Informations- och kodningsteori: Tenta 2004-08-19

Skrivtid: 14–19
Hjälpmedel:
Miniräknare, läroboken, utdelade stenciler, egna anteckningar.

• 1. Betrakta följderna $(1,1,2,2,3,3,3)$, $(1,1,2,2,3,3,3,3)$ och $(2,2,2,2,2,2,2,2,3,3)$. Vilka av dessa kan beskriva ordlängderna till någon ternär prefixfri kod? Ange en sådan kod i varje fall då det är möjligt!

• 2. Låt $\mathcal{S}$ vara en källa med 7 källsymboler med sannolikheter $0.4, 0.2, 0.1, 0.1, 0.1, 0.05, 0.05$. Beräkna den binära entropin $H_2(\mathcal{S})$ och medelordlängden i en optimal binär kod för $\mathcal{S}$. Ange alla kodorden i en sådan kod!

• 3. Betrakta koden $\mathcal{C} = \{01, 02, 100, 11, 20, 200\}$. Är denna kod prefixfri? Bevisa att koden $\mathcal{C}$ är entydigt avkoderbar.

• 4. Låt $\mathcal{C}$ vara den linjära kod över $\mathbb{Z}_3$ som har paritets-checks-matris

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 2 & 1 & 0 & 2 \\ 0 & 0 & 2 & 1 & 1 \end{pmatrix}$$

Ange $\mathcal{C}$'s dimension, dess hastighet (dvs "rate"), och en generatormatris för $\mathcal{C}$. Ange även $\mathcal{C}$'s minimalavstånd.

• 5. Låt $\mathcal{A}$ och $\mathcal{B}$ vara källor med alfabeten $\{a_1, a_2, a_3\}$ och $\{b_1, b_2, b_3\}$, respektive. Låt Γ vara en kanal från $\mathcal{A}$ till $\mathcal{B}$ med kanalmatris

$$\begin{pmatrix} 0.75 & 0.25 & 0 \\ 0 & 1 & 0 \\ 0.5 & 0 & 0.5 \end{pmatrix}$$

Låt a_1, a_2, a_3 ha sannolikheterna 0.4, 0.4, 0.2. Beräkna sannolikheterna för utdata-symbolerna b_1, b_2, b_3, de binära systementropierna $H(\mathcal{A}, \mathcal{B})$, $H(\mathcal{A}|\mathcal{B})$, $H(\mathcal{B}|\mathcal{A})$, och informationen $I(\mathcal{A}, \mathcal{B})$.

• 6. Beräkna kapaciteten för kanalen med kanalmatris $\begin{pmatrix} 0.7 & 0.3 \\ 0.5 & 0.5 \end{pmatrix}$.

Var god vänd!

• 7. Låt $\mathcal{C}$ vara den linjära koden över $\mathbb{Z}_2$ som har generatormatris

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

Ange en paritets-checks-matris till denna kod. Bestäm restklassledare och deras syndromer! Syndrom-avkodera sedan följande ord:

$$(0,1,1,0,0,1), \qquad (0,1,1,1,0,1), \qquad (1,1,0,1,1,1).$$

• 8. Låt Γ vara en kanal med inalfabete $\mathbb{Z}_2$ och utalfabete $T = \{0, 1, ?\}$, med kanalmatris

$$\begin{pmatrix} 0.9 & 0 & 0.1 \\ 0 & 0.9 & 0.1 \end{pmatrix}.$$

(Detta är en så kallad "Binary Erasure Channel".) Låt $\mathcal{A}$ vara den källa vars alfabete är $\mathbb{Z}_2^7$, och där sannolikheterna är $\frac{1}{16}$ för vart och ett av de 16 orden i en Hammingkod $\mathcal{H}_7 \subset \mathbb{Z}_2^7$, medan alla andra ord i $\mathbb{Z}_2^7$ har sannolikhet 0. För varje ord $w \in T^7$ låter vi q_w vara sannolikheten att w erhålls som utdata från kanalen Γ^7 då källan $\mathcal{A}$ tas som indata. Precis hur många ord $w \in T^7$ finns det som har sannolikhet $q_w \geqq \dfrac{9^4}{10^7}$?

