Cyclic Codes

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Overview

The ring $\mathbb{Z}_2[x]/ < x^n + 1 >$

Relationship betweem F_2^n and $\mathbb{Z}_2[x]/ < x^n + 1 >$

Systematic encoding

Generator matrix

Parity-check matrix

G in systematic form

Syndrome computation and error detection

Error correction

Error detection

1. Introduction

Strong algebraic properties of cyclic codes $\rightarrow$ easy encoded and decoded

Very important subclass of linear codes.

Particularly efficient for error detection.

1. Introduction

Strong algebraic properties of cyclic codes $\rightarrow$ easy encoded and decoded

Very important subclass of linear codes.

Particularly efficient for error detection.

Cyclic codes contains important subclass of codes referred to as CRC codes

2. Description of cyclic codes

$\overline{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{Z}^n$

Cyclic Shift

$\overline{v}^{(1)} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2}) \rightarrow$ cyclic shift of $\overline{v}$.

$\overline{v}^{(i)} = (v_{n-i}, \ldots, v_{n-1}, v_0, \ldots, v_{n-i-1}) \rightarrow$ components of $\overline{v}$ shifted i positions forward

(n, k) Cyclic Code

(n, k) linear code $C \rightarrow$ Every cyclic shift of every codeword is again a codeword in C.

3. The ring $\mathbb{Z}_2[x]/ < x^n + 1 >$

Polynomial ring: $\mathbb{Z}_2[x]/ < x^n + 1 >$

$a(x) \equiv b(x) \mod (x^n + 1)$ if $(x^n + 1) | a(x) - b(x)$.

$[a(x)] = \{b(x) \in \mathbb{Z}_2[x] : a(x) \equiv b(x) \mod (x^n + 1)\}$

$\mathbb{Z}_2[x]/ < x^n + 1 >= \{[a(x)] : a(x) \in \mathbb{Z}_2[x]\}$ forms a ring under multiplication and addition.

3. The ring $\mathbb{Z}_2[x]/ < x^n + 1 >$

Note that $x^n \equiv 1 \mod (x^n + 1)$, because $x^n - 1 = x^n + 1$

$\therefore [x^n] = [1]$

Furthermore, $x^{n+1} \equiv x \mod (x^n + 1)$, because
$x^{n+1} - x = x^{n+1} + x = x(x^n + 1)$

$\therefore [x^{n+1}] = [x]$, etc.

$[a(x)]$ is simply written as $a(x)$

3. The ring $\mathbb{Z}_2[x]/ < x^n + 1 >$

using shorthand notation: $a(x) = b(x)$ if $x^n + 1 | a(x) - b(x)$

Ring $\mathbb{Z}_2[x]/ < x^n + 1 >$ contains all polynomials of degree less than n.

This ring has 2^n elements.

if $a(x) = q(x)(x^n + 1) + r(x)$, then
$a(x) = r(x) \in \mathbb{Z}_2[x]/ < x^n + 1 >$

4. The relation between $\mathbb{Z}_2^n$ and $\mathbb{Z}_2[x]/ < x^n + 1 >$

1-to-1 correspondence between $\mathbb{Z}_2^n$ and $\mathbb{Z}_2[x]/ < x^n + 1 >$

$\overline{v} = (v_0, v_1, \ldots, v_{n-1}) \mapsto v(x) = v_0 + v_1 x + v_2 x^2 + \ldots + v_{n-1} x^{n-1}$

$v(x) \rightarrow$ code polynomial, if $\overline{v} \rightarrow$ codeword.

