Construction:

$$w(x) = u(x) \cdot g(x) \bmod x^n \oplus 1$$

n ... code length, k ... number of data bits

m ... number of parity bits

$g(x)$: generator polynomial

$\deg(g(x)) = m$

$g(x) \mid x^n \oplus 1$ (it divides $x^n \oplus 1$)

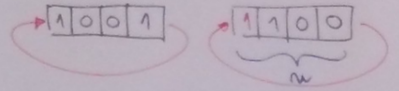
$\Rightarrow g(x) \cdot h(x) = x^n \oplus 1$

$h(x)$: parity check polynomial

$$w(x) \cdot h(x) = 0$$

BINARY CYCLIC CODES

- a bit rotation of a code word yields again a code word



Can be represented as polynomials of degree $n-1$

$\Rightarrow$ all operations performed in $\bmod x^n \oplus 1$

$\vec{w} = (1001) \Rightarrow w(x) = 1 \oplus x^3$

$\vec{w}' = (0110) \Rightarrow w'(x) = x \oplus x^2$

Ex $w = (1001) \Rightarrow w(x) = 1 \oplus x^3$

rotate one bit to the right:

$w'(x) = x \cdot w(x) = x \oplus x^4 \bmod x^4 \oplus 1$

$= 1 \oplus x$

$x^4 \oplus x : x^4 \oplus 1 = 1$ ← not interesting for us

$x^3 \oplus 1$

$x \oplus 1$ but this is

rotate 2 bits:

$w''(x) = x^2 \cdot w(x) = x^2 \oplus x^5 \bmod x^4 \oplus 1$

$= x \oplus x^2$

$x^5 \oplus x^2 : x^4 \oplus 1 = x$

$x^5 \oplus x$

$x^2 \oplus x$

Ex: $w = (1001)$ is a cyclic code

other code word are for sure: (0011), (0110), (1100)

001001

$\oplus 010001$

011000

CYCLIC CODES

parity check polynomial:

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

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

Divison with reminder: $a(x) = q(x) \cdot (x^n \oplus 1) + r(x)$

How to construct $g(x)$?

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

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

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

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

$\vdots$

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

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

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

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

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

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

$g(x) = \varphi_2(x) \cdot \varphi_3(x)$ Parity!

$h(x) = x \oplus 1$

RELATION TO LINEAR CODES

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

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

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

$\Rightarrow \vec{g} = (1101) = (g_0\, g_1\, g_2\, g_3)$

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

non-systematic code

$x^6 : x^3 \oplus x \oplus 1 = x^3 \oplus x \oplus 1$

$x^6 \oplus x^4 \oplus x^3$

$x^4 \oplus x^3$

$x^4 \oplus x^2 \oplus x$

$x^3 \oplus x^2 \oplus x$

$x^3 \oplus x \oplus 1$

$x^2 \oplus 1$

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

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

coincidence

→ systematic code?

parity sub-matrix:

$r_0(x) = x^{n-1} \bmod g(x) \rightarrow \vec{r}_0$

$r_1(x) = x^{n-2} \bmod g(x) \rightarrow \vec{r}_1$

$\vdots$

$r_{k-1}(x) = x^{n-k} \bmod g(x) \rightarrow \vec{r}_{k-1}$

$\Rightarrow P = \begin{bmatrix} \vec{r}_0 \\ \vec{r}_1 \\ \vdots \\ \vec{r}_{k-1} \end{bmatrix}$

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

$r_0(x) = x^6 \bmod g(x) = x^2 \oplus 1 \quad \vec{r}_0 = (101)$

$r_1(x) = x^5 \bmod g(x) = x^2 \oplus x \oplus 1 \quad \vec{r}_1 = (111)$

$r_2(x) = x^4 \bmod g(x) = x^2 \oplus x \quad \vec{r}_2 = (011)$

$r_3(x) = x^3 \bmod g(x) = x \oplus 1 \quad \vec{r}_3 = (110)$

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

systematic!