

CYCLIC CODES

parity check polynomial:

$$h(x) = \frac{x^m \oplus 1}{g(x)}$$

$$h(x) \cdot g(x) \equiv x^m \oplus 1 \equiv 0$$

Division with remainder: $a(x) = g(x) \cdot (x^m \oplus 1) + r(x)$

How to construct $g(x)$?

$$x^m \oplus 1 = \prod_{i=1}^m \varphi_i(x) \dots \text{irreducible polynomials}$$

$$x^m \oplus 1 = \varphi_1(x) \cdot \varphi_2(x) \cdot \varphi_3(x)$$

or

$$g(x) = \varphi_1(x) \quad h(x) = \varphi_2(x) \cdot \varphi_3(x)$$
$$g(x) = \varphi_1(x) \cdot \varphi_3(x) \quad h(x) = \varphi_2(x)$$

$$g(x) = \varphi_2(x)$$

$$h(x) = \varphi_1(x) \cdot \varphi_3(x) \quad \text{dual code}$$

Ex: $m=7$ $x^7 \oplus 1 = (x \oplus 1)(x^3 \oplus x + 1)(x^3 \oplus x^2 \oplus 1)$

$\varphi_1(x) \quad \varphi_2(x) \quad \varphi_3(x)$

$$g(x) = x^3 \oplus x \oplus 1 \quad \text{Hamming!}$$

$$h(x) = \varphi_1(x) \cdot \varphi_3(x) = x^4 \oplus x^3 \oplus x \oplus x^3 \oplus x^2 \oplus 1$$

$$h(x) = x^4 \oplus x^2 \oplus x \oplus 1$$

$$g(x) = \varphi_2(x) \cdot \varphi_3(x) \quad \text{Parity!}$$

$$h(x) = x \oplus 1$$

RELATION TO LINEAR CODES

$$g(x) = g_{m-k} \cdot x^{n-k} \oplus \dots \oplus g_1 \cdot x \oplus g_0 \cdot 1$$

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_{m-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{m-k} & \dots & 0 \\ \vdots & \dots & \dots & \dots & \dots & \dots & \vdots \\ & & & & & & g_{m-k} \end{bmatrix}$$

Ex: $g(x) = x^3 \oplus x \oplus 1$ $n=7, k=4$

$\Rightarrow \vec{g} = (1101) = (g_0 \ g_1 \ g_2 \ g_3)$ $x^6 = g(x) \cdot g(x) \oplus x^2 \oplus 1$

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

non-systematic code

$$\begin{array}{r} x^6 : x^3 \oplus x \oplus 1 = x^3 \oplus x \oplus 1 \\ \underline{x^6 \oplus x^4 \oplus x^3} \\ x^4 \oplus x^3 \\ \underline{x^4 \oplus x^2 \oplus x} \\ x^3 \oplus x^2 \oplus x \\ \underline{x^3 \oplus x \oplus 1} \\ \underline{\underline{x^2 \oplus 1}} \end{array}$$

$x^6 = (x^3 \oplus x \oplus 1) \cdot g(x) \oplus x^2 \oplus 1$
 $x^6 = g(x) \cdot g(x) \oplus x^2 \oplus 1$
 coincidence

→ systematic code?

parity sub-matrix:

$$\begin{array}{l} r_0(x) = x^{n-1} \pmod{g(x)} \\ r_1(x) = x^{n-2} \pmod{g(x)} \\ \vdots \\ r_{k-1}(x) = x^{n-k} \pmod{g(x)} \end{array}$$

$\rightarrow r_0, r_1, \dots, r_{k-1} \Rightarrow P = \begin{bmatrix} r_0 \\ r_1 \\ \dots \\ r_{k-1} \end{bmatrix}$

Ex: $g(x) = x^3 \oplus x \oplus 1$ $n=7$; $k=4 = n - \deg[g(x)]$

$r_0(x) = x^6 \pmod{g(x)} = x^2 \oplus 1$	$\vec{r}_0 = (101)$
$r_1(x) = x^5 \pmod{g(x)} = x^2 \oplus x \oplus 1$	$\vec{r}_1 = (111)$
$r_2(x) = x^4 \pmod{g(x)} = x^2 \oplus x$	$\vec{r}_2 = (011)$
$r_3(x) = x^3 \pmod{g(x)} = x \oplus 1$	$\vec{r}_3 = (110)$

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

systematic!

ENCODING USING LSR

LSR ... linear shift register

$$u(x) \rightarrow \vec{u} = (u_0 u_1 u_2 \dots u_{k-1})$$

$$g(x) \rightarrow \vec{g} = (g_0 g_1 \dots g_{n-k-1})$$

$$v(x) = u(x) \cdot g(x) \pmod{x^n \oplus 1}$$

↓

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

