Teoria informacji – Lab1

Patryk Lisik

19 Listopad 2023

Problem 1

Dane jest niepamiętające dyskretne źródło informacji z alfabetem $A = \{a, b, c, d\}$ i prawdopodobieństwem nadania każdego znaku odpowiednio $P(X = a) = \frac{1}{2}, P(X = b) = P(X = c) = \frac{1}{8}, P(X = d) = \frac{1}{2}$. Jaka jest entropia źródła?

x_i	a	b	c	d
p_i	1/2	1/8	1/8	1/4
I_i	1b	3b	3b	2b

Ilość informacji $I_i = \log_2 \frac{1}{p_i}$

$$H(X) = \sum p_i I_i = 1.75b$$

Problem 2

Źródło o szerokości pasma $W = 4000Hz$ zostało poddane próbkowaniu z częstotliwością Nyquista. Przyjmując

x_i	-2	-1	0	1	2
p_i	1/2	1/4	1/8	1/16	1/16
I_i	1b	3b	3b	2b	2b

$$H(X) = 1.875b$$

Musimy próbkowań z częstotliwością dwukrotnie większą niż źródło = 8000 hz

$$8000 \cdot 1.875b = 15000b/s$$

Problem 3

Oblicz tempo informacji źródła nadającego r = 3000 znaków na sekundę z zakresu czterech znaków z prawdopodobieństwami danymi w tabeli.

x_i	A	B	C	C
P_i	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{6}$
$I_i(bit)$	$\log_2 3$	$\log_2 3$	$1 + \log_2 3$	$1 + \log_2 3$

$$\log_2 6 = \log_2(2 \cdot 3) = \log_2 2 + \log_2 3 = 1 + \log_2 3$$

$$\log_2 3 \approx 1.585$$

$$H(X) = \frac{1}{3}\log_2 3 + \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6 \frac{1}{6}\log_2 6 = \frac{1}{3} + \log_2 3 \approx= 1.918b$$

Problem 4

Zbuduj rozszerzenie 2. rzędu źródła z Problemu 1 i oblicz jego entropię.

$y_1 = x_j x_k$	aa	ab	ac	ad	ba	bb	bc	bd	ca	cb	cc	cd	da	db	dc	dd
p_1	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	$\frac{1}{16}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{16}$
I_i	2b	4b	4b	3b	4b	6b	6b	5b	4b	6b	6b	5b	3b	5b	5b	4b

Tabela 1: Rozszeżenie źródła z problmu 1

$$H(X^2) = \frac{1}{4} \cdot 2b + \frac{2}{8} \cdot 3b + \frac{5}{16} \cdot 4b + \frac{4}{32} \cdot 5b + \frac{4}{64} 6b = 3.5b = 2H(X)$$

Problem 5

Rozważ kanał binarny (niesymetryczny) o macierzy kanału

$$\mathbf{P} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{8} & \frac{7}{8} \end{pmatrix}$$

o prawdopodobieństwach wejścia $P(X = 0) = \frac{4}{5}, P(X = 1) = \frac{1}{5}$. Oblicz prawdopodobieństwo wyjściowe i prawdopodobieństwo wstecz.

$$p = \begin{pmatrix} \frac{4}{5} \frac{1}{5} \end{pmatrix}$$

$$H(X) = \frac{4}{5} \log_2(\frac{5}{4}) + \frac{1}{5} \log_2 5 = \log_2 5 - \frac{8}{5}$$

Prawdopodobieństwa wyjścia wyjścia:

$$q = p\mathbf{P} = (\frac{4}{5} \frac{1}{5}) \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{8} & \frac{7}{8} \end{pmatrix} = \begin{pmatrix} \frac{25}{40} \frac{15}{40} \end{pmatrix} = \begin{pmatrix} \frac{5}{8} \frac{3}{8} \end{pmatrix}$$

Entropia wyjściowa:

$$H(Y) = \frac{5}{8} \log_2 \frac{8}{5} + \frac{3}{8} \log_2 \frac{8}{3} = 0.954b$$

Macierz prawdopodobieństw włączanych

$$R = \begin{pmatrix} \frac{4}{5} & 0 \\ 0 & \frac{1}{5} \end{pmatrix} \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{8} & \frac{7}{8} \end{pmatrix} = \begin{pmatrix} \frac{3}{5} & \frac{1}{5} \\ \frac{1}{40} & \frac{7}{40} \end{pmatrix}$$

Entropia łączna Wynik powinien sumować się do 1.

