IN1150 – Logiske metoder

Eksamen våren 2018 (med løsningsforslag)

Dette er et utkast til løsningsforslag til eksamen i IN1150 våren 2018, og feil kan forekomme. Hvis du finner noen feil, si ifra til oss på `in1150-ansvarlige@ifi.uio.no`.

Små oppgaver [70 poeng]

1 Grunnleggende mengdelære [3 poeng]

(a) Et n-tuppel er det samme som en mengde med n elementer. (Sant / **Usant**)

> Dette er usant, fordi både antall og rekkefølge av elementene er av betydning i tupler, men ikke i mengder. Dette er to forskjellige konsepter.

(b) Hvis $x = y$, så er $\{x\} = \{y\}$. (**Sant** / Usant)

> Dette er sant, fordi mengden $\{x\}$ har kun ett element x, og fordi x er lik y, er dette også et element i mengden $\{y\}$. Det vil si at $\{x\} \subseteq \{y\}$. På samme måte er $\{y\} \subseteq \{x\}$, og derfor har vi at $\{x\} = \{y\}$.

(c) Det er sant at $0 \subseteq \mathbb{N}$. (Sant / **Usant**)

> Dette er usant, fordi 0 er et tall, og ikke en mengde, og et tall kan ikke være en delmengde av en annen mengde. På den annen side vil $0 \in \mathbb{N}$. Det finnes formaliseringer av naturlige tall som definerer 0 som den tomme mengden, men det gjorde vi ikke i dette kurset.

2 Utsagnslogikk [3 poeng]

(a) Det finnes nøyaktig seksten forskjellige utsagnslogiske formler med kun to utsagnsvariabler P og Q. (Sant / **Usant**)

> Dette er usant, fordi det finnes uendelig mange formler, selv med kun to utsagnsvariabler. For eksempel har vi formlene P, $\neg P$, $\neg\neg P$, etc.

(b) Hvis F er en utsagnslogisk formel, så er også $(\neg F \land F)$ en utsagnslogisk formel. (**Sant** / Usant)

> Dette er sant, fordi hvis F er en utsagnslogisk formel, forteller definisjonen av utsagnslogisk formler oss at $\neg F$ også er en utsagnslogisk formel. Og hvis disse to er formler så er også konjunksjonen $(\neg F \land F)$ en formel.

(c) Hvis R står for utsagnet «det regner» og P for «jeg bruker paraplyen» så står $R \to P$ for utsagnet «jeg bruker paraplyen bare hvis det regner». (Sant / **Usant**)

> Dette er usant, fordi setningen «jeg bruker paraplyen bare hvis det regner» sier det samme som «hvis jeg bruker paraplyen, så regner det». Dette tilsvarer formelen $P \to R$.

3 Semantikk for utsagnslogikk [3 poeng]

(a) Formlene $\neg(Q \to P)$ og $(Q \wedge \neg P)$ er ekvivalente. (**Sant** / Usant)

Dette er sant, fordi den eneste måte å gjøre formlene sanne på, er ved å gjøre Q sann og P usann.

(b) Hvis $v \not\models (P \to (\neg P \vee Q))$, så følger det at $v \models P$. (**Sant** / Usant)

Dette er sant, fordi hvis valuasjonen gjør $(P \to (\neg P \vee Q))$ usann, må den gjøre P sann og Q usann.

(c) Hvis $v \models P$, så følger det at $v \not\models (P \to (\neg P \vee Q))$. (Sant / **Usant**)

Dette er usant, fordi hvis valuasjonen gjør Q sann, som kan være tilfellet, vil vi ha $v \models (P \to (\neg P \vee Q))$.

4 Utsagnslogiske begreper [3 poeng]

(a) Enhver formel er enten oppfyllbar eller falsifiserbar, eller begge deler. (**Sant** / Usant)

Dette er sant. Anta at en formel F ikke er oppfyllbar. Da er den usann under alle valuasjoner. Og dermed er den falsifiserbar.

(b) Enhver logisk konsekvens av en oppfyllbar formel er også oppfyllbar. (**Sant** / Usant)

Dette er sant. Hvis en formel F er oppfyllbar, finnes det en valuasjon v med $v \models F$. Hvis G er en logisk konsekvens av F så gjelder også $v \models G$. Og dermed er også G oppfyllbar.

(c) La F være en formel som har samme sannhetsverdi uansett valuasjon. Da er F enten en tautologi eller en kontradiksjon. (**Sant** / Usant)

Dette er sant, fordi enten er F sann uansett valuasjon, og da er den en tautologi, eller usann uansett valuasjon, og da er den en kontradiksjon.

5 Bevis, formodninger og moteksempler [2 poeng]

(a) Et motsigelsesbevis er et bevis for en påstand som ikke holder. (Sant / **Usant**)

Dette er usant, fordi et *motsigelsebevis* er en bestemt type bevis for en påstand, og når en påstand er bevist, så vet vi at den holder. Et *moteksempel* derimot kan brukes til å bevise at en påstand ikke holder.

(b) Det er mulig å bevise en påstand for alle naturlige tall m og n ved to tilfeller $m < n$ og $m \geqslant n$. (**Sant** / Usant)

Dette er sant, fordi for to tall, m og n, er enten $m < n$ eller $m \geqslant n$. Gitt en påstand $P(m, n)$, hvis vi viser den (1) for alle m og n med $m < n$, og (2) for alle m og n med $m \geqslant n$, så har vi vist den for alle m og n. Dette et bevis ved tilfeller; vi har delt beviset opp i to tilfeller som sammen dekker alle muligheter.