LYCKA TILL!

Informations- och kodningsteori:
Lösningar till omtenta 2004-08-19.

• 1. Enligt Krafts olikhet så finns en ternär prefixfri kod med ordlängder $\ell_1, \ell_2, ..., \ell_r$ om och endast om $\sum_{j=1}^{r} 3^{-\ell_j} \leqq 1$. Vi beräknar:

$$3^{-1} + 3^{-1} + 3^{-2} + 3^{-2} + 3^{-3} + 3^{-3} + 3^{-3} = 1,$$

$$3^{-1} + 3^{-1} + 3^{-2} + 3^{-2} + 3^{-3} + 3^{-3} + 3^{-3} + 3^{-3} = \frac{28}{27} > 1,$$

$$3^{-2} + 3^{-2} + 3^{-2} + 3^{-2} + 3^{-2} + 3^{-2} + 3^{-2} + 3^{-2} + 3^{-3} + 3^{-3} = \frac{26}{27} < 1.$$

Alltså finns det inte någon prefixfri ternär kod med ordlängder $(1, 1, 2, 2, 3, 3, 3, 3)$, men i de andra två fallen går det bra.

Exempel på en prefixfri ternär kod med ordlängder $(1, 1, 2, 2, 3, 3, 3)$:

$$0, 1, 20, 21, 220, 221, 222.$$

Exempel på en prefixfri ternär kod med ordlängder $(2, 2, 2, 2, 2, 2, 2, 2, 3, 3)$:

$$00, 01, 02, 10, 11, 12, 20, 21, 220, 221.$$

• 2. Binär entropi:

$$H_2(\mathcal{S}) = -0.4 \cdot \log_2 0.4 - 0.2 \cdot \log_2 0.2 - 3 \cdot 0.1 \cdot \log_2 0.1 - 2 \cdot 0.05 \cdot \log_2 0.05$$
$$= 2.42192809...$$

Vi tar nu fram en optimal binär kod för $\mathcal{S}$. Enligt en känd sats är varje binär Huffmankod för $\mathcal{S}$ optimal; och en sådan Huffmankod kan tas fram så här

$\mathcal{S}$							0.4	0.2	0.1	0.1	0.1	0.05	0.05
$\mathcal{S}'$:						0.1	0.4	0.2	0.1	0.1	0.1		
$\mathcal{S}''$:					0.2	0.1	0.4	0.2	0.1				
$\mathcal{S}'''$:				0.2	0.2		0.4	0.2					
$\mathcal{S}^{(4)}$:			0.4	0.2			0.4						
$\mathcal{S}^{(5)}$:		0.6	0.4										
$\mathcal{S}^{(6)}$:	1.0												

$\mathcal{C}$							01	11	001	100	101	0000	0001
$\mathcal{C}'$:						000	01	11	001	100	101		
$\mathcal{C}''$:					10	000	01	11	001				
$\mathcal{C}'''$:				00	10		01	11					
$\mathcal{C}^{(4)}$:			1	00			01						
$\mathcal{C}^{(5)}$:		0	1										
$\mathcal{C}^{(6)}$:	ε												

(Tabellen med kodord fylls i baklänges, efter att hela tabellen med sannolikheter har utarbetats.)
Medelordlängd: $L(\mathcal{C}) = 1 + 0.6 + 0.4 + 0.2 + 0.2 + 0.1 = 2.5$.
Kodord: $01, 11, 001, 100, 101, 0000, 0001$.

• 3. Koden $\mathcal{C}$ är *ej* prefixfri, ty kodordet 20 är prefix till kodordet 200.
De rekursiva prefixmängderna är:

$$\begin{aligned}
&\mathcal{C}_0 = \mathcal{C} = \{01, 02, 100, 11, 20, 200\},\\
&\mathcal{C}_1 = \{0\},\\
&\mathcal{C}_2 = \{1, 2\},\\
&\mathcal{C}_3 = \{0, 00, 1\},\\
&\mathcal{C}_4 = \{00, 1, 2\},\\
&\mathcal{C}_5 = \{0, 00, 1\},\\
&\dots
\end{aligned}$$