$$H(X,Y) = \frac{3}{5} \log_2 \frac{5}{3} + \frac{1}{5} \log_2 5 + \frac{1}{40} \log_2 40 + \frac{7}{40} \frac{40}{7}$$
$$= \frac{5}{3} \log_2 5 - \frac{3}{5} \log_2 3 + \frac{1}{5} \log 25 + \frac{1}{40} \log 25 + \frac{3}{40} + \frac{7}{40} \log 25 + \frac{21}{40} - \frac{7}{40} \log_2 7$$
$$= \frac{3}{5} + \log 25 - \frac{3}{5} \log_2 3 - \frac{7}{40} \log_2 7 \approx 1.780b$$

Entropia szumu :

$$H(Y|X) = \frac{3}{5} \log_2 \frac{4}{3} + \frac{1}{5} \log_2 4 + \frac{1}{40} \log_2 8 + \frac{7}{40} \log_2 \frac{7}{8} =$$
$$= \frac{6}{5} - \frac{3}{5} \log_2 3 + \frac{2}{5} + \frac{3}{40} + \frac{21}{40} - \frac{7}{40} \log_2 7 = \frac{11}{5} - \frac{3}{5} \log_2 3 - \frac{7}{40} \log_2 7$$

Macierz Q / Macierz wstecz

$$Q = \begin{pmatrix} \frac{3}{5} & \frac{1}{5} \\ \frac{1}{40} & \frac{7}{40} \end{pmatrix} \begin{pmatrix} \frac{8}{5} & 0 \\ 0 & \frac{8}{3} \end{pmatrix} = \begin{pmatrix} \frac{24}{25} & \frac{8}{15} \\ \frac{1}{25} & \frac{7}{15} \end{pmatrix}$$

Ważne

Tu nie ma mnożenie macierzowego

$$p_i P_{ij} = R_{ij} = Q_{ij} q_j$$

$$q_j = \sum_i p_i P_{ij}$$

Problem 6

Wyznacz entropię *a priori* i *a posteriori* dla poprzedniego kanału.

Ekwiwokacja

$$H(X|Y) = \frac{3}{5} \log \frac{25}{24} + \frac{1}{5} \log 158 + \frac{1}{40} \log_2 25 + \frac{7}{40} \log_2 \frac{15}{7} = \frac{6}{5} \log_2 5 - \frac{3}{5} \log_2 3 - \frac{9}{5} + \frac{1}{5} \log_2 3 + \frac{1}{20} \log_2 5 +$$

Informacja wzajemna

$$I(X,Y) = H(X) + H(Y) - H(X,Y) = \frac{4}{5} + \frac{9}{40} \log_2 3 - \frac{5}{8} \log_2 5 + \frac{7}{40} \log_2 7 \approx 0.197b$$

Problem 7

Wyznacz pojemność poniższego kanału:

$$\mathbf{P} = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix}$$

$$p = \begin{pmatrix} x & y & z \end{pmatrix}$$

$$x + y + z = 1$$

$$C = \max I(X,Y) = \max[H(X) + H(Y) - H(X,Y)]$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

$$q = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{2x+y+z}{4} & \frac{x+2y+z}{4} & \frac{x+y+2z}{4} \end{pmatrix} = \begin{pmatrix} \frac{1+x}{4} & \frac{1+y}{4} & \frac{1+z}{4} \end{pmatrix}$$

$$H(X) = -x\log_2 X - y\log y - z\log z$$

$$H(Y) = -\frac{2x+y+z}{4}\log_2\frac{2x+y+z}{4} - \frac{x+2y+z}{4}\log_2\frac{x+2y+z}{4} - \frac{x+y+2z}{4}\log_2\frac{x+y+2z}{4} =$$

$$= 2 - \frac{1}{4}\cdot[(1+x)\log_2(1+x) + (1+y)]\log_2(1+y) + (1+z)\log_2(1+z)]$$

$$R = \overline{p}P = \begin{pmatrix} x & & \\ & y & \\ & & z \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{x}{2} & \frac{x}{4} & \frac{x}{4} \\ \frac{y}{4} & \frac{y}{2} & \frac{y}{4} \\ \frac{z}{4} & \frac{z}{4} & \frac{z}{2} \end{pmatrix}$$

$$H(X,Y) = -\frac{x}{2}\log_2\frac{x}{2} - \frac{x}{4}\log_2\frac{x}{4} - \frac{y}{2}\log_2\frac{y}{2} - \frac{y}{4}\log_2\frac{y}{4} = \cdots == \frac{3}{2} - x\log_2 x - y\log_2 y - z\log_2 z$$

$$I(X,Y) = \frac{1}{2} - \frac{1}{4}[(1+x)\log_2(1+x) + (1+y)\log_2(1+y) + (1+z)\log_2(1+z)]$$

$$F(x,y,z) = \frac{1}{2} - \frac{1}{4}[(1+x)\log_2(1+x) + (1+y)\log_2(1+y) + (1+z)\log_2(1+z)] - \lambda(x+y+z-1)$$

