SF2715 Applied Combinatorics
Supplementary exercises
Part 5

Jakob Jonsson

17 maj 2011

Innehåll

Ö Övningsuppgifter

The exercises are in Swedish. If you have trouble understanding them ask the course teacher, Svante Linusson.

Ö.1 Två koder med sju kodord

(a) Låt C vara koden bestående av följande sju kodord av längd 10:

$$a = 00000\,00000$$
$$b = 11000\,11100$$
$$c = 00110\,01110$$
$$d = 10001\,00111$$
$$e = 01100\,10011$$
$$f = 00011\,11001$$
$$g = 11111\,11111$$

Beräkna avståndet mellan varje par av kodord i C, och ange det minimala avståndet i C.

(b) Låt C' vara koden bestående av följande sju kodord av längd 11:

$$\begin{aligned} a &= 00000\,00000\,0 \\ b &= 11000\,11100\,1 \\ c &= 00110\,01110\,1 \\ d &= 10001\,00111\,1 \\ e &= 01100\,10011\,1 \\ f &= 00011\,11001\,1 \\ g &= 11111\,11111\,0 \end{aligned}$$

Vi lägger alltså till en bit till vart och ett av kodorden i (a). Beräkna avståndet mellan varje par av kodord i C', och ange också det minimala avståndet i C'.

Svårighetsgrad: E

Ö.2 Övre och nedre gränser på binära koder av längd 90

(a) Visa att det finns en 1-rättande binär kod av längd 90 med 2^{78} element.

(b) Visa att det inte finns någon 2-rättande binär kod av längd 90 med fler än 2^{78} element.

Svårighetsgrad: D

Ö.3 Tillämpning av Plotkin-gränsen

(a) Låt $q \geq 2$, och låt d vara ett positivt heltal sådant att $d-1$ är delbart med $q-1$. Definiera

$$n = \frac{qd-1}{q-1} = d + \frac{d-1}{q-1}.$$

Använd Plotkin-gränsen för att visa att qd är en övre begränsning på antalet kodord i en kod av längd n över ett alfabet av storlek q med egenskapen att kodens minimala avstånd är d.

(b) Låt C vara den binära kod som består av följande 8 kodord av längd 7:

$$\begin{aligned} a &= 0000\,000 \\ b &= 1111\,000 \\ c &= 1100\,110 \\ d &= 0011\,110 \\ e &= 1010\,101 \\ f &= 0101\,101 \\ g &= 1001\,011 \\ h &= 0110\,011 \end{aligned}$$

Beräkna avståndet mellan varje par av kodord i C.

(c) Finns det någon kod av längd 7 med fler än 8 kodord och med samma minimala avstånd som C?

Svårighetsgrad: (a): C, (b): E, (c): E

Ö.4 Utvidgad kod I

Låt C vara en e-rättande kod vars kodord har längd n. Låt $k \geq 1$. För ett givet kodord c, definiera c^k att vara det ord av längd kn som man erhåller om man upprepar ordet c sammanlagt k gånger. Exempelvis är $(0111)^3 = (0111\ 0111\ 0111)$. Låt

$$C^{(k)} = \{c^k : c \in C\}.$$

(a) Visa att $C^{(k)}$ är e_k-rättande, där e_k är lika med $ke + \frac{k-1}{2}$ avrundat nedåt.

(b) Anta att en avkodningsmetod för C är given. För ett givet ord w av längd n kan vi alltså beräkna det unika kodord $c \in C$ med egenskapen att Hammingavståndet mellan c och w är högst e (om ett sådant kodord c finns). Definiera en avkodningsmetod för $C^{(k)}$ i termer av denna avkodningsmetod. Avkodningsmetoden ska fungera för alla ord som är på Hammingavstånd högst e_k från något ord i $C^{(k)}$, där e_k är definierat som i (a).

Svårighetsgrad: (a): D, (b): A

Ö.5 Dubbla antalet kodord

Låt C vara en binär kod av längd n med minimalt avstånd d sådan att alla kodord består av högst $\frac{n-d}{2}$ ettor. Utvidga C till en binär kod av längd n med dubbelt så många kodord som C och med samma minimala avstånd d.

Svårighetsgrad: B

Ö.6 Linjär kod I

Låt C vara den binära linjära kod av längd 11 som har generatormatris

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

(a) Avgör om C är 2-rättande. Motivera ditt svar med ett bevis eller motexempel.

