SIF5015 Diskret matematikk
Onsdag 2. august 2000
løsningsforslag

Norges teknisk-naturvitenskapelige universitet
Institutt for matematiske fag

1 Sannhetstabellen blir

$(p$	$\wedge$	$((\neg q)$	$\rightarrow$	$r))$	$\oplus$	$((\neg p)$	$\rightarrow$	$(q$	$\oplus$	$(\neg r)))$
1	1	0	1	1	0	0	1	1	1	0
1	1	0	1	0	0	0	1	1	0	1
1	1	1	1	1	0	0	1	0	0	0
1	0	1	0	0	1	0	1	0	1	1
0	0	0	1	1	1	1	1	1	1	0
0	0	0	1	0	0	1	0	1	0	1
0	0	1	1	1	0	1	0	0	0	0
0	0	1	0	0	1	1	1	0	1	1

Fra denne ser vi at formelen er ekvivalent med fomelen

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

som kan forenkles til $(\neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r)$.

2 Vi kan regne ut antall skilt i U ved å ta differansen mellom alle skilt og skilt som har bare forskjellige bokstaver i første linje, det gir $|U| = (5^3 - 5 \cdot 4 \cdot 3) \cdot 5^3 = 13 \cdot 5^4$. Videre får vi $|V| = 4^2 \cdot 5^4$. Mengden $U \cap V$ kan det lønne seg å dele inn i tre deler ettersom det er 0, 1 eller 2 A'er i første rad. Vi finner da $|U \cap V| = 40 \cdot 4 \cdot 5^2 + 8 \cdot 4 \cdot 5^2 + 4 \cdot 4 \cdot 5^2 = 13 \cdot 4^2 \cdot 5^2$, og fra inklusjon-eksklusjonsprinsippet får vi $|U \cup V| = 8125 + 10000 - 5200 = 12925$.

3 **a)** Ligningen $16x + 2 \equiv 15 - 3x \pmod{241}$ er ekvivalent med $19x \equiv 17 \pmod{241}$.

Euklids algoritme med tilbakesubstitusjon gir at

$1 = -38 \cdot 19 + 3 \cdot 241.$

Multipliserer vi med -38 på begge sider får vi

$x \equiv 77 \pmod{241}$, eller

$x = 77 + k \cdot 241$ for alle $k \in \mathbb{Z}$.

b) Standardmetoden for å løse denne typen oppgaver er som følger. Som i punkt a) kan vi bruke Euklids algoritme med tilbakesubstitusjon til å løse ligningene

$x_1 \equiv 7a + 1 \equiv 0 \pmod{72}$

$x_2 \equiv 8b + 1 \equiv 0 \pmod{63}$

$x_3 \equiv 9c + 1 \equiv 0 \,(\mathrm{mod}\, 56)$

Vi finner da f.eks. $a = 41$, $b = -8$ og $c = 31$, og dette gir oss $x_1 = 288$, $x_2 = -63$ og $x_3 = 280$. Tilslutt får vi $x \equiv 4 \cdot x_1 + 5 \cdot x_2 + 1 \cdot x_3 \equiv 1117 \,(\mathrm{mod}\, 504)$. Mulige løsninger er $x = 109$ og $x = 613$.

c) Vi har at $72723 = 240 \cdot 303 + 3$. Altså har vi ifølge Fermats lille teorem at

$x = 235^{72723} \,\mathbf{mod}\, 241 = 235^3 \,\mathbf{mod}\, 241 = (-6)^3 \,\mathbf{mod}\, 241 = -216 \,\mathbf{mod}\, 241 = 25.$

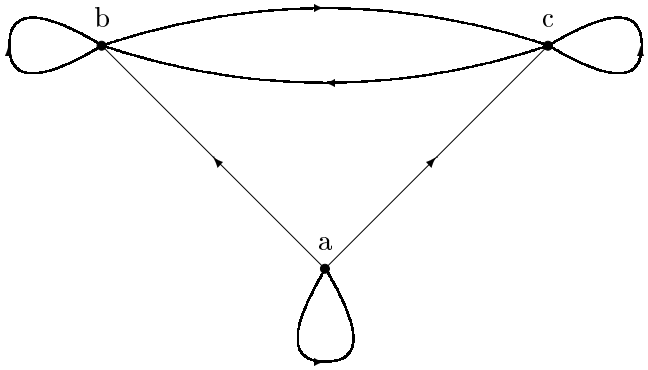
4 **a)** Matrisen til relasjonen blir

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Vi har at $R^* = R \cup R^2 \cup R^3$, og matrisen til R^* er $M_{R^*} = M_R \vee M_R \odot M_R \vee M_R \odot M_R \odot M_R$. Litt regning gir

$$M_{R^*} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \vee \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \vee \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

b)



