Skriftlig Eksamen
Algoritmer og Sandsynlighed (DM538)

Institut for Matematik og Datalogi
Syddansk Universitet, Odense

Fredag den 25. januar 2013 kl. 10–13

Alle hjælpemidler (computer, lærebøger, notater, osv.) er tilladt. Det er ikke tilladt at bruge internettet, undtagen til den elektroniske aflevering.

Eksamenssættet består af 4 opgaver på 4 nummererede sider (1–4).
Fuld besvarelse er besvarelse af alle 4 opgaver.
De enkelte opgavers vægt ved bedømmelsen er angivet i procent. Bemærk, at de enkelte spørgsmål i en opgave ikke nødvendigvis har samme vægt.

Der må gerne refereres til resultater fra kursets lærebøger og øvelsesopgaver. Henvisninger til andre bøger accepteres ikke som besvarelse af et spørgsmål.

Bemærk, at hvis der er et spørgsmål, man ikke kan besvare, må man gerne besvare de efterfølgende spørgsmål og blot antage, at man har en løsning til de foregående spørgsmål.

Husk at begrunde dine svar!

Opgave 1 (30%)

Denne opgave handler om rekursionsligninger.

Spørgsmål a–c handler om ternære strenge. En ternær streng er en streng, som kan indeholde tre forskellige cifre, 0, 1 og 2 (ligesom bitstrenge er strenge, der kan indeholde to forskellige cifre, 0 og 1).

Lad a_n, $n \geq 0$, betegne antallet af ternære strenge af længde n, som ikke indeholder to 0'er i træk.

a) Angiv en rekursionsligning for a_n.

b) Hvad er begyndelsesbetingelserne for rekursionsligningen fra spørgsmål a?
(Bemærk, at det er muligt at besvare dette spørgsmål, selvom du ikke har besvaret spørgsmål a.)

c) Angiv værdien af a_3.
(Bemærk, at det er muligt at besvare dette spørgsmål, selvom du ikke har besvaret spørgsmål a og b.)

d) Løs rekursionsligningen

$$b_n = b_{n-1} + 2b_{n-2}$$

med begyndelsesbetingelser

$$b_0 = b_1 = 3$$

Opgave 2 (40%)

I denne opgave ser vi på følgende problem. Der er 5 opgaver, som skal løses, og 10 mennesker til at løse dem. Hver person skal løse præcis én opgave; d.v.s. nogle opgaver bliver løst af flere personer.

a) Hvor mange forskellige fordelinger af opgaver til de 10 personer findes der, hvis det *ikke* er et krav, at alle opgaver bliver løst?

b) Hvor mange forskellige fordelinger af opgaver til de 10 personer findes der, hvis det *er* et krav, at alle opgaver bliver løst?

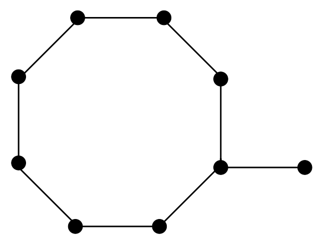
Antag nu, at vi bruger følgende algoritme til at fordele opgaverne. Hver af de 10 personer tildeles en uniformt tilfældig opgave (d.v.s. hver person tildeles hver opgave med sandsynlighed $\frac{1}{5}$).

c) Hvad er sandsynligheden for, at alle opgaver bliver løst?

d) Hvad er det forventede antal gange, algoritmen skal udføres, før man opnår en tildeling, hvor alle opgaver bliver løst?

e) For en given opgave, hvad er det forventede antal personer, som tildeles denne opgave?

f) Vis, at for en given opgave er sandsynligheden for, at opgaven bliver løst af mere end 6 personer, mindre end 0,1.



Figur 1: Et eksempel på graferne i opgave 3 b)

Opgave 3 (20%)

Denne opgave handler om at finde et globalt minimum snit i en graf v.h.a. contraction-algoritmen, som er beskrevet på side 715-716 i noterne.

a) Hvis input-grafen er et træ, hvad er da sandsynligheden for, at contraction-algoritmen finder et minimum snit i grafen?
Hint: Hvor mange sammentrækninger (contractions) udfører algoritmen?

b) Antag nu, at input-grafen er en kreds med en kant, der "stikker ud". D.v.s. hvis grafen har n knuder, da består den af en kreds med $n-1$ knuder og en kant, som har præcis et endepunkt i kredsen. I Figur 1 er grafen illustreret for $n = 9$.

Hvad er sandsynligheden for, at contraction-algoritmen finder et minimum snit i en sådan graf?

Opgave 4 (10%)

I denne opgave ser vi på familier af hash-funktioner, som afbilder et univers U på $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.

En familie $\mathcal{H}$ af hash-funktioner er *uniform*, hvis der for enhver nøgle $x \in U$ og ethvert $z \in \mathbb{Z}_p$ gælder, at

$$\Pr\bigl(h(x) = z\bigr) = \frac{1}{p},$$

når h trækkes uniformt tilfældigt fra $\mathcal{H}$.

I kurset så vi på familien $\mathcal{H}$ af hash-funktioner defineret på følgende måde (på side 739 i noterne):
Del bits'ne i hver nøgle x op i r grupper $x_1, x_2, \ldots, x_r$ a $\lceil \log p \rceil$ bits.
Lad $\mathcal{A}$ være mængden af alle vektorer på formen

$$a = (a_1, a_2, \ldots, a_r), \text{ hvor } a_i \in \mathbb{Z}_p \text{ for } 1 \leq i \leq r,$$

og lad

$$h_a(x) = \left(\sum_{i=1}^{n} a_i x_i \right) \bmod p.$$

Da er $\mathcal{H} = \{h_a \mid a \in \mathcal{A}\}$.
Vi viste, at $\mathcal{H}$ er universel.

Vis, at $\mathcal{H}$ *ikke* er uniform.
Hint: Find en nøgle, som afbildes på den samme hash-værdi, uanset hvilken af hash-funktionerne i $\mathcal{H}$ der vælges.