DATO: 28. november 1995

HØGSKOLEN I STAVANGER

Institutt for elektroteknikk og databehandling

EKSAMEN I: 4542 Informasjonsteori og feilkorrigerende koding

VARIGHET: 5 timer

TILLATTE HJELPEMIDLER: Kalkulator

OPPGAVESETTET BESTÅR AV 4 SIDER

MERKNADER: Noen nyttige formler er oppgitt på siste side.

Oppgave 1

En kilde S genererer 6 forskjellige symboler med sannsynlighet $P(s_1), \ldots, P(s_6)$. Tabell 1 viser endel mulige koder for kilden.

Symbol	$P(s_i)$	A	B	C	D	E	F
s_1	$\frac{1}{2}$	000	0	0	0	0	0
s_2	$\frac{1}{4}$	001	01	10	10	10	100
s_3	$\frac{1}{16}$	010	011	110	110	1100	101
s_4	$\frac{1}{16}$	011	0111	1110	1110	1101	110
s_5	$\frac{1}{16}$	100	01111	11110	1011	1110	111
s_6	$\frac{1}{16}$	101	011111	111110	1101	1111	001

Tabell 1: 6 mulige koder for S.

a) Finn kildens entropi, $H(S)$.

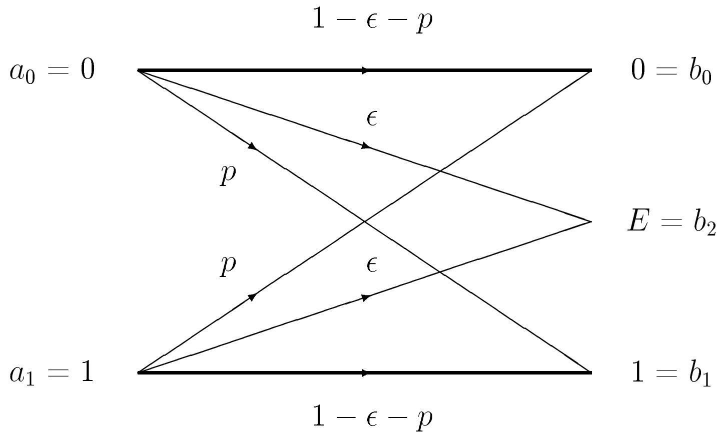
b) Hvilke koder er *entydig dekodbare*? Begrunn hvert svar kort.

c) Hvilke koder er *instantane*? Begrunn hvert svar kort.

d) Finn midlere kodeordslengde for hver av kodene. Sammenlign med svaret i a), og kommentér kort.

Oppgave 2

Ved dataoverføring hender det at feil oppstår på en slik måte at mottakeren vet *hvor* feilen er oppstått. Et eksempel på slike datafeil er en diskstasjon hvor det er mekaniske skader på disketten: De lagrede dataene er utradert i visse områder, og en vet dermed hvor bitfeilene ligger. I denne oppgaven skal vi se på en modell for en slik dataoverføring. Figur 1 viser en binær, symmetrisk kanal med utraderingssannsynlighet ϵ.



Figur 1: Binær, symmetrisk kanal med utradering (E står for "erasure").

a) Finn sannsynlighetene for de mottatte symbolene, uttrykt ved $p(a_0)$ og kanalparameterne.

b) Finn kanalkapasiteten som en funksjon av p og ϵ.

c) Se på spesialtilfellene $p = 0$ og $\epsilon = 0$ og plott i begge tilfeller kanalkapasiteten som en funksjon av den andre variabelen. Gitt valget mellom en vanlig binær, symmetrisk kanal med bitfeilsannsynlighet $p = 0.125$ og en ren utraderingskanal med $\epsilon = 0.5$, hvilken ville du foretrekke? Fortolk konklusjonen.