(det fortsätter sedan periodiskt). Alltså blir $\mathcal{C}_\infty = \bigcup_{j=1}^{\infty} \mathcal{C}_j = \{0, 00, 1, 2\}$. Härur följer $\mathcal{C} \cap \mathcal{C}_\infty = \emptyset$. Alltså säger Sardinas-Pattersons sats att $\mathcal{C}$ *är entydigt avkoderbar.*

• 4. Vi ser från H's storlek att $\mathcal{C}$ är en linjär kod av längd $n = 5$, dvs $\mathcal{C} \subset \mathbb{Z}_3^5$, och av dimension $k = 5 - 3 = 2$. Alltså är $\mathcal{C}$'s hastighet: $R = k/n = 2/5$.

Vi söker nu en generatormatris. Vi har per definition att $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}_3^5$ är ett kodord i $\mathcal{C}$ om och endast om $\mathbf{x}H^T = 0$, dvs om och endast om:

$$\begin{cases}
x_1 + x_2 + x_4 + x_5 = 0 & \\
+ 2x_2 + x_3 + 2x_5 = 0 & (\cdot 2)\\
+ 2x_3 + x_4 + x_5 = 0 & (\cdot 2)
\end{cases}$$

$$\Leftrightarrow \begin{cases}
x_1 + x_2 + x_4 + x_5 = 0 & (-\text{ekv nr } 2)\\
+ x_2 + 2x_3 + x_5 = 0 & (+\text{ekv nr } 3)\\
+ x_3 + 2x_4 + 2x_5 = 0 &
\end{cases}$$

$$\Leftrightarrow \begin{cases}
x_1 + x_3 + x_4 = 0 & (-\text{ekv nr } 3)\\
+ x_2 + 2x_4 = 0 &\\
+ x_3 + 2x_4 + 2x_5 = 0 &
\end{cases}$$

$$\Leftrightarrow \begin{cases} x_1 & & & + 2x_4 & + x_5 & = 0 \\ & + x_2 & & + 2x_4 & & = 0 \\ & & + x_3 & + 2x_4 & + 2x_5 & = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x_1 = s + 2t \\ x_2 = s \\ x_3 = s + t \\ x_4 = s \\ x_5 = t \end{cases} \qquad (s, t \in \mathbb{Z}_3, \text{ godtyckliga}).$$

Alltså utgör $(1,1,1,1,0)$, $(2,0,1,0,1)$ en bas i lösningsrummet till ekvationen $\mathbf{x}H^T = 0$, så en generatormatris till $\mathcal{C}$ ges av:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Slutligen visar vi att $\mathcal{C}$ *har minimalavstånd* $d(\mathcal{C}) = 3$. (Det finns många sätt att visa detta, genom en eller annan uttömmande prövning.) Eftersom $(2,0,1,0,1) \in \mathcal{C}$ så är minimalavståndet *mindre än eller likamed* 3. Å andra sidan, antag att $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \in \mathcal{C}$ och $\mathbf{x} \neq 0$; enligt ovan kan vi då skriva $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) = (s + 2t, s, s+t, s, t)$ för några $s, t \in \mathbb{Z}_3$. Eftersom $\mathbf{x} \neq 0$ så är inte $s = t = 0$. Om *både* s och t är skilda från 0 så är $x_2 \neq 0$, $x_4 \neq 0$, $x_5 \neq 0$, och därmed $d(\mathbf{x}, 0) \geqq 3$. Om $s = 0$ och $t \neq 0$ så är $x_1 \neq 0$, $x_3 \neq 0$, $x_5 \neq 0$, och därmed $d(\mathbf{x}, 0) \geqq 3$. Slutligen, om $t = 0$ och $s \neq 0$ så är $x_1 \neq 0$, $x_2 \neq 0$, $x_3 \neq 0$, $x_4 \neq 0$, och därmed $d(\mathbf{x}, 0) \geqq 4$. I alla möjliga fall gäller alltså säkert $d(\mathbf{x}, 0) \geqq 3$. Detta visar att $d(\mathcal{C})$ är *större än eller likamed* 3. Alltså måste $d(\mathcal{C}) = 3$.

