Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

LØSNINGSFORSLAG SIF5015 DISKRET MATEMATIKK

Onsdag 18. desember 2002

Oppgave 1

a) Vi vil ha $77x \equiv 1 \pmod{13}$, så vi trenger en x som er en løsning til $77x - 1 = 13c$ eller $77x - 13c = 1$. Ved Euklid's algoritme har vi

$$\begin{array}{rcccl} 77 & = & 13 \cdot 5 & + & 12 \\ 13 & = & 12 & + & 1 \end{array}$$

så 77 og 13 har 1 som største felles divisor, så ligningssettet har en løsning:

$$\begin{array}{rcccl} 1 & = & 13 & - & 12 \\ & = & 13 & - & (77 - 13 \cdot 5) = 6 \cdot 13 - 77. \end{array}$$

Dermed er -1 en invers til 77 modulo 13, så den inversen vi søker er $x = 12$.

b) 13 er et primtall og $13 \not| 119$, så Fermats lille setning forteller oss at $119^{12} \equiv 1 \pmod{13}$. $1477 = 123 \cdot 12 + 1$ og $119 \equiv 2 \pmod{13}$, så $119^{1477} \equiv 2 (\text{mod } 13)$. Dermed må vi løse systemet

$$\begin{array}{rcrcll} 2x & + & 5y & \equiv & 3 & \pmod{13} \\ 15x & - & y & \equiv & 2 & \pmod{13} \end{array}$$

Multipliser den andre ligningen med 5 og legg til den første ligningen. Dette gir

$$77x \equiv 13 \pmod{13}.$$

Multipliser hver side med en invers til 77 modulo 13 (eller se direkte) at vi har $x \equiv 0 \pmod{13}$. Hvis vi setter dette inn i den andre ligningen får vi

$$y \equiv -2 \pmod{13}.$$

Dermed er $(0, 11)$ og $(13, 11)$ de mulige løsningene for (x, y) som tilfredsstiller alle kravene.

Oppgave 2 Hvis x er tallet gjesten tenker på kan vi uttrykke at restene er 2, 3 og 5 ved

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

$7 \cdot 11 \cdot 13 = 1001$, så den kinesiske restsetningen forteller oss at det finnes en unik løsning til systemet over slik at $0 \leq x < 1001$. For hver ligning finner vi en løsning som er kongruent med null i de to andre ligningene:

Invers til $11 \cdot 13 = 143$ modulo 7, $143 \equiv 3 \pmod{7}$, og 5 er en invers til 3 modulo 7, så 5 er en invers til $11 \cdot 13$ modulo 7. Dermed er $x_1 = 2 \cdot 5 \cdot 11 \cdot 13 = 1430$ en løsning til den første ligningen, og x_1 er kongruent med null i de to andre.

Invers til $7 \cdot 13 = 91$ modulo 11, $91 \equiv 3 \pmod{11}$, og 4 er en invers til 3 modulo 11, så 4 er en invers til $7 \cdot 13$ modulo 11. Ta $x_2 = 3 \cdot 4 \cdot 7 \cdot 13 = 1092$.

Inversen til $7 \cdot 11 = 77$ modulo 13, $77 \equiv -1 \pmod{13}$, og -1 er en invers til -1 modulo 13, så -1 er en invers til $7 \cdot 11$ modulo 13. Ta $x_3 = 5 \cdot (-1) \cdot 7 \cdot 11 = -385$.

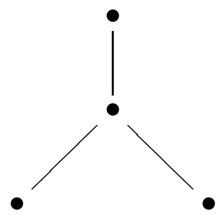
Dermed vil $x_1 + x_2 + x_3 = 1430 + 1092 - 385 = 2137$ være en løsning til systemet over. Alle tall som er kongruent med dette tallet modulo $7 \cdot 11 \cdot 13 = 1001$ er også løsninger, så løsningen vi ser etter er $x = 2137 - 2 \cdot 1001 = 135$. Så tallet gjesten tenkte på var 135.

Oppgave 3

a) Siden et tre ikke kan ha kretser kan et tre med 4 hjørner bare ha tre kanter. Et slikt tre kan heller ikke ha færre kanter, siden det da ikke kan være sammenhengende. Alle slike trær med et hjørne med grad 3 er isomorfe: La isomorfien sende hjørnet med grad 3 i det ene treet til hjørnet med grad 3 i det andre treet. De andre hjørnene kan knyttes sammen tilfeldig, siden den eneste naboen de kan ha er hjørnet med grad 3.