(b) Bestäm en kontrollmatris (*check matrix*) till C.

(c) Vad är den maximala storleken på en binär 2-rättande linjär kod av längd 11? *Ledning:* Studera Hamming-gränsen.

Svårighetsgrad: (a): E, (b): E, (c): C

Ö.7 Linjär kod II

Låt nu C vara den binära linjära kod av längd 11 som har *kontrollmatris*

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

(a) Hur många kodord innehåller C?

(b) Visa att C är 1-rättande.

(c) Bestäm en generatormatris till C.

(d) Bestäm bitarna a_1, a_2, a_3, a_4 så att vektorn

$$w = (a_1, a_2, a_3, a_4, 1, 1, 0, 1, 1, 0, 0)$$

blir ett kodord.

Svårighetsgrad: E

Ö.8 Linjär kod III

Låt C vara den binära linjära kod av längd 11 som har generatormatris

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

(a) Avgör om C är 2-rättande. Motivera ditt svar med ett bevis eller motexempel.

(b) Bestäm en kontrollmatris till C.

Svårighetsgrad: E

Ö.9 Utvidgad kod II

Låt C vara en linjär e-rättande binär kod av längd n med 2^k kodord.

(a) Låt C' vara den binära koden av längd $3n$ bestående av alla tripplar $(a, b, a + b)$, där $a, b \in C$. Visa att C' är $2e$-rättande och består av 2^{2k} kodord.

(b) Låt nu C' vara den binära koden av längd $6n$ bestående av alla följder $(a, b, c, a + b, a + c, b + c)$, där $a, b, c \in C$. Visa att C' är $(3e + 1)$-rättande och består av 2^{3k} kodord.

Svårighetsgrad: (a): C, (b): B

Ö.10 Brus som skapar sviter av fel

I en tillämpning har man tillgång till en brusig kanal genom vilken man kan skicka binära ord av längd n. Tråkigt nog kan godtyckligt många bitar i ett givet ord bli felaktiga, men i gengäld bildar de felaktiga bitarna alltid en sammanhängande svit i ordet. Skickar vi ordet $(a_1, \ldots, a_n)$ blir slutresultatet alltså antingen ordet självt eller ett ord på formen

$$(a_1, \ldots, a_{i-1}, \overline{a_i}, \overline{a_{i+1}}, \ldots, \overline{a_{j-1}}, \overline{a_j}, a_{j+1}, \ldots, a_n),$$

där $1 \leq i \leq j \leq n$; $\overline{a_k} = 1 - a_k$.

Låt nu C vara en binär 2-rättande kod av längd n, alltså samma längd som på de ord som kan skickas genom kanalen. Man vill definiera en transformation $\varphi : C \to \{0,1\}^n$ med följande egenskap för varje kodord $\mathsf{b} \in C$:

- Om $\varphi(\mathsf{b})$ skickas genom kanalen, så är b entydigt bestämt av det mottagna ordet.

Hitta en lämplig transformation φ, och visa att den har önskade egenskaper för varje val av C.

Svårighetsgrad: A

Ö.11 Fördjupningsuppgift: Kod bestående av multiplar av ett polynom

Låt $r \geq 1$, och låt $f(x)$ vara ett polynom av grad r över kroppen med q element, där q är en primtalspotens. Låt $k \geq 1$, och studera koden

$$C = \{f(x)g(x) : \deg g \leq k-1\}.$$

Här identifierar vi ett polynom $\sum_{i=0}^{r+k-1} a_i x^i$ med vektorn $(a_0, a_1, \ldots, a_{r+k-1})$, vilket innebär att C är en kod av längd $r+k$.

(a) Visa att C ej är 1-rättande om k är tillräckligt stort. *Ledning:* Studera Hamming-gränsen.

(b) Anta att $f(x)$ har en nollskild konstantterm. Visa att det finns ett polynom $g(x)$ sådant att $f(x)g(x) = x^N - b$ för något $N \geq 1$ och någon nollskild skalär b.

Ö.12 Fördjupningsuppgift: Polynombaserade koder

Låt $\mathbb{F}$ vara en ändlig kropp, och låt $x_1, \ldots, x_n$ vara olika element i $\mathbb{F}$. Låt $k \leq n$, och definiera

$$C = \{(f(x_1), \ldots, f(x_n)) : f \text{ polynom över } \mathbb{F} \text{ av grad högst } k-1\}.$$

Visa att C är en linjär kod över $\mathbb{F}$ med minimalt avstånd $n-k+1$.

