HØGSKOLEN I STAVANGER

Institutt for elektroteknikk og databehandling

Stavanger, 9. mai 1995

Utlevering: 24/3/95
Innlevering: 7/4/95

Digital transmisjon: Øving 5

Oppgave 1 Morsom

Hamming-koden: En Hammingkode med blokkstørrelse $n = 7$ kan rette opp én bitfeil. En slik kode er en såkalt $(7,4)$ blokk kode fordi en bruker 4 av 7 binære symboler i en blokk av 7 til selve informasjonen. De resterende 3 bit brukes til paritetsinformasjon (svarer til introduksjon av redundans på sendersiden). Et kodeord for en kildestreng av 4 binære symboler, $d_0d_1d_2d_3$, vil se ut som følger:

$$p_0p_1d_0p_2d_1d_2d_3 \tag{1}$$

der p_0, p_1 og p_2 er *paritetsbit* som beregnes slik:

$$\begin{aligned} p_0 &= d_0 \oplus d_1 \oplus d_3 \\ p_1 &= d_0 \oplus d_2 \oplus d_3 \\ p_2 &= d_1 \oplus d_2 \oplus d_3 \end{aligned} \tag{2}$$

$\oplus$ betegner addisjon modulo 2 ($0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$). $d_0, \ldots, d_3$ er databitene i den meldingen vi ønsker å overføre.

Eksempel: Anta at vi ønsker å sende den binære meldingen

$$00111010. \tag{3}$$

Vi deler meldingen opp i to grupper hver med 4 binære symboler; 0011 og 1010. Paritetsbitene beregnes ved:

$$\begin{aligned} p_0 &= 0 \oplus 0 \oplus 1 &= 1 \\ p_1 &= 0 \oplus 1 \oplus 1 &= 0 \\ p_2 &= 0 \oplus 1 \oplus 1 &= 0 \end{aligned} \tag{4}$$

for første gruppe og

$$\begin{aligned} p_0 &= 1 \oplus 0 \oplus 0 &= 1 \\ p_1 &= 1 \oplus 1 \oplus 0 &= 0 \\ p_2 &= 0 \oplus 1 \oplus 0 &= 1 \end{aligned} \tag{5}$$

Sven Ole Aase
Førsteamanuensis, dr.ing.
Høgskolen i Stavanger
Institutt for elektroteknikk og databehandling
Postboks 2557 Ullandhaug
4004 Stavanger
Tel.: 51 83 20 09
Fax.: 51 83 17 50
E-mail: aase@hsr.no

for den andre. Utsendte kodeord blir dermed:

$$1000011 \qquad 1011010 \tag{6}$$

Anta at for hver gruppe av 7 binær symboler er *ett* blitt overført feil over vår kanal. La oss anta at mottatt melding er:

$$10\underline{1}0011 \qquad 1011\underline{1}10 \tag{7}$$

Dekoding foregår på følgende vis: (for å antyde at mottatte binære symboler kan være ulik de sendte, merkes de med "hatt"). En beregner *syndromene* s_0, s_1 og s_2 ved:

$$\begin{aligned} s_2 &= \hat{p_0} \oplus \hat{d_0} \oplus \hat{d_1} \oplus \hat{d_3} \\ s_1 &= \hat{p_1} \oplus \hat{d_0} \oplus \hat{d_2} \oplus \hat{d_3} \\ s_0 &= \hat{p_2} \oplus \hat{d_1} \oplus \hat{d_2} \oplus \hat{d_3} \end{aligned} \tag{8}$$

Strengen $s_0 s_1 s_2$ vil nå peke på den posisjon i motttatt kodeord hvor feil binært symbol er mottatt ($s_0 s_1 s_2 = 000$ angir at ingen feil er detektert). Anvendt på ovenstående eksempel får en for første gruppe av 7 mottatte binære symboler

$$\begin{aligned} s_2 &= 1 \oplus 1 \oplus 0 \oplus 1 &= 1 \\ s_1 &= 0 \oplus 1 \oplus 1 \oplus 1 &= 1 \\ s_0 &= 0 \oplus 0 \oplus 1 \oplus 1 &= 0 \end{aligned} \tag{9}$$

Dette indikerer en feil i posisjon $s_0 s_1 s_2 = 011 = 3_{10}$. Dermed kan vi, hvis vi er sikre på at det kun er her det er feil, rette opp feilen og dekode meldingen som 0011.

