REVIEW OF LAST LECTURE

* ERROR DETECTION DECODING.

- SIMPLIFY THE DECODING PROCESS (LUT USED IN MAPPING ERROR SYNDROME TO THE ERROR PATTERN CAN BECOME PROHIBITIVELY LARGE.

- SOLUTION: MORE MATHEMATICAL STRUCTURE ⇒ CYCLIC CODES

* CODE PERFORMANCE

- RANDOM ERRORS: (REMEMBER WHAT WE SAID ABOUT RANDOM & BURST ERRORS IN LECTURE #1

- ERROR CORRECTION: FEC

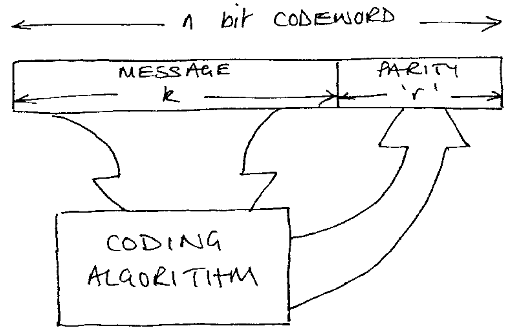
- ERROR DETECTION & RE-Tx : ARQ

NOTE

WE INTRODUCED THE CONCEPT OF SYSTEMATIC CODES BECAUSE WE COULD USE A NEAT MATHEMATICAL DESCRIPTION: THE SAME APPLIES TO CYCLIC CODES

CYCLIC POLYNOMIAL CODING

WE NEED TO DEFINE AN ALGEBRA WHICH WHICH ALLOWS THE CODEWORD TO BE DEFINED UNAMBIGUOUSLY. IT SHOULD ALSO ALLOW THE CHECK (OR PARITY) FIELDS TO BE SYSTEMATICLY CALCULATED



A 'k' BIT MESSAGE BLOCK HAS BEEN DESCRIBED AS A k-TUPLE (OR k-VECTOR)

$$M = \{m_1, m_2, m_3, \ldots\ m_k\}$$

WHERE $m_i \in \{0,1\}$

WE CAN EXPRESS M AS A POLYNOMIAL IN x, WHERE x IS AN OPERATOR, HENCE

$$M(x) = m_1 x^{k-1} + m_2 x^{k-2} + m_3 x^{k-3} + \ldots\ m_{k-1} x^1 + m_k \underset{=1}{x^0}$$

EACH POWER OF THE OPERATOR x REPRESENTS A ONE-BIT SHIFT IN TIME.

- THE LSB IS THE COEFFICIENT OF x^0
- THE MSB IS THE COEFFICIENT OF x^{k-1}

THE MESSAGE BLOCK IS SHIFTED OUT FOR TRANSMISSION MSB FIRST, i.e. FROM LEFT TO RIGHT.

FOR EXAMPLE

$$M = \underset{MSB}{\overset{M_1 x^6}{\{1}}, 0, 1, 1, 0, 1, \underset{LSB}{\overset{M_7 x^0}{1\}}} \qquad k=7$$

SO

$$M(x) = x^6 \oplus x^4 \oplus x^3 \oplus x \oplus 1$$

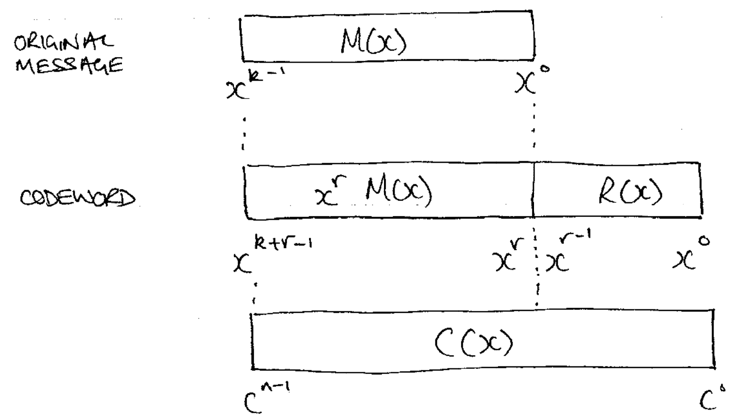
WE CAN ALSO WRITE

$$M(x) = \bigoplus_{i=1}^{k} M_i x^{k-i}$$

WHEN A CODEBLOCK IS TRANSMITTED A CHECK (PARITY) FIELD OF r BITS $(r = n-k)$ IS ADDED TO THE MESSAGE.