6 Relasjoner [3 poeng]

(a) Den tomme mengden, $\emptyset$, er en binær relasjon på mengden $\{42\}$. (**Sant** / Usant)

Dette er sant, fordi en binær relasjon på $\{42\}$ er en delmengde av $\{42\} \times \{42\}$, som er lik $\{\langle 42, 42\rangle\}$. Den tomme mengden er en delmengde av alle mengder, også denne. I denne sammenhengen kaller vi den også for den tomme relasjonen på $\{42\}$.

(b) Den tomme mengden, $\emptyset$, er *den eneste* binære relasjonen på mengden $\{42\}$. (Sant / **Usant**)

Dette er sant, av samme grunn som over. Også $\{\langle 42, 42\rangle\}$ er en relasjon på mengden $\{42\}$.

(c) La R være en relasjon på $\{a, b\}$ som er symmetrisk og transitiv. Da er den enten refleksiv eller den tomme relasjonen. (Sant / **Usant**)

Dette er usant, fordi $\{\langle a, a\rangle\}$ er symmetrisk og transitiv, men den er ikke tom og den er ikke refleksiv, fordi $\langle b, b\rangle$ mangler.

7 Funksjoner [3 poeng]

(a) En *funksjon* fra A til B er definert som en binær relasjon R slik at for *enhver* x, y og z, hvis $\langle x, y\rangle \in R$ og $\langle x, z\rangle \in R$, så er $y = z$. (Sant / **Usant**)

Dette er usant, fordi for å være en funksjon, må det også for enhver x finnes en y med $\langle x, y\rangle \in R$.

(b) Hvis en funksjon $f : A \to B$ er surjektiv, er det slik at bildemengden, $f[A]$, er lik verdiområdet B. (**Sant** / Usant)

Dette er sant, fordi det at den er surjektiv betyr at for hver $y \in B$ finnes $x \in A$ med $f(x) = y$. Det betyr det samme som at $y \in f[A]$.

(c) Hvis en funksjon $f : A \to B$ er bijektiv, er det slik at bildemengden, $f[A]$, er lik definisjonsområdet A. (Sant / **Usant**)

Dette er usant, fordi det finnet et moteksempel. Funksjonen $f : \{a\} \to \{b\}$, med $f(a) = b$, er bijektiv, men bildemengden $f[A] = \{b\} \neq \{a\}$.

8 Litt mer mengdelære [3 poeng]

(a) Det finnes to uendelige mengder A og B som har ulik kardinalitet (**Sant** / Usant)

Dette er sant. For eksempel er $\mathbb{N}$ en tellbar mengde, og $\mathbb{R}$ er en overtellbar mengde. Disse har ulik kardinalitet.

(b) Den tomme mengden er en delmengde av alle mengder. Derfor er den tomme mengden et element i potensmengden til enhver mengde. (**Sant** / Usant)

Dette er sant, fordi potensmengden til en mengde A er mengden av alle delmengder av A. Vi har at $\emptyset \subseteq A$, og dermed at $\emptyset$ er et element i potensmengden til A.

(c) La $f : \mathbb{Q} \to A$ være en bijektiv funksjon fra brøktallene til en mengde A. Da er A tellbar. (**Sant** / Usant)

Dette er sant. Vi har lært at $\mathbb{Q}$ er tellbar. La funksjonen $g : \mathbb{N} \to \mathbb{Q}$ være en bijeksjon fra $\mathbb{N}$ til $\mathbb{Q}$. Det vil si at g teller opp alle brøktallene. Nå definerer vi $h : \mathbb{N} \to A$ ved $h(n) = f(g(n))$. Dette er en bijeksjon fra $\mathbb{N}$ til A, så da er også A tellbar.

9 Tillukninger og induktivt definerte mengder [3 poeng]

(a) La relasjonen R på mengden $\{1, 2, 3\}$ være $\{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$. Da er

$$\{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle\}$$

den symmetriske tillukningen av R. (**Sant** / Usant)

Dette er sant, fordi for alle tupler $\langle x, y\rangle$, så er også $\langle y, x\rangle$ med.

(b) Relasjonen $<$ på de naturlige tallene $\mathbb{N}$ er det samme som den transitive tillukningen av $\{\langle n, n+1\rangle \mid n \in \mathbb{N}\}$. (**Sant** / Usant)

Dette er sant, fordi $a < b$ er sant hvis og bare hvis det finnes en menge tupler

$$\{\langle a, a+1\rangle, \langle a+1, a+2\rangle, \ldots, \langle a+k, b\rangle\}.$$

Da må $\langle a, b\rangle$ være med i den transitive tillukningen. (I oppgaven som ble gitt på eksamen stod det $\{\langle n, n+1\rangle \mid \mathbb{N}\}$ i stedet for $\{\langle n, n+1\rangle \mid n \in \mathbb{N}\}$.)

(c) Anta at du har en relasjon S der alt er relatert til noe. Hvis du tar den symmetriske tillukningen, og deretter tar den transitive tillukningen av S, da får du en refleksiv relasjon. (**Sant** / Usant)

Dette er sant. Hvis x er et vilkårlig element, og dette er relatert til y, har vi at $\langle x, y\rangle \in S$. Da må $\langle y, x\rangle$ være med i den symmetriske tillukningen, og da må $\langle x, x\rangle$ være med i den transitive tillukningen. Dermed må denne være refleksiv.

