Information and Coding Theory

University of Chinese Academy of Sciences

Fall 2023

Kewei Lv, Liping Wang

Homework 10

Chenkai GUO

2023.12.4

1. *Let $g(x) = 1 + x^4 + x^6 + x^7 + x^8 \in F_2[x]$ be the generator polynomial of a binary $[15, 7]$-cyclic code C. Write down a generator matrix and a parity-check matrix for C. Construct a generator matrix of the form $(I_7|A)$*

   SOLUTION

   Since $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, *thus* $g_0 = 1, g_3 = 1, g_5 = 1, g_6 = 1, g_7 = 1$, *thus:*

$$G = \begin{pmatrix} 1&0&0&0&1&0&1&1&1&0&0&0&0&0&0 \\ 0&1&0&0&0&1&0&1&1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&1&0&1&1&1&0&0&0&0 \\ 0&0&0&1&0&0&0&1&0&1&1&1&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&1&1&1&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&1&1&1&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \end{pmatrix}_{7\times 15}$$

   then calculate $h(x) = (x^{15} - 1)/g(x)$*:*

$$\begin{array}{r|l}
 & x^7 + x^6 + x^4 + 1 \\ \hline
x^8 + x^7 + x^6 + x^4 + 1 & x^{15} + 1 \\
 & x^{15} + x^{14} + x^{13} + x^{11} + x^7 \\ \hline
 & \quad x^{14} + x^{13} + x^{11} + x^7 + 1 \\
 & \quad x^{14} + x^{13} + x^{12} + x^{10} + x^6 \\ \hline
 & \qquad x^{12} + x^{11} + x^{10} + x^7 + x^6 + 1 \\
 & \qquad x^{12} + x^{11} + x^{10} + x^8 + x^4 \\ \hline
 & \qquad\quad x^8 + x^7 + x^6 + x^4 + 1 \\
 & \qquad\quad x^8 + x^7 + x^6 + x^4 + 1 \\ \hline
 & \qquad\qquad\qquad\qquad 0
\end{array}$$

thus $h(x) = x^7 + x^6 + x^4 + 1$, *and then the reciprocal polynomial of* $h(x)$ *is* $h_R(x) = x^7 + x^3 + x + 1$, *thus a parity-check matrix for* C *is as follows:*

$$H = \begin{pmatrix} 1&1&0&1&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&1&0&1&0&0&0&1&0&0&0&0&0 \\ 0&0&0&1&1&0&1&0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&1&0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \end{pmatrix}_{8\times 15}$$

Transform the generator matrix G *above through* $r_1 = r_1 + r_5 + r_7, r_2 = r_2 + r_6, r_3 = r_3 + r_7$, *we got the generator matrix with standard form as follows:*

$$G_{std} = \begin{pmatrix} 1&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \\ 0&1&0&0&0&0&0&1&1&0&0&1&1&1&0 \\ 0&0&1&0&0&0&0&0&1&1&0&0&1&1&1 \\ 0&0&0&1&0&0&0&1&0&1&1&1&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&1&1&1&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&1&1&1&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&1 \end{pmatrix}_{7\times 15}$$

2. *Let* α *be a primitive element of* F_2^m *and let* $g(x) \in F_2[x]$ *be the minimal polynomial of* α *with respect to* F_2. *Show that the cyclic code of length* $2^m - 1$ *with* $g(x)$ *as the generator polynomial is in fact a binary* $[2^m - 1, 2^m - 1 - m, 3]$*-Hamming code*

   SOLUTION

   Since α *be a primitive element of* F_2^m, *thus* $deg(g(x)) = m = n - k, k = 2^m - 1 - m$
   Let $\forall c \in C, c = (c_0, c_1, c_2, \cdots, c_{n-1})$ *and* $f(x) = \pi(c)$
   Thus $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$
   Since $f(x) \in < g(x) >, g(\alpha) = 0$
   Thus $f(\alpha) = 0$, *thus* $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0$
   i.e. $\vec{c} \cdot \vec{\alpha} = 0, \vec{c} = (c_0, c_1, c_2, \cdots, c_{n-1})^T, \vec{\alpha} = (1, \alpha, \alpha^2, \cdots, \alpha^{n-1})^T$
   Then we could use $\vec{\alpha} = (1, \alpha, \alpha^2, \cdots, \alpha^{n-1})^T$ *to construct the parity-check matrix* $H_{(n-k)\times n}$ *of* C, *i.e.* $H_{m\times(2^m-1)}$
   Since α *be a primitive element of* F_2^m, *thus the columns of* $H_{m\times(2^m-1)}$ *are exactly all the nonzero vectors of* F_2^m, *thus* C *is a* $Ham[2^m - 1, 2]$ *hamming codes, and obviously the minimal distance of a* $2-ary$ *hamming code is* 3
   Summarizing: C *a binary* $[2^m - 1, 2^m - 1 - m, 3]$*-Hamming code*
   Q.E.D