. For $n > 0$ får vi følgende utregning: $|f(n+1)| = |f(n)\mathtt{b}f(n)| = |f(n)| + |\mathtt{b}| + |f(n)| = 2 \cdot |f(n)| + 1$. Tallet $2 \cdot |f(n)|$ er et partall, så $2 \cdot |f(n)| + 1$ er et oddetall.

1.11 Strukturell induksjon [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Anta at påstanden P holder for 23 men ikke for 22. For eksempel $P(x)$: «x er primtall». Da vil $P(x)$ ikke være egnet som induksjonshypotese i et bevis ved matematisk induksjon. (**Sant** / Usant)

Hvis induksjonsbeviset lykkes, har vi bevist at induksjonshypotesen er sann for alle tall. Så hvis vi starter med en hypotese som ikke er det, kan ikke beviset lykkes.

- Induksjonssteget i et bevis ved matematisk induksjon består i å vise at det finnes et tall n slik at $P(n+1)$ følger fra $P(n)$. (Sant / **Usant**)

Induksjonssteget består i å vise dette for alle tall n. Det holder ikke med at det finnes ett.

- I et bevis ved strukturell induksjon på mengden av bitstrenger er induksjonshypotesen at påstanden holder for strengene $\mathtt{0}$ og $\mathtt{1}$. (Sant / **Usant**)

Dette er basissteget, ikke induksjonshypotesen.

1.12 Førsteordens språk [4 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- $(\forall x Rx, Qx)$ er en formel. (Sant / **Usant**)

Ingenting i definisjonen av syntaksen til førsteordens logikk tillater en konstruksjon $(\ldots, \ldots)$

- $(Px \land \neg Px)$ er en formel. (**Sant** / Usant)

Dette er en uoppfyllbar formel, men en formel.

- $(\forall x Pxy \land \forall y Qxy)$ er en formel. (**Sant** / Usant)

Det har ingenting å si at noen variabler er bundet og andre ikke.

- $((\forall x \land \forall y)Pxy)$ er en formel. (Sant / **Usant**)

Her står tegnet $\wedge$ mellom to kvantorer; det er ikke tillatt i syntaksen.

1.13 Representasjon av kvantifiserte utsagn [3 poeng]

Anta at H er et relasjonssymbol slik at Hx tolkes som «x er en hund».

Anta at K er et relasjonssymbol slik at Kx tolkes som «x er en katt ».

Anta at L er et relasjonssymbol slik at Lxy tolkes som «x liker y».

Avgjør om følgende påstander er sanne eller usanne.

- Formelen $\forall x(\exists y(Hy \wedge Lxy) \to Hx)$ representerer utsagnet «enhver som liker en hund er selv en hund». (**Sant** / Usant)

Alle x som er slik at det finnes en y som er en hund, og x liker y, er hunder

- Formelen $\forall x \forall y((Kx \wedge Ky) \wedge Lxy)$ representerer utsagnet «enhver katt liker alle katter». (Sant / **Usant**)

Denne sier at for alle x og y, så er x og y katter og x liker y. En mulig formel for utsagnet hadde vært $\forall x \forall y((Kx \wedge Ky) \to Lxy)$.

- Formelen $\exists x \forall y(Hx \wedge (Ky \to Lxy))$ representerer utsagnet «det finnes en hund som liker alle katter». (**Sant** / Usant)

Det kan være forvirrende at allkvantoren $\forall$, for alle katter, står utenfor utsagnet at x er en hund, men det er ingenting galt med den måten å skrive det på.

1.14 Tolkning i modeller [4 poeng]

La $\mathcal{M}$ være en modell med domene $\{1, 2, 3, 4\}$, slik at

- $P^M = \{1, 3\}$,
- $Q^M = \{2, 4\}$ og
- $R^M = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 4\rangle, \langle 4, 1\rangle\}$.

Avgjør om følgende påstander er sanne eller usanne.

- Det er slik at $M \models \forall x(Px \vee Qx)$. (**Sant** / Usant)

Hvert element i domenet gjør enten P eller Q sann.