10 Rekursive funksjoner [3 poeng]

(a) La funksjonen $s : \mathbb{N} \to \mathbb{N}$ være gitt ved $s(0) = 0$ og $s(n+1) = s(n) + 1$.
Funksjonen s er lik identitetsfunksjonen for de naturlige tallene. (**Sant** / Usant)

> Dette er sant, fordi identitetsfunksjonen er definert som $\mathrm{id}(n) = n$. Funksjonen s summerer n enere. Summen av n enere er nøyaktig n (for alle n), og derfor er funksjonene like. Dette kan vises mer formelt ved et induksjonsbevis.

(b) Funksjonen f over bitstrenger er definert som:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 0 \\ f(b0) &= 1f(b) \\ f(b1) &= 0f(b) \end{aligned}$$

Da er $f(010011) = 001011$. (Sant / **Usant**)

> Dette er usant, fordi $f(010011) = 001101$.

(c) Anta at f og g er operasjoner på A og L er en liste over A.
Da er $\textsc{map}(f, \textsc{map}(g, L)) = \textsc{map}(f \circ g, L)$. (**Sant** / Usant)
(Husk at $\textsc{map}$ er definert som

$$\begin{aligned} &\textsc{map}(f, ()) = () \\ &\textsc{map}(f, x :: L) = (f(x) :: \textsc{map}(f, L)) \end{aligned}$$

og at $\circ$ er definert ved at $(f \circ g)(x) = f(g(x))$.)

> Dette er sant. Intuisjonen her er at hvis L er listen $(x_1, x_2, \ldots, x_n)$, får vi
>
> $$\textsc{map}(f, \textsc{map}(g, L)) = \textsc{map}(f, (g(x_1), g(x_2), \ldots, g(x_n))) = (f(g(x_1)), f(g(x_2)), \ldots, f(g(x_n))),$$
>
> og dette er det samme som $\textsc{map}(f \circ g, L)$. Dette kan også vises mer formelt ved et induksjonsbevis.

11 Matematisk induksjon [2 poeng]

(a) For et bevis i matematisk induksjon er det tilstrekkelig å vise at *hvis* påstanden holder for et vilkårlig naturlig tall n, *så* holder den også for $n + 1$. (Sant / **Usant**)

> Dette er usant, fordi vi må også vise at påstanden holder for 0.

(b) *Sterk* induksjon er når man bruker induksjon for å bevise noe for alle heltall $a \in \mathbb{Z}$. (Sant / **Usant**)

> Dette er usant, fordi sterk induksjon er at man styrker induksjonshypotesen til å holde for alle naturlige tall mindre eller lik n, ikke bare n.

12 Strukturell induksjon [3 poeng]

(a) Basissteget i strukturell induksjon er å sjekke om påstanden holder for ett av elementene i basismengden. (Sant / **Usant**)

> Dette er usant, fordi ved strukturell induksjon må man vise at påstanden holder for *alle* elementene i basismengden.

(b) Strukturell induksjon er en generalisering av matematisk induksjon. (**Sant** / Usant)

> Dette er sant. Matematisk induksjon er bare strukturell induksjon over $\mathbb{N}$.

(c) Induksjonssteget kan bevises ved et kontrapositivt bevis. (**Sant** / Usant)

> Dette er sant, fordi man står helt fri til å velge hvordan man beviser induksjonssteget.

13 Førsteordens språk [3 poeng]

(a) Et førsteordens språk består av logiske og ikke-logiske symboler. (**Sant** / Usant)

> Dette er sant, fordi dette er definisjonen av førsteordens språk.

(b) La signaturen for et førsteordens språk være gitt som $\langle a ; f ; R \rangle$ der f har aritet 1 og R har aritet 2. Da er $\forall x R(f(f(x)), a)$ en atomær formel. (Sant / **Usant**)

> Dette er usant, fordi en atomær formel ikke kan inneholde kvantorer eller konnektiver. Formelen i oppgaven er sammensatt.

(c) Egenskapen *irrefleksiv* kan uttrykkes som $\forall x \neg Rxx$. (**Sant** / Usant)

> Dette er sant, fordi dette uttrykker at ingen elementer er relatert til seg selv.

14 Representasjon av kvantifiserte utsagn [3 poeng]

(a) Formelen $\exists x \exists y (Px \land Qy \land Rxy)$ er lukket. (**Sant** / Usant)

> Dette er sant, fordi både x og y er innenfor skopet til en eksistenskvantor, og da er formelen lukket.

(b) Setningen «Hvis noen liker alle, så blir alle likt av noen» kan representeres med formelen

$$\exists x \forall y Lxy \rightarrow \forall x \exists y Lyx$$

der Lxy betyr «x liker y». (**Sant** / Usant)

Dette er sant, fordi $\exists x \forall y Lxy$ uttrykker «det finnes en x som liker alle y» (det vil si at «noen liker alle») og $\forall x \exists y Lyx$ uttrykker «for alle x finnes det en y som liker x» (det vil si at «alle blir likt av noen»).

(c) Formelen $\forall x \exists y Rxy$ betyr det samme som formelen $\exists y \forall x Rxy$. (Sant / **Usant**)

Dette er usant, fordi $\forall x \exists y Rxy$ uttrykker «for alle x finnes det en y slik at [...]», men $\exists y \forall x Rxy$ uttrykker «det finnes en y slik at for alle x [...]».

