E.g. $\quad x^3\ x^2\ x^1\ x^0$

$k = 4 \quad : \quad (1\ 1\ 0\ 0)$

$n-k = 3 \quad : \quad g(x) = x^3 + x + 1$

$(1\ 0\ 1\ 1)$

$n = 7$

① $i(x) = x^3 + x^2$

② $g(x) = x^3 + x + 1$

③ $a(x) = i(x) * x^3 = x^6 + x^5 = g(x) * q(x) + r(x)$

④

$$x^3 + x^2 + x \leftarrow q(x)$$

$$x^3+x+1 \ \big)\ x^6 + x^5 \leftarrow a(x)$$

$g(x)$

$$x^6 + x^4 + x^3$$
$$x^5 + x^4 + x^3$$
$$x^5 + x^3 + x^2$$
$$x^4 + x^2$$
$$x^4 + x^2 + x$$
$$x \Leftarrow r(x)$$

⑤ $b(x) = a(x) + r(x) = x^6 + x^5 + x$

⑥ $b(x) = x^6 + x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + x + 0 \cdot x^0$

$(1\ 1\ 0\ 0 \ \vdots\ 0\ 1\ 0)$

codeword bits

$$1011 \ \big)\ 1\ 1\ 0\ 0\ 0\ 0\ 0$$
$$1\ 0\ 1\ 1$$
$$1\ 1\ 1\ 0$$
$$1\ 0\ 1\ 1$$
$$1\ 0\ 1\ 0$$
$$1\ 0\ 1\ 1$$
$$0\ 1\ 0$$

(n-k) check bits

n-k=3

codeword : $(1\ 0\ 1\ 1\ 0\ 1\ 0) = 1\ 1\ 0\ 0\ 0\ 0\ 0 + 1\ 0 = 1\ 1\ 0\ 0\ 0\ 1\ 0$

E.g.

$$x^3\ x^2\ x^1\ x^0$$

$k = 4$: $(0\ 1\ 0\ 1)$

$n-k = 3$: $g(x) = x^3 + x + 1$

$n = 7$

① $i(x) = x^2 + 1$

② $g(x) = x^3 + x + 1$

③ $a(x) = (x^2 + 1) * x^3 = x^5 + x^3$

④

$$
\begin{array}{r l}
 & x^2 \\
\Rightarrow x^3 + x + 1 \,\big) & x^5 + x^3 \\
 & x^5 + x^3 + x^2 \\
\hline
 & x^2 = r(x)
\end{array}
$$

⑤ $b(x) = a(x) + r(x)$

$= x^5 + x^3 + x^2$

⑥ codeword bits:

0 1 0 1 1 0 0

(*)

"Pattern"

$b(x) = a(x) + r(x)$

$= g(x) * q(x) + r(x) + r(x)$

$= g(x) * q(x) + \boxed{r(x) + r(x)}$

⇑ ?

0

$= g(x) * q(x)$ ← quotient poly.

↑

generator poly.

* b(x) is a multiple of g(x)

e.g.

$r(x) = x$

$r(x) + r(x) = x + x = 0$

At decoder:

n received bits $\longrightarrow$ $R(x)$ (dividend poly.) $\xrightarrow{g(x) \text{ as divisor poly.}}$ remainder poly. = 0 ?

- Yes: no error
- No: Error!

At encoder:

k info bits $\xrightarrow{①}$ $i(x)$ $\longrightarrow$ $a(x)$ $\longrightarrow$ $r(x)$ $\longrightarrow$ $\oplus$ $\longrightarrow$ $b(x)$ $\xrightarrow{⑥}$ n codeword bits

③ $a(x) = i(x) * x^{n-k}$

④ $a(x) \to r(x)$, with $g(x)$ as divisor poly

⑤ $\oplus$: $a(x)$ added to $r(x)$

② $g(x)$; degree of $g(x)$ = n-k

Polynomial Codes

- They are also known as CRC codes
  - Check bits are generated in the form of a Cyclic Redundancy Check
  - Implemented using the shift-register circuit

- The k information bits ($i_{k-1}, i_{k-2}, \ldots, i_1, i_0$) are used as binary coefficients to form the information polynomial of degree (k – 1):

$$i(x) = i_{k-1}x^{(k-1)} + i_{k-2}x^{(k-2)} + \ldots + i_1x + i_0$$

- The polynomial code uses binary polynomial arithmetic to calculate the codeword corresponding to the information polynomial

Binary Polynomial Arithmetic

Addition: $(x^7 + x^6 + 1) + (x^6 + x^5) = x^7 + (1 + 1)x^6 + x^5 + 1 = x^7 + x^5 + 1$