For andre gruppe får en

$$\begin{aligned} s_2 &= 1 \oplus 1 \oplus 1 \oplus 0 &= 1 \\ s_1 &= 0 \oplus 1 \oplus 1 \oplus 0 &= 0 \\ s_0 &= 1 \oplus 1 \oplus 1 \oplus 0 &= 1 \end{aligned} \tag{10}$$

Dette indikerer en feil i posisjon $s_0 s_1 s_2 = 101 = 5_{10}$. Dermed kan vi, hvis vi er sikre på at det kun er her det er feil, rette opp feilen og dekode meldingen som 1010.

Konklusjon: (7,4) Hamming-koden kan rette opp feil i inntil ett bit når 4 informasjonsbit kodes ved bruk av kodeord med 7 binære symboler. Hamming-koden er altså et eksempel på at en kan oppnå mer pålitelig informasjonsoverføring gjennom introduksjon av redundans.

Så til oppgaven:

a) Finn kodeordene til alle kombinasjoner av 4 informasjonsbit. Kontroller gjerne mot tabell 6.6 i *Bissel & Chapman*. Hva er kodens effektivitet?

b) Definér Hammingavstanden mellom to kodeord som antallet bitposisjoner der de to kodeordene er forskjellige. Hva er minste Hammingavstand, d_{min}, for koden du konstruerte i forrige delspørsmål? Hvor mange feil kan koden *korrigere*? Begrunn svaret.

c) Hammingkoden er et eksempel på en *lineær* blokk-kode. Det betyr at dersom $\mathbf{c}_i$ og $\mathbf{c}_j$ er kodeord, så vil ogsaa

$$\mathbf{c}_k = \mathbf{c}_i \oplus \mathbf{c}_j \tag{11}$$

være et kodeord (her betyr $\oplus$ bit-for-bit modulo-2 addisjon). Summen av 2 kodeord vil altså alltid danne et annet kodeord. Det betyr at

$$d_H(\mathbf{c}_i, \mathbf{c}_j) = w(\mathbf{c}_k), \tag{12}$$

hvor $w(\mathbf{c}_k)$ betyr vekten, eller antall enere, i kodeordet $\mathbf{c}_k$. Denne egenskapen kan brukes til lettere å finne d_{min} – istedetfor å måtte regne ut Hammingavstanden mellom alle mulige kombinasjoner av to kodeord. Finn en alternativ måte å gjøre dette på, og sjekk om du får samme svar for d_{min} som i b).
Og dessuten: Kan du se hvordan man med den nye metoden lett kan finne d_{min} for en *foldingskode*, når vi vet at denne også er lineær?

d) Dekod, med eventuell feil-korrigering, følgende kodeord når vi vet at hvert kodeord har maksimalt en bitposisjon feil:

$$\begin{array}{c} 0011101 \\ 1011001 \\ 0110010 \\ 0111011 \\ 1000101 \end{array} \tag{13}$$

e) Hva skjer hvis fremgangsmåten blir brukt på mottatte kodeord med mer enn én feil?

f) Vi antar at sannsynligheten for bitfeil er konstant, og gitt ved $P_e = 10^{-5}$, dvs vi har en stasjonær kanal. Det betyr at dersom vi ikke bruker koding for feilbeskyttelse, så vil ett av 10^5 overførte databit i gjennomsnitt være feil. Estimer feilsannsynligheten når (7,4) Hammingkoden benyttes.
Hint: For å forenkle beregningen kan du anta at man ved dekoding til feil kodeord i gjennomsnitt får 2 bitfeil i $d_0d_1d_2d_3$. Bruk binomisk fordeling.