THE PARITY FIELD IS DESCRIBED BY THE POLYNOMIAL $R(x)$

HENCE;



THE x^r FACTOR INDICATES THAT THE MESSAGE FIELD IS SHIFTED TO THE LEFT BY 'r' BITS. HENCE;

$$C(x) = x^r M(x) \oplus R(x)$$

THAT IS TO SAY THE TRANSMITTED CODEWORD IS THE ADDITION OF THE MESSAGE FIELD AND THE PARITY FIELD i.e THE TWO ARE CONCATENATED

PROPERTIES OF CYCLIC CODES

CYCLIC CODES HAVE TWO FUNDAMENTAL PROPERTIES;

1) LINEARITY: THE SUM OF ANY TWO VALID CODEWORD YIELDS ANOTHER VALID CODEWORD.

2) CYCLIC: ANY CYCLIC SHIFT OF A CODEWORD YIELDS ANOTHER VALID CODEWORD

FOR A CODEWORD OF 'n' BITS (e.g. 7)

$$C(x) = \underset{\uparrow\, x^6}{c_1 x^{n-1}} \oplus c_2 x^{n-2} \oplus \dots \oplus c_{n-1} x^1 + c_n x^0$$

NOW WE SHIFT THE CODE TO THE LEFT BY MULTIPLYING THROUGH BY x;

$$x\,C(x) = \underset{\uparrow\, x^7}{c_1 x^{n}} \oplus c_2 x^{n-1} \oplus \dots \oplus c_{n-1} x^2 + c_n x$$

THIS IS NOT A CODEWORD SINCE IT IS OF DEGREE n (e.g $n=7$, degree 7)

HOWEVER IF WE DIVIDE $x\,C(x)$ BY $x^n \oplus 1$ WE HAVE . . .

QUOTIENT

$$\begin{array}{r|l} & c_1 \\ \hline x^n \oplus 1 & c_1 x^n \oplus c_2 x^{n-1} \oplus \dots \oplus c_n x^1 \\ & c_1 x^n \oplus \qquad\qquad\qquad\qquad c_1 \\ \hline & 0 \quad \underbrace{c_2 x^{n-1} \oplus \dots \oplus c_n x^1 \oplus c_1}_{\text{REMAINDER.}} \end{array}$$

THAT IS

$$\frac{x\,C(x)}{x^n \oplus 1} = c_1 + \frac{C'(x)}{x^n \oplus 1}$$

OR

$$x\,C(x) = c_1(x^n \oplus 1) + C'(x)$$

WHERE;

$$C'(x) = c_2 x^{n-1} \oplus \dots \oplus c_n x^1 \oplus c_1$$

<u>NOTE</u> $C'(x)$ IS THE CODEWORD $C(x)$ SHIFTED CYCLICALLY BY ONE POSITION (RECALL THAT;

$$C(x) = c_1 x^{n-1} \oplus c_2 x^{n-2} \oplus \dots c_{n-1} x^1 + c_n x^0$$

$C'(x)$ IS THE REMAINDER OBTAINED BY DIVIDING $x\,C(x)$ BY $x^n \oplus 1$.

i.e. $\quad C'(x) = x\,C(x) \bmod (x^n \oplus 1)$

SIMILARLY; $\quad x^i C(x) = Q(x)(x^n \oplus 1) + c^i(x)$

A CYCLIC CODE CAN BE GENERATED BY USING A <u>GENERATOR POLYNOMIAL</u> $g(x)$ OF DEGREE $r = n-k$.

