

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 $P(X = a) = \frac{1}{2}$, $P(X = b) = P(X = c) = \frac{1}{8}$, $P(X = d) = \frac{1}{4}$. 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 $W = 4000\text{Hz}$ 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 próbkować 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: Rozszerzenie źródła z problemu 1

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

Problem 5

Rozważ kanał binarny (niesymetryczny) o macierzy kanału

$$\mathbf{P} = \begin{pmatrix} \frac{3}{8} & \frac{1}{8} \\ \frac{4}{5} & \frac{7}{5} \end{pmatrix}$$

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

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

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

Prawdopodobieństwa wyjścia wyjścia:

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

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

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

Entropia łączna Wynik powinien sumować się do 1.

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

Entropia szumu :

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

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

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

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:

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

$$p = (x \quad y \quad z)$$

$$x + y + z = 1$$

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

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

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

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

$$\begin{aligned}
H(Y) &= -\frac{2x+y+z}{4} \log_2 \frac{2x+y+z}{4} - \frac{x+2y+z}{4} \log_2 \frac{x+2y+z}{4} - \\
&\quad \frac{x+y+2z}{4} \log_2 \frac{x+y+2z}{4} = \\
&= 2 - \frac{1}{4} \cdot [(1+x) \log_2(1+x) + (1+y)] \log_2(1+y) + (1+z) \log_2(1+z)
\end{aligned}$$

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

$$\begin{aligned}
H(X, Y) &= -\frac{x}{2} \log_2 \frac{x}{2} - \frac{x}{4} \log_2 \frac{x}{4} - \\
&\quad -\frac{y}{2} \log_2 \frac{y}{2} - \frac{y}{4} \log_2 \frac{y}{4} = \dots = \frac{3}{2} - x \log_2 x - y \log_2 y - z \log_2 z
\end{aligned}$$

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

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

Metoda Lagranga

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

$$\log_2(1+x) = 4\lambda - \ln 2$$

$$1+x = \frac{2^{4\lambda}}{2^{\ln 2}}$$

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

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

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

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

Lab 2

Problem 1

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

\oplus		0	1
0		0	1
1		1	1

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

\cdot	\mid	0	1
0	\mid	0	0
1	\mid	0	1

$$v = a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 a_i \in GF(2)$$

$$v = (a_1 \quad a_2 \quad a_3 \quad a_4) \quad a_i \in GF(2)$$

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

$$v = (a_1 a_2 a_3 a_4$$

$$w = (b_1 b_2 b_3 b_4$$

Definicje działań

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

$$aV = (aa_1 \quad aa_1 \quad aa_3 \quad aa_3 \quad aa_4$$

$$\forall_{c \text{ inv}_4} 0(a_1 a_2 a_3 a_4) = (0000)$$

$$\forall_{c \text{ inv}_4} 1(a_1 a_2 a_3 a_4) = (a_1 a_2 a_3 a_4)$$

$$\forall_{c \text{ inv}_4} v \oplus c = 0$$

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

v_x odpowiada char w C

$$v_0 \oplus v_0 = 0$$

$$v_0 \oplus v_9 = v_9 \quad v_9 \oplus v_9 = v_0$$

$$v_0 \oplus v_2 = v_2 \quad v_0 \oplus v_2 = v_1 1 \quad v_2 \oplus v_2 = 0$$

$$v_0 \oplus v_{11} = v_{11} \quad v_9 \oplus v_1 1 = v_2 \quad v_2 \oplus v_{11} = v_9 \quad v_{11} \oplus v_{11} = 0$$

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

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

$$\langle (1001), (0100) \rangle = \{(0000), (1001), (0100), (1101)\} = S$$

Chyba nowe zadanie???

$$S \subset V_4$$

$$S = v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11} \quad S^\perp = ?$$

$$S^\perp = \{w \in V_4 : \forall v \in S, wv = 0\}$$

Dokończyć jak ktoś wstawi zdjęcie

To z macieżą G

Deklarujemy że można przekształcić 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

$$u_0 = 0g_1 \oplus 0g_2 \oplus 0g_3 = 00000 \quad u_1 = 1g_1 \oplus 0g_2 \oplus 0g_3 = 10110 \quad u_2 = 0g_1 \oplus 1g_2 \oplus 0g_3 = 01001 \quad u_3 = 1g_1 \oplus 1g_2 \oplus 1g_3 = 11111$$

Problem 7?

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

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

$$S \in a_1g_1 \oplus a_2g_2 \oplus a_3g_3 = u$$

$$S^\perp \in b_1h_1 \oplus b_2h_2 = v$$

$$v \cdot u = (b_1h_1 \oplus b_2h_2)$$

Lab 3

Problem 8

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

$$c = mG = (1001) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(m_0m_1m_2m_3) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$(m_0 \oplus m_2 \oplus m_0 \oplus m_0 \oplus)$$
tu nie wiem co on napisał

$$c_0 \oplus c_3 \oplus c_5 \oplus c_6 = 0$$

$$c_1 \oplus c_3 \oplus c_4 \oplus c_5 = 0$$

$$c_2 \oplus c_4 \oplus c_5 \oplus c_6 = 0$$

$$c_0 = m_0 \oplus m_2 \oplus m_3 = c_3 \oplus c_5 \oplus c_6$$

$$c_1 = m_0 \oplus m_1 \oplus m_2 = c_3 \oplus c_4 \oplus c_5$$

$$c_2 = m_0 \oplus m_2 \oplus m_3 = c_4 \oplus c_5 \oplus c_6$$

$$c_3 = m_0$$

$$c_4 = m_1$$

$$c_5 = m_2$$

$$c_6 = m_3$$

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

$$cH^T = 0$$

$$s = rH^T(s_0s_1s_2) = (r_1r_2r_3r_4r_5r_6) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} =$$

$$= (r_0 \oplus r_3 \oplus r_5 \oplus r_6, r_1 \oplus r_3 \oplus r_4 \oplus r_5, r_4 \oplus r_2 \oplus r_4 \oplus r_5 \oplus r_6)$$

W macierzy H wszystkie kolumny są liniowo niezależne

Prawdopodobieństwo nie wykrycia błędu.(undetected error)

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

Prawdopodobieństwo nie możliwości poprawienia błędu

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

TO DO przepisać to długie równanie ze zdjęcia

Prawdopodobieństwo niemożliwości zdekodowania (uncodeded)

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

$p = 0.01 = 1\%$ błędnych bitów

$P_{uc} = 0.04\%$ błędnych wiadomości 4-bitowych

$P_{we} = 0.0021 = 2.1 \%$ - niepoprawialnych błędów $Pr_{ue} = 3 \cdot 10^{-6}$ - niewykrytych błędów

Nowe 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 ?

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

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

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

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 ??

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

$$\begin{aligned} m_0 &= (0000) & m_0(x) &= 0 & p_0(x) &= x^3 m(x) \mod g(x) = 0 \\ c_0(x) &= p_0(x) \oplus x^3 m(x) = 0 & c_0 &= (00000000) \end{aligned}$$

$$\begin{aligned} m_1 &= (1000) & m_1(x) &= 0 & p_1(x) &= x^3 m(x) \mod g(x) = 1 \oplus x \\ c_1(x) &= p_1(x) \oplus x^3 m(x) = 0 & c_0 &= (1101000) \end{aligned}$$