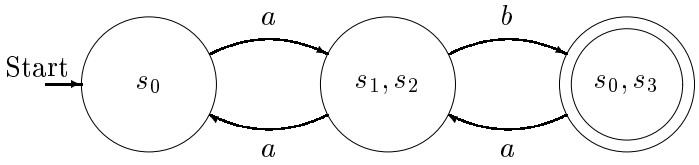
5 **a)** Et mulig regulært for L uttrykk er f.eks. $R = (a(a \cup b))^* ab$.

b) En deterministisk endelig automat N som er slik at $L = \mathrm{L}(N)$ er gitt av tabellen under.

	a	b	F
$\{s_0\}$	$\{s_1,\ s_2\}$	$\emptyset$	
$\{s_1\}$	$\{s_0\}$	$\{s_0\}$	
$\{s_2\}$	$\emptyset$	$\emptyset$	
$\{s_3\}$	$\emptyset$	$\emptyset$	$*$
$\{s_1\ s_2\}$	$\{s_0\}$	$\{s_0\ s_3\}$	
$\{s_0\ s_3\}$	$\{s_1\ s_2\}$	$\emptyset$	$*$
$\emptyset$	$\emptyset$	$\emptyset$	

Her er grafen til en deterministisk endelig automat N' som gjenkjenner språket $L =$

L(M). Vi har droppet alle overflødige tilstander, samt den universelt tiltrekkende tilstanden $\emptyset$.



Fra denne ser vi at et annet mulig regulært uttrykk for L er $R' = a(aa)^*(ba)^*b$.

6 Vi finner først $s(2) = 9$ og $s(3) = 34$ Ved direkte utregning stemmer alle tre formlene for $n = 2$ og for $n = 3$. Vi gjetter at det er formel 3) som er korrekt.

For å vise at formelen er korrekt er det nok å vise at for en vilkårlig n, så gjelder

$$\frac{4}{3}n^3 - \frac{1}{3}n - 1 = \sum_{j=2}^{n}(2j-1)^2 \Rightarrow \frac{4}{3}(n+1)^3 - \frac{1}{3}(n+1) - 1 = \sum_{j=2}^{n+1}(2j-1)^2$$

Differansen mellom venstresidene er $(\frac{4}{3}(n+1)^3 - \frac{1}{3}(n+1) - 1) - (\frac{4}{3}n^3 - \frac{1}{3}n - 1) = 4n^2 + 4n + 1$, og differansen mellom høyresidene er $(2(n+1)-1)^2 = 4n^2 + 4n + 1$ ∎

7 Et privat kryptosystem er å sammenligne med en lås som man lukker og åpner med samme nøkkel. Et offentlig kryptosystem derimot er å sammenligne med en lås som man lukker og åpner med forskjellige nøkler, og besittelse av lukkenøkkelen har ingen betydning når det gjelder å åpne låsen.

I et offentlig kryptosystem har alle personene to nøkler, en krypteringsnøkkel, som er offentlig kjent, og en dekrypteringsnøkkel, som er ukjent for alle andre enn en selv.

Dette gjør det mulig for enhver person å sende en kryptert melding til en vilkårlig annen person, slik at bare den ønskede personen kan dekryptere den.

I et privat kryptosystem har alle personene en kopi av samme nøkkel, som kan brukes både til kryptering og til dekryptering.

Dette gjør det mulig for en gruppe å sende krypterte meldinger til hverandre, uten at utenforstående kan forstå meldingene eller lage falske meldinger.

En mulig måte å sende en signert kryptert melding, slik at mottakeren kan være rimelig sikker på at meldingen ble sent av den personen som utga seg for senderen, er å (før krypteringen) kvittere meldingen med sin egen signatur samt sin egen signatur dekryptert (med egen dekrypteringsnøkkel).

Når mottakeren dekrypterer meldingen vil en signatur være uleselig, men ved å *kryptere* denne med senderens krypteringsnøkkel, dukker senderens signatur opp. Siden ingen andre enn senderen kunne ha laget denne andre signaturen, kan mottakeren være temmelig sikker i sin sak.