THE $g(x)$ OF AN (n,k) CYCLIC CODE IS A FACTOR OF $x^n \oplus 1$ SINCE;

$$g(x) = x^{n-k} \oplus x^{n-k-1} \oplus \dots \quad \dots \oplus 1$$

WITH THE MESSAGE POLYNOMIAL GIVEN AS;

$$M(x) = m_1 x^{k-1} \oplus m_2 x^{k-2} \oplus \dots \quad \dots \oplus m_k x^0$$

THEN $C(x) = M(x)\,g(x)$ IS A POLYNOMIAL OF DEGREE $(n-1)$ OR LESS, AND IS A MULTIPLE OF $g(x)$.

THERE ARE 2^k POLYNOMIALS CORRESPONDING TO THE 2^k MESSAGE BLOCKS.

THE CODE PRODUCED IS CYCLIC BECAUSE,

$$x\,C(x) = C_1(x^n+1) \oplus C'(x)$$

AND SINCE $g(x)$ DIVIDES INTO BOTH $x\,C(x)$ $[= x\,M(x)\,g(x)]$ AND $x^n \oplus 1$ IT WILL ALSO DIVIDE INTO $C'(x)$. $C'(x)$ MUST BE A CODE POLYNOMIAL ie. $C'(x) = M'(x)\,g(x)$

<u>NB</u> CODEWORDS PRODUCED IN THIS WAY WILL NOT BE SYSTEMATIC

THE GENERATOR MATRIX $[G]$ THAT WE TALKED ABOUT IN LECTURE #3 CAN ALSO BE REPRESENTED IN POLY-NOMIAL FORM

eg $(7,3)$ SYSTEMATIC CODE

$$[G] = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right] \equiv \left[\begin{array}{ccc|cccc} x^6 & - & - & x^3 & x^2 & x & - \\ - & x^5 & - & - & x^2 & x & 1 \\ - & - & x^4 & x^3 & x^2 & - & 1 \end{array}\right]$$

THE GENERATOR MATRIX FOR A CYCLIC CODE IS MADE UP OF 'k' ROWS OF LINEARLY INDEPENDENT CODEWORDS.

GIVEN $g(x)$ THEN ...

$$[G] = \begin{bmatrix} x^{k-1} g(x) \\ \vdots \\ x^2\, g(x) \\ x^1\, g(x) \\ x^0\, g(x) \end{bmatrix}$$

OPERATING ON $[G]$ BY THE MESSAGE BLOCK (VECTOR)

$$M = [M_1\ M_2\ M_3\ \dots\ M_k]$$

GIVES THE CYCLIC POLYNOMIAL;

$$C = M[G]$$

HENCE

$$C(x) = M_1\, x^{k-1} g(x) \oplus M_2\, x^{k-2} g(x) \oplus \ldots$$

$$\ldots \oplus M_{k-1}\, x^1 g(x) \oplus M_k\, x^0 g(x)$$

$$C(x) = M(x)\, g(x)$$

SUCH A TECHNIQUE WILL PRODUCE A CYCLIC LINEAR CODE, (BUT NOT SYSTEMATIC)

ALL 2^k CODEWORDS SO PRODUCED ARE MULTIPLES OF $g(x)$ (CODEWORDS ARE THE ROWS OF [G] OR SUMS OF THE ROWS OF [G])

IN SYSTEMATIC FORM [G] CAN BE OBTAINED BY USING $g(x)$ AS BEFORE FOR THE k^{th} ROW, BUT

* FOR THE $(k-1)^{th}$ ROW, SHIFT k^{th} ROW $g(x)$ LEFT ONE COLUMN. IF NOT IN SYSTEMATIC FORM, ADD $g(x)$ TO IT.

* FOR THE $(k-2)^{th}$ ROW, SHIFT $(k-1)^{th}$ ROW $g(x)$ LEFT ONE COLUMN. IF NOT IN SYSTEMATIC FORM, ADD $g(x)$ TO IT.

* FOR THE $(k-3)^{th}$ ROW ....

