Lecture 9
Information Redundancy - Part III

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
  - Two properties: linear and cyclic
  - Generator polynomial
  - Encoding
  - Polynomial multiplication
- Next class: decoding and error detection in cyclic codes

Code distance in error detection

To detect *d* bit errors, the code distance for the codewords must be larger or equal to *d+1*.

Example

Code: {000, 001}

$C_d = 1$

Transmitting codeword: 000

A single-bit error happens, 000 becomes 001

We cannot tell there is an error in 001.

Analogy

Dictionary: {accept, accent}

Distance = 1

Typed word: accept

A typo happens, accept becomes accent

We cannot tell it is a typo.

Code distance in error correction

To correct *d* bit errors, the code distance for the codewords must be larger or equal to *2d+1*.

Example

Code: {000, 111}

$C_d = 3$

Transmitting codeword: 000

A single-bit error happens, 000 becomes 001

We can correct 001 to 000 (closest).

Analogy

Dictionary: {except, exception}

Distance = 3

Spelling word: except

A typo happens, except becomes eccept

We can correct the typo.

Error detection and correction

-	1	1	0
0	1	0	1
0	0	1	0
0	1	0	0

No error (0)

Parity bit at position 1

-	1	1	0
0	1	0	1
0	0	1	0
0	1	0	0

Error (1)

Parity bit at position 2

-	1	1	0
0	1	0	1
0	0	1	0
0	1	0	0

Error (1)

Parity bit at position 4

-	1	1	0
0	1	0	1
0	0	1	0
0	1	0	0

No error (0)

Parity bit at position 8

Binary	0	1	1	0
Decimal value	8	4	2	1

→ 6

Decimal

Extended Hamming codes

Bit flip

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

Bit flip

Extended Hamming code
(even parity)

- There are six 1s in the whole block.
- That is an even number of 1s, the parity check at position 0 passes.
- However, the other parity checks (at position 1, 2 and 4) detect an error.
- Therefore, there are at least two errors.

Cyclic codes

Cyclic code is a special class of codes used in systems where burst errors can happen.

- Burst errors can happen in digital communication and storage devices (e.g., Disks, CDs)

Examples of cyclic codes:

- Cyclic Redundancy Check (CRC)
- Reed-Solomon codes (RS codes)

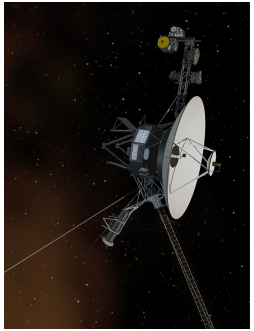
Burst error = more than one bits have been changed

Application of Reed-Solomon codes

RS codes have been widely applied in modern systems thanks to its efficiency in error correction.

Examples of modern systems:

- Data storage
    - E.g., DVD and CD
- Satellite communication
    - E.g., Voyager II
- Hi-speed modems



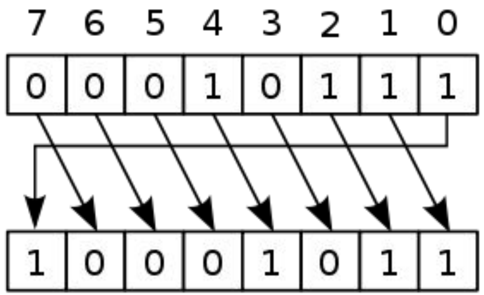
Cyclic codes

Cyclic: any circular shift of a codeword produces another codeword

- Move the rightmost bit 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
- …



Cyclic codes are not necessary linear

Cyclic codes are not necessary linear.

- a linear code is code for which any linear combination of codewords is also a codeword.
- any linear combination of codewords is also a codeword

For cyclic codes, the addition of two codewords does not necessarily lead to another codeword.

A linear code is an error-correcting code for which any linear combination of codewords is also a codeword.

Example of linear/cyclic codes

Linear code

- Suppose the code {0000, 0100, 0011, 1100, 0111, 1000, 1011, 1111}
- The sum of any codewords must produce another codeword

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

Cyclic code

- Suppose the code {10110, 01011, 10101, 11010, 01101}
- Their sum does not produce a codeword

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

Addition for codewords

The notion of “addition” here is different from the ordinary addition of numbers.