Metoda Lagranga

$$\begin{cases} \frac{\partial F}{x} = \frac{1}{4}[\log_2(1+x) + \frac{1}{\ln 2}] + \lambda = 0 \\ \frac{\partial F}{y} = \frac{1}{4}[\log_2(1+y) + \frac{1}{\ln 2}] + \lambda = 0 \\ \frac{\partial F}{z} = \frac{1}{4}[\log_2(1+z) + \frac{1}{\ln 2}] + \lambda = 0 \\ G(x,y,z) = x + y + z - 1 = 0 \end{cases}$$

$$\log_2(1+x) = 4\lambda - \ln 2$$
$$1 + x = \frac{2^{4\lambda}}{2^{\ln 2}}$$

$$x = \frac{2^{4\lambda}}{2^{\ln 2}} - 1$$
$$y = \frac{2^{4\lambda}}{2^{\ln 2}} - 1$$
$$z = \frac{2^{4\lambda}}{2^{\ln 2}} - 1$$

$$x = \frac{1}{3}y = \frac{1}{3}z = \frac{1}{3}$$

Lab 2

Problem 1

$$GF(2) = \mathcal{F} =< \{0,1\} >, \oplus\cdot$$

$\oplus$	0	1
0	0	1
1	1	1

$$e_1 = (1000)e_2 = (0100)e_3 = (0010)e_4 = (0001)$$

$\cdot$	0	1
0	0	0
1	0	1

$$v = a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4a_i \quad \in GF(2)$$
$$v = (a_1 \quad a_2 \quad a_3 \quad a_4) \quad a_i \in GF(2)$$

$$V_4 = \begin{Bmatrix} v_0 = (0000) & v_4 = (0010) & v_8 = (0001) & v_{12} = (0011) \\ v_1 = (1000) & v_5 = (1010) & v_9 = (0011) & v_{13} = (1011) \\ v_2 = (0100) & v_6 = (0110) & v_{10} = (0101) & v_{14} = (0111) \\ v_3 = (1100) & v_7 = (1110) & v_{11} = (1101) & v_{15} = (1111) \end{Bmatrix}$$

$$v = (a_1a_2a_3a_4$$
$$w = (b_1b_2b_3b_4$$

Definicje działań

$$v \oplus w = (a_1 \oplus b_1 \quad a_2 \oplus b_2 \quad a_3 \oplus b_3 \quad a_4 \oplus b_4$$
$$aV = (aa_1 \quad aa_1 \quad aa_3 \quad aa_3 \quad aa_4$$

$$\forall_{c\ inv_4} 0(a_1a_2a_3a_4) = (0000)$$

$$\forall_{c\ inv_4} 1(a_1a_2a_3a_4) = (a_1a_2a_3a_4)$$
$$\forall_{c\ inv_4} v \oplus c = 0$$

$$S = \{(0000), (1001), (0100), (1101)\} = \{v_1, v_9, v_2, v_{11}\}$$

v_x odpowida char w C

$v_0 \oplus v_0 = 0$
$v_0 \oplus v_9 = v_9 \qquad v_9 \oplus v_9 = v_0$
$v_0 \oplus v_2 = v_2 \qquad v_0 \oplus v_2 = v_11 \quad v_2 \oplus v_2 = 0$
$v_0 \oplus v_{11} = v_{11} \quad v_9 \oplus v_11 = v_2 \quad v_2 \oplus v_{11} = v_9 \quad v_{11} \oplus v_{11} = 0$

$$f_1 = (1001) \quad f_2 = (0100) \quad u = a_1 f_1 + a_2 f_2 \quad a_1 \in GF(2)$$

$$\begin{aligned} u_0 = 0f_1 + 0f_2 = (0000) = v_0 \\ u_1 = 1f_1 + 0f_2 = f_1 = (1001) = v_9 \\ u_2 = 0f_1 + 1f_2 = f_2 = (0100) = v_2 \\ u_3 = 1f_1 + 1f_2 = (1101) = v_{11} \end{aligned}$$

$$< (1001), (0100) >= \{(0000), (1001), (0100), (1101)\} = S$$

Chyba nowe zadanie???