Ledning. Använd faktorsatsen, som säger följande: Om f är ett polynom över $\mathbb{F}$ och $a_1, \ldots, a_k$ är olika element från $\mathbb{F}$ sådana att

$$f(a_1) = f(a_2) = \cdots = f(a_k) = 0,$$

så är

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)g(x)$$

för något polynom g.

(I fallet då $\{x_1, \ldots, x_n\}$ är lika med $\mathbb{F} \setminus \{0\}$ är koden en så kallad Reed-Solomon-kod. Felkorrigering med Reed-Solomon-koder används i bland annat CD- och DVD-skivor och vid en rad former av dataöverföring.)

Lösningsförslag till övningsuppgifter, del V

Obs! Preliminär version!

Ö.1.

(a) Vi kan lösa uppgiften genom att helt enkelt räkna ut avståndet mellan vart och ett av de $\binom{7}{2} = 21$ paren. Först noterar vi att de fem orden b, c, d, e och f alla innehåller fem ettor. Eftersom a inte innehåller några ettor och g innehåller maximala tio ettor är dessa båda ord på avståndet 10 från varandra och på avståndet 5 från övriga kodord. Det återstår att beräkna avståndet mellan orden b, c, d, e och f. Genom att göra detta för hand noterar man att alla avstånd är exakt 6. Vi drar slutsatsen att det minimala avståndet i C är 5.

(b) Vi noterar följande:

- Avståndet mellan a och g är detsamma som i C, alltså 10.
- Avståndet är oförändrat mellan alla par i $\{b, c, d, e, f\}$, alltså 6.
- Avståndet har ökat med 1 mellan alla x och y sådana att $x \in \{a, g\}$ och $y \in \{b, c, d, e, f\}$, alltså 6.

Slutsatsen är att alla avstånd är 6 utom avståndet mellan a och g, vilket är 10. Det minimala avståndet är 6.

Ö.2.

(a) Låt $n = 90$ och $e = 1$. Enligt VG-gränsen (sats 17.4.1 i Cameron) finns det en e-rättande binär kod av längd n av storlek minst

$$\frac{2^n}{\sum_{k=0}^{2e}\binom{n}{k}} = \frac{2^{90}}{\sum_{k=0}^{2}\binom{90}{k}} = \frac{2^{90}}{1 + 90 + \frac{90\cdot 89}{2}} = \frac{2^{90}}{4096} = \frac{2^{90}}{2^{12}} = 2^{78}.$$

(b) Låt nu $n = 90$ och $e = 2$. Enligt Hamming-gränsen (sats 17.4.2 i Cameron) finns det ingen e-rättande binär kod av längd n av storlek överstigande

$$\frac{2^n}{\sum_{k=0}^{e}\binom{n}{k}} = \frac{2^{90}}{\sum_{k=0}^{2}\binom{90}{k}} = 2^{78}.$$

Ö.3.

(a) Plotkin-gränsen säger att

$$|C| \leq \frac{d}{d-\theta n},$$

där $\theta = 1 - 1/q = (q-1)/q$. I vårt fall är

$$\theta n = \frac{q-1}{q} \cdot \left(d + \frac{d-1}{q-1}\right) = \frac{(q-1)d + (d-1)}{q} = \frac{qd-1}{q} = d - \frac{1}{q}.$$

Detta ger att

$$|C| \leq \frac{d}{d-\theta n} = \frac{d}{d - d + \frac{1}{q}} = qd.$$

En kod med givna egenskaper har alltså storlek högst qd.

(b) Genom en direkt beräkning ser man att alla avstånd är 4. (Man kan underlätta sina beräkningar genom att notera vissa mönster i koden.)

(c) Enligt (a) innehåller en kod av längd $n = 7$ med minimalt avstånd $d = 4$ högst $n + 1 = 8$ kodord, ty $7 = 2 \cdot 4 - 1$. Svaret är alltså nej.

Ö.4.