• 5. Utdata-sannolikheterna blir:

$$\begin{pmatrix} 0.4 & 0.4 & 0.2 \end{pmatrix} \begin{pmatrix} 0.75 & 0.25 & 0 \\ 0 & 1 & 0 \\ 0.5 & 0 & 0.5 \end{pmatrix} = \begin{pmatrix} 0.4 & 0.5 & 0.1 \end{pmatrix}.$$

(dvs ut-källan $\mathcal{B}$ har $slh(b_1) = 0.4$, $slh(b_2) = 0.5$, $slh(b_3) = 0.1$).

Bakåt-sannolikheterna Q_{ij} ges av Bayes formel:

$$Q_{ij} = slh(a = a_i \mid b = b_j) = \frac{p_i}{q_j} P_{ij}.$$

Alltså:

$$Q_{11} = \frac{0.4}{0.4} \cdot 0.8 = 0.75, \quad Q_{12} = \frac{0.4}{0.5} \cdot 0.25 = 0.2, \quad Q_{13} = 0,$$
$$Q_{21} = 0 \qquad\qquad Q_{22} = \frac{0.4}{0.5} \cdot 1 = 0.8, \qquad Q_{23} = 0$$
$$Q_{31} = \frac{0.2}{0.4} \cdot 0.5 = 0.25, \quad Q_{32} = 0 \qquad\qquad Q_{33} = \frac{0.2}{0.1} \cdot 0.5 = 1,$$

Systementropier (vi använder basen 2, och notationen $H_2(x_1, x_2, x_3) = -x_1 \log_2 x_1 - x_2 \log_2 x_2 - x_3 \log_2 x_3$ där vi alltid kommer att ha $x_1 + x_2 + x_3 = 1$):

$$\begin{aligned} H_2(\mathcal{A}|\mathcal{B}) &= 0.4 \cdot H_2(\mathcal{A}|b = b_1) + 0.5 \cdot H_2(\mathcal{A}|b = b_2) + 0.1 \cdot H_2(\mathcal{A}|b = b_3) \\ &= 0.4 \cdot H_2(0.75, 0, 0.25) + 0.5 \cdot H_2(0.2, 0.8, 0) + 0.1 \cdot H_2(0, 0, 1) = 0.685475... \\ H_2(\mathcal{B}|\mathcal{A}) &= 0.4 \cdot H_2(\mathcal{B}|a = a_1) + 0.4 \cdot H_2(\mathcal{B}|a = a_2) + 0.2 \cdot H_2(\mathcal{B}|a = a_3) \\ &= 0.4 \cdot H_2(0.75, 0.25, 0) + 0.4 \cdot H_2(0, 1, 0) + 0.2 \cdot H_2(0.5, 0, 0.5) = 0.5245112... \\ H_2(\mathcal{A}, \mathcal{B}) &= H_2(\mathcal{B}) + H_2(\mathcal{A}|\mathcal{B}) = H_2(0.4, 0.5, 0.1) + H_2(\mathcal{A}|\mathcal{B}) = 2.0464393... \end{aligned}$$

Alternativ beräkning: Vi beräknar förenade sannolikheterna $R_{ij} = p_i P_{ij}$:

$$\begin{aligned} &R_{11} = 0.3, && R_{12} = 0.1, && R_{13} = 0 \\ &R_{21} = 0 && R_{22} = 0.4, && R_{23} = 0 \\ &R_{31} = 0.1, && R_{32} = 0 && R_{33} = 0.1. \end{aligned}$$

Härur följer $H(\mathcal{A}, \mathcal{B}) = -\sum_{i,j} R_{ij} \log_2 R_{ij} = 2.0464393...$.