$$S \subset V_4$$

$$S = v_0, v_1 2, v_6, v_2, v_1 0, v_1 4, v_4, v_8 \quad S^{\perp} =?$$

$$S^{\perp} = \{w \in V_4 : \quad \forall_{V \in S} wv = 0\}$$

Dokończyć jak ktoś wstawi zdjęcie

To z macieżą G

Deklarujmy że można perzekszałcić macież G w G' za pomocą działań elementarnych. Czyli zamiana wierszy, kombinacja liniowa wierszy.

$$g = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} \quad G' = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$G = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} \quad G` = \begin{pmatrix} g_1 \\ g_2 \\ g_2 \oplus g_3 \end{pmatrix}$$

chyba kolejne zadanie

$$u_0 = 0g_1 \oplus 0g_2 \oplus 0g_3 = 00000 u_1 = 1g_1 \oplus 0g_2 \oplus 0g_3 = 10110 u_2 = 0g_1 \oplus 1g_2 \oplus 0g_3 = 01001 u_3 = 1g_1 \oplus$$

Problem 7?

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad H = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}$$

$v_0 = 0h_1 \oplus 0h_2 = 00000 v_1 = 1h_1 \oplus 0h_2 = 01001 v_2 = 0h_1 \oplus 1h_2 = 10010 v_3 = 1h_1 \oplus 1h_2 = 11011$

$$S \in a_1 g_1 \oplus a_2 g_2 \oplus a_3 g_3 = u$$
$$S^{\perp} \in b_1 h_1 \oplus b_2 h_2 = v$$

$$v \cdot u = (b_1 h_1 \oplus b_2 h_2)$$

Lab 3

Problem 8

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$
$$c = mG = (1001) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$
$$(m_0 m_1 m_2 m_3) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} =$$
$(m_0 \oplus m_2 \oplus m_0 \oplus m_0 \oplus)$tu nie wiem co on napisał

$$c_0 \oplus c_3 \oplus c_5 \oplus c_6 = 0$$
$$c_1 \oplus c_3 \oplus c_4 \oplus c_5 = 0$$
$$c_2 \oplus c_4 \oplus c_5 \oplus c_6 = 0$$

$$c_0 = m_0 \oplus m_2 \oplus m_3 = c_3 \oplus c_5 \oplus c_6$$
$$c_1 = m_0 \oplus m_1 \oplus m_2 = c_3 \oplus c_4 \oplus c_5$$
$$c_2 = m_0 \oplus m_2 \oplus m_3 = c_4 \oplus c_5 \oplus c_6$$
$$c_3 = m_0$$
$$c_4 = m_1$$
$$c_5 = m_2$$
$$c_6 = m_3$$
$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$
$$cH^T = 0$$
$$s = rH^T(s_0s_1s_2) = (r_1r_2r_3r_4r_4r_5r_6)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} =$$
$$= (r_0 \oplus r_3 \oplus r_5 \oplus r_6, r_1 \oplus r_3 \oplus r_4 \oplus r_5, r_4 \oplus r_2 \oplus r_4 \oplus r_5 \oplus r_6)$$

W macierzy H wszystkie kolumny są liniowo nie zależne

Prawdopodobieństwo nie wykrycia błędu.(undetected error)

$$Pr_{ue} = \sum_{i=l+1}^{n} A_i p^i (1-p)^{n-1}$$

Prawdobododobieńswto nie możliwośic poprawnia błędu

$$Pr_{ue} = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} = 1 - \left[\sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}\right] = \cdots = 21p^2 \quad p << 1$$

TO DO przepisać to długie równanie ze zdjęcia

Prawdopodobieństwo niemożliwości zdekodowania (uncodeded)

$$
\begin{aligned}
Pr_{uc} = 1-(1-p)^4 = 1 - \binom{1}{0} + \binom{4}{1}p + \binom{4}{2}p^2\binom{4}{3}p^3 + \binom{4}{4}p^4 &= \\
= 1 - 1 + 4p + 6p^2 + 4p^3 - p^4 &= \\
= 4p - 6p^2 + 4p^3 - p^4 & \\
\approx 4p &
\end{aligned}
$$

$p = 0.01 = 1\%$ błędnych bitów
$P_{uc} = 0.04\%$ błędnych wiadomości 4-bitowych
$P_{we} = 0.0021 = 2.1$ ‰- niepoprawialncyh błędów $Pr_{ue} = 3 \cdot 10^{-6}$ - niewykrytych błędów

