Lecture 10
Information Redundancy - Part IV

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Key concepts from last class
- Cyclic codes
  - One more example on encoding
  - Decoding
  - Error detection
- TODOs

Cyclic codes

Cyclic: any circular shift of a codeword produces another codeword

- Move the bit at the rightmost position to the leftmost position
- Shift all other bits by one position to the right

For example:

- Consider the codeword 10110
- Circular shift by one position to the right: 01011
- Circular shift by two positions to the right: 10101
- …

Properties of linear cyclic codes

In practice, cyclic codes designed for error detection should have two main properties:

Property 1: Linear

- The sum of any two or more codewords in C is again a codeword in C.

Property 2: Cyclic

- For a codeword in C, all its cyclic shifts are also codewords.

Example: (7, 4) cyclic code

Question: Find a generator polynomial for (7, 4) cyclic code.

Answer:

(7, 4) cyclic code means 7 bits to encode 4 bits of data (n=7, k=4).

g(x) must contain the two following properties:

- g(x) should be of a degree (n - k) = 7 - 4 = 3
- g(x) should divide $1+x^7$ without a remainder

Two important properties to remember:

- g(x) has a degree (n-k)
- g(x) divides $1 + x^n$ without a remainder

$1+x^7$ can be factored as:

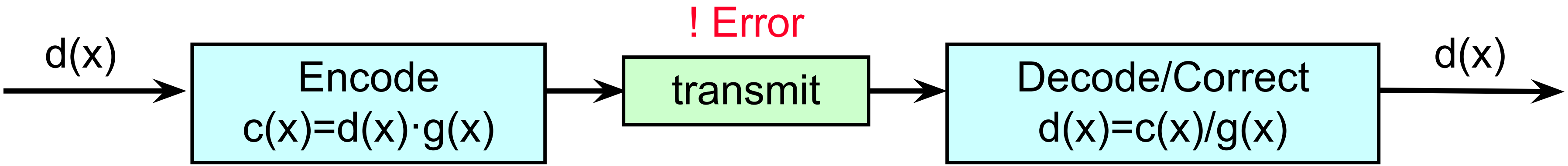
$$1+x^7 = (1+x+x^3)(1+x^2+x^3)(1+x)$$

- so, we can choose for g(x) either $1+x+x^3$ or $1+x^2+x^3$

Generator polynomial

Generator polynomial, denoted as g(x), is used to:

- encode the data polynomial into codeword polynomial.
- decode the codeword polynomial back to the data polynomial.



Example on encoding

Suppose $g(x) = (1+x+x^3)$ for a (7,4) cyclic code

Question: Find the codewords for the following data: 0001, 1001, 0110, 1000

Multiply data polynomial by generator polynomial:

$$c(x) = d(x).g(x)$$

Example on encoding

Suppose $g(x) = (1+x+x^3)$ for a (7,4) cyclic code

Question: Find the codewords for the following data: 0001, 1001, 0110, 1000

Solution: For each entry in the data (e.g., 0001, 1001):

- Step 1: convert it into a data polynomial
- Step 2: solve the codeword polynomial multiplication

Hint: use the circular shifting property to calculate the codeword polynomial instead. It is much faster.

Step 1: data polynomial

Data = {1001}

The data can be represented as a polynomial:

$$a(x) = a_0.x^0 + a_1.x^1 + \ldots + a_{n-1}.x^{n-1}$$

The data can also be visualized as:

$$\underline{1}\ \underline{0}\ \underline{0}\ \underline{1}$$

$$\boxed{1 \cdot x^0} \quad \boxed{0 \cdot x^1} \quad \boxed{0 \cdot x^2} \quad \boxed{1 \cdot x^3}$$

So we represent 1001 as:

$$d(x) = 1 \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + 1 \cdot x^3 = 1 + x^3$$

Step 2: solve polynomial multiplication

Data polynomial: $d(x) = 1 + x^3$

Generator polynomial: $g(x) = 1 + x + x^3$

Solve $c(x) = d(x).g(x)$

$$
\begin{aligned}
c(x) = d(x).g(x) &= (1 + x^3)(1 + x + x^3) \\
&= 1 + x + \boxed{x^3 + x^3} + x^4 + x^6 \\
&= 1 + x + x^4 + x^6
\end{aligned}
$$