Slutligen, informationen:

$$I_2(\mathcal{A}, \mathcal{B}) = H_2(\mathcal{A}) - H_2(\mathcal{A}|\mathcal{B}) = 0.83645...$$

• 6. Antag att vi ger indata fördelningen $(x, 1 - x)$ där $0 \leqq x \leqq 1$. Då får utdata fördelningen $(0.7x + 0.5(1 - x), 0.3x + 0.5(1 - x)) = (0.5 + 0.2x, 0.5 - 0.2x)$, så

$$\begin{aligned} I(\mathcal{A}, \mathcal{B}) &= H(\mathcal{B}) - H(\mathcal{B}|\mathcal{A}) \\ &= -(0.5 + 0.2x) \log(0.5 + 0.2x) - (0.5 - 0.2x) \log(0.5 - 0.2x) \\ &\quad - \Big(x \cdot H(0.7) + (1 - x) \cdot H(0.5)\Big). \end{aligned}$$

där vi använder förkortningen $H(u) = -u \log u - (1 - u) \log(1 - u)$. Kalla ovanstående uttryck för $f(x)$. Då är (om "log" står för naturlig

logaritm)

$$\begin{aligned} f'(x) &= -0.2\log(0.5+0.2x) + 0.2\log(0.5-0.2x) \\ &\quad - \frac{0.5+0.2x}{0.5+0.2x}\cdot 0.2 - \frac{0.5-0.2x}{0.5-0.2x}\cdot(-0.2) \\ &\quad + H(0.5) - H(0.7) \\ &= 0.2\log\left(\frac{0.5-0.2x}{0.5+0.2x}\right) + H(0.5) - H(0.7). \end{aligned}$$

Alltså gäller:

$$\begin{aligned} f'(x) = 0 &\iff 0.2\log\left(\frac{0.5-0.2x}{0.5+0.2x}\right) = H(0.7) - H(0.5) \\ &\iff \frac{0.5-0.2x}{0.5+0.2x} = e^{(H(0.7)-H(0.5))/0.2} \\ &\iff x = \frac{5}{2}\cdot\frac{1-e^{(H(0.7)-H(0.5))/0.2}}{1+e^{(H(0.7)-H(0.5))/0.2}} \\ &\iff x = 0.7208911738... \end{aligned}$$

Vi ser också att funktionen $f'(x)$ är avtagande för $0 < x < 1$, alltså är $f'(x) > 0$ för $0 < x < 0.7208911738...$ och $f'(x) < 0$ för $0.7208911738... < x < 1$. Alltså antar $f(x)$ sitt maximum (över $0 \leqq x \leqq 1$) för $x_0 = 0.7208911738....$

Den sökta kapaciteten är alltså, om vi nu använder 2-logaritmer (dvs vi anger den *binära* kapaciteten):

$$f(x_0) = 0.0303112699...$$

Svar: Den binära kapaciteten är $C = 0.0303112699...$

• 7. Eftersom G är på systematisk form,

$$G = (I \mid P) \qquad \text{med} \qquad P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

så kan vi direkt ge en paritets-checks-matris med hjälp av den kända formeln $H = (-P^T \mid I)$:

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

Här är ett möjligt val av restklassledare och deras syndromer:

Restklassledare	syndrom
000000	000
100000	011
010000	101
001000	110
000100	100
000010	010
000001	001
100100	111

Vi syndromavkoderar slutligen de tre givna orden: Ordet 011001 har syndrom 010 och avkodas alltså som:

$$\Delta(011001) = 011001 - 000010 = 011011.$$

Ordet 011101 har syndrom 110 och avkodas alltså som:

$$\Delta(011101) = 011101 - 001000 = 010101.$$

Ordet 110111 har syndrom 001 och avkodas alltså som:

$$\Delta(110111) = 110111 - 000001 = 110110.$$

• 8. Sannolikheten att $w = w_1w_2...w_7 \in T^7$ fås som utdata från Γ^7 givet att indata är ordet $a = a_1a_2...a_7 \in \mathbb{Z}_2^7$ är:

$$\mathrm{Slh}\Big(\text{utdata} = w_1w_2...w_7 \mid \text{indata} = a_1a_2...a_7\Big)$$
$$= \prod_{j=1}^{7} \begin{cases} 0.9 & \text{om } w_j = a_j \in \{0,1\} \\ 0.1 & \text{om } w_j = ? \\ 0 & \text{annars, dvs om } w_j \in \{0,1\},\ w_j \neq a_j \end{cases}.$$