15 Tolkning i modeller [3 poeng]

(a) En modell $\mathcal{M}$ består av et domene og en tolkning av alle ikke-logiske symboler. (**Sant** / Usant)

Dette er sant. Dette en litt uformell variant av definisjonen av en modell.

(b) La $\mathcal{A}$ være en modell med domene $\{1, 2, 3, 4\}$ der $f^{\mathcal{A}}(1) = 1$, $f^{\mathcal{A}}(2) = 1$, $f^{\mathcal{A}}(3) = 4$ og $f^{\mathcal{A}}(4) = 4$ og R er en refleksiv relasjon. Da er $\forall x R(fx, ffx)$ sann i $\mathcal{A}$. (**Sant** / Usant)

Dette er sant, fordi fx enten blir 1 eller 4, og $f(1) = 1$ og $f(4) = 4$.

(c) For endelige modeller kan man tenke på $\forall$-kvantoren som en sammensatt disjunksjon og $\exists$-kvantoren som en sammensatt konjunksjon. (Sant / **Usant**)

Dette er usant, fordi det er motsatt. Vi kan tenke på $\forall$-kvantoren som en sammensatt konjunksjon og $\exists$-kvantoren som en sammensatt disjunksjon.

16 Resonnering om modeller [3 poeng]

(a) Ingen falsifiserbare formler er oppfyllbare. (Sant / **Usant**)

Dette er usant, fordi en formel kan være sann i én modell og usann i en annen. Da er den både falsifiserbar og oppfyllbar.

(b) Alle gyldige formler er ekvivalente. (**Sant** / Usant)

Dette er sant. To formler er ekvivalente hvis de er sanne i nøyaktig de samme modellene. To gyldige formler er begge sanne i alle modeller, som vil si at de er sanne i nøyaktig de samme modellene.

(c) Formelen $\forall x \exists y Rxy$ er en logisk konsekvens av $\exists y \forall x Rxy$. (**Sant** / Usant)

Dette er sant. La oss tenke på R som «liker»-relasjonen. Da uttrykker formelen $\exists y \forall x Rxy$ at det finnes en som blir likt av alle. Da må det være slik at alle liker noen, som er det formelen $\forall x \exists y Rxy$ uttrykker.

17 Abstraksjon med ekvivalenser og relasjoner [3 poeng]

(a) Enhver mengde med to elementer vil ha nøyaktig to partisjoner. (**Sant** / Usant)

Dette er sant, fordi envher mengde som består av to elementer vil ha nøyaktig to partisjoner. For eksempel, se på $\{X, Y\}$. Vi får kun to partisjoner: $\{\{X\}, \{Y\}\}$ og $\{\{X, Y\}\}$.

(b) Mengden $\{1, 2\}$ er en partisjon av $\{\{1, 2\}, \{3\}\}$. (Sant / **Usant**)

Dette er usant, fordi $\{1, 2\}$ er ikke en partisjon. Men, $\{\{1, 2\}, \{3\}\}$ er en partisjon av mengden $\{1, 2, 3\}$.

(c) Enhver ekvivalensklasse har minst ett element. (**Sant** / Usant)

Dette er sant, fordi på grunn av hvordan ekvivalensklasser er definert. Vi sier at ekvivalensklassen til et element $x \in S$ er mengden $\{y \in S \mid y \sim x\}$, med andre ord mengden av elementer i S som er relatert til x.

18 Kombinatorikk [3 poeng]

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

Dette er sant, fordi for hver delmengde er det slik at ett av de fem elementene enten er med eller ikke. Det blir $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$ muligheter.

(b) Ordet «kombinasjon» handler om å velge noe *uavhengig* av rekkefølge, mens ordet «permutasjon» handler å velge noe *avhengig* av rekkefølge. (**Sant** / Usant)

Dette er sant, fordi en k-kombinasjon av en mengde A er en delmengde av A med k elementer. Her er rekkefølgen uviktig. Når vi teller permutasjoner, er rekkefølgen viktig.

(c) Det er slik at $n!$ er lik $(k - n)! \cdot \binom{n}{k}$ for alle naturlige tall slik at $n \geqslant k$. (Sant / **Usant**)

Dette er usant. Definisjonen av binomialkoeffisienten $\binom{n}{k}$ sier følgende:

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

Dersom vi ganger med $(n - k)! \cdot k!$ på hver side får vi at $n!$ er lik $(n - k)! \cdot k! \cdot \binom{n}{k}$.

19 Litt mer kombinatorikk [3 poeng]

(a) Det er nøyaktig n^k funksjoner fra en mengde med k elementer til en mengde med n elementer. (**Sant** / Usant)

Dette er sant, fordi for hvert av de k elementene er det n å velge mellom.

(b) Det er nøyaktig ti forskjellige permutasjoner av strengen `aabbb`. (**Sant** / Usant)

Dette er sant, fordi vi kan tenke at det er $\binom{5}{2} = 10$ måter å velge hvor `a`-ene skal være. Eller så kan vi regne det ut direkte ved å ta 5! og dele på $2! \cdot 3!$.

(c) Det er nøyaktig 120 injektive funksjoner fra $\{1, 2, 3\}$ til $\{1, 2, 3, 4, 5\}$. (Sant / **Usant**)

Det er nøyaktig $5 \cdot 4 \cdot 3 = 60$ injektive funksjoner fra $\{1, 2, 3\}$ til $\{1, 2, 3, 4, 5\}$.

