SF2715 Applied Combinatorics
Supplementary exercises
Part 5

Jakob Jonsson

10 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.)