Denna sannolikhet blir 0 om det finns något $j \in \{1, 2, ..., 7\}$ för vilket $w_j \in \{0, 1\}$ och $w_j \neq a_j$. *Annars,* dvs om $w_j = a_j$ eller $w_j = ?$ för alla j; låt $f(w)$ vara antalet tecken "?" i ordet $w = w_1w_2...w_7$; då blir ovanstående sannolikhet

$$= 0.1^{f(w)}0.9^{7-f(w)} = \frac{9^{7-f(w)}}{10^7}.$$

Låt nu $\mathcal{H}_7(w)$ vara delmängden av alla ord $a = a_1a_2...a_7$ i $\mathcal{H}_7$ som uppfyller $a_j = w_j$ för alla j med $w_j \in \{0, 1\}$; då följer ur ovanstående

att q_w, sannolikheten att w erhålls som utdata från kanalen Γ^7 då källan $\mathcal{A}$ tas som indata, ges av:

$$(*) \qquad q_w = \sum_{a \in \mathcal{H}_7(w)} \frac{9^{7-f(w)}}{10^7} = \frac{9^{7-f(w)}}{10^7} \cdot |\mathcal{H}_7(w)| \,.$$

Vi söker nu antalet ord $w \in T^7$ som har $q_w \geqq \dfrac{9^4}{10^7}$. Vi ser direkt ur (*) ovan att om $f(w) \leqq 3$ så gäller $q_w \geqq \dfrac{9^4}{10^7}$ om och endast om $\mathcal{H}_7(w) \neq \emptyset$. Vi ser också att om $f(w) \geqq 5$ så är $q_w \leqq 16 \cdot \frac{9^2}{10^7} < \frac{9^4}{10^7}$, dvs villkoret är *inte* uppfyllt. Slutligen, om $f(w) = 4$ så kan man visa att $|\mathcal{H}_7(w)| \leqq 2$ (se nedan), och därmed $q_w \leqq 2 \cdot \frac{9^3}{10^7} < \frac{9^4}{10^7}$, dvs villkoret är *inte* uppfyllt. Vi har därmed visat att $w \in T^7$ uppfyller $q_w \geqq \dfrac{9^4}{10^7}$ om och endast om $f(w) \leqq 3$ och $\mathcal{H}_7(w) \neq \emptyset$.

[Bevis för "$f(w) = 4 \implies |\mathcal{H}_7(w)| \leqq 2$", som utnyttjades ovan: Antag, i syfte att erhålla en motsägelse, att $f(w) = 4$ och $|\mathcal{H}_7(w)| \geqq 3$. Då finns (minst) tre olika ord $a^{(k)} = a_1^{(k)} a_2^{(k)} ... a_7^{(k)}$ $(k = 1, 2, 3)$ i $\mathcal{H}_7(w)$. Vi vet att Hammingkoden $\mathcal{H}_7(w)$ har minimalavstånd 3, alltså gäller $d(a^{(1)}, a^{(2)}) \geqq 3$ och $d(a^{(1)}, a^{(3)}) \geqq 3$ och $d(a^{(2)}, a^{(3)}) \geqq 3$. Alltså måste $a^{(1)}$ och $a^{(2)}$ skilja sig åt i minst tre olika positioner, dvs det finns index $j_1 < j_2 < j_3$ så att $a_{j_1}^{(1)} \neq a_{j_1}^{(2)}$, $a_{j_2}^{(1)} \neq a_{j_2}^{(2)}$, $a_{j_3}^{(1)} \neq a_{j_3}^{(2)}$. Men $a_j^{(k)}$ är antingen likamed 0 eller 1, alltså måste $a_{j_1}^{(3)} = a_{j_1}^{(1)}$ *eller* $a_{j_1}^{(3)} = a_{j_1}^{(2)}$, och på samma sätt måste $a_{j_2}^{(3)} = a_{j_2}^{(1)}$ eller $a_{j_2}^{(3)} = a_{j_2}^{(2)}$, och $a_{j_3}^{(3)} = a_{j_3}^{(1)}$ eller $a_{j_3}^{(3)} = a_{j_3}^{(2)}$. Alltså stämmer $a^{(3)}$ överrens med *ett* av orden $a^{(1)}$ eller $a^{(2)}$ i två eller tre av positionerna j_1, j_2, j_3; vi kan anta att det är för ordet $a^{(1)}$.