20 Litt abstrakt algebra [3 poeng]

(a) Hvis f er en idempotent funksjon, så vil $f(x) = x$ for alle x. (Sant / **Usant**)

Dette er usant, fordi definisjonen gir bare at $f(f(x)) = f(x)$. Det er *ikke* tilstrekkelig for å vise at $f(x) = x$.

(b) Operasjonen som konkatenerer strenger er kommutativ. (Sant / **Usant**)

Dette er usant, fordi fordi vi for eksempel har at `aa` · `bb` er noe annet enn `bb` · `aa`.

(c) Den algebraiske strukturen $\langle \mathbb{Z}, + \rangle$, hvor $\mathbb{Z}$ står for heltallene og $+$ står for den vanlige addisjonsoperasjonen, er en abelsk gruppe. (**Sant** / Usant)

Dette er sant, fordi det er en gruppe fordi det finnes et identitetselement, 0, alle elementer x har en invers, $-x$, og operasjonen $+$ er assosiativ. I tilleg er gruppen abelsk fordi $+$ er kommutativ.

21 Grafteori [3 poeng]

(a) En graf har alltid minst én node. (**Sant** / Usant)

Dette er sant, fordi dette følger fra definisjonen av en graf.

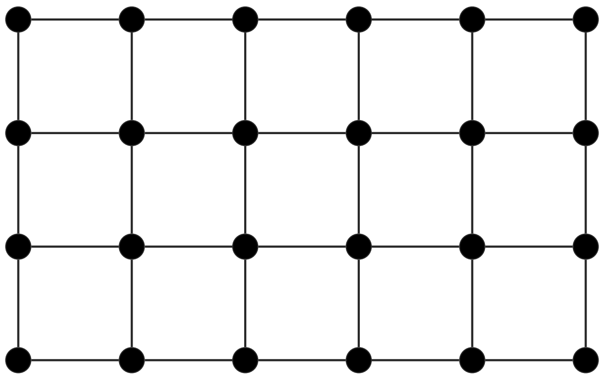
(b) Komplementet til en tom graf er alltid en komplett graf. (**Sant** / Usant)

Dette er sant, fordi dette følger direkte fra definisjonene av tom og komplett.

(c) Det finnes en enkel graf med 10 noder og 100 kanter. (Sant / **Usant**)

Dette er usant, fordi det blir for mange kanter. Det meste antall kanter en enkel graf med n noder kan ha er $\binom{n}{2}$, og for 10 noder blir det 45.

22 Vandringer i grafer [3 poeng]



(a) Denne grafen har mer en tretti forskjellige sykler. (**Sant** / Usant)

Dette er sant. En sykel er en lukket sti, og det er mer enn tretti slike. (Se for deg at du starter øverst i venstre hjørne og går rundt i grafen.)

(b) Denne grafen har en eulerkrets. (Sant / **Usant**)

Dette er usant. Vi har lært at en graf har en eulerkrets hvis og bare hvis det ikke finnes noen noder med odde grad, men her er det mange noder som har odde grad.

(c) Denne grafen har en hamiltonsykel. (**Sant** / Usant)

Dette er sant. Det går an å lage en sti som begynner og slutter i samme node og som går over alle nodene nøyaktig en gang.

23 Formelle språk og grammatikker [3 poeng]

(a) Det regulære uttrykket `a[a|b]*` definerer mengden av alle strenger over alfabetet {`a`, `b`}. (Sant / **Usant**)

Dette er usant, fordi for eksempel er ikke den tomme strengen med.

(b) Det regulære uttrykket `0(Λ|1)(Λ|2)0` beskriver språket {`00`, `010`, `020`, `0120`}. (**Sant** / Usant)

Dette er sant, fordi alle strenger må begynne og slutte med `0`, og mellom `0`-ene må det være `Λ`, `1Λ`, `Λ2` eller `12`.

(c) Grammatikken som er gitt ved de to produksjonsreglene $S \to \texttt{ab}S \mid T$ og $T \to \texttt{ba}T \mid \Lambda$ er regulær. (**<u>Sant</u>** / Usant)

> Dette er sant, fordi fordi enhver produksjonsregel er på formen $A \to X$, hvor A er et ikke-terminalsymbol og X består av maksimalt ett ikke-terminalsymbol som i så fall forekommer lengst til høyre. Dette språket beskriver det samme språket som det regulære uttrykket `(ab)*(ba)*`.

24 Naturlig deduksjon 1 [1 poeng]

$$\dfrac{\dfrac{\dfrac{\dfrac{[P \wedge R]^1}{P}\wedge\text{E} \qquad \dfrac{[(P \to Q) \wedge (R \to Q)]^2}{P \to Q}\wedge\text{E}}{Q}\to\text{E}}{(P \wedge R) \to Q}\to\text{I}_1}{(P \to Q) \wedge (R \to Q) \to ((P \wedge R) \to Q)}\to\text{I}_2$$

Her er reglene i naturlig deduksjon anvendt på riktig måte. (**<u>Sant</u>** / Usant)

25 Naturlig deduksjon 2 [1 poeng]

$$\dfrac{\dfrac{[A \vee B]^2 \qquad \dfrac{[A]^1 \qquad \neg A}{\bot}\to\text{E} \qquad \dfrac{[B]^1 \qquad \neg B}{\bot}\to\text{E}}{\boxed{F}}\vee\text{E}_1}{\neg(A \vee B)}\to\text{I}_2$$

Hva er formelen F i denne utledningen?