Oppgave 3

En (N, K) lineær blokk–kode er definert ved paritetsjekkmatrisen $\mathbf{H}$, gitt ved

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}. \qquad (1)$$

a) Hvor mange feil kan denne koden korrigere? Begrunn svaret.

b) Finn en generatormatrise $\mathbf{G}$ som svarer til paritetsjekkmatrisen, dvs. slik at $\mathbf{GH}^T = \mathbf{0}$. Hva blir N og K?

c) Anta at et kodeord sendes, og at et ukjent antall feil oppstår ved overføring. Finn syndromet som svarer til mottatt sekvens $\mathbf{y} = (1\ 0\ 0\ 1\ 1\ 0)$. Hva blir dekodet ord når vi foretar "maximum–likelihood" (ML) dekoding? Du kan anta at bitfeilsannsynligheten er mindre enn 0.5.

d) Er koden *perfekt*? Begrunn kort svaret.

Oppgave 4

a) Forklar hva vi mener med en *syklisk, lineær, blokk*–kode. Hvilke fordeler har en ved at koden er syklisk?

b) En binær kode kan defineres ved hjelp av et generatorpolynom, $g(D)$. Forklar hvordan $g(D)$ kan brukes til å generere *systematiske* og *ikke–systematiske* koder. Tegn også to kretser, hver bestående av et skift–register som realiserer koderen.

c) Vis at dersom vi har en blokklengde N, så må $g(D)$ være faktor av polynomet $D^N - 1$, dvs. $D^N - 1 = g(D)h(D)$, dersom koden generert av $g(D)$ skal være syklisk.

Vi skal i resten av denne oppgaven studere to binære BCH–koder. En slik kode fås syklisk ved at $g(D)$ dannes ved en faktorisering av $D^N - 1$. For å få til dette kan en se på den utvidede Galois–kroppen, $GF(2^m)$, hvor $N = 2^m - 1$. Alle nullpunktene til $D^N - 1$ er da gitt ved de 2^m elementene i $GF(2^m)$, unntatt 0-elementet. I denne oppgaven setter vi blokklengden til $N = 7$.

d) Konstruér den utvidede kroppen $GF(2^3)$ via det primitive polynomet $p(D) = D^3 + D^2 + 1$.

e) Finn $g(D)$ når vi setter $t = 1$. Hvor mange databit K kodes i hvert kodeord?

f) Finn $g(D)$ når vi setter $t = 2$. Hvor mange databit K kodes i hvert kodeord? Hva slags kode er dette?

g) Finn paritetsjekkpolynomet til koden i forrige deloppgave. Hvordan kan vi her bruke polynomet til å sjekke om mottatt ord er et kodeord?

h) Hva er minste Hamming–avstand for de to BCH–kodene du har konstruert?

i) Koden i f) kan faktisk rette 3 feil. Stemmer dette med formelen for generatorpolynomet for BCH–koder? Begrunn svaret.

Oppgitte formler:

- Betinget entropi:

$$H(B|A) = \sum_{A,B} p(a,b) \log_2 \frac{1}{p(b|a)} \tag{2}$$

- Minimalpolynomet til $\alpha^j \in GF(2^m)$ er gitt ved

$$\phi_{\alpha^j}(D) = \prod_{i=0}^{l-1} (D + (\alpha^j)^{2^i}), \tag{3}$$

  hvor l er største heltall slik at α^j, $(\alpha^j)^2$, $(\alpha^j)^{2^2}$, $(\alpha^j)^{2^3}$,...,$(\alpha^j)^{2^{l-1}}$ er forskjellige.

- Generatorpolynomet til en binær BCH–kode som kan rette t feil kan skrives som

$$g(D) = LCM[\phi_\alpha(D), \phi_{\alpha^3}(D), \phi_{\alpha^5}(D), \ldots, \phi_{\alpha^{2t-1}}(D)], \tag{4}$$

  hvor $\phi_{\alpha^j}(D)$ er minimalpolynomet til α^j, α er et primitivt element i $GF(2^m)$ og LCM betyr minste felles multiplum.