(a) Att C är e-rättande innebär att C har minimalt avstånd minst $2e+1$. Låt c_1 och c_2 vara två olika kodord i C. Eftersom dessa båda ord skiljer sig åt på minst $2e+1$ positioner måste vi ha att c_1^k och c_2^k skiljer sig åt på minst $d' = k(2e+1)$ positioner. Alltså är $C^{(k)}$ e'-rättande för alla e' sådana att

$$e' \leq \frac{d'-1}{2} = \frac{k(2e+1)-1}{2} = ke + \frac{k-1}{2}.$$

(b) Studera ett ord $w = w_1 w_2 \dots w_k$, där varje w_i är ett ord av längd n. Anta att w är på avstånd högst e_k från $C^{(k)}$, och låt c^k var det unika kodord som är på avstånd högst e_k från w. Notera att det genomsnittliga avståndet mellan w_i och c är högst lika med

$$\frac{e_k}{k} \leq e + \frac{k-1}{2k} < e + 1.$$

Minst ett av orden $w_1, \dots, w_k$ är alltså på avstånd högst e från c. Använd nu avkodningsmetoden för C på vart och ett av orden $w_1, \dots, w_k$. För varje i sådant att w_i ligger på avstånd högst e från C får vi ut ett kodord c_i på avstånd högst e från w_i. Enligt ovan kommer c att finnas med bland de funna kodorden, och vi kan lätt bestämma vilket av kodorden som är c genom att beräkna avståndet mellan w och c_i^k för varje i. Kodordet c^k är nämligen unikt med egenskapen att avståndet till w är högst e_k.

Ö.5. För ett ord c, låt $\overline{c}$ vara ordet som erhålls om vi ersätter varje nolla med en etta och vice versa. Låt

$$\overline{C} = \{\overline{c} : c \in C\}.$$

Definiera $C' = C \cup \overline{C}$. Vi hävdar att denna kod har minimalt avstånd d och storlek $2|C|$. Låt $\delta(c_1, c_2)$ beteckna avståndet mellan två kodord c_1 och c_2. Studera två kodord i C'. Vi har tre fall:

- Båda kodorden tillhör C. Då är avståndet minst d enligt egenskaperna hos C.
- Båda kodorden tillhör $\overline{C}$ och är alltså på formen $\overline{c_1}$ och $\overline{c_2}$, där $c_1, c_2 \in \overline{C}$. Då är avståndet också minst d, ty $\delta(\overline{c_1}, \overline{c_2}) = \delta(c_1, c_2)$.
- Det ena kodordet tillhör C och det andra $\overline{C}$. Låt c_1 och $\overline{c_2}$ vara kodorden; $c_1, c_2 \in C$. Eftersom c_2 har ettor på högst $\frac{n-d}{2}$ positioner har $\overline{c_2}$ ettor på minst $n - \frac{n-d}{2} = \frac{n+d}{2}$ positioner, nämligen de positioner där c_2 har nollor. På högst $\frac{n-d}{2}$ av dessa positioner har c_1 en etta, vilket innebär att antalet positioner där c_1 och $\overline{c_2}$ har olika värden är minst

  $$\frac{n+d}{2} - \frac{n-d}{2} = d.$$

  Alltså är $\delta(c_1, \overline{c_2}) \geq d$.

Slutsatsen är att alla avstånd är minst lika med d. Vi ser också att C och $\overline{C}$ är disjunkta, vilket medför att antalet kodord i C' är $|C| + |\overline{C}| = 2|C|$.

Ö.6.

(a) Denna uppgift kan lösas genom att man helt enkelt bestämmer de 2^4 kodorden. I nedanstående tabell står a, b, c och d för de fyra kodorden i generatormatrisen.

$$
\begin{array}{lcccccccc}
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & & & & & & & & \\
1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0 & = & a & & & & & & \\
0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0 & = & & & b & & & & \\
0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1 & = & & & & & c & & \\
0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1 & = & & & & & & & d \\
1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0 & = & a & + & b & & & & \\
1\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1 & = & a & & & + & c & & \\
1\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1 & = & a & & & & & + & d \\
0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1 & = & & & b & + & c & & \\
0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1 & = & & & b & & & + & d \\
0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,0 & = & & & & & c & + & d \\
1\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1 & = & a & + & b & + & c & & \\
1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1 & = & a & + & b & & & + & d \\
1\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0 & = & a & & & + & c & + & d \\
0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0 & = & & & b & + & c & + & d \\
1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 & = & a & + & b & + & c & + & d
\end{array}
$$

Samtliga nollskilda vektorer innehåller minst 5 nollskilda element, vilket innebär att koden är e-rättande, där $e = (5-1)/2 = 2$.