Now zadanie

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

m	c	w(c)
0000	00000	0
100	01001	2
010	10110	3
110	11111	5
001	10010	2
101	11011	4
011	00100	1
111	01101	3

$$d_{\min} = 1 \quad l = 0 \quad t = 0$$

Tablica standardowa do dekodowania

$$\Delta(00011) = 101$$

Odległość nie musi być najbliższa.

$$\Delta(011000) = 011$$
$$d(01100, 00100) = d(01100, 01101)$$

0000	100	010	110	001	101	011	111
00000	01001	10110	11111	10010	11011	00100	01101
10000	11001	00110	01111	00010	01011	10100	11101
01000	00001	11110	10111	11010	10011	01100	00101
11000	10001	01110	00111	01010	00011	11100	10101

Nowe zadanie ?

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

$$d_{\min} = 3 \quad t = \lfloor \frac{d_{\min} - 1}{2} \rfloor = 1$$

$$r = (1101101) rH^T = (1101101) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \implies e = (0001000)$$

Zestaw 3?

Zadanie 1

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

$$c_0 = m_0 G = (0000000)$$
$$c_1 = m_1 G = (1101000)$$
$$c_2 = m_2 G = (0110100)$$
$$c_3 = m_3 G = (1011100)$$

to jest postać systematyczna ??

$$g(x) = 1 \oplus x \oplus x^3$$

$$m_0 = (0000) \quad m_0(x) = 0 \quad p_0(x) = x^3 m(x) \mod g(x) = 0$$
$$c_0(x) = p_0(x) \oplus x^3 m(x) = 0 \quad c_0 = (0000000)$$

$$m_1 = (1000) \quad m_1(x) = 0 \quad p_1(x) = x^3 m(x) \mod g(x) = 1 \oplus x$$
$$c_1(x) = p_1(x) \oplus x^3 m(x) = 0 \quad c_0 = (1101000)$$

$$m_2 = (0100) \quad m_1(x) = 0 \quad p_1(x) = x^3 m(x) \mod g(x) = 1 \oplus x$$
$$c_1(x) = p_1(x) \oplus x^3 m(x) = 0 \quad c_0 = (1101000)$$

$$m_3 = (1000) \quad m_1(x) = 0 \quad p_1(x) = x^3 m(x) \mod g(x) = 1 \oplus x$$
$$c_1(x) = p_1(x) \oplus x^3 m(x) = 0 \quad c_0 = (1101000)$$

Lab 4

Problem 4

Działamy w ciele $GF2$

$$1 \oplus x^7 = (1 \oplus x)(x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^3 \oplus x^2 \oplus x \oplus 1) = (1 \oplus x)(1 \oplus x \oplus x^3)(1 \oplus x^2 \oplus x^3)$$

$g1(x) = 1 \oplus x$ $\qquad$ $C_{cyc}(7,6)$ wielomian cykiczny o długości 6

$m(x) = m_0 \oplus m_1 x \oplus m_2 x^2 \oplus m_3 x^3 \oplus m_4 x^4 \oplus m_5 x^5$

$$\begin{aligned} p(x) &= x m(x) \mod g(x) \\ &= (m_0 \oplus m_1 x \oplus m_2 x^2 \oplus m_3 x^3 \oplus m_4 x^4 \oplus m_5 x^5) \mod (1 \oplus x) \end{aligned}$$
$$c(x) = m_0 \oplus m_1 \oplus_2 \oplus m_3 \oplus m_4 \oplus_5 \oplus m_0 x \oplus x \oplus m_1 x^2 \oplus m_2 x^3 \oplus m_4 \oplus x^4 \oplus m_5 x^5$$

Macier nieusystematyzowana i maccierz usystematyzowa

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

$$g_3(x) = 1 \oplus x \oplus x^3 \quad {}_{\text{cyc}}(7,4)$$

$$m(x) = m_0 m_1 x \oplus m_2 x^2 \oplus m_3 x^3$$

$$p(x) = x^3 m(x) \mod g(x) =$$

$$(m_0 x_3 \oplus m_1 x^4 \oplus m_2 x^5 \oplus m_3 x^6) \mod (1 \oplus x \oplus x^3)$$

$$c(x) = (m_0 \oplus m_2 \oplus m_6) \oplus (m_0 \oplus m_1 \oplus m_3) x \oplus (m_1 \oplus m_2 \oplus m_3) x^2 \oplus m_0 x^3 m_1 \oplus x^4 \oplus m_2 \oplus x^5 \oplus m_3 x^6$$