(a) $\bot$ (riktig)

(b) $\neg(A \vee B)$

26 Naturlig deduksjon 3 [1 poeng]

$$\dfrac{\dfrac{\dfrac{\dfrac{[P]^1 \qquad \neg P}{\bot}\to\text{E}}{Q}\bot}{P \to Q}\to\text{I}_1 \qquad \boxed{F}}{P}\to\text{E}$$

Hva er formelen F i denne utledningen?

(a) Q

(b) $(P \to Q) \to P$ (riktig)

Større oppgaver [70 poeng]

27 Utsagnslogikk [10 poeng]

Fyll inn resten av sannhetsverdiene, enten 0 eller 1, i følgende tabell.

$\neg$	$\neg$	$\neg$	$\neg$	P	$\wedge$	$\neg$	$\neg$	$\neg$	$\neg$	Q
$\boxed{0}$	$\boxed{1}$	0	1	0	$\boxed{0}$	$\boxed{1}$	0	1	0	1

$\neg$	((	P	$\vee$	$\neg$	P	)	$\vee$	(	Q	$\wedge$	$\neg$	Q	))
$\boxed{0}$			$\boxed{1}$				$\boxed{1}$			$\boxed{0}$			

(	P	$\rightarrow$	Q	)	$\vee$	(	$\neg$	Q	$\rightarrow$	$\neg$	P	)
	$\boxed{1}$	1	$\boxed{0}$		0		$\boxed{1}$	0	0	$\boxed{0}$	1	

$\neg$	(	P	$\rightarrow$	Q	)	$\rightarrow$	(	R	$\vee$	$\neg$	S	)
1		$\boxed{1}$	0	$\boxed{0}$		0		$\boxed{0}$	0	0	$\boxed{1}$	

(((	$\neg$	P	$\rightarrow$	$\neg$	Q	)	$\rightarrow$	$\neg$	R	)	$\rightarrow$	$\neg$	S	)
	0	1	$\boxed{1}$	0	1		$\boxed{0}$	$\boxed{0}$	1		$\boxed{1}$	0	1	

Her er de fem formlene uten tabellen:

$$\neg\neg\neg\neg P \wedge \neg\neg\neg\neg Q$$
$$\neg((P \vee \neg P) \vee (Q \wedge \neg Q))$$
$$(P \rightarrow Q) \vee (\neg Q \rightarrow \neg P)$$
$$\neg(P \rightarrow Q) \rightarrow (R \vee \neg S)$$
$$(((\neg P \rightarrow \neg Q) \rightarrow \neg R) \rightarrow \neg S)$$

28 Induktivt definerte mengder og språk [10 poeng]

(a) [3 poeng] Gi en induktiv definisjon av følgende mengde:

$$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, \ldots\}$$

La M være den minste mengden som er slik at $1 \in M$ og $2 \in M$, og som er slik at hvis $x \in M$, så $x + 3 \in M$.

(Det finnes mange andre løsninger, men dette er kanskje den enkleste. En annen løsning er å la M være den minste mengden slik at $1 \in M$, som er slik at hvis $x \in M$, så både $2x \in M$ og $x + 3 \in M$. Dette blir det samme, men det å lukke under $2x$ er kun nødvendig for å få tallet 2 med i M; resten tar jo $3x + 1$ seg av.)

(b) [3 poeng] Gi en induktiv definisjon av følgende språk:

$$L = \{\Lambda, a, b, aa, ab, bb, aaa, aab, abb, bbb, \ldots\} = \{a^n b^m \mid n, m \in \mathbb{N}\}$$

La L være det minste språket som er slik at $\Lambda \in L$, og som er slik at hvis $s \in L$, så er `as` $\in L$ og `sb` $\in L$. Legg merke til at det står `as` og `sb` her; det står for eksempel ikke `sa`, som ville ha blitt feil; da ville vi ha fått med alle mulige strenger over alfabetet.

(c) [2 poeng] Gi et regulært uttrykk som definerer språket L.

Det enkleste regulære uttrykket er nok dette: `a*b*` Dette sier at vi skal ha med null eller flere `a`-er, og deretter null eller flere `b`-er.

(d) [2 poeng] Finnes det en deterministisk, endelig tilstandsmaskin som definerer L?
(Det holder med ja eller nei; du trenger ikke å begrunne svaret ditt.)

Ja. Alt som kan uttrykkes med et regulært uttrykk kan også defineres ved en deterministisk, endelig tilstandsmaskin, og vice versa.

29 Abstrakt algebra [10 poeng]

La $*$ være en operasjon på mengden $\{e, f, g, r, s, t\}$ som er definert ved følgende tabell. Tabellen viser hva $F * G$ blir, hvor F kommer fra første kolonne og G kommer fra første rad. For eksempel vil $f * g = e$ og $r * s = g$.

$*$	e	f	g	r	s	t
e	e	f	g	r	s	t
f	f	g	e	s	t	r
g	g	e	f	t	r	s
r	r	t	s	e	g	f
s	s	r	t	f	e	g
t	t	s	r	g	f	e

(a) [2 poeng] Hva er inversen til $(r * s)$?

Svaret er f. Vi har at $(r * s) = g$ og inversen til g er lik f fordi $(g * f) = e$.