(b) Låt I_k beteckna enhetsmatrisen med k rader och k kolumner. En kod med en generatormatris av storlek $k \times n$ på formen $[I_k \ A]$ har en kontrollmatris som är lika med $[-A^T \ I_{n-k}]$. I vårt fall är $k = 4$, $n = 11$ och $n - k = 7$, vilket innebär att kontrollmatrisen har storlek 7×11. Eftersom vi arbetar med binära tal kan vi bortse från minustecknet, vilket ger kontrollmatrisen

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

(Observera att kontrollmatrisen till en linjär kod inte är entydigt bestämd, utan det finns många tänkbara val.)

(c) En binär linjär kod har en storlek på formen 2^a för något heltal a. Det totala antalet binära ord av längd 11 är 2^{11}. Hamming-gränsen säger att en binär 2-rättande kod C av längd 11 uppfyller olikheten

$$
|C| \leq \frac{2^{11}}{1 + 11 + \binom{11}{2}} = \frac{2048}{67} \approx 30,6.
$$

Alltså är kodens storlek som mest $2^4 = 16$, ty $2^5 = 32 > \frac{2048}{67}$. Enligt (a) finns en linjär 2-rättande kod av storlek 16, vilket ger svaret 16.

Ö.7.

(a) C är lika med lösningsrummet till matrisekvationen $A \cdot w^T = 0$. Detta är ett ekvationssystem med 11 obekanta och 4 ekvationer. Eftersom ekvationerna är linjärt oberoende (de första fyra kolumnerna i A utgör en enhetsmatris) kommer lösningsrummet att ha rang $11 - 4 = 7$, vilket ger att C består av $2^7 = 128$ kodord.

(b) En linjär kod är 1-rättande om och endast om varje par av kolumner i kontrollmatrisen är linjärt oberoende (se Proposition 17.5.5 i Cameron). För binära koder innebär detta att ingen kolumn är lika med noll och att alla kolumner är olika. Eftersom detta uppenbarligen gäller följer påståendet.

(c) Precis som i lösningen till uppgift Ö.6 låter vi I_k beteckna enhetsmatrisen med k rader och k kolumner. En kod med en kontrollmatris av storlek $k \times n$ på formen $[I_k \ A]$ har en generatormatris som är lika med $[-A^T \ I_{n-k}]$. I vårt fall är $k = 4$, $n = 11$ och $n - k = 7$, vilket innebär att generatormatrisen har storlek 7×11. Eftersom vi arbetar med binära tal kan vi bortse från minustecknet, vilket ger generatormatrisen

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

(Observera att lösningen är identisk med lösningen till (b) i övningsuppgift Ö.6, sånär som på att vi har bytt plats på "kontrollmatris" och "generatormatris". Observera också att inte heller generatormatrisen till en linjär kod är entydigt bestämd. Även här finns många tänkbara val.)

(d) Det finns bara en linjärkombination av raderna i generatormatrisen i (c) som ger ett kodord som slutar med $(1, 1, 0, 1, 1, 0, 0)$, nämligen kombinationen bestående av raderna 1, 2, 4 och 5. Summering av dessa rader ger vektorn

$$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0),$$

vilket innebär att $(a_1, a_2, a_3, a_4) = (1, 1, 0, 0)$.

(En alternativ metod är att lösa ekvationen $A \cdot w^T = 0$, där A är kontrollmatrisen och $w = (a_1, a_2, a_3, a_4, 1, 1, 0, 1, 1, 0, 0)$.

Ö.8.

(a) Genom att studera de sexton kodorden i C upptäcker vi att summan av de fyra kodorden i generatormatrisen är

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

Detta är ett kodord med bara fyra nollskilda positioner, vilket ger att koden ej är 2-rättande.

(b) Precis som i lösningen till uppgift Ö.6 låter vi I_k beteckna enhetsmatrisen med k rader och k kolumner. För att lätt kunna hitta en kontrollmatris skriver vi om generatormatrisen så att vi får den på formen $[I_4\ A]$. För att åstadkomma detta adderar vi först den fjärde raden till den första och den tredje raden:

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

Sedan adderar vi den tredje raden till den andra raden och den resulterande andra raden till den första raden:

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

Nu är matrisen på formen $[I_4\ A]$. Matrisen $[-A^T\ I_7]$ är en kontrollmatris till koden. Denna matris ser ut på följande vis:

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

(Vi påminner om att kontrollmatrisen till en kod inte är entydigt bestämd, så det finns många andra korrekta svar.)