- Det er slik at $M \models \exists x \forall y Rxy$. (Sant / **Usant**)

Tolkningen av R relaterer hvert element i denne modellen til kun ett annet element. Det finnes ikke ett element som blir relatert til alle andre.

- Det er slik at $M \models \forall x(Px \lor \exists y(Rxy \land Py))$. (**<u>Sant</u>** / Usant)

For alle elementer i domenet er enten P sann, eller man kommer ved hjelp av $R^{\mathcal{M}}$ til et element som gjør det.

- Det er slik at $M \models \forall x \exists y(Px \lor Qy)$. (**<u>Sant</u>** / Usant)

For alle x kan ett og det samme element for y brukes, for eksempel 2. Da blir formelen ekvivalent med $\forall x(Px \lor Q_2)$, og Q_2 er oppfyllt uansett hva verdien til x er.

1.15 Resonnering om modeller [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Formelen $\exists x(Px \lor Q)$ er en logisk konsekvens av $(\exists x Px \lor Q)$. (**<u>Sant</u>** / Usant)

En modell som gjør $(\exists x Px \lor Q)$ sann gjør enten $\exists x Px$ sann, eller Q sann. I første tilfelle så finnes d i domenet slik at den gjør $P\bar{d}$ sann. Da er også $P\bar{d} \lor Q$ sann. Og dermed blir $(\exists x Px \lor Q)$ sann.

- Enhver modell som gjør $\forall x(Px \lor Qx)$ sann, må også gjøre $\exists x \neg Qx$ sann. (Sant / **<u>Usant</u>**)

Ta for eksempel en modell hvor P og Q er sanne for alle elementer i domenet.

- Enhver modell som gjør $\forall x(Px \to \neg Px)$ sann, må også gjøre $\neg \exists x Px$ sann. (**<u>Sant</u>** / Usant)

Formelen $(Px \to \neg Px)$ er sann kun hvis Px er usann. Da er $\forall x(Px \to \neg Px)$ sann i en modell hvor P ikke holder for noen elementer i domenet. Og da er også $\neg \exists x Px$ sann.

1.16 Ekvivalensrelasjoner [4 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- $\{\langle 1,1 \rangle, \langle 2,2 \rangle, \langle 3,3 \rangle, \langle 4,4 \rangle\}$ er en ekvivalensrelasjon på $\{1,2,3,4\}$. (**<u>Sant</u>** / Usant)

Relasjonen er refleksiv, symmetrisk, og transitiv.

- $\{\langle 1,2 \rangle, \langle 2,3 \rangle, \langle 3,1 \rangle, \langle 4,4 \rangle\}$ er en ekvivalensrelasjon på $\{1,2,3,4\}$. (Sant / **<u>Usant</u>**)

Relasjonen er ikke refleksiv; for eksempel er ikke $\langle 1, 1\rangle$ med. Heller ikke symmetrisk, fordi $\langle 1, 2\rangle$ er med, men ikke $\langle 2, 1\rangle$. Og ikke transitiv heller, ford $\langle 1, 2\rangle$ og $\langle 2, 3\rangle$ er med, men ikke $\langle 1, 3\rangle$.

- $\{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$ er en ekvivalensrelasjon på $\{1, 2\}$. (**Sant** / Usant)

Denne relaterer hvert element til ethvert annet element. Dermed er den refleksiv, symmetrisk og transitiv.

- $\{1\}$ er en ekvivalensrelasjon på $\{1\}$. (Sant / **Usant**)

Denne mengden er ikke en binær relasjon, og derfor kan den heller ikke være en ekvivalensrelasjon.

1.17 Kombinatorikk [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Det finnes nøyaktig 12 måter å velge to elementer fra mengden $\{1, 2, 3, 4\}$ på. (Sant / **Usant**)

Med «valg» mener vi at rekkefølgen mellom de valgte elementene ikke har noe å si. Da blir det $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$, altså seks muligheter. Noen spurte om de to elementene kunne være like – nei, fordi ellers hadde jo bare vært ett element i mengden, og ikke to.

