Chap. 5 Polynomials and Cyclic Codes

□ Main topics

- Polynomial Representation
- Generator and Parity-check Polynomials
- Systematic Encoding of Cyclic Codes

□ Polynomial Representation

Any vector $\boldsymbol{c} = (c_0, c_1, \dots, c_{n-1})$ is represented by a polynomial

$$c(x) \;=\; c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \;\triangleq\; \sum_{i=0}^{n-1} c_i x^i.$$

Example: $\mathbb{F}_8$ defined by $p(x) = x^3 + x + 1$.

Elements	Power of primitive element α	Binary representation
0	$\alpha^{-\infty}$	0 0 0
1	α^0	0 0 1
α	α^1	0 1 0
α^2	α^2	1 0 0
$\alpha + 1$	α^3	0 1 1
$\alpha^2 + \alpha$	α^4	1 1 0
$\alpha^2 + \alpha + 1$	α^5	1 1 1
$\alpha^2 + 1$	α^6	1 0 1

Consider the [7,4] Hamming code whose parity check matrix is given by

$$\boldsymbol{H} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \left[\; \alpha^0 \;\; \alpha^1 \;\; \alpha^2 \;\; \alpha^3 \;\; \alpha^4 \;\; \alpha^5 \;\; \alpha^6 \;\right].$$