ETC

FOR EXAMPLE

#1 CONSIDER A (7,4) CODE WITH THE GENERATOR POLYNOMIAL $g(x) = x^3 \oplus x \oplus 1$ (i.e. $x^r \ldots 1$)

$$[G] = \left[\begin{array}{cccc|ccc} x^6 & - & - & \cancel{x^3} & x^2 & - & 1 \\ - & x^5 & - & \cancel{x^3} & x^2 & x & 1 \\ - & - & x^4 & - & x^2 & x & - \\ - & - & - & x^3 & - & x & 1 \end{array}\right]_{k \times n = 4 \times 7}$$

#2. (7,3) CODE $g(x) = x^4 \oplus x^3 \oplus x^2 \oplus 1$

$$[G] = \left[\begin{array}{ccc|cccc} x^6 & - & - & x^3 & x^2 & x & - \\ - & x^5 & - & - & x^2 & x & 1 \\ - & - & x^4 & x^3 & x^2 & - & 1 \end{array}\right]_{k \times n = 3 \times 7} = [I_3 \mid P]$$

THE 2^k CODEWORDS ARE; $(2^k = 2^3 = 8)$

0 0 0	0 0 0 0
0 0 1	1 1 0 1
0 1 0	0 1 1 1
0 1 1	1 0 1 0
1 0 0	1 1 1 0
1 0 1	0 0 1 1
1 1 0	1 0 0 1
1 1 1	0 1 0 0

GENERATED BY LINEAR COMBINATIONS OF ROWS OF THE GENERATOR MATRIX (MOD-2 SUMS).

AS BEFORE, WE CAN RECONSTRUCT THE PARITY CHECK MATRIX;

$$[H] = [P^T \vdots I_r] = \left[\begin{array}{ccc:cccc} \multicolumn{3}{c}{\overbrace{\hphantom{1\ 0\ 1}}^{P^T}} & \multicolumn{4}{c}{\overbrace{\hphantom{1\ 0\ 0\ 0}}^{I_4}} \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]_{r \times n = 4 \times 7}$$

$$[H]^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}_{7 \times 4}$$

PROPERTIES OF $g(x)$ FOR (n,k) CODES

1. POLY-NOMIAL OF DEGREE $r = n-k$, with $x^0 \equiv 1$
   i.e. $x^r \oplus \ldots \oplus 1$

2. $g(x)$ IS A FACTOR OF $x^n \oplus 1$, so $\dfrac{x^n \oplus 1}{g(x)}$ GIVES NO REMAINDER.

ALL CYCLIC CODES CAN BE GENERATED BY AN APPROPRIATE $g(x)$.

HOW DO WE CHOOSE $g(x)$?

DISCUSSION OF HOW WE CHOOSE $g(x)$ IS BEYOND THE SCOPE OF THIS COURSE.

FOR LARGE VALUE OF n THE POLYNOMIAL $x^n \oplus 1$ MAY HAVE MANY FACTORS OF DEGREE $(n-k)$.

SOME $g(x)$ WILL GENERATE GOOD CYCLIC CODES OTHERS NOT SO GOOD.

FOR EXAMPLE; CONSIDER A $(7,k)$ CODE

$$x^7 \oplus 1 = (x \oplus 1)(x^3 \oplus x \oplus 1)(x^3 \oplus x^2 \oplus 1)$$

IF $k=4$; $(7,4)$ WE COULD USE; $(r=3)$

$$x^3 \oplus x \oplus 1 \quad \underline{\underline{\text{OR}}} \quad x^3 \oplus x^2 \oplus 1$$

IF $k=3$; $(7,3)$ WE COULD USE; $(r=4)$

$$(x \oplus 1)(x^3 \oplus x \oplus 1) \quad \underline{\underline{\text{OR}}} \quad (x \oplus 1)(x^3 \oplus x^2 \oplus 1)$$