- Det finnes nøyaktig 32 delmengder av mengden $\{1, 2, 3, 4, 5\}$. (**Sant** / Usant)

Hvert element kan enten være med eller ikke, og det er uavhengig av om de andre elmentene er med. Dermed har vi $2^5 = 32$ delmengder.

- Det finnes nøyaktig 8 bijektive funksjoner fra $\{1, 2, 3\}$ til $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. (Sant / **Usant**)

En bijektiv funksjon f fra $\{1, 2, 3\}$ til $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ tilsvarer en permutasjon $\langle f(1), f(2), f(3)\rangle$ av $\langle a, b, c\rangle$. Vi vet at det finnes $3! = 6$ forskjellige permutasjoner av tre elementer.

1.18 Litt mer kombinatorikk [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Antall måter å velge to elementer i rekkefølge på (2-permutasjoner) av en mengde med n elementer er $n(n - 1)(n - 2)$. (Sant / **Usant**)

Antallet 2-permutasjoner er $n(n - 1)$: Det er n måter å velge det første elementet på, og $n - 1$ muligheter å velge det andre elementet blant de resterende på. Tallet $n(n - 1)(n - 2)$ er antallet 3-permutasjoner.

- Antall funksjoner fra $\{1, 2\}$ til $\{1, 2, \ldots, k\}$ er 2^k. (Sant / **Usant**)

Antall funksjoner fra $\{1,2\}$ til $\{1,2,\ldots,k\}$ er k^2. Det er antallet funksjoner fra $\{1,2,\ldots,k\}$ til $\{1,2\}$ som er 2^k.

- Antall måter å fordele 22 spillere i to fotballag à 11 på er $22!/(2 \cdot 11! \cdot 11!)$. (**Sant** / Usant)

Det er $22!/(11! \cdot 11!)$ måter å velge 11 spiller til "det ene" laget på. De resterende spillerne kommer da på det andre laget. Men fordi lagene ikke har noe navn, er det den samme inndelingen hvis spillerne $A \cdots K$ kommer på det "ene" laget og $L \cdots V$ på det "andre" laget, eller omvendt. For eksempel kan vi dele 4 spillere i to lag på tre måter: $\{1,2\}:\{3,4\}$, $\{1,3\}:\{2,4\}$ og $\{1,4\}:\{2,3\}$; altså $4!(2 \cdot 2! \cdot 2!)$.

1.19 Litt abstrakt algebra [3 poeng]

Avgjør om følgende påstander er sanne eller usanne.

- Funksjonen $f(x) = 3x$ på de reelle tallene har en invers funksjon. (**Sant** / Usant)

Inversen er funksjonen g er definert ved $g(x) = x/3$. Den er definert på alle reelle tall. På de naturlige tallene hadde ikke funksjonen hatt en invers funksjon.

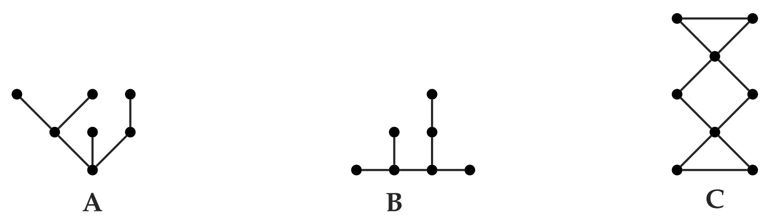
- Operasjonen *konkatenering* på strenger er assosiativ. (**Sant** / Usant)

For eksempel er $(\texttt{abc} \cdot \texttt{def}) \cdot \texttt{ghi} = \texttt{abcdefghi} = \texttt{abc} \cdot (\texttt{def} \cdot \texttt{ghi})$.

- Den algebraiske strukturen $\langle S, \cdot \rangle$, hvor S står for strengene over $\{\texttt{a}, \texttt{b}, \texttt{c}\}$, og $\cdot$ står for konkatenering, er en gruppe. (Sant / **Usant**)

Det finnes et identitetselement, den tomme strengen. Og konkatenering er assosiativt. Men det finnes ikke inverse elementer for konkatenering. For eksempel finnes det ikke en streng s slik at $\texttt{abc}$ konkatenert med s blir den tomme strengen. (Dette kalles en monoide).