$a_3 = 2$, same as 0

Step 2: solve polynomial multiplication

Data polynomial: $d(x) = 1 + x^3$

Generator polynomial: $g(x) = 1 + x + x^3$

Solve $c(x) = d(x).g(x)$

$$
\begin{aligned}
c(x) = d(x).g(x) &= (1 + x^3)(1 + x + x^3) \\
&= 1 + x + x^3 + x^3 + x^4 + x^6 \\
&= 1 + x + x^4 + x^6
\end{aligned}
$$

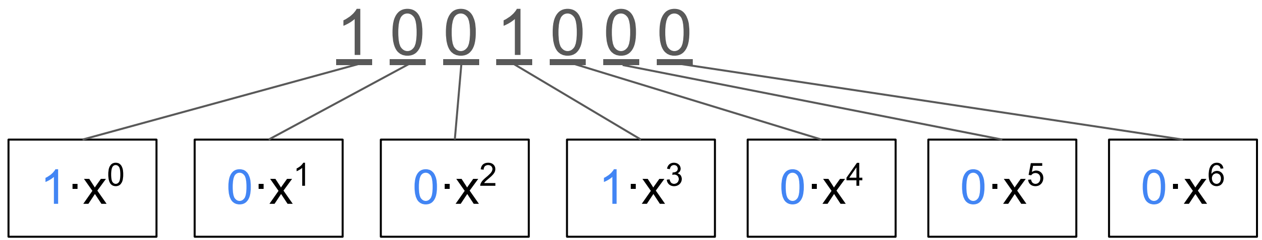
$c(x) = \{1100101\}$

Time-consuming if you need to calculate more than one codeword!

Alternative solution: with cyclic property

Given (7,4) cyclic code, n = 7

$d(x) = 1 + x^3 = 1001000$



- In codeword polynomial, we always write least significant digit on the left
- $1001000 = 1 + x^3 = 1001$

Alternative solution: with cyclic property

Given (7,4) cyclic code, n = 7

$d(x) = 1 + x^3 = 1001000$

Updated Lecture 9 - slide 29

$$\underline{1}\ \underline{0}\ \underline{0}\ \underline{1}\ \underline{0}\ \underline{0}\ \underline{0}$$

$$\boxed{1 \cdot x^0}\quad \boxed{0 \cdot x^1}\quad \boxed{0 \cdot x^2}\quad \boxed{1 \cdot x^3}\quad \boxed{0 \cdot x^4}\quad \boxed{0 \cdot x^5}\quad \boxed{0 \cdot x^6}$$

- In codeword polynomial, we write least significant digit on the left
- $1001000 = 1 + x^3 = 1001$

Alternative solution: with cyclic property

$d(x) = 1 + x^3 = 1001000$

$g(x) = 1 + x + x^3$

We multiply d(x) by g(x) to get c(x):

Cyclic property on multiplication: $x \cdot c(x)$ is the same as shifting c(x) by one position

We can use the cyclic property to compute the multiplication for each term in g(x):

- Multiplication $(1 \cdot (1 + x^3))$: No shifting, 1001000

Alternative solution: with cyclic property

$d(x) = 1 + x^3 = 1001000$

$g(x) = 1 + x + x^3$

We multiply d(x) by g(x) to get c(x):

> **Cyclic property on multiplication**: $x \cdot c(x)$ is the same as shifting c(x) by one position

We can use the cyclic property to compute the multiplication for each term in g(x):

- Multiplication $(1 \cdot (1 + x^3))$: No shifting, 1001000
- Multiplication $(x \cdot (1 + x^3))$: Shifting by one position, 1001000 → 0100100

Alternative solution: with cyclic property

$d(x) = 1 + x^3 = 1001000$

$g(x) = 1 + x + x^3$

We multiply d(x) by g(x) to get c(x):

> Cyclic property on multiplication: $x \cdot c(x)$ is the same as shifting c(x) by one position

We can use the cyclic property to compute the multiplication for each term in g(x):