(b) [2 poeng] Hva står X for i følgende uttrykk: $(r * X) * s = e$

Svaret er g. Vi får at X står for g fordi $(r * g) * s = s * s = e$, og fordi g er det eneste elementet dette stemmer for.

(c) [2 poeng] Vis at $*$ ikke er kommutativ.

Den er ikke kommutativ fordi for eksempel $g = r * s \neq s * r = f$.

(d) [4 poeng] Bevis at dette er en gruppe. Du kan anta at den er assosiativ; du trenger ikke å vise dette.

For å vise at dette er en gruppe må vi vise **(1)** at det finnes et identitetselement for $*$ og **(2)** at alle elementer har en invers. Vi trenger ikke å vise at den er assosiativ.

(1) Identitetselement: Her er e et identitetselement, fordi $e * x = x * e = x$ for alle x i mengden.

(2) Alle elementer har en invers: Det ser vi fra tabellen ved at e forekommer nøyaktig en gang per rad og nøyaktig en gang per kolonne.

30 Kombinatorikk [10 poeng]

I denne oppgaven skal vi jobbe med kvadratiske rutenett på formen $\begin{array}{|c|c|}\hline 0&1\\\hline 3&2\\\hline\end{array}$, hvor hver rute inneholder nøyaktig ett av tallene fra mengden $\{0, 1, 2, 3\}$ og hvert tall forekommer nøyaktig én gang i rutenettet. Vi kaller dem bare for *kvadrater*.

(a) Hvor mange forskjellige kvadrater finnes det?

Her er svaret $4! = 24$. Det er det samme som antall permutasjoner av strengen 0123. Vi har fire elementer å velge mellom for den første ruten, tre muligheter for den neste, to muligheter for den neste, og til slutt bare én mulighet for den siste ruten.

(b) La oss nå si at to kvadrater er *like* dersom man kan få det ene fra det andre ved å *rotere* tallene enten med eller mot klokken. For eksempel er $\begin{array}{|c|c|}\hline 0&1\\\hline 3&2\\\hline\end{array}$ lik både $\begin{array}{|c|c|}\hline 1&2\\\hline 0&3\\\hline\end{array}$ og $\begin{array}{|c|c|}\hline 2&3\\\hline 1&0\\\hline\end{array}$ og $\begin{array}{|c|c|}\hline 3&0\\\hline 2&1\\\hline\end{array}$. Hvor mange *forskjellige* kvadrater finnes det da?

Her er svaret $24/4 = 6$. Når ett kvadrat er gitt, er det *fire* måter å rotere det rundt på. Når fire og fire kvadrater blir identifisert med hverandre på denne måten, sitter vi igjen med en fjerdedel av det vi begynte med, det vil si seks kvadrater. For hvert av disse seks, finner vi vi fire forskjellige rotasjoner. Her er representater for alle seks:

$$\begin{array}{|c|c|}\hline 0&1\\\hline 3&2\\\hline\end{array} \quad \begin{array}{|c|c|}\hline 0&1\\\hline 2&3\\\hline\end{array} \quad \begin{array}{|c|c|}\hline 0&2\\\hline 3&1\\\hline\end{array} \quad \begin{array}{|c|c|}\hline 0&2\\\hline 1&3\\\hline\end{array} \quad \begin{array}{|c|c|}\hline 0&3\\\hline 2&1\\\hline\end{array} \quad \begin{array}{|c|c|}\hline 0&3\\\hline 1&2\\\hline\end{array}$$

Legg for eksempel merke at dersom du begynner å lese 0, og leser med klokka, så leser du rett og slett følgende strenger:

0123 0132 0213 0231 0312 0321

(c) La oss i tillegg si at to kvadrater er like dersom man kan få det ene fra andre ved å *speile* tallene om enten den vertikale eller den horisontale aksen. Det vil si at $\begin{array}{|c|c|}\hline 0&1\\\hline 3&2\\\hline\end{array}$ er lik både $\begin{array}{|c|c|}\hline 3&2\\\hline 0&1\\\hline\end{array}$ (ved horisontal speiling) og $\begin{array}{|c|c|}\hline 1&0\\\hline 2&3\\\hline\end{array}$ (ved vertikal speiling). Hvor mange *forskjellige* kvadrater finnes det da?

Her er svaret $6/2 = 3$. Det er fordi to og to kvadrater blir identifisert på denne måten. For eksempel vil $\begin{array}{|c|c|}\hline 0&1\\\hline 3&2\\\hline\end{array}$ bli identifiseres med $\begin{array}{|c|c|}\hline 0&3\\\hline 1&2\\\hline\end{array}$, og $\begin{array}{|c|c|}\hline 0&1\\\hline 2&3\\\hline\end{array}$ vil bli identifisert med $\begin{array}{|c|c|}\hline 0&2\\\hline 1&3\\\hline\end{array}$, og $\begin{array}{|c|c|}\hline 0&2\\\hline 3&1\\\hline\end{array}$ med $\begin{array}{|c|c|}\hline 0&3\\\hline 2&1\\\hline\end{array}$. Det å speile rektanglene svarer til å reversere strengene. For eksempel vil 0123 bli identifisert med 0321, og 0132 vil bli identifisert med 0231, og 0213 med 0312.

31 Ekvivalenser og ekvivalensrelasjoner [10 poeng]

Anta at R og S er ekvivalensrelasjoner på en mengde M. Vi vet at M/R er mengden av alle ekvivalensklasser for relasjonen R og at M/S er mengden av alle ekvivalensklasser for relasjonen S. Anta også at M/R og M/S er like. Bevis at da må også R og S være like.