1.20 Grafteori [3 poeng]



Se på grafene over. Avgjør om følgende påstander er sanne eller usanne.

- Grafene A og B er isomorfe. (**Sant** / Usant)

Den nederste noden i A tilsvarer andre noden fra høyre, nederst i B.

- Grafen C har en eulerkrets, det vil si en krets som inneholder hver kant fra grafen nøyaktig én gang. (**Sant** / Usant)

Alle noder har partall grad, og grafen er sammenhengende. Derfor finnes det en eulerkrets.

- Grafen C har en hamiltonsti, det vil si en sti som inneholder hver node fra grafen nøyaktig én gang. (Sant / **Usant**)

Skal man komme innom hver node må man forbi nodene i midten, de med grad fire, flere ganger.

1.21 Regulære språk [4 poeng]

La L være språket definert av det regulære uttrykket `(a|b)(a*b*)*(a|b)`.

- Det er slik at `baaab` $\in L$. (**Sant** / Usant)

For eksempel kan den første `b` svare til `(a|b)`, så `aaa` svare til uttrykket `(a*b*)` og derfor `(a*b*)*`. Og den siste `b` svarer da til den siste `(a|b)`.

- Det er slik at `babbab` $\in L$. (**Sant** / Usant)

For eksempel svarer `abb` (tegn 2–4) til uttrykket `a*b*`, og `a` (tegn 5) svarer også til `a*b*`. Derfor svarer tilsammen `abba` (tegn 2–5) til uttrykket `(a*b*)*`. Merk at hvis en streng svarer til r^* for et regulært uttrykk r, så trenger ikke strengene som svarer til r-ene være like.

- Det er slik at det regulære uttrykket `(a|b)(a|b)(a|b)*` definerer det samme språket. (**Sant** / Usant)

Uttrykket `(a*b*)*` matcher alle strenger over $\{a, b\}$. Alle strenger kan deles opp i biter med noen (eller ingen) `a`-er, fulgt av noen (eller ingen) `b`-er, fulgt av `a`-er, og så `b`-er, osv. Uttrykket `(a|b)(a*b*)*(a|b)` krever et ekstra tegn i starten og i slutten. Dermed består språket av alle strenger med lengde større eller lik to.

- Det er slik at $\{(ab)^n \mid n > 0\} \subseteq L$. (**Sant** / Usant)

Se forklaringen over. $(ab)^n$ er en streng med lengde $2n$, og derfor lengde større enn eller lik 2 når $n > 0$.

1.22 Naturlig deduksjon 1 [1 poeng]

$$
\begin{prooftree}
\AxiomC{$[P]^1$}
\AxiomC{$[(P \to Q) \wedge (Q \to R)]^2$}
\RightLabel{$\wedge$E}
\UnaryInfC{$P \to Q$}
\RightLabel{$\to$E}
\BinaryInfC{Q}
\AxiomC{$[(P \to Q) \wedge (Q \to R)]^2$}
\RightLabel{$\wedge$E}
\UnaryInfC{$Q \to R$}
\RightLabel{$\to$E}
\BinaryInfC{R}
\RightLabel{$\to$I$_1$}
\UnaryInfC{$P \to R$}
\RightLabel{$\to$I$_2$}
\UnaryInfC{$\boxed{F}$}
\end{prooftree}
$$

Hva er formelen F i dette beviset?

- $(P \to Q) \wedge ((Q \to R) \to (P \to R))$
- $((P \to Q) \wedge (Q \to R)) \to (P \to R)$ **Riktig**

1.23 Naturlig deduksjon 2 [1 poeng]

$$
\begin{prooftree}
\AxiomC{$[\neg P]^1$}
\RightLabel{$\vee$I}
\UnaryInfC{$P \vee \neg P$}
\AxiomC{$\neg(P \vee \neg P)$}
\RightLabel{$\to$E}
\BinaryInfC{$\bot$}
\RightLabel{$\boxed{R}$}
\UnaryInfC{$\neg\neg P$}
\end{prooftree}
$$

Hva er regelen R i denne utledningen?