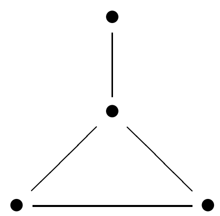
Hvis et tre med fire hjørner og 3 kanter ikke har et hjørne med grad 3 må vi ha to hjørner med grad 1 og to med grad 2. Slike trær vil også alltid være isomorfe: Velg et hjørne med grad en i hvert tre og knytt disse sammen med isomorfien. De vil kun ha en nabo, så knytt disse sammen. Dette hjørnet vil ha to naboer. Den ene er hjørnet vi startet ved, den andre er et hjørne med grad 2. Knytt disse sammen. Deretter står det bare et hjørne i hver graf igjen, så disse skal knyttes sammen.

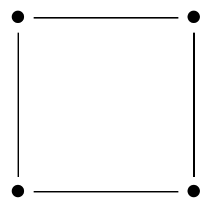
Dermed finnes det 2 forskjellige typer trær med 4 hjørner.



b) En sammenhengende enkel graf med fire hjørner kan ha enten 3, 4, 5 eller 6 kanter. De med 3 kanter er nøyaktig beskrevet i deloppgaven over. Det finnes også bare en type slik graf med 6 kanter (alle hjørnene har grad 3 og er naboer med hverandre). Vi trenger derfor finne ut hvor mange muligheter vi har med enten 4 eller 5 kanter.

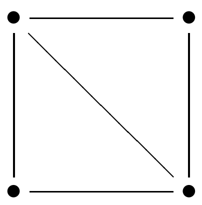
4 kanter: Vi kan ta utgangspunkt i grafene med 3 kanter, og legge til en kant. Siden vi skal ha en enkel graf er det begrensede muligheter. Til den til høyre over kan vi lage følgende to typer:





Fra den til venstre i deloppgaven over kan vi bare lage en type graf ved å legge til en kant, nemlig den til venstre over. Dermed finnes det 2 typer enkle sammenhengende grafer med 4 hjørner og fire kanter.

5 kanter: Vi kan enten få disse ved å legge til en kant på de med fire kanter eller trekke fra en kant fra de med 6 kanter. Uansett får vi bare en type graf: To hjørner med grad 2; disse er ikke naboer. To hjørner med grad 3; disse er naboer med alle.



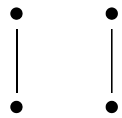
Dermed har vi $2 + 2 + 1 + 1 = 6$ forskjellige enkle sammenhengende grafer med 4 hjørner

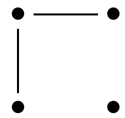
Hvis vi i tillegg regner med de ikkesammenhengende grafene:

En graf uten kanter.

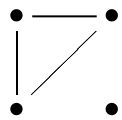
En med en kant.

To med 2 kanter.





Med tre kanter kan vi få en graf til

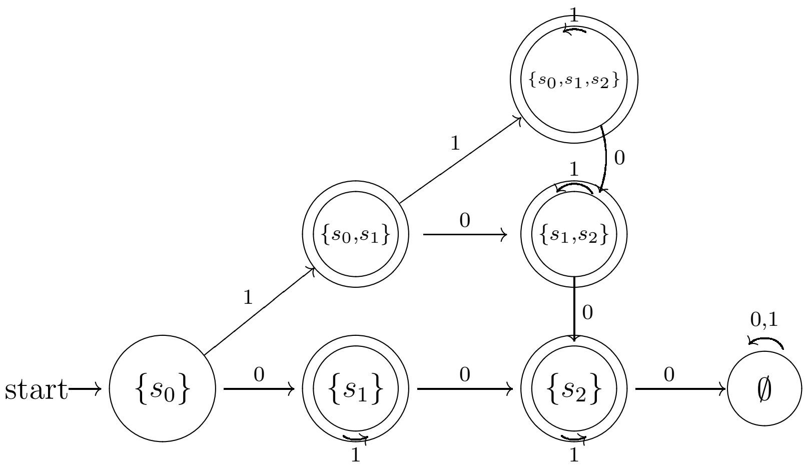


Med fire eller flere kanter må grafen være sammenhengende for å være enkel.