Multiplication: $(x + 1)(x^2 + x + 1) = x^3 + x^2 + x + x^2 + x + 1 = x^3 + 1$

Division:

$$
\begin{array}{rl}
 & x^3 + x^2 + x \quad = q(x) \quad \text{quotient} \\
\cline{2-2}
x^3 + x + 1 \;\big) & x^6 + x^5 \quad \text{dividend} \\
 & x^6 + \quad\;\; x^4 + x^3 \\
\cline{2-2}
 & \quad x^5 + x^4 + x^3 \\
 & \quad x^5 + \quad\;\; x^3 + x^2 \\
\cline{2-2}
 & \qquad x^4 + \quad\;\; x^2 \\
 & \qquad x^4 + \quad\;\; x^2 + x \\
\cline{2-2}
 & \qquad\qquad\quad x \quad = r(x) \quad \text{remainder}
\end{array}
$$

divisor

Polynomial Encoding

- k information bits define the information polynomial of degree $(k – 1)$

$$i(x) = i_{k-1}x^{(k-1)} + i_{k-2}x^{(k-2)} + \ldots + i_2x^2 + i_1x + i_0$$

- A CRC code is specified by its generator polynomial of degree $(n – k)$ to generate $(n – k)$ check bits

$$g(x) = x^{(n-k)} + g_{n-k-1}x^{(n-k-1)} + \ldots + g_2x^2 + g_1x + 1$$

- $x^{(n-k)}\, i(x)$ is the dividend polynomial
- Find the remainder polynomial $r(x)$ of at most degree $(n – k – 1)$

$$x^{(n-k)}\, i(x) = q(x)\, g(x) + r(x)$$

- Get the codeword polynomial of degree $(n – 1)$

$$\boxed{b(x) = x^{(n-k)}\, i(x) + r(x)}$$

The Pattern in Polynomial Code

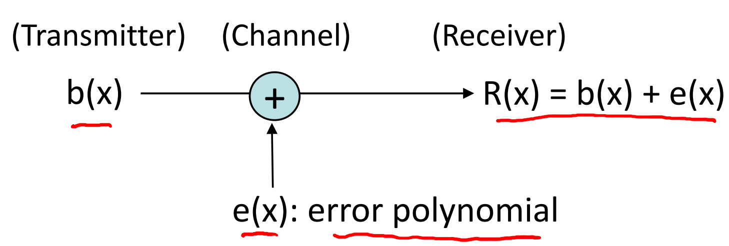
- All codeword polynomials satisfy the following pattern:

  $b(x) = x^{(n-k)} i(x) + r(x) = q(x)g(x) + r(x) + r(x) = q(x)g(x)$

  In other words, all codeword polynomials are multiples of g(x)!

- Receiver should
  - Convert the received n-bit block into a degree-(n-1) dividend polynomial
  - Divide the dividend polynomial by g(x)
  - Check whether the remainder polynomial is zero
  - If the remainder polynomial is non-zero, then the received n-bit block is not a valid codeword → error detected

Undetectable Errors



e : error vector

- e(x) has "1" coefficients in error locations & "0" coefficients elsewhere

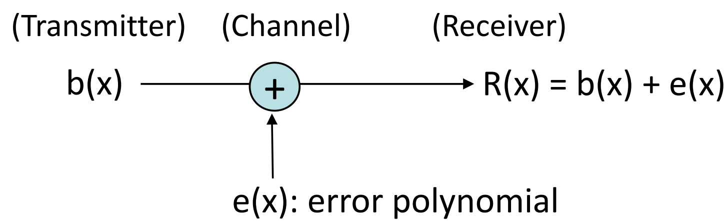
$\boxed{R(x)} = b(x) + e(x)$ ← undetectable

$g(x) * q''(x) = g(x) * q(x) + e(x)$

↑ if e(x) is also a multiple of g(x)

$e(x) = g(x) * q'(x)$

Undetectable Errors



- e(x) has "1" coefficients in error locations & "0" coefficients elsewhere

- If e(x) is a multiple of g(x), then:
  R(x) = b(x) + e(x) = q(x)g(x) + q'(x)g(x) = [q(x) + q'(x)] g(x)

⊛ ⇒ If a non-zero error polynomial is divisible by g(x),
then the corresponding error is undetectable

E.g. $g(x) = x^3 + x + 1$ (1 0 1 1) $k = 4$, $n = 7$

$e = [1\ 0\ 0\ 0\ 0\ 0\ 1]_{1\times 7}$ (x^6 … x^1 x^0)

$e(x) = x^6 + 1$

M = 2 : 2-bit error
L = 7

$$
\begin{array}{r|l}
 & x^3 + x + 1 \\
\hline
x^3 + x + 1 & x^6 + 1 \\
 & x^6 + x^4 + x^3 \\
\hline
 & x^4 + x^3 + 1 \\
 & x^4 + x^2 + x \\
\hline
 & x^3 + x^2 + x + 1 \\
 & x^3 + x + 1 \\
\hline
 & x^2
\end{array}
$$

x^2 ⇐ non-zero remainder poly.

$$
\begin{array}{r|l}
1011 & 1000001 \\
 & 1011 \\
\hline
 & 1100 \\
 & 1011 \\
\hline
 & 1111 \\
 & 1011 \\
\hline
 & 100
\end{array}
$$

100 ← non-zero

⇒ e is detectable

$$\overbrace{(1\ 0\ 1\ 1)}$$

$g(x) = x^3 + x + 1$ $\qquad k=4 \qquad n=7$

$e = [\,0\ \underbrace{1\ 0\ 1\ 1}\ 0\ 0\,]_{1\times 7}$

$e(x)$ is divisible by $g(x)$? Yes $\Rightarrow$ undetectable

$$
\begin{array}{r|l}
1011 & 0\ 1\ 0\ 1\ 1\ 0\ 0 \\
 & \ \ \ 1\ 0\ 1\ 1 \\
\hline
 & \ \ \ 0\ 0\ 0\ 0\ 0\ 0
\end{array}
\leftarrow \underline{\text{zero}}
$$

$e(x)$ is multiple of $g(x)$