- RAA$_1$
- $\to$I$_1$ **Riktig**

1.24 Naturlig deduksjon 3 [1 poeng]

$$
\begin{prooftree}
\AxiomC{$[P \wedge \neg P]^1$}
\RightLabel{$\wedge$E}
\UnaryInfC{$\neg P$}
\AxiomC{$[P \wedge \neg P]^1$}
\RightLabel{$\wedge$E}
\UnaryInfC{P}
\RightLabel{$\to$E}
\BinaryInfC{$\bot$}
\RightLabel{$\bot$}
\UnaryInfC{Q}
\RightLabel{$\to$I$_1$}
\UnaryInfC{$(P \wedge \neg P) \to Q$}
\end{prooftree}
$$

Er dette et gyldig *bevis* i naturlig deduksjon?

- Ja **Riktig**
- Nei

2 Større oppgaver [70 poeng]

2.1 Potensmengden [5 poeng]

Forklar hva potensmengden til en mengde er, ved å bruke definisjonen av potensmengden.

Potensmengden $\mathcal{P}(M)$ av en mengde M er mengden av alle delmengder av M. Det vil si $\mathcal{P}(M) = \{A \mid A \subseteq M\}$. Alternativt: For en mengde A gjelder $A \in \mathcal{P}(M)$ hvis og bare hvis $A \subseteq M$. For eksempel er $\mathcal{P}(\{A, B\}) = \{\emptyset, \{A\}, \{B\}, \{A, B\}\}$.

2.2 Kardinalitet av potensmengden [7 poeng]

Forklar hvorfor potensmengden $\mathcal{P}(M)$ til en (endelig eller uendelig) mengde M alltid har kardinalitet større eller lik M. Hint: beskriv en injektiv funksjon $f : M \to \mathcal{P}(M)$

I følge definisjonen av «større eller lik kardinalitet» må vi vise at det finnes en injektiv funksjon fra M til potensmengden $\mathcal{P}(M)$. Det vil si at for hvert element x i M, må f gi en delmengde $f(x) \subseteq M$ som er forskjellig fra delmengdene valgt for alle andre elementer av M. Dette gjør vi ved å definere $f(x) = \{x\}$. Dette er en funksjon fra M til $\mathcal{P}(M)$ fordi $\{x\} \subseteq M$, altså $\{x\} \in \mathcal{P}(M)$. Dessuten er f injektiv: Anta at $f(x) = f(y)$. Det betyr at $\{x\} = \{y\}$. For at to mengder skal være like, må alle elementer i den ene være elementer i den andre og omvendt. Her er det bare ett element i hver mengde, og derfor følger det at $x = y$.

2.3 Førsteordens modeller [5 poeng]

Spesifiser en førsteordens modell M for signaturen $\langle ; ; P, R\rangle$ slik at følgende egenskaper holder:

(1) P har aritet 1 og R har aritet 2.

(2) Domenet til modellen er $\{1, 2, 3\}$.

(3) $\langle 1, 2\rangle \in R^{\mathcal{M}}$.

(4) Formelen $\forall x \forall y(Rxy \to Py)$ er sann i $\mathcal{M}$.

(5) Formelen $\forall x \forall y(Rxy \to Ryx)$ er sann i $\mathcal{M}$.

(6) $P^{\mathcal{M}} \neq \{1, 2, 3\}$

Domenet til modellen, $|M| = \{1, 2, 3\}$ er gitt. Hvis $\langle 1, 2\rangle \in R^{\mathcal{M}}$ gjelder også $\langle 2, 1\rangle \in R^{\mathcal{M}}$, ellers blir ikke formelen i 5 sann. Dessuten må vi ha $1 \in P^{\mathcal{M}}$ og $2 \in P^{\mathcal{M}}$ for å oppfylle formelen i 4. Hvis vi setter $R^{\mathcal{M}} = \{\langle 1, 2\rangle, \langle 2, 1\rangle\}$ og $P^{\mathcal{M}} = \{1, 2\}$ er alle kravene oppfylt.