For å vise at R og S er like, er det tilstrekkelig å vise at $\langle x, y\rangle \in R$ hvis og bare hvis $\langle x, y\rangle \in S$, eller, skrevet på en annen måte, at xRy hvis og bare hvis xSy. Anta derfor at xRy for to vilkårlige elementer i M. Ved definisjonen av ekvivalensklasser, må x og y være elementer i den samme ekvivalensklassen K. Da vil $K \in M/R$ og, ved antakelsen om at M/R og M/S er like, må $K \in M/S$. Da følger det, ved definisjonen av ekvivalensklasser, at xSy. Fordi x og y var vilkårlig valgt, må dette holde for alle elementer x og y. Da følger det at hvis $\langle x, y\rangle \in R$, så $\langle x, y\rangle \in S$. På tilsvarende måte kan vi vise at hvis $\langle x, y\rangle \in S$, så $\langle x, y\rangle \in R$. Da må R og S være identiske.

32 Matematisk induksjon [10 poeng]

Bevis ved matematisk induksjon at summen av de n første partallene er $n(n+1)$, det vil si at påstanden

$$0 + 2 + \cdots + 2n = n(n+1)$$

er sann for alle naturlige tall n.

(Her har det sneket seg inn en liten uklarhet. Det er jo slik at 0 er det første naturlige partallet, og dermed burde det ha stått «de første $n+1$ første naturlige partallene» i stedet for. Alternativt kunne bare hele frasen «summen av de [...] $n(n+1)$» ha vært tatt ut.)

Vi viser påstanden ved matematisk induksjon.

Basissteget er sant fordi summen av de 0 første partallene, 0, er lik $0(0+1) = 0$.

Induksjonssteget går slik: Anta at $0 + 2 + \cdots + 2n = n(n+1)$; dette er vår **induksjonshypotese**. Vi må nå vise at $0 + 2 + \cdots + 2n + 2(n+1) = (n+1)((n+1)+1)$. Ved regning får vi følgende:

$$\begin{aligned}
0 + 2 + \cdots + 2n + 2(n+1) &= n(n+1) + 2(n+1) \quad \text{(ved induksjonshypotesen)} \\
&= n(n+1) + 2n + 2 \\
&= n^2 + n + 2n + 2 \\
&= n^2 + 3n + 2 \\
&= (n+1)(n+1) + (n+1) \\
&= (n+1)((n+1)+1)
\end{aligned}$$

Ved matematisk induksjon har vi nå vist at $0 + 2 + \cdots + 2n = n(n+1)$ er sann for alle naturlige tall n.

33 Idempotens og transitivitet [10 poeng]

Husk at vi kaller en funksjon $f : A \to A$ *idempotent* hvis $f(f(x)) = f(x)$ for enhver $x \in A$. Husk dessuten at en funksjon $f : A \to A$ er en bestemt type binær *relasjon* på A. Gitt en funksjon $f : A \to A$, vis at f er idempotent hvis og bare hvis f er en transitiv relasjon.

Det er to deler av dette beviset:

(«Hvis»-delen:) Hvis f er transitiv, så er f idempotent.

(«Bare hvis»-delen:) Hvis f er idempotent, så er f transitiv.

(«Hvis»-delen:) Anta at f er transitiv, altså for alle $x, y, z \in A$ med $f(x) = y$ og $f(y) = z$ gjelder $f(x) = z$. Siden f er en funksjon har den nøyaktig én verdi for hvert argument x, altså må y være lik z. Altså er $f(f(x)) = f(y) = z = y = f(x)$.

(«Bare hvis»-delen:) Anta at f er idempotent, altså $f(f(x)) = f(x)$ for alle $x \in A$. Hvis $\langle x, y\rangle \in f$ og $\langle y, z\rangle \in f$, betyr det at $f(x) = y$ og $f(y) = z$. Men $f(y) = f(f(x)) = f(x) = y$ på grunn av idempotens, så $z = y$, og derfor $f(x) = z$, eller $\langle x, z\rangle \in f$. Altså er f transitiv.

Alternativt svar:

Vi bruker skrivemåten fra boken og skriver xfy når $\langle x, y\rangle \in f$.

(«Hvis»-delen:) Anta at f er transitiv. La x være et vilkårlig element, og anta at $f(x) = y$. Vi må fra dette vise at $f(f(x)) = y$, for da har vi vist at f er idempotent. Det at $f(x) = y$ betyr at xfy. La oss anta at $f(f(x)) = z$, som er det samme som å si at $f(y) = z$. Det at $f(y) = z$ betyr at yfz. Transitivitet av f gir nå at xfz, det vil si at $f(x) = z$. Vi har allerede antatt at $f(x) = y$, og fordi f er en funksjon, må $y = z$ og $f(f(x)) = y$. Da må f være idempotent.

(«Bare hvis»-delen:) Anta at f er idempotent. For å vise at f er transitiv, anta at xfy og yfz, det vil si at $f(x) = y$ og $f(y) = z$. Vi må fra dette vise at xfz, det vil si at $f(x) = z$, for da har vi vist at f er transitiv. Det at $f(x) = y$ og $f(y) = z$ gir umiddelbart at $f(f(x)) = z$. Idempotens av f gir nå at $f(f(x)) = f(x)$ og dermed at $f(x) = z$, som betyr det samme som at xfz. Da må f være transitiv.