Ö.9.

(a) Det minimala avståndet i C är minst $d = 2e + 1$. Eftersom C är linjär är detta ekvivalent med att varje nollskilt kodord i C innehåller minst d ettor. Att C' är $2e$-rättande är ekvivalent med att det minimala avståndet i C' är minst $2 \cdot (2e) + 1 = 2d - 1$. Eftersom C' också är linjär räcker det att visa att varje nollskilt kodord i C' innehåller minst $2d - 1$ ettor.

Studera ett nollskilt kodord $c = (a, b, a + b)$ i C'. Vi delar in i fall:

- $a = 0$. Då är $c = (0, b, b)$, och b är nollskilt. Eftersom b innehåller minst d ettor kommer c att innehålla minst $2d$ ettor.
- $b = 0$. Då är $c = (a, 0, a)$, och a är nollskilt. Än en gång drar vi slutsatsen att c innehåller minst $2d$ ettor.
- a och b är båda nollskilda. Då har vi nollskilda kodord från C på de två första positionerna i c och därmed minst $2d$ ettor.

Alltså är det minimala avståndet i C' minst $2d$, vilket medför det önskade resultatet.

Eftersom antalet kodord i C' sammanfaller med antalet par (a, b) sådana att $a, b \in C$ har vi att $|C'| = |C|^2 = 2^{2k}$.

(b) Denna gång vill vi visa att varje nollskilt kodord i C' innehåller minst $3d = 6e + 3$ ettor. Detta medför nämligen att C' är $(3e + 1)$-rättande. Studera ett nollskilt kodord $(a, b, c, a + b, a + c, b + c)$. Att kodordet är nollskilt innebär att minst ett av orden a, b och c är nollskilt. Vi delar in i fall:

- a, b och c är alla nollskilda. Vi har då nollskilda kodord från C på de tre första positionerna och därmed minst $3d$ ettor.
- Något av orden a, b och c är lika med noll. Anta att $c = 0$; övriga fall är analoga. Vi har då att kodordet är lika med

$$(a, b, 0, a + b, a, b).$$

  - Om $a = 0$ måste b vara nollskilt. Kodordet blir $(0, b, 0, b, 0, b)$, och antalet ettor i detta ord är minst $3d$.
  - Om $b = 0$ får vi på samma sätt ett ord med minst $3d$ ettor.
  - Om a och b båda är nollskilda har vi nollskilda kodord från C på positionerna 1, 2, 5 och 6 och därmed minst $4d$ ettor.

Detta visar att det minimala avståndet i C' är minst $3d$, vilket avslutar beviset.

Eftersom antalet kodord i C' sammanfaller med antalet tripplar (a, b, c) sådana att $a, b, c \in C$ har vi att $|C'| = |C|^3 = 2^{3k}$.

Ö.10. Idén är att använda sig av det faktum att antalet övergångar mellan "felaktig bit" och "korrekt bit" alltid är högst två. Låt $\mathsf{b} = (b_1, \ldots, b_n)$ vara ett kodord. Vi definierar

$$\varphi(\mathsf{b}) = \mathsf{a} = (a_1, \ldots, a_n)$$

på följande vis: Sätt $a_0 = 0$ och $a_k = a_{k-1} + b_k$ för $1 \leq k \leq n$. Observera att

$$b_k = a_k - a_{k-1}$$

för $1 \leq k \leq n$.

Anta nu att vi skickar ordet a genom kanalen. Beteckna det mottagna ordet med $\mathsf{a}' = (a'_1, \ldots, a'_n)$, och sätt $a'_0 = 0$. Definiera ordet $\mathsf{b}' = (b'_1, \ldots, b'_n)$ som $b'_k = a'_k - a'_{k-1}$ för $1 \leq k \leq n$. Vi har att a' antingen är lika med a eller är ett ord på formen

$$(a_1, \ldots, a_{i-1}, \overline{a_i}, \overline{a_{i+1}}, \ldots, \overline{a_{j-1}}, \overline{a_j}, a_{j+1}, \ldots, a_n),$$

för något $i \leq j$. I det första fallet har vi att $\mathsf{b} = \mathsf{b}'$. I det andra fallet har vi att $b'_k = b_k$ för alla k utom $k = i$ och $k = j + 1$. Vi har nämligen att

$$b'_k = a'_k - a'_{k-1} = \begin{cases} a_k - a_{k-1} = b_k & \text{om } 1 \leq k \leq i-1, \\ \overline{a_k} - a_{k-1} = \overline{b_k} & \text{om } k = i, \\ \overline{a_k} - \overline{a_{k-1}} = b_k & \text{om } i+1 \leq k \leq j, \\ a_k - \overline{a_{k-1}} = \overline{b_k} & \text{om } k = j+1, \\ a_k - a_{k-1} = b_k & \text{om } j+2 \leq k \leq n. \end{cases}$$

Antalet fel är alltså högst 2. Med hjälp av vår 2-rättande kod kan vi därmed återskapa kodordet b från ordet b'.