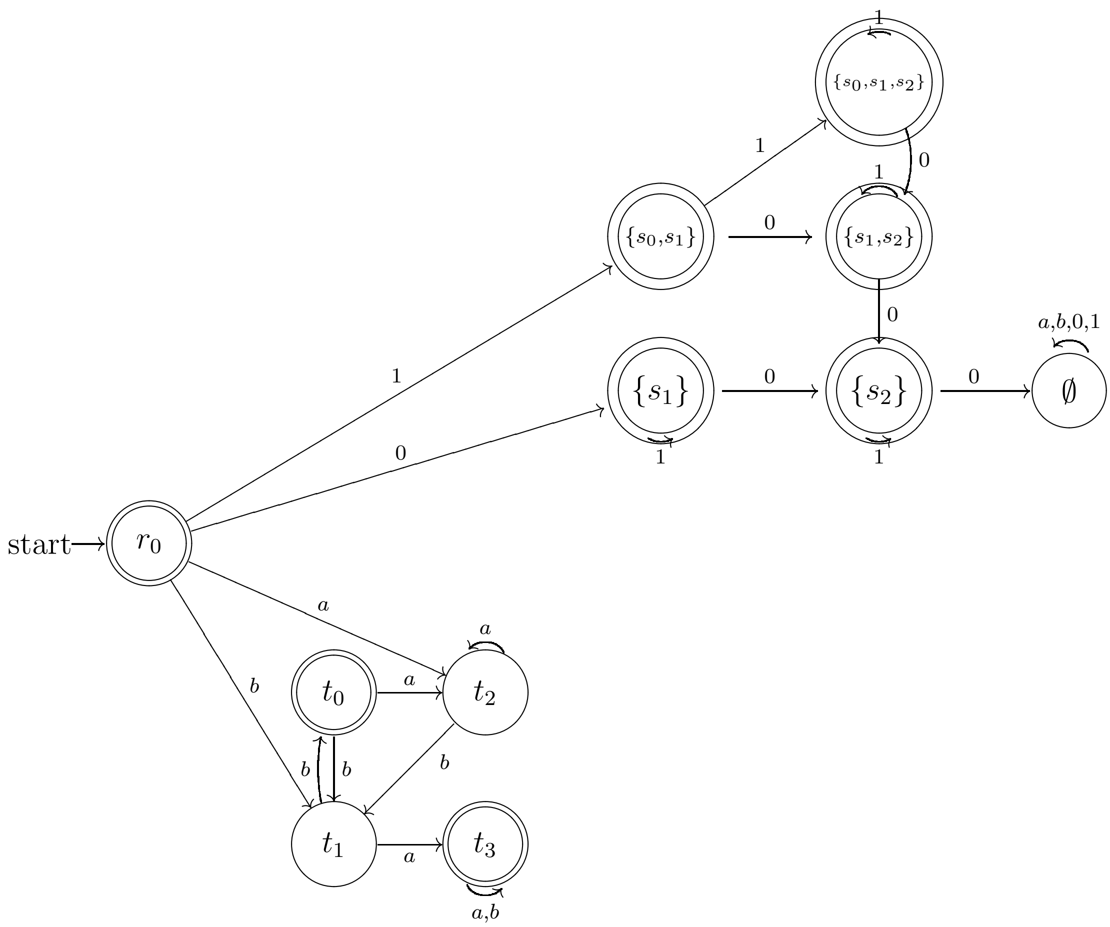
Dermed har vi totalt 11 forskjellige grafer.

Oppgave 4

a) Vi vet at et språk som gjennkjennes av en ikkedeterministisk endeligtilstandsautomat også kan gjennkjennes av en deterministisk en. Vi følger bokens bevis for dette og får en deterministisk N_1 som gjennkjenner L_1 (M_2 er allerede deterministisk):



Vi kan nå slå sammen N_1 og M_2 for å få en automat som beskriver L. Vi endrer navn på tilstandene i M_2 til t_j for å ikke blande dem sammen med tilstandene fra M_1.



I tillegg skal det gå piler fra alle tilstandene til tilstanden $\emptyset$ slik at 0, 1, a og b går ut fra hver tilstand. (M.a.o. fra "tilstandene med s'er" skal det gå en "a-pil" og en "b-pil" til $\emptyset$, og fra "tilstandene med t'er skal det gå en "0-pil" og en "1-pil" til $\emptyset$.)

Det er også mulig å slå sammen M_1 og M_2 først, og deretter lage en deterministisk automat ut av den som da oppstår, men det er kanskje litt mer arbeid?

b) Vi vet at regulære mengder er nøyaktig de som generers av regulære grammatikker. Kleenes setning sier at L er en regulær mengde siden L gjennkjennes av en endeligtilstandsautomat, så det finnes en regulær grammatikk som genererer L.

Oppgave 5 For at R skal være en delvis ordning kreves det at R er refleksiv, transitiv og antisymmetrisk.

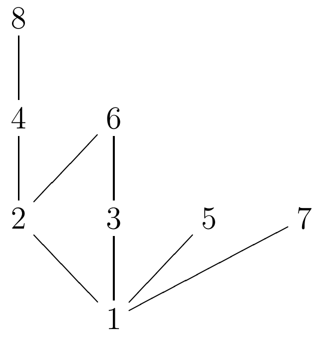
refleksiv: Hvis a er et tall, så vet vi at a deler seg selv.

transitiv: Hvis a deler b og b deler c så vet vi at a deler c. ($b = sa$, $c = tb$ så $c = tsa$.)

antisymmetrisk: Hvis a deler b så vet vi at $a \leq b$. Hvis b deler a har vi den motsatte ulikheten, så hvis begge deler hverandre ser vi at vi må ha $a = b$.