- Multiplication $(1 \cdot (1 + x^3))$: No shifting, 1001000
- Multiplication $(x \cdot (1 + x^3))$: Shifting by one position, 1001000 → 0100100
- Multiplication $(x^3 \cdot (1 + x^3))$: Shifting by three positions, 1001000 → 0001001

Alternative solution: with cyclic property

We get the codeword by adding the three terms together (distributive law)

$$\begin{array}{rl} & 1\,0\,0\,1\,0\,0\,0 \\ & 0\,1\,0\,0\,1\,0\,0 \\ + & 0\,0\,0\,1\,0\,0\,1 \\ \hline & 1\,1\,0\,0\,1\,0\,1 \end{array}$$

By cyclic property, $d(x)\cdot g(x) = 1100101$

Example on encoding

No shifting, 1 shifting, 3 shifting

Suppose $g(x)$ = $\boxed{(1+x+x^3)}$ for a (7,4) cyclic code

Question: Find the codewords for the following data: 0001, 1001, 0110, 1000

Solution: Using the circular shifting property, compute for d(x)·g(x)

For data = {0001000}, d(x)·g(x) = 0001000 + 0000100 + 0000001 = 0001101

Example on encoding

Suppose $g(x) = (1+x+x^3)$ for a (7,4) cyclic code

Question: Find the codewords for the following data: 0001, 1001, 0110, 1000

Solution: Using the circular shifting property, compute for d(x)·g(x)

For data = {0001000}, d(x)·g(x) = 0001000 + 0000100 + 0000001 = 0001101

For data = {1001000}, d(x)·g(x) = 1001000 + 0100100 + 0001001 = 1100101

Example on encoding

Suppose $g(x) = (1+x+x^3)$ for a (7,4) cyclic code

Question: Find the codewords for the following data: 0001, 1001, 0110, 1000

Solution: Using the circular shifting property, compute for d(x)·g(x)

For data = {0001000}, d(x)·g(x) = 0001000 + 0000100 + 0000001 = 0001101

For data = {1001000}, d(x)·g(x) = 1001000 + 0100100 + 0001001 = 1100101

For data = {0110000}, d(x)·g(x) = 0110000 + 0011000 + 0000110 = 0101110

For data = {1000000}, d(x)·g(x) = 1000000 + 0100000 + 0001000 = 1101000

Schedule for today

- Key concepts from last class
- Cyclic codes
  - One more example on encoding
  - Decoding
  - Error detection
- TODOs

Decoding

Divide codeword polynomial c(x) by
the generator polynomial g(x):
d(x) = c(x)/g(x)

If no error occurred:

- The received codeword is the correct codeword c(x)
- Therefore, d(x) = c(x)/g(x), the remainder from the division is zero

Polynomial division

To divide two polynomials:

- We do the division of polynomials the same way as we do long division.
- Except the subtraction is modulo 2.

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\ \hline
 &
\end{array}
$$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\
\cline{2-2}
x^6 + x^4 + x^3 & x^3 \\
\cline{1-1}
\quad x^5 + x^2 + x + 1 &
\end{array}
$$

We define addition and subtraction as modulo 2 with no carries.

This means addition = subtraction = XOR.

Subtraction for codewords

The “subtraction” here is different from the ordinary subtraction of numbers in two respects:

- No borrowing, each bit is independent of each other bit
- If 1 + 1 = 0, then 0 - 1 = 1, hence:
  - 0 - 0 = 0, or $0 \oplus 0 = 0$
  - 0 - 1 = 1, or $0 \oplus 1 = 1$
  - 1 - 0 = 1, or $1 \oplus 0 = 1$
  - 1 - 1 = 0, or $1 \oplus 1 = 0$

-	**0**	**1**
0	0	1
1	1	0

Polynomial division (1)

$$
\begin{array}{l|l}
\boxed{x^6} + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\
\underline{\boxed{x^6} + x^4 + x^3} & \overline{x^3} \\
\quad x^5 + x^2 + x + 1 &
\end{array}
$$

Think of the xor operation

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + \boxed{x^5} + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\
\underline{x^6 + x^4 + x^3} & \overline{x^3} \\
\quad x^5 &
\end{array}
$$