Ö.11.

(a) Längden på koden är $n = r + k$, och storleken på koden är $|C| = q^k$. För att koden ska vara 1-rättande måste vi ligga under Hamming-gränsen:

$$\begin{aligned} |C| \leq \frac{q^n}{1 + n(q-1)^n} &\iff q^k \leq \frac{q^{r+k}}{1 + (r+k)(q-1)^{r+k}} \\ &\iff 1 + (r+k)(q-1)^{r+k} \leq q^r. \end{aligned}$$

Om vi väljer $k \geq q^r - r$ erhåller vi att

$$q^r \geq 1 + (r+k)(q-1)^{r+k} \geq 1 + (r+k) \geq 1 + q^r,$$

vilket är en motsägelse.

(b) Vi använder oss av (a). Låt k vara stort nog för att C inte ska vara 1-rättande. Det finns då ett nollskilt polynom $g(x)$ sådant att $f(x)g(x)$ har högst två nollskilda koefficienter. Detta följer av att koden C är linjär och ej 1-rättande. Vi kan anta att $g(x)$ har nollskild konstantterm; annars delar vi bara $g(x)$ med x^i, där i är minimalt sådant att koefficienten framför x^i i $g(x)$ är nollskild. Eftersom $f(x)$ har grad $r \geq 1$ och därmed inte är konstant måste $f(x)g(x)$ innehålla minst en nollskild term på formen $a_i x^i$, där $i \geq 1$. Eftersom $f(x)g(x)$ har en nollskild konstantterm och högst två nollskilda termer innebär det att $f(x)g(x) = a_0 + a_i x^i$ där a_0 och a_i är nollskilda. Genom att byta ut $g(x)$ mot $a_i^{-1} g(x)$ kan vi anta att $a_i = 1$, vilket avslutar beviset.

Ö.12. Skriv

$$f(\mathbf{x}) = (f(x_1), \ldots, f(x_n)).$$

För att visa att C är en linjär kod noterar vi att om f och g är polynom av grad högst $k-1$ och a och b är skalärer, så är

$$af(\mathbf{x}) + bg(\mathbf{x}) = (af + bg)(\mathbf{x}).$$

Detta är ett kodord i C, ty $af + bg$ är ett polynom av grad högst $k-1$. Alltså är C en linjär kod.

För att visa att C har minimalt avstånd $n-k+1$ antar vi att $f(\mathbf{x})$ är ett kodord med högst $n-k$ nollskilda element. Om vi kan visa att $f(\mathbf{x})$ är lika med noll kan vi dra slutsatsen att kodens minimala avstånd är minst $n-k+1$. Detta följer av att koden är linjär.

Enligt antagandet innehåller $f(\mathbf{x})$ minst k nollor. Det finns alltså k olika index $i_1, i_2, \ldots, i_k$ sådana att $f(x_{i_r}) = 0$ för $1 \leq r \leq k$. Faktorsatsen ger att vi kan skriva

$$f(x) = (x - x_{i_1})(x - x_{i_2}) \cdots (x - x_{i_k}) f_0(x),$$

där f_0 är ett polynom. Nu är f ett polynom av grad högst $k-1$, medan produkten $(x - x_{i_1})(x - x_{i_2}) \cdots (x - x_{i_k})$ är ett polynom av grad k. Därmed måste vi ha att $f_0 = 0$, vilket innebär att $f = 0$, alltså det vi ville visa.

Det som återstår att visa är att det minimala avståndet är precis $n-k+1$. Definiera

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_{k-1}).$$

Vi ser att $f(x_1) = f(x_2) = \cdots = f(x_{k-1}) = 0$, medan $f(x_i) \neq 0$ för $k \leq i \leq n$. Alltså är avståndet mellan $f(\mathbf{x})$ och nollvektorn precis $n-k+1$.