> BOTH OF THESE ARE SINGLE ERROR CORRECTION CODES

CYCLIC CODE GENERATION - POLYNOMIAL ENCODING

(n,k) CODE $r = n-k$ $\quad g(x) = x^r \dots x^0$
$= x^{n-k} \dots x^0$

THE MESSAGE SEQUENCE;

$$M(x) = m_1 x^{k-1} \oplus m_2 x^{k-2} \oplus \dots \oplus m_{k-1} x^1 \oplus m_k x^0$$

THE OPERATION $x^r M(x)$ GENERATES A POLYNOMIAL OF DEGREE $n-1$ OR LESS (i.e SHIFT LEFT BY 'r' PLACES)

QUOTIENT

REMAINDER

$$\frac{x^r M(x)}{g(x)} = Q(x) \oplus \frac{R(x)}{g(x)}$$

OF ORDER $k-1$ OR LESS

(mod-2 add^n same as sub^n)

$$\Rightarrow \quad \frac{x^r M(x)}{g(x)} \oplus \frac{R(x)}{g(x)} = Q(x)$$

MULTIPLYING BY $g(x)$

$$\Rightarrow \quad x^r M(x) \oplus R(x) = Q(x)\,g(x) = C(x)$$

MULTIPLYING $Q(x)$ BY $g(x)$
SO MUST BE A CODE WORD.

WHERE:

$$R(x) = \text{rem.}\ \frac{x^r M(x)}{g(x)}$$

AND

$$C(x) = x^r M(x) \oplus R(x) \quad \text{IS DIVISIBLE BY } g(x)$$

FOR EXAMPLE #3 $(7,3)$ CODE WITH $g(x) = x^4 \oplus x^3 \oplus x^2 \oplus 1$
WITH $M(x) = 1$ (ie $m = (001)$)

REMAINDER $R(x) = \text{rem.}\ \dfrac{x^r M(x)}{g(x)} = \dfrac{x^4 . 1}{x^4 \oplus x^3 \oplus x^2 \oplus 1}$

$$\begin{array}{r l}
 & 1 \\
x^4 \oplus x^3 \oplus x^2 \oplus 1 \,) & x^4 \\
 & x^4 \oplus x^3 \oplus x^2 \oplus 1 \\
\hline
 & 0 \quad x^3 \oplus x^2 \oplus 1 \quad = R(x)
\end{array}$$

$$R(x) = x^3 \oplus x^2 \oplus 1$$

$$C(x) = x^r M(x) \oplus R(x)$$
$$\Rightarrow C(x) = x^4 . 1 \oplus [x^3 \oplus x^2 \oplus 1]$$
$$= x^4 \oplus x^3 \oplus x^2 \oplus 1$$

ie $C(x) = [0\,0\,1\,1\,1\,0\,1]$

EXAMPLE #4 $(7,3)$ AS BEFORE, $M(x) = (1,1,1)$

$$R(x) = \text{rem.}\ \frac{x^r M(x)}{g(x)} = \text{rem.}\ \frac{x^4(x^2 \oplus x \oplus 1)}{x^4 \oplus x^3 \oplus x^2 \oplus 1}$$

$$R(x) = \text{rem.}\ \frac{x^6 \oplus x^5 \oplus x^4}{x^4 \oplus x^3 \oplus x^2 \oplus 1}$$

$$\begin{array}{r|l} & x^2 \\ \hline x^4 \oplus x^3 \oplus x^2 \oplus 1 & x^6 \oplus x^5 \oplus x^4 \\ & x^6 \oplus x^5 \oplus x^4 \quad \oplus x^2 \\ \hline & 0 \quad 0 \quad 0 \quad\quad x^2 \end{array}$$

$$R(x) = x^2; \quad \Rightarrow \quad C(x) = x^r M(x) \oplus R(x)$$
$$= x^4(x^2 \oplus x \oplus 1) \oplus x^2$$
$$= x^6 \oplus x^5 \oplus x^4 \oplus x^2$$

$$\Rightarrow C(x) = (1,1,1,0,1,0,0)$$

NOTE: IN EACH OF THE PREVIOUS EXAMPLES THE CODEWORD POLYNOMIAL $C(x)$ IS DIVISIBLE BY $g(x)$ WITH NO REMAINDER.