$c(x)$ - kod Hamminga H_7 (równoważny)

$$g_{3'} = 1 \oplus x^2 \oplus x^3$$

$$\overline{G}_{3'} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad G_{3'} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

3 pierwsze bity to bity parzystości

Kody dualne do kodu Hamminga H_7

$$g_6(x) = 1 \oplus x \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^6$$

$$m(x) = m_0$$

$$p(x) = (x^6 m_0) \mod (1 \oplus x \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^6)$$

$$c(x) = m_0 \oplus m_0 x \oplus m_0 x^2 \oplus m_0 x^3 \oplus m_0 x^4 \oplus m_0 x^5 \oplus m_0 x^6$$

jest to kod powtórzeniowy R_7

Problem 5

Zestaw 4

Problem 1

Ciało $GF(2^4)$

Generowane przez $1 \oplus \alpha \oplus \alpha^4$

$$\alpha^4 = 1 \oplus \alpha$$

Ciało ma 16 elementów. Można zapisać je jako potęgi α. (Poza jednym)

$\oplus$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	$\alpha 12$	α^{13}	α^{14}
0	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	$\alpha 12$	α^{13}	α^{14}
α																
α^2																
α^3																
α^4																
α^5																
α^6																
α^7																
α^8																
α^9																
α^{10}																
α^{11}																
α^{12}																
α^{13}																
α^{14}																

$1 \oplus \alpha \oplus \alpha^4 = 0$

$$\alpha^{15} = 1$$
$$\alpha^4 = 1 \oplus \alpha$$
$$\alpha^5 = \alpha \oplus \alpha^2$$
$$\alpha^6 = \alpha^2 \oplus \alpha^3$$
$$\alpha^7 = \alpha^3 \oplus \alpha^4$$
$$\alpha^8 = \alpha^4 \oplus \alpha^5$$
$$\alpha^9 = \alpha^5 \oplus \alpha^6$$
$$\alpha^{10} = \alpha^6 \oplus \alpha^7$$
$$\alpha^{11} = \alpha^7 \oplus \alpha^8$$
$$\alpha^{12} = \alpha^8 \oplus \alpha^9$$
$$\alpha^{13} = \alpha^9 \oplus \alpha^{10}$$
$$\alpha^{14} = \alpha^{10} \oplus \alpha^{11}$$

$$1 \oplus \alpha^6 = 1 \oplus \alpha^2 \oplus \alpha^3 = \alpha^{13}$$

$$1 \oplus \alpha^9 = 1 \oplus \alpha \oplus \alpha^3 = \alpha^7$$

$$\alpha \oplus \alpha^6 = \alpha \oplus \alpha^2 \oplus \alpha^3 = \alpha^{11}$$

$$\alpha \oplus \alpha^7 = 1 \oplus \alpha^3 = \alpha^1 4$$

Chyba jakieś nowe zadanie

$$GF(2^4) \quad \alpha^4 = 1 \oplus \alpha \quad \alpha^{15} = 1$$

$$\alpha^{2^0} = \alpha^1 = \alpha$$
$$\alpha^{2^1} = \alpha^1 = \alpha^2$$
$$\alpha^{2^2} = \alpha^4$$

$$\alpha^{2^3} = \alpha^8$$
$$\alpha^{2^4} = \alpha^{16} = \alpha$$

$$\phi_1(x) = (\alpha \oplus x)(\alpha^2 \oplus x)(\alpha^4 \oplus x)(\alpha^8 \oplus x)$$
$$= \alpha^{15} \oplus (\alpha^7 \oplus \alpha^1 1 \oplus \alpha^{13} \oplus \alpha^{14})x \oplus (\alpha^3 \oplus \alpha^5 \oplus \alpha^6 \oplus \alpha^9 \oplus \alpha^{10} \oplus \alpha^{12})x^2 \oplus (\alpha \oplus \alpha^2 \oplus \alpha^4 \oplus \alpha^8)x^3 \alpha x^4$$

$$\phi_3 = (\alpha^3 \oplus x)(a^6 \oplus x)(\alpha^9 \oplus x)(\alpha^1 2 \oplus x) = 1 \oplus (\alpha^3 \oplus \alpha^6 \oplus \alpha^9 \oplus \alpha^1 2)x \oplus (\alpha^9 \alpha^1 2 \oplus \cancel{1} \oplus \cancel{1} \oplus \alpha^3 \alpha^6)x^2 \oplus (\alpha^3)$$
$$\ldots \text{starł z tablicy} = 1 \oplus x \oplus x^2 \oplus x^3 \oplus x^4$$

$$\phi_5(x) = (\alpha^5 \oplus x)(\alpha^{10} \oplus x) = 1 \oplus x \oplus x^2$$
$$\phi_7(x) = (\alpha^7 \alpha x)(\alpha^1 1 \oplus x)(\alpha^1 3 \oplus x)(\alpha^1 1 \oplus x) = 1 \oplus x^3 \oplus x^4$$