I varje position j där $w_j \neq ?$ har vi $a_j^{(1)} = a_j^{(2)} = a_j^{(3)} = w_j$, eftersom $a^{(1)}, a^{(2)}, a^{(3)} \in \mathcal{H}_7(w)$. Alltså måste $w_{j_1} = w_{j_2} = w_{j_3} = ?$ och eftersom $f(w) = 4$ så finns det precis en till position $j_4 \notin \{j_1, j_2, j_3\}$ med $w_{j_4} = ?$. Nu kan orden $a^{(1)}$ och $a^{(3)}$ endast skilja sig åt i de fyra positionerna j_1, j_2, j_3, j_4, och vi såg ovan att de skiljer sig åt i *högst en* av de tre positionerna j_1, j_2, j_3. Alltså är $d(a^{(1)}, a^{(3)}) \leqq 2$. Detta är en motsägelse mot $d(a^{(1)}, a^{(3)}) \geqq 3$.]

Vi har ovan sett att vår uppgift är att räkna antalet ord $w \in T^7$ som har $f(w) \leqq 3$ och $\mathcal{H}_7(w) \neq \emptyset$. Observera att om $w \in T^7$ har $|\mathcal{H}_7(w)| \geqq 2$ så finns två olika ord $a^{(1)}$ och $a^{(2)}$ i $\mathcal{H}_7$; då är $d(a^{(1)}, a^{(2)}) \geqq 3$, och orden $a^{(1)}, a^{(2)}$ kan endast skilja sig åt i positioner där w har tecknet "?", alltså måste $f(w) \geqq 3$. Alltså: Om $f(w) \leqq 2$ så är och $\mathcal{H}_7(w) \neq \emptyset$

så är $|\mathcal{H}_7(w)| = 1$. Vi kan alltså lätt räkna alla ord $w \in T^7$ som har $f(w) \leqq 2$ och $\mathcal{H}_7(w) \neq \emptyset$: För varje sådant ord w finns det ett *unikt* ord $a \in \mathcal{H}_7(w)$, och ordet w fås ur a genom att ersätta noll eller ett eller två av tecknena i a med "?". (Och omvänt uppfyller verkligen varje ord w som skapas på detta sätt ur ett ord $a \in \mathcal{H}_7$ kraven $f(w) \leqq 2$ och $\mathcal{H}_7(w) \neq \emptyset$.) Det finns 16 ord i $\mathcal{H}_7$ och antalet sätt att välja ut noll eller en eller två av tecknena i ett sådant ord är $\binom{7}{0} + \binom{7}{1} + \binom{7}{2}$. Alltså är antalet ord $w \in T^7$ som har $f(w) \leqq 2$ och $\mathcal{H}_7(w) \neq \emptyset$:

$$= 16 \cdot \left(\binom{7}{0} + \binom{7}{1} + \binom{7}{2} \right).$$

Slutligen, orden $w \in T^7$ som har $f(w) = 3$ och $\mathcal{H}_7(w) \neq \emptyset$ kan räknas upp med samma metod, men mer försiktighet krävs: Låt M vara mängden av ord $w \in T^7$ med $f(w) = 3$ och $\mathcal{H}_7(w) \neq \emptyset$, och låt P vara mängden

$$\big\{(j_1, j_2, j_3) \in \mathbb{Z}^3 \mid 1 \leqq j_1 < j_2 < j_3 \leqq 7\big\}.$$

För varje par $\langle a, (j_1, j_2, j_3)\rangle \in \mathcal{H}_7 \times P$ får vi nu ett ord $w = w_1 w_2 ... w_7 \in M$ genom att utgå från a och byta tecken nummer j_1, j_2, j_3 mot "?", dvs genom att sätta

$$w_j = \begin{cases} a_j & \text{om } \ j \notin \{j_1, j_2, j_3\} \\ ? & \text{om } \ j \in \{j_1, j_2, j_3\}. \end{cases}$$

