Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristin Krogh Arnesen 469 32 840

EKSAMEN I MA0301 ELEMENTÆR DISKRET MATEMATIKK

Bokmål
Torsdag 31. mai 2012
Tid: 0900-1300
Hjelpemiddel D: Bestemt, enkel kalkulator.
Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Alle oppgaver teller likt. Alle svar skal begrunnes.

Oppgave 1 Nøkkelen til blokkchifferet DES består av 56 binære siffer (0 eller 1). Det er fire såkalt "svake" nøkler.

Hvor mange forskjellige nøkler finnes det? Hvor mange nøkler er ikke svake?

Trippel-DES (3DES) er et blokkchiffer der nøkkelen består av tre DES-nøkler. Hvor mange 3DES-nøkler finnes det? Hvor mange 3DES-nøkler finnes det der ingen av DES-nøklene er svake? Hvor mange 3DES-nøkler finnes det der minst én av DES-nøklene ikke er svak?

Oppgave 2 Du jobber med kvalitetskontroll av kode, og en rutine du ser på skal oppfylle utsagnet $p \to q$. Bak en skuff i et gjenglemt arkivskap på loftet i de gamle lokalene til firmaet som opprinnelig skrev koden finner du dokumentasjonen til rutinen.

a) Dokumentasjonen påstår at følgende utsagn gjelder for koden:

$$\neg s \leftrightarrow \neg q, \qquad \neg t \to \neg p, \qquad \neg t \vee s$$

Avgjør om utsagnet $p \to q$ følger fra de tre overstående utsagnene, enten ved å bruke de logiske regnereglene til å utlede $p \to q$ fra de overstående, eller ved å gi et moteksempel.

b) Koden har endret seg siden dokumentasjonen ble skrevet. Nå gjelder følgende utsagn for koden:

$$s \leftrightarrow \neg q, \qquad \neg t \rightarrow \neg p, \qquad \neg t \vee s$$

Avgjør om utsagnet $p \rightarrow q$ følger fra de tre overstående utsagnene, enten ved å bruke de logiske regnereglene til å utlede $p \rightarrow q$ fra de overstående, eller ved å gi et moteksempel.

Oppgave 3 Lag en maskin som gjenkjenner språket $\{1\}\{01\}^* \cup \{11\}\{10\}^*$.

Oppgave 4 Følgende to programmer tar inn et tall $x > 0$ og et ikke-negativt heltall a, og gir ut innholdet i variabelen u. Tallet a har $n+1$ binære siffer $a_n a_{n-1} \ldots a_1 a_0$, $a_j \in \{0, 1\}$, det vil si at $a = a_0 + 2a_1 + 2^2 a_2 + \cdots + 2^n a_n$.

1. $u \leftarrow 1$.
2. for i fra 1 til a, gjenta:
   (a) $u \leftarrow u \cdot x$.

1. $u \leftarrow 1$.
2. for i fra 0 til n, gjenta:
   (a) $u \leftarrow x^{a_{n-i}} \cdot u^2$.

a) Du kan anta at multiplikasjon er den eneste tidkrevende operasjonen. Analyser kjøretiden til begge programmene og angi svaret ved hjelp av $O(\cdot)$-notasjon.

Vi skal vise at det høyre programmet gir ut tallet x^a. La $P(i)$ og $Q(i)$ være følgende to utsagn:

- $P(i)$: før iterasjon i av løkken begynner har u verdien
$$x^{a_{n-i+1}+2a_{n-i+2}+2^2 a_{n-i+3}+\cdots+2^{i-1}a_n}.$$
- $Q(i)$: etter at iterasjon i av løkken er ferdig har u verdien
$$x^{a_{n-i}+2a_{n-i+1}+2^2 a_{n-i+2}+\cdots+2^{i}a_n}.$$

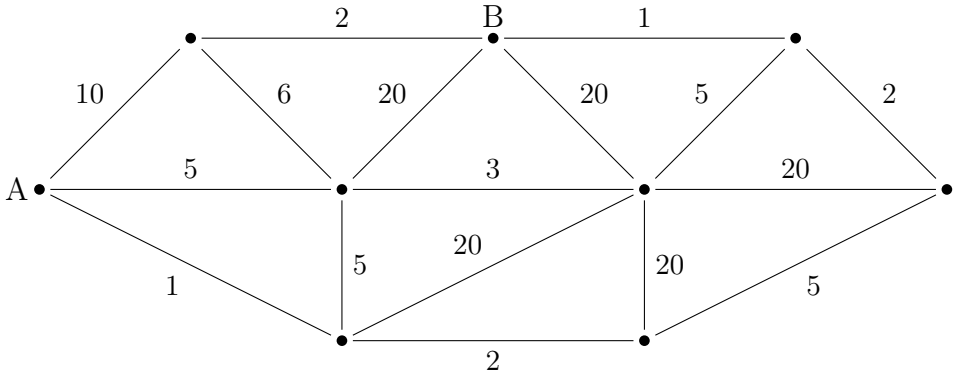
Programmet er altså korrekt hvis $Q(n)$ er sann. For alle i gjelder det at $Q(i) \rightarrow P(i+1)$.

b) Vis at $P(i) \rightarrow Q(i)$ er sant for alle i.

c) Bruk matematisk induksjon til å vise at $Q(n)$ er sann.

Hint: Du kan bruke resultatet fra forrige deloppgave selv om du ikke har besvart deloppgaven.

Oppgave 5 Bruk Dijkstras algoritme til å finne korteste vei fra A til B i følgende vektede graf.

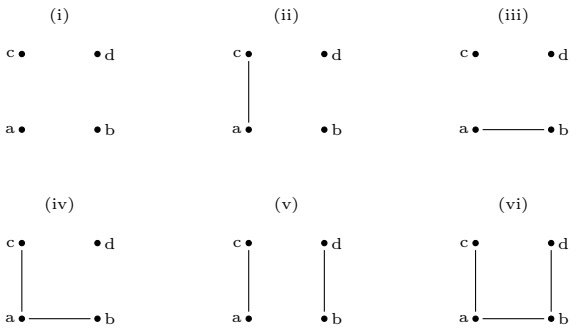


Oppgave 6 La $\mathcal{G}$ være en mengde grafer. La $\sim$ og $\sqsubseteq$ være relasjonene på $\mathcal{G}$ gitt ved

$$G_1 \sim G_2 \quad \Leftrightarrow \quad G_1 \text{ og } G_2 \text{ er isomorfe.}$$
$$G_1 \sqsubseteq G_2 \quad \Leftrightarrow \quad G_1 \text{ er en undergraf av } G_2.$$

a) Vis at $\sim$ er en ekvivalensrelasjon og at $\sqsubseteq$ er en delvis ordning.

b) La $\mathcal{G}$ være følgende mengde med grafer:



Bestem ekvivalensklassene til $\sim$ og tegn Hasse-diagrammet til $\sqsubseteq$.