2.4 Rekursiv funksjon på naturlige tall [5 poeng]

Gi en rekursiv definisjon av *fakultetfunksjonen*, $f(n) = n! = 1 \cdot 2 \cdot \cdots \cdot n$ på de naturlige tallene.

La f være funksjonen definert rekursivt ved $f(0) = 1$ og $f(n + 1) = (n + 1) \cdot f(n)$.

2.5 Rekursiv funksjon på strenger [5 poeng]

La $A = a, b, c$. Definer en rekursiv funksjon f på A^* som bytter ut hver $\texttt{c}$ med tre $\texttt{b}$-er og hver $\texttt{b}$ med to $\texttt{a}$-er. For eksempel vil $f(\texttt{c}) = \texttt{bbb}$ og $f(\texttt{cba}) = \texttt{bbbaaa}$.

$$f(\Lambda) = \Lambda$$

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

$$f(\texttt{b}s) = \texttt{aa}f(s)$$

$$f(\texttt{c}s) = \texttt{bbb}f(s)$$

2.6 Bevis ved strukturell induksjon [10 poeng]

La $A = \{\texttt{a}, \texttt{b}, \texttt{c}\}$. Anta at f er en rekursiv funksjon på A^* som bytter ut hver $\texttt{c}$ med tre $\texttt{b}$-er og hver $\texttt{b}$ med to $\texttt{a}$-er, akkurat som i forrige oppgave. For eksempel vil $f(\texttt{c}) = \texttt{bbb}$ og $f(\texttt{cba}) = \texttt{bbbaaa}$. La nå g være en funksjon fra A^* til $\mathbb{N}$ definert på følgende måte:

$$g(\Lambda) = 0$$

$$g(\texttt{a}s) = 1 + g(s)$$

$$g(\texttt{b}s) = 2 + g(s)$$

$$g(\texttt{c}s) = 3 + g(s)$$

Bevis ved strukturell induksjon på mengden A^* at for alle strenger s, er det slik at lengden til strengen $f(s)$ er lik $g(s)$.

Basissteget består av å vise at påstanden holder for den tomme strengen: $|f(\Lambda)| = 0 = g(\Lambda)$

Induksjonssteg: Anta at $|f(s)| = g(s)$ for en streng s. Dette er *induksjonshypotesen*.

Vi viser at påstanden holder for alle mulige første tegn i strengen:

$$|f(\texttt{a}s)| = |\texttt{a}f(s)| = 1 + |f(s)| = 1 + g(s) = g(\texttt{a}s)$$

$$|f(\texttt{b}s)| = |\texttt{aa}f(s)| = 2 + |f(s)| = 2 + g(s) = g(\texttt{b}s)$$

$$|f(\texttt{c}s)| = |\texttt{ccc}f(s)| = 3 + |f(s)| = 3 + g(s) = g(\texttt{c}s)$$

2.7 Mer om rekursive funksjoner [8 poeng]

La $f(n) = n^n$ for naturlige tall n. For eksempel vil $f(2) = 2^2 = 4$ og $f(3) = 3^3 = 27$.

Lag en definisjon for f ved å først lage en rekursiv definisjon for $g(m, n) = m^n$ for vilkårlige tall m, n, ved rekursjon på n.

Vi definerer først hjelpefunksjonen $g(m, n)$ ved at $g(m, 0) = 1$ og $g(m, n + 1) = m \cdot g(m, n)$. Deretter definerer vi f ved at $f(n) = g(n, n)$.

2.8 Definisjon og utregning [3 poeng]

La max være funksjonen på naturlige tall som gir det største av de to tallene:

$$x \max y = \begin{cases} x & \text{hvis } x > y \\ y & \text{ellers} \end{cases}$$

Og la min være funksjonen på naturlige tall som gir det minste av de to tallene:

$$x \min y = \begin{cases} x & \text{hvis } x < y \\ y & \text{ellers} \end{cases}$$

For eksempel har vi at $5 \max 3 = 5$ og $10 \min 1 = 1$.

Regn ut $(12 \max 13) \min (5 \max 10)$.

$(12 \max 13) \min (5 \max 10) = 13 \min 10 = 10$

2.9 Definisjon og idempotens [4 poeng]

La max være definert som i forrige oppgave. For eksempel har vi at $3 \max 5 = 5$ og $10 \max 1 = 10$. Er dette en idempotent operasjon?

