Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristian Gjøsteen 73 55 02 42

EKSAMEN I TMA4185 KODETEORI

Bokmål
Tirsdag 24. mai 2011
Tid: 0900-1300
Sensurdato: 14. juni 2011
Alle trykte og håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

Alle deloppgaver teller likt. Alle svar skal begrunnes.

Oppgave 1 I denne oppgaven skal vi arbeide med kroppen $\mathbb{F}_8$, vektorrommet $\mathbb{F}_8^7$ og ringen $\mathbb{F}_8[x]/\langle x^7+1\rangle$. Som vektorrom er de to sistnevnte isomorfe, og vi bruker isomorfien

$$(c_0, c_1, \ldots, c_6) \longmapsto c_0 + c_1x + \cdots + c_6x^6 + \langle x^7+1\rangle.$$

La α være et primitivt element i kroppen som tilfredsstiller $\alpha^3+\alpha+1=0$.

La $\mathcal{C}_1$ være den sykliske koden av lengde 7 over $\mathbb{F}_8$ generert av $g(x) = x^4 + (\alpha+1)\,x^3 + x^2 + \alpha x + (\alpha+1)$.

a) Hva er dimensjonen til $\mathcal{C}_1$? Hva er nullpunktene til $\mathcal{C}_1$? Hva er minimumsavstanden til $\mathcal{C}_1$?

b) Finnes det koder av lengde 7 over $\mathbb{F}_8$ med samme minimumsavstand som $\mathcal{C}_1$, men med flere kodeord?

c) Vis at

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha+1 & \alpha & 1 & \alpha+1 \\ 0 & 1 & 0 & \alpha^2+1 & \alpha^2+1 & 1 & \alpha^2 \\ 0 & 0 & 1 & \alpha^2+\alpha+1 & \alpha^2+\alpha & 1 & \alpha^2+\alpha \end{pmatrix}$$

er en generatormatrise for $\mathcal{C}_1$. Finn en paritetssjekkmatrise for $\mathcal{C}_1$ og sjekk om vektoren $\mathbf{c} = (\alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, 1, \alpha, \alpha^2, \alpha+1)$ er med i koden.

d) $\mathcal{C}_1$ er en Reed-Solomon-kode og dermed en MDS-kode. En melding $\mathbf{m}$ ble kodet med generatormatrisen G. Deretter ble noen koordinater i kodeordet strøket under overføring med resultatet $(-, \alpha, -, 1, -, -, 1)$, der $-$ betegner en strykning. Finn $\mathbf{m}$.

I resten av oppgaven skal vi se på hvordan vi kan dekode Reed-Solomon-koder når det i tillegg til strykninger (feil med kjent posisjon) også er feil (med ukjent posisjon).

Anta at vi har en Reed-Solomon-kode $\mathcal{C}$ med nullpunkter $\{1, 2, \ldots, \delta - 1\}$. Vi har mottatt vektoren $\mathbf{y}$ som vi tolker som polynomet $y(x)$. Vi har syndromene $S_l = y(\alpha^l)$, $1 \leq l < \delta$.

Anta at det har skjedd t feil i posisjoner $j_1, j_2, \ldots, j_t$ med feilverdier $e_1, e_2, \ldots, e_t$. Anta også at $2t + 1 \leq \delta$. Da vet vi at syndromene $S_1, \ldots, S_{2t}$ tilfredsstiller

$$S_l = \sum_{i=1}^{t} e_i (\alpha^{j_i})^l. \tag{1}$$

Uten strykninger vet vi at det finnes et feillokaliseringspolynom $\sigma(x) = \sum_{i=0}^{t} \sigma_i x^i$, $\sigma_0 = 1$, som tilfredsstiller

$$\sum_{i=0}^{t} \sigma_i S_{l+t-i} = 0,\ 1 \leq l \leq t. \tag{2}$$

e) Anta at vi i tillegg til t feil også har s strykninger. For hvilke s og t er riktig dekoding mulig?

Hvis strykningene er på posisjoner $j'_1, j'_2, \ldots, j'_s$ der kodeordet hadde verdiene $d_1, d_2, \ldots, d_t$, vis at syndromene tilfredstiller

$$S_l = \sum_{i=1}^{t} e_i (\alpha^{j_i})^l + \sum_{i=1}^{s} d_i (\alpha^{j'_i})^l. \tag{1'}$$

f) Vi bruker koden $\mathcal{C}_1$ som beskrevet over, og har mottatt $\mathbf{y} = (-, 1, -, 1, 0, 1, 1)$. Erstatt strykningene med 0 og regn ut syndromene.

g) La $\sigma(x) = \prod_{i=1}^{t}(1 - x\alpha^{j_i}) = \sum_{i=0}^{t} \sigma_i x^i$ og $\tau(x) = \prod_{i=1}^{s}(1 - x\alpha^{j'_i}) = \sum_{i=0}^{s} \tau_i x^i$ være lokaliseringspolynomer for henholdsvis feilene og strykningene. Definer nye syndromer som

$$T_l = \sum_{i=0}^{s} \tau_i S_{l+s-i}, 1 \leq l \leq d - s - 1.$$

Vis at

$$\sum_{i=0}^{t} \sigma_i T_{l+t-i} = 0,\ 1 \leq l \leq t. \tag{2'}$$

Hint: Uttrykk T_l som en sum på formen $\sum_{i=1}^{t} E_i(\alpha^{j_i})^l$.

h) Vi bruker koden $\mathcal{C}_1$ som beskrevet over, og har mottatt $\mathbf{y} = (-, 1, -, 1, 0, 1, 1)$ kodet med generatormatrisen G. Gitt at det har skjedd tre feil under overføring og at vi vet at det er feil på plass 1 og 3, finn syndromene, posisjonen til den siste feilen og dekodingen.

Hint: Trenger du å finne hele kodeordet?

Oppgave 2 Bruk konvolusjonskoden gitt ved generatormatrisen $(1 + D^3 \quad 1 + D + D^3)$ til å kode meldingen 01 01 01 01 00 00.