$1 \oplus 0 = 1$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + \boxed{x^4} + x^3 + x^2 + x + 1 & x^3 + x + 1 \\
\cline{2-2}
x^6 + \boxed{x^4} + x^3 & x^3 \\
\cline{1-1}
\quad x^5 &
\end{array}
$$

$1 \oplus 1 = 0$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + \boxed{x^3} + x^2 + x + 1 & x^3 + x + 1 \\
\underline{x^6 + x^4 + \boxed{x^3}} & \hline \\
\quad x^5 & x^3
\end{array}
$$

$\boxed{1 \oplus 1 = 0}$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + \boxed{x^2} + x + 1 & x^3 + x + 1 \\ \hline
x^6 + x^4 + x^3 & x^3 \\ \cline{1-1}
\quad x^5 + x^2 &
\end{array}
$$

$1 \oplus 0 = 1$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + \boxed{x + 1} & x^3 + x + 1 \\
\cline{2-2}
x^6 + x^4 + x^3 & x^3 \\
\cline{1-1}
\quad x^5 + x^2 + x + 1 &
\end{array}
$$

$1 \oplus 0 = 1$

Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\ \hline
x^6 + x^4 + x^3 & x^3 + x^2 \\ \hline
x^5 + x^2 + x + 1 & \\
x^5 + \boxed{x^3} + x^2 & \\ \hline
x^3 + x + 1 &
\end{array}
$$

$0 \oplus 1 = 1$

Polynomial division (1)

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

No error

Polynomial division (2)

$$
\begin{array}{r|l}
x^8 + x^5 + x^4 + x^2 + 1 & x^3 + x + 1 \\
\cline{2-2}
x^8 + x^6 + x^5 & x^5 + x^3 + 1 \\
\hline
x^6 + x^4 + x^2 + 1 & \\
x^6 + x^4 + x^3 & \\
\cline{1-1}
x^3 + x^2 + 1 & \\
x^3 + x + 1 & \\
\cline{1-1}
x^2 + x & \boxed{\text{Error}}
\end{array}
$$

Decoding (no error)

- If no error occurred
  - The received codeword is the correct codeword $c(x)$
  - Therefore, $d(x) = c(x)/g(x)$, the remainder from the division is zero

Decoding (in presence of error)

- Suppose an error has occurred, then

  $c^{received}(x) = c(x) + e(x)$, $e(x)$ = error polynomial

  $d^{received}(x) = (c(x) + e(x))/g(x)$

Unless $e(x)$ is a multiple of $g(x)$, the received codeword will not be evenly divisible by $g(x)$.

- If $e(x)$ is a multiple of $g(x)$, the remainder of $e(x)/g(x)$ is 0 and the error will not be detected.

Schedule for today

- Key concepts from last class
- Cyclic codes
  - One more example on encoding
  - Decoding
  - Error detection
- TODOs

Example of error detection

Suppose that there is an error during transmission with the following polynomials:

$d(x) = (1011) = x^3 + x^2 + 1$ $\quad g(x) = x^3 + x + 1$ $\quad e(x) = x^3 + 1$

Question: Prove that this cyclic code can detect the error, then find the remainder.

- Calculate the codeword polynomial:

$$c(x) = d(x).g(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

- Calculate the received codeword:

$$c^{received} = c(x) + e(x) = x^6 + x^5 + x^4 + x^2 + x$$

- Calculate the data polynomial through division:

$$d(x) = c^{received}/g(x) = (x^6 + x^5 + x^4 + x^2 + x) / (x^3 + x + 1)$$

- Remainder is x, so the error is detected.

Summary of cyclic code

- Any circular shift of a codeword produces another codeword.
- Code is characterized by its generator polynomial g(x), with a degree (n-k), where n = bits in codeword, k = bits in data.
- All calculations are done in mod 2 arithmetic.
  - Multiplication of polynomial for encoding
  - Division of polynomial for decoding
- Cyclic code detects all single errors and all multiple adjacent error affecting (n-k) bits or less.
  - It does not correct the error.

TODOs

- Demo guide is available on eClass (posted last Friday), it will help you to implement the system.
- The deadline for the final report is extended to Friday, 9 February 2024, 11:59 PM.