FROM EXAMPLE #4 $g(x) = x^4 \oplus x^3 \oplus x^2 \oplus 1$

$$\begin{array}{r|l} & x^2 \\ \hline x^4 \oplus x^3 \oplus x^2 \oplus 1 & x^6 \oplus x^5 \oplus x^4 \oplus x^2 \\ & x^6 \oplus x^5 \oplus x^4 \oplus x^2 \\ \hline & 0 \quad 0 \quad 0 \quad 0 \end{array}$$

$g(x)\overline{)C(x)}$

FROM EXAMPLE #3; $C(x) = x^4 \oplus x^3 \oplus x^2 \oplus 1 \equiv g(x)$

SYNDROME CALCULATION: ERROR DETECTION & ERROR CORRECTION

THE TRANSMITTED CODEWORD $C(x)$;

$$C(x) = x^r M(x) \oplus R(x)$$

SINCE THE REMAINDER HAS BEEN SUBTRACTED FROM THE DIVISION, $C(x)$ IS NOW EXACTLY DIVISIBLE BY $g(x)$, AND IS $k+r=n$ DIGITS LONG.

AT THE RECEIVER THE DIVISION IS CARRIED OUT AGAIN AND THE REMAINDER EXAMINED

THE <u>ERROR PATTERN</u> CAN BE DEFINED BY THE ERROR POLYNOMIAL $E(x)$, WHICH LOCATES THE POSITION OF THE ERRORS.

THUS;

$$R_x(x) = C(x) \oplus E(x)$$

RECEIVED CODEWORD POLY.

PERFORMING THE DIVISION AT THE RECEIVER OF $R_x(x)$ BY $g(x)$;

$$\frac{R_x(x)}{g(x)} = \frac{C(x)}{g(x)} \oplus \frac{E(x)}{g(x)}$$

NO REMAINDER BY DEFINITION

IF $E(x)$ IS NOT DIVISIBLE BY $g(x)$ THE ERROR CODE WILL BE RECOGNIZED

THE ADVANTAGE OF THIS TECHNIQUE IS THAT THE POLYNOMIAL DIVISION CAN BE CARRIED OUT BY SIMPLE, SHORT (r-STAGES) SHIFT REGISTER FEED BACK CIRCUITS, WHICH CAN OPERATE AT HIGH DATA RATES

SYNDROME CALCULATION FOR CYCLIC-CODES

THE SYNDROME;

$$S(x) = \frac{R_x(x)}{g(x)} = \frac{E(x)}{g(x)}$$

IS EQUAL TO THE REMAINDER RESULTING FROM THE DIVISION AND CONTAINS INFORMATION ABOUT THE ERROR PATTERN WHICH CAN BE USED FOR ERROR CORRECTION.

* IF THE SYNDROME IS <u>ZERO</u> EITHER THE BLOCK IS ERROR-FREE <u>OR</u> AN UNDETECTABLE ERROR HAS OCCURED

* THERE ARE 2^r-1 <u>NON-ZERO</u> SYNDROMES WHICH CAN INDICATE THE NUMBER OF ERROR PATTERNS THAT CAN OCCUR, AND BE CORRECTED

AS FOR NON-CYCLIC CODES, TABLE LOOK-UP DECODING CAN BE USED TO OBTAIN THE ERROR PATTERN ONCE THE SYNDROME HAS BEEN CALCULATED.

THIS IS EASY ENOUGH FOR SHORT CODES BUT CAN SOON BECOME IMPRACTICAL.

SPECIAL CLASSES OF CYCLIC CODES HAVE BEEN DEVELOPED FOR ERROR CORRECTION WITHOUT REQUIRING EXCESSIVELY COMPLEX DECODING CIRCUITS;

* BCH (BOSE-CHAUDHURI-HOQUENGHEM)

* GOLAY

* REED-SOLOMON (R-S)