=======

Lab 4

jedno zadanie zrobione wcześniej. Jedno ominięte.

$$r(x) = 1 \oplus x^2$$

$$s_1 = r(\alpha) = 1 \oplus \alpha^2 = \cancel{\mathcal{X}} \oplus \alpha^2 = \alpha^2$$

$$s_2 = r(\alpha^2) = 1 \oplus \alpha^{16} = 1 \oplus \alpha = \alpha^4$$

$$s_3 = r(\alpha^3) = 1 \oplus \alpha^{24} = 1 \oplus \alpha^9 = 1 \oplus \alpha \oplus \alpha^3 = \alpha^7$$

$$s_4 = r(\alpha^4) = 1 \oplus \alpha^{32} = 1 \oplus \alpha^4 = \alpha^2$$

$$s(x)\sigma(x) - \mu(x)x^4 = -w(x)$$

i	q_i	$r_i = r_{i-1} - q_i r_{i-2}$	$t_1 = t_{i-1} - q_i t_{i-2}$
-1	–	x^4	1
0	–	$\alpha^2 x^3 \oplus \alpha^7 x^2 \oplus \alpha^4 \oplus \alpha^2$	1
1	$\alpha^7 x \oplus \alpha^6$	$\alpha^4 x^2 \oplus \alpha^{13} x \oplus \alpha^2$	$\alpha^7 x \oplus \alpha^6$
2	$\alpha^4 x \oplus \alpha^2$	α^4	$\alpha^{11} x^2 \oplus \alpha^5 x \alpha^3$

Jakieś inne zadanie
Wzmianka o rozszeżonym algorytmie euklidesa.

$$w(x) = \lambda r_1(x) = \lambda \alpha^5$$

$$\omega(x) = \lambda t_1(x) = \lambda(\alpha^{11} x^2 \oplus \alpha^5 x \oplus \alpha^3)$$

Pochodne nie istnieją bo nie ma pojęcia granicy

x	$\omega(x)$	
0	$\omega(0) = \alpha^7$	
α^9	$\omega(0) = 1 \oplus \alpha^9 \oplus \alpha^7 = 0$	$j_1 = 0$
α^7	$\omega(\alpha^7) = \alpha^1 1 \oplus \alpha \oplus \alpha^7 = 0$	

Zestaw 6 - ostanie zajęcia

$$C_{BCH}(15,7) \quad t = 2 \quad GF(2^4) \quad p(x) = 1 \oplus x \oplus x^4$$

$$r(x) = 1\oplus^8$$

$$s_1 = r(\alpha) = 1 \oplus \alpha^8 = \alpha^2$$

$$s_2 = r(\alpha^2) = 1 \oplus \alpha = \alpha^4$$

$$s_3 = r(\alpha^3) = 1 \oplus \alpha^9 = \alpha^4$$

$$s_4 = r(\alpha^4) = 1 \oplus \alpha^2 = \alpha^8$$

$$\rho^{(-1)}(x) = 1$$
$$l_{-1} = 0$$
$$d_{-1} = -1$$

$$\rho^{(0)}(x) = 1$$
$$l_0 = 0$$
$$d_0 = s_1$$

$$d_u = s_{\mu H} \oplus \rho$$

Kolejne zadanie - chyba 5

$$C_{BCH}(7,3) \quad GF(2^3) \quad p(x) = 1 \oplus x \oplus x^3$$

0	0	000	α^3	$1 \oplus \alpha$	110
1	1	100	α^4	$\alpha \oplus \alpha$	011
α	α	010	α^5	$1 \oplus \alpha \oplus \alpha^2$	111
α^2	α^2	001	α^5	$1 \oplus \alpha^2$	101