Alle egenskapene er tilfredsstilt, så R er en delvis ordning.

Hassediagrammet:



Oppgave 6 La T være mengden av studenter som misliker tomater, $\O$ de som misliker øl og S de som misliker Samantha. Hvis vi normerer antallet studenter til 200 får vi $|T| = 60$, $|\O| = 80$, $|S| = 125$, $|T \cup \O \cup S| = 180$ og $|T \cap \O \cap S| = 40$. Vi ønsker å finne $|(T \cup \O) \cap \bar{S}|$.

Fra inklusjon-ekslusjonsprinsippet har vi

$$|T \cup \O \cup S| = |T| + |\O| + |S| - |T \cap \O| - |T \cap S| - |\O \cap S| + |T \cap \O \cap S|$$

og fordi S og $\bar{S}$ er disjunkte mengder:

$$|(T \cup \O) \cap S| + |(T \cup \O) \cap \bar{S}| = |T \cup \O| = |T| + |\O| - |T \cap \O|.$$

I tillegg vet vi at $(T \cup \O) \cap S = (T \cap S) \cup (\O \cap S)$, så

$$|(T \cup \O) \cap S| = |T \cap S| + |\O \cap S| - |T \cap \O \cap S|.$$

Setter vi alt dette sammen får vi

$$|(T \cup \O) \cap \bar{S}| = |T \cup \O \cup S| - |S| = 180 - 125 = 55$$

Dermed blir andelen studenter vi ser etter lik $\frac{11}{40}$.

Eller vi kan bruke Venn-diagramm for å løse oppgaven. (mye enklere...)

Oppgave 7

Vi kan se på $(p \to (\neg q \wedge r)) \vee (r \leftrightarrow p)$ som en Boolesk funksjon, og setter først opp en tabell for funksjonen (sannhetstabell).

p	q	r	$\neg q \wedge r$	$p \to (\neg q \wedge r)$	$r \leftrightarrow p$	$(p \to (\neg q \wedge r)) \vee (r \leftrightarrow p)$
0	0	0	0	1	1	1
0	0	1	1	1	0	1
0	1	0	0	1	1	1
0	1	1	0	1	0	1
1	0	0	0	0	0	0
1	0	1	1	1	1	1
1	1	0	0	0	0	0
1	1	1	0	0	1	1

Fra denne tabellen ser vi at

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r)$$

er et utsagn med samme sannhetstabell, og dermed et logisk ekvivaleent utsagn. (Dette utsagnet er til og med på disjunktiv normal form, men det kreves ikke her.)

Oppgave 8

a)

$$f(3) = \sum_{i=1}^{3} \sum_{j=1}^{i} (i+j) = [(1+1)] + [(2+1)+(2+2)] + [(3+1)+(3+2)+(3+3)] = 24$$

b)

$$f(n) = \sum_{i=1}^{n} \sum_{j=1}^{i} (i+j) = \sum_{i=1}^{n} (i^2 + \sum_{j=1}^{i} j) = \sum_{i=1}^{n} (i^2 + \frac{i(i+1)}{2}) = \frac{1}{2} \sum_{i=1}^{n} (3i^2 + i)$$

Vi tipper $q = 3$. Vi må vise at $f(n)$ er $O(n^3)$ og $\Omega(n^3)$.

$O(n^3)$: For $f(n)$ er det n ledd som skal legges sammen, alle mindre enn eller lik $\frac{3}{2}n^2 + \frac{1}{2}n$ som igjen er mindre enn $2n^2$. Dermed er $f(n) < 2n^3$ for alle n.

$\Omega(n^3)$: Vi vil prøve å vise at $f(n) > \frac{1}{3}n^3$. (Hintet) Vi vet fra deloppgaven over at dette er sant for $n = 3$. La oss vise at det er sant for alle $n \geq 3$ ved induksjon:

Induksjonshypotese: $f(n) > \frac{1}{3}n^3$. Vi ønsker å vise: $f(n+1) > \frac{1}{3}(n+1)^3$:

$$f(n+1) = f(n) + \frac{3}{2}(n+1)^2 + \frac{1}{2}(n+1) > \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{7}{2}n + 2 > \frac{1}{3}n^3 + n^2 + n + \frac{1}{3} = \frac{1}{3}(n+1)^3$$