Ja. Den er idempotent hvis $x \max x = x$. Og siden $x < x$ aldri er tilfelle, kommer vi til *ellers*-tilfellet. Uansett blir svaret x.

2.10 Definisjon og bevis 1 [7 poeng]

La max være definert som i forrige oppgave.

For eksempel har vi at $5 \max 3 = 5$ og $1 \max 10 = 10$.

Bevis at max er kommutativ, det vil si at $x \max y = y \max x$ for alle naturlige tall x og y.

Vi ser på tre tilfeller:

(1) $x < y$: Da er ikke $x > y$, og derfor er $x \max y = y$ (det andre tilfellet i definisjonen). Men $y > x$ og $y \max x = y$ (det første tilfellet i definisjonen). Tilsammen får vi at $x \max y = y \max x$.

(2) $x = y$: Da er ikke $x > y$, og derfor $x \max y = y$. Men heller ikke $y > x$, og derfor $y \max x = x$. Men, fordi $x = y$, gjelder allikevel $x \max y = y = x = y \max x$.

(3) $x > y$: Da er $x \max y = x$. Men, ikke $y > x$, så $y \max x = x$. Tilsammen får vi at $x \max y = y \max x$.

Påstanden holder altså i alle tre tilfeller.

2.11 Definisjon og bevis 2 [11 poeng]

La min være definert som før. For eksempel har vi at $5 \min 3 = 5$ og $1 \min 10 = 10$.

Bevis at min er assosiativ, det vil si at $(x \min y) \min z = x \min (y \min z)$ for alle naturlige tall x, y og z.

Vi ser først på forholdet mellom x og y, og så på undertilfeller avhengig av hvor z ligger i forhold til x og y.

(1) $x < y$: Da er $x \min y = x$.
   (a) $x < z$: Da er $(x \min y) \min z = x$.
      i. $y < z$: Da er $y \min z = y$. Men, siden $x < y$ er $x \min (y \min z) = x$.
      ii. $y \geqslant z$: Da er $y \min z = z$. Men, siden $x < z$ er $x \min (y \min z) = x$.
   (b) $x \geqslant z$: Da er $(x \min y) \min z = z$. Det følger også at $y \geqslant z$. Dermed $y \min z = z$ og $x \min (y \min z) = z$.

(2) $x \geqslant y$: Da er $x \min y = y$.
   (a) $y < z$: Da er $(x \min y) \min z = y$. Og $y \min z = y$ og $x \min (y \min z) = y$.
   (b) $y \geqslant z$: Da er $(x \min y) \min z = z$. Det følger også at $x \geqslant z$, og dermed $y \min z = z$ og $x \min (y \min z) = z$.

Alternativt bevis: Vi ser på alle mulige ordninger mellom x, y, og z. Det er 6 forskjellige, en for hver permutasjon.

(1) $x \leqslant y \leqslant z$: Da er $(x \min y) \min z = x \min z = x = x \min y = x \min (y \min z)$

(2) $x \leqslant z \leqslant y$: Da er $(x \min y) \min z = x \min z = x = x \min z = x \min (y \min z)$

(3) $y \leqslant x \leqslant z$: Da er $(x \min y) \min z = y \min z = y = x \min y = x \min (y \min z)$

(4) $y \leqslant z \leqslant x$: Da er $(x \min y) \min z = y \min z = y = x \min y = x \min (y \min z)$

(5) $z \leqslant x \leqslant y$: Da er $(x \min y) \min z = x \min z = z = x \min z = x \min (y \min z)$

(6) $z \leqslant y \leqslant x$: Da er $(x \min y) \min z = y \min z = z = x \min z = x \min (y \min z)$

(Hvorfor er det bare fem tilfeller i det første beviset? Jo, fordi tilfelle 2a har $y \leqslant x$ og $y < z$. Dermed kan resultatet y utregnes uten å vite om $x > z$ eller ikke. Det er tilfellene 3 og 4 i det andre beviset som er identiske.)