- Done in a mod 2 arithmetic system
- The terms “addition” and “xor” are used interchangeably

It differs in two respects:

- No carry over, each bit is independent of each other bit
- 2 is the same as 0, so 1 and 1 is none.
  - E.g., $1 + 0 \equiv 1 \pmod 2$
  - E.g., $1 + 1 \equiv 0 \pmod 2$

+	**0**	**1**
0	0	1
1	1	0

Example of addition of codewords

For example:

- Codeword 1: 10111
- Codeword 2: 00011
- Calculate the sum of these two codewords:

$$\boxed{\begin{array}{r} 1\,0\,1\,1\,1 \\ +\quad 0\,0\,0\,1\,1 \\ \hline 1\,0\,1\,0\,0 \end{array}}$$

or

$$\boxed{\begin{array}{r} 1\,0\,1\,1\,1 \\ \oplus\quad 0\,0\,0\,1\,1 \\ \hline 1\,0\,1\,0\,0 \end{array}}$$

Cyclic codes are not necessary linear

Linear code

- Suppose the code {0000, 0100, 0011, 1100, 0111, 1000, 1011, 1111}
- The sum of any codewords must produce another codeword

A linear code is an error-correcting code for which any linear combination of codewords is also a codeword.

$$\begin{array}{r} 0\,1\,0\,0 \\ +\quad 0\,0\,1\,1 \\ \hline 0\,1\,1\,1 \end{array}$$

Cyclic code

- Suppose the code {10110, 01011, 10101, 11010, 01101}
- Their sum does not produce a codeword

For cyclic codes, the addition of two codewords does not necessarily lead to another codeword.

$$\begin{array}{r} 1\,0\,1\,1\,0 \\ +\quad 0\,1\,0\,1\,1 \\ \hline 1\,1\,1\,0\,1 \end{array}$$

Properties of linear cyclic codes

In practice, cyclic codes designed for error detection and correction 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 of linear cyclic codes

Code {000000, 100100, 110110, 010010, 011011, 001001, 101101, 111111} is both linear and cyclic.

Question: Prove that the above code contains both cyclic and linear 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 of linear cyclic codes

Question: Is the code {000, 100, 010, 001} a linear cyclic code?

Polynomials

Cyclic codes represent codewords as polynomials.

- E.g., a codeword $[a_0 a_1 \ldots a_{n-1}]$ is represented as a polynomial

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

Polynomials

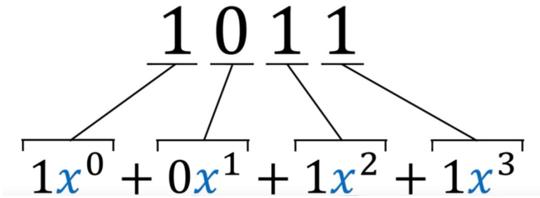
Cyclic codes represent codewords as polynomials.

- E.g., a codeword $[a_0 a_1 \ldots a_{n-1}]$ is represented as a polynomial

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

Note that:

- Since the code is binary, the coefficients are 0 and 1
- For example, $d(x) = 1 \cdot x^0 + 0 \cdot x^1 + 1 \cdot x^2 + 1 \cdot x^3$ represents the data (1011)
- Polynomial: $x^3 + x^2 + 1$



Polynomials

The degree of a polynomial equals to its highest exponent:

- E.g., the degree of $1+ x^1+ x^3$ is 3

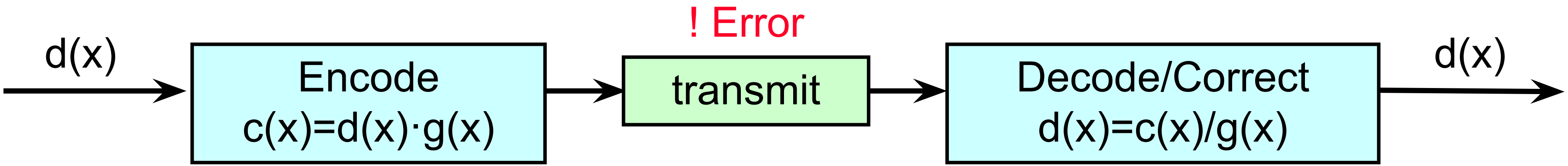
A cyclic code with the generator polynomial of degree (n-k) detects all burst errors affecting (n-k) bits or less.

- n is the number of bits in codeword
- k is the number of bits in data

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.