Detta definierar en avbildning $F : \mathcal{H}_7 \times P \to M$. Det är klart ur definitionerna att varje ord i M kan erhållas på detta sätt på precis $|\mathcal{H}_7(m)|$ sätt (speciellt: F är surjektiv), ty om $w \in M$ så gäller $F(\langle a, (j_1, j_2, j_3)\rangle) = w$ om och endast om $a \in \mathcal{H}_7(m)$ och $j_1 < j_2 < j_3$ är de tre positionerna med $w_{j_1} = w_{j_2} = w_{j_3} =?$. Eftersom koden $\mathcal{H}_7$ har minimalavstånd 3 så måste $|\mathcal{H}_7(w)| = 1$ eller 2 för alla $w \in M$. Det följer att om A är antalet ord $w \in M$ med $|\mathcal{H}_7(w)| = 2$ så är

$$\big|M\big| = \Big|\mathcal{H}_7 \times P\Big| - A = 16 \cdot \binom{7}{3} - A.$$

Det återstår alltså att beräkna A. Men observera att om $\langle a, (j_1, j_2, j_3)\rangle \in \mathcal{H}_7 \times P$ så gäller att ordet $w = F(\langle a, (j_1, j_2, j_3)\rangle)$ uppfyller $|\mathcal{H}_7(w)| = 2$ om och endast om $a^{(j_1,j_2,j_3)} \in \mathcal{H}_7$, där $a^{(j_1,j_2,j_3)}$ är det ord som erhålls ur a genom att invertera positionerna j_1, j_2, j_3, dvs

$$a_j^{(j_1,j_2,j_3)} = \begin{cases} a_j & \text{om } \ j \notin \{j_1, j_2, j_3\} \\ a_j + 1 & \text{om } \ j \in \{j_1, j_2, j_3\}. \end{cases}$$

(Här ska "$a_j + 1$" såklart räknas ut i $\mathbb{Z}_2$.) Men eftersom $a \in \mathcal{H}_7$ och koden $\mathcal{H}_7$ är linjär så gäller ovanstående om och endast om ordet

$e^{(j_1,j_2,j_3)} := a^{(j_1,j_2,j_3)} - a$ tillhör $\mathcal{H}_7$. Observera att detta ord $e^{(j_1,j_2,j_3)}$ har ettor i positionerna j_1, j_2, j_3 och nollor i de fyra övriga positionerna; det är alltså ett ord av vikt 3. Genom att skriva upp de sexton orden i (ett precist val av) $\mathcal{H}_7$ finner man att det finns *precis sju* ord av vikt 3 i $\mathcal{H}_7$. (Detta är också lätt att räkna ut med ett resonemang: Genom att tolka i termer av paritets-checks-matrisen kan man se att det för varje *par* av positioner i $\{1, 2, ..., 7\}$ finns *precis en* tredje position som gör att motsvarande vikt-3-ord tillhör $\mathcal{H}_7$; alltså är totala antalet vikt-3-ord i $\mathcal{H}_7$ likamed $\binom{7}{2}/3 = 7$.) Sammantaget visar detta att för varje $a \in \mathcal{H}_7$ finns precis *sju* val av $(j_1, j_2, j_3) \in P$ som ger att ordet $w = F(\langle a, (j_1, j_2, j_3)\rangle)$ uppfyller $|\mathcal{H}_7(w)| = 2$. Totalt finns alltså $16 \cdot 7$ stycken val av $\langle a, (j_1, j_2, j_3)\rangle \in \mathcal{H}_7 \times P$ som gör att $w = F(\langle a, (j_1, j_2, j_3)\rangle)$ uppfyller $|\mathcal{H}_7(w)| = 2$. Alltså är $A = \frac{1}{2} \cdot 16 \cdot 7 = 56$.

Det sökta antalet ord är alltså:

$$\begin{aligned} &16 \cdot \left(\binom{7}{0} + \binom{7}{1} + \binom{7}{2} \right) + \left|M\right| \\ &= 16 \cdot \left(\binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3} \right) - A \\ &= 16 \cdot \left(\binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3} \right) - 56 = 968. \end{aligned}$$

Svar: 968 stycken ord.