UNIVERSITETET I OSLO

Det matematisk-naturvitenskapelige fakultet

Eksamen i: MAT 2250 — Kalkulus

Eksamensdag: 15. juni 2022

Tid for eksamen: 15.00 – 19.00

Oppgavesettet er på 3 sider.

Vedlegg: Ingen

Tillatte hjelpemidler: Ingen

Kontroller at oppgavesettet er komplett før
du begynner å besvare spørsmålene.

Eksamen inneheld 13 deloppgaver som kvar tel 5 eller 10 poeng. Du skal grunngje alle svar og vise nok mellomrekning til at ein lett kan følgje argumenta dine.

Oppgave 1

La $G = (H, K)$ vere ein graf med $|H| \times |K|$ insidensmatrise

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

1a (5pt)

Tegn grafen G.

1b (5pt)

Skriv opp $|H| \times |H|$ nabomatrisen til G.

(Fortsettes på side 2.)

1c (10pt)

Kva tyder det at ein graf er Eulersk eller Hamiltonsk? Er grafen G Eulersk eller Hamiltonsk? Grunngje svaret.

1d (10pt)

Finn antall utspenningstrær i G. Grunngje svaret (gjerne med tekning).

Oppgave 2

Ein permutasjon av tala $\{1, .., n\}$ er ein bijektiv avbilding

$$\pi : \{1, .., n\} \to \{1, .., n\}.$$

Lat $A_{n,k}$ vere antalet permutasjoner av $\{1, .., n\}$ med nøyaktig k tal i slik at $\pi(i) < \pi(i+1)$. For eksempel er $A_{3,0} = 1, A_{3,1} = 4$ og $A_{3,2} = 1$.

2a (5pt)

Finn $A_{4,0}, A_{4,1}, A_{4,2}$ og $A_{4,3}$.

2b (10pt)

Vis rekursjonen

$$A_{n,k} = (n-k)A_{n-1,k-1} + (k+1)A_{n-1,k} \quad n > 0$$

der du set $A_{0,0} = 1, A_{0,k} = 0 \quad (k > 0)$.

Oppgave 3

Lat $C \subset \{0,1\}^6$ vere den binære koden

$$C = \{000000, 110100, 101110, 011011, 100111\}$$

3a (5pt)

Er C en lineær kode? Grunngje svaret.

(Fortsettes på side 3.)

3b (5pt)

Finn minimumsavstanden til koden, den minste Hammingavstanden mellom kodeord.

3c (10pt)

Finn eit ord $v \in \{0,1\}^6$ som har Hammingavstand 1 til nøyaktig eitt kodeord i C. Kva er den største t slik at koden C finn t feil? Kva er den største t slik at koden retter t feil?

3d (10pt)

Finn ein syklisk kode i $\{0,1\}^6$ med minimumsavstand 2?

Oppgave 4

Anna og Bjørn utveksler krypterte meldinger, og bruker RSA protokollen. Anna offentliggjør $(n,k) = (33,3)$ som sine (offentlege) nøklar.

4a (5pt)

Kva er Annas private nøkkel? Grunngje svaret.

4b (5pt)

Bjørn vil sende meldingen "8" til Anna etter å ha kryptert den med RSA protokollen og Annas offentlege nøklar. Hvilken kryptert melding sender Bjørn? Vis korleis du kom fram til svaret.

4c (10pt)

Bjørns offentlege nøklar er $(n,k) = (33,7)$. Anna skriv ein koda melding med bokstavane $A = 01, B = 02, C = 03, ..., J = 10, K = 11, ...$, krypterer den koda meldingen med Bjørns offentlege nøklar og får

$$27 \quad 20 \quad 13 \quad 16 \quad 01 \quad 28$$

Bjørn dekrypterer med sin private nøkkel. Kva er meldingen?