Encoding

Multiply data polynomial by generator polynomial:
$c(x) = d(x).g(x)$

- $g(x)$ is the generator polynomial for a linear cyclic code of length n if and only if $g(x)$ divides $1 + x^n$ without a reminder.

$$1 + x^n \textbf{ mod } g(x) = 0$$

- Multiplication in modulo 2 arithmetic = AND operation

Polynomial multiplication

To multiply two polynomials:

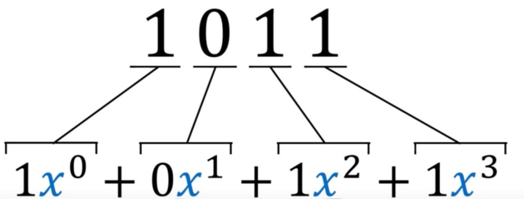
- multiply each term in one polynomial by each term in the other polynomial
- add those answers together, and simplify if needed

Example of polynomial multiplication

$d(x) = (1011) = x^3 + x^2 + 1$

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

Data bits k = 4



$$
\begin{aligned}
c(x) &= d(x).g(x) \\
&= (x^3 + x^2 + 1).(x^3 + x + 1) \\
&= x^6 + x^4 + x^3 + x^5 + x^3 + x^2 + x^3 + x + 1 \\
&= x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1
\end{aligned}
$$

Length n = 7

Cyclic property on multiplication

Suppose a codeword $\{b_0b_1b_2b_3\}$, and $g(x) = (x^4 - 1) \equiv 0$, or $x^4 \equiv 1$

$c(x) = b_0 + b_1x + b_2x^2 + b_3x^3$

Let's multiply the codeword by x:

$x.c(x) = x(b_0 + b_1x + b_2x^2 + b_3x^3)$

$x.c(x) = b_0x + b_1x^2 + b_2x^3 + b_3x^4$

Cyclic property on multiplication

Suppose a codeword $\{b_0b_1b_2b_3\}$, and $g(x) = (x^4 - 1) \equiv 0$, or $x^4 \equiv 1$

$c(x) = b_0 + b_1x + b_2x^2 + b_3x^3$

Let's multiply the codeword by x:

$x.c(x) = x(b_0 + b_1x + b_2x^2 + b_3x^3)$

$x.c(x) = b_0x + b_1x^2 + b_2x^3 + b_3x^4$

$x.c(x) = b_3 + b_0x + b_1x^2 + b_2x^3$

Cyclic property on multiplication

Suppose a codeword $\{b_0b_1b_2b_3\}$, and $g(x) = (x^4 - 1) \equiv 0$, or $x^4 \equiv 1$

$c(x) = b_0 + b_1x + b_2x^2 + b_3x^3$

Let's multiply the codeword by x:

$x.c(x) = x(b_0 + b_1x + b_2x^2 + b_3x^3)$

$x.c(x) = b_0x + b_1x^2 + b_2x^3 + b_3x^4$

$x.c(x) = b_3 + b_0x + b_1x^2 + b_2x^3$

codeword $\{b_3b_0b_1b_2\}$ is a circular shift of $\{b_0b_1b_2b_3\}$

Take-home: x.c(x) is basically shifting c(x) by one position

Example of polynomial multiplication

$d(x) = (1011000) = x^3 + x^2 + 1$

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

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

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

$$(x^3 + x^2 + 1).(x^3 + x + 1)$$

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

Example of polynomial multiplication

$d(x) = (1011000) = x^3 + x^2 + 1$

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

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

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

$(x^3 + x^2 + 1).(x^3 + x + 1)$

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

$1011000 \rightarrow 1x^0 + 0x^1 + 1x^2 + 1x^3 + 0x^4 + 0x^5 + 0x^6 + 0x^7$

Example of polynomial multiplication

$d(x) = (1011000) = x^3 + x^2 + 1$

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

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

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

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

Shift 1011000 by three positions to the right

$= 00010111$

Example of polynomial multiplication

$d(x) = (1011000) = x^3 + x^2 + 1$

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

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

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

$(x^3 + x^2 + 1).(x^3 + x + 1)$

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

Shift 1011000 by one position to the right

$= 00010111 + 0101100$

Example of polynomial multiplication

$d(x) = (1011000) = x^3 + x^2 + 1$

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

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

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

$(x^3 + x^2 + 1).(x^3 + x + 1)$

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

No shifting, add 1011000

$= 00010111 + 0101100 + 1011000$

$= 1111111 = x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1$

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 $1+x^2+x^3$

Next class: decoding and error detection in cyclic codes