μ	$\rho^\mu(x)$	l_μ	d_μ	$\mu - l_\mu$	ρ	$\mu - \rho$
-1	1	0	1	-1		
0	1	0	0	0	-1	1
1	1	0	α^2	1	-1	2
2	$1 \oplus \alpha^2 x^2$	2	α^3	0	1	1
3	$1 \oplus \alpha x \oplus \alpha^2 x^2$	2	α^3	0	1	2
4	$1 \oplus \alpha x \oplus \alpha^6 x^2$					

$$
\begin{align}
\rho(x) &= 1 \oplus \alpha x \oplus \alpha^6 x^2 = (1 \oplus \alpha^4)(1 \oplus \alpha^2 x) \tag{1}\\
\beta_1 &= \alpha^4 \quad d_1 = 4 \tag{2}\\
\beta_2 &= \alpha^2 \quad d_2 = 2 \tag{3}\\
z(x) &= 1 \oplus \alpha \oplus x^2 \tag{4}\\
e_4 &= \frac{z(\beta_1^{-1}}{1 \oplus \beta_2\beta_1^{-1}} = \frac{z(\alpha^3)}{1 \oplus \alpha^2\alpha^3} = \frac{1 \oplus \alpha^4 \oplus \alpha^6}{1 \oplus \alpha^5} = \frac{\alpha}{\alpha^5} = \alpha^{-3} = \alpha^4 \tag{5}\\
e_2 &= \frac{z(\beta_2^{-1}}{1 \oplus \beta_1\beta_2^{-1}} = \frac{z(\alpha^5)}{1 \oplus \alpha^4\alpha^5} = \frac{1 \oplus \alpha^6 \oplus \alpha^3}{1 \oplus \alpha^5} = \frac{\alpha^5}{\alpha^6} = \alpha^{-1} = \alpha^6 \tag{6}\\
e(x) &= \alpha^6 x^2 \oplus \alpha^4 x^4 \tag{7}\\
& \tag{8}
\end{align}
$$

Zadanie 6?

$$
\begin{aligned}
s_1(0) &= 0\\
s_2(0) &= 0\\
s_1(t+1) &= m(t)\\
s_2(t+1) &= s_1(t)\\
s_1(t) &= m(t-1)\\
s_2(t) &= m(t-2)
\end{aligned}
$$

$$m = (100011)$$

$$
\begin{aligned}
C^{(1)}(\mathcal{D}) &= M(\mathcal{D}G^{(1)}(\mathcal{D})\\
C^{(2)}(\mathcal{D}) &= M(\mathcal{D}G^{(2)}(\mathcal{D})\\
\begin{pmatrix} C^{(1)}(\mathcal{D}) \\ C^{(2)}(\mathcal{D}) \end{pmatrix} &= M(\mathcal{D}) \begin{pmatrix} 1 \oplus \mathcal{D}^2 \\ 1 \oplus \mathcal{D} \oplus \mathcal{D}^2 \end{pmatrix}
\end{aligned}
$$

i	m_1	$S_i^{(1)}$	$S_i^{(1)}$	$C_i^{(1)}$	$C_i^{(2)}$
1	1	0	0	1	1
2	0	1	0	0	1
3	0	0	1	1	1
4	0	0	0	0	0
5	1	0	0	1	1
6	1	1	0	1	0
7	0	1	1	1	0
8	0	0	1	1	1
9	0	0	0	0	0

$$\begin{pmatrix} C^{(1)}(\mathcal{D}) \\ C^{(2)}(\mathcal{D}) \end{pmatrix} = (1 \oplus \mathcal{D}^4 \oplus \mathcal{D}^5) \begin{pmatrix} 1 \oplus \mathcal{D}^2 \\ 1 \oplus \mathcal{D} \oplus \mathcal{D}^2 \end{pmatrix}$$

$$\begin{pmatrix} C^{(1)}(\mathcal{D}) \\ C^{(2)}(\mathcal{D}) \end{pmatrix} = \begin{pmatrix} (1 \oplus \mathcal{D}^4 \oplus \mathcal{D}^5)(1 \oplus \mathcal{D}^2) \\ (1 \oplus \mathcal{D}^4 \oplus \mathcal{D}^5)(1 \oplus \mathcal{D} \oplus \mathcal{D}^2) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 \oplus \mathcal{D}^4 \oplus \mathcal{D}^5 \oplus \mathcal{D}^2 \oplus \mathcal{D}^6 \oplus \mathcal{D}^7 \\ 1 \oplus \mathcal{D}^4 \oplus \cancel{\mathcal{D}^8}\text{reszta starta z tablicy :(} \end{pmatrix}$$