$$x^i v(x) = v^{(i)}(x) \in \mathbb{Z}_2[x]/ < x^n + 1 >$$

4. The relation between $\mathbb{Z}_2^n$ and $\mathbb{Z}_2[x]/ < x^n + 1 >$

Minimum degree polynomial is unique

(n, k) cyclic codeword

Code polynomial $g(x) = g_0 + g_1 x + \ldots + g_{r-1} x^{r-1} + x^r$

Minimum degree $\rightarrow$ unique

$g(x) \rightarrow g_0 = 1.$

Go through proof on own time

4. The relation between $\mathbb{Z}_2^n$ and $\mathbb{Z}_2[x]/ < x^n + 1 >$

Multiples of $g(x)$ forms codewords

$g(x) = 1 + g_1 x + g_2 x^2 + \ldots + g_{r-1} x^{r-1} + x^r$

Deg$(g(x)) \rightarrow$ minimum degree in code C

$C = \{a(x)g(x) \in \mathbb{Z}_2[x]/ < x^n + 1 >: a(x) \in \mathbb{Z}_2[x]\}.$

Go through proof on own time

5. Example

Messages	Codewords	Code polinomials
(0 0 0 0)	(0 0 0 0 0 0 0)	$0 = 0 \cdot g(x)$
(1 0 0 0)	(1 1 0 1 0 0 0)	$1 + x + x^3 = 1 \cdot g(x)$
(0 1 0 0)	(0 1 1 0 1 0 0)	$x + x^2 + x^4 = x \cdot g(x)$
(1 1 0 0)	(1 0 1 1 1 0 0)	$1 + x^2 + x^3 + x^4 = (1 + x) \cdot g(x)$
(0 0 1 0)	(0 0 1 1 0 1 0)	$x^2 + x^3 + x^5 = x^2 \cdot g(x)$
(1 0 1 0)	(1 1 1 0 0 1 0)	$1 + x + x^2 + x^5 = (1 + x^2) \cdot g(x)$
(0 1 1 0)	(0 1 0 1 1 1 0)	$x + x^3 + x^4 + x^5 = (x + x^2) \cdot g(x)$
(1 1 1 0)	(1 0 0 0 1 1 0)	$1 + x^4 + x^5 = (1 + x + x^2) \cdot g(x)$
(0 0 0 1)	(0 0 0 1 1 0 1)	$x^3 + x^4 + x^6 = (x^3) \cdot g(x)$
(1 0 0 1)	(1 1 0 0 1 0 1)	$1 + x + x^4 + x^6 = (1 + x^3) \cdot g(x)$
(0 1 0 1)	(0 1 1 1 0 0 1)	$x + x^2 + x^3 + x^6 = (x + x^3) \cdot g(x)$
(1 1 0 1)	(1 0 1 0 0 0 1)	$1 + x^2 + x^6 = (1 + x + x^3) \cdot g(x)$
(0 0 1 1)	(0 0 1 0 1 1 1)	$x^2 + x^4 + x^5 + x^6 = (x^2 + x^3) \cdot g(x)$
(1 0 1 1)	(1 1 1 1 1 1 1)	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ $= (1 + x^2 + x^3) \cdot g(x)$
(0 1 1 1)	(0 1 0 0 0 1 1)	$x + x^5 + x^6 = (x + x^2 + x^3) \cdot g(x)$
(1 1 1 1)	(1 0 0 1 0 1 1)	$1 + x^3 + x^5 + x^6 = (1 + x + x^2 + x^3) \cdot g(x)$

4. The relation between $\mathbb{Z}_2^n$ and $\mathbb{Z}_2[x]/ < x^n + 1 >$

$g(x)$ is a factor of $x^n + 1$

The generator $g(x)$ of a (n, k) cyclic code C is a factor of $x^n + 1$.

Go through proof on own time

$g(x)$ generates a cyclic code

$\mathbf{Deg}(g(x)) = n - k$

$g(x)|x^n + 1$
$\Rightarrow g(x)$ generates an (n, k) cyclic code.

$x^n + 1 \rightarrow$ numerous factors of degree $n - k$

Some 'good' codes, others 'bad' codes

6. Systematic encoding of cyclic codes

1. $\overline{u} = (u_0, u_1, \ldots, u_{k-1}) \rightarrow u(x) = u_0 + u_1 x + \ldots + u_{k-1}x^{k-1}$
2. $x^{n-k}u(x) = u_0 x^{n-k} + u_1 x^{n-k+1} + \ldots + u_{k-1}x^{n-1}$
3. $x^{n-k}u(x) = a(x)g(x) + b(x)$
   $$b(x) = \begin{cases} 0 & x^{n-k}u(x) \in C \\ \mathbf{Deg}(b(x)) < \mathbf{Deg}(g(x)) & x^{n-k}u(x) \notin C \end{cases}$$
4. $b(x) + x^{n-k}u(x) = a(x)g(x) \rightarrow$ codeword

$$(b_0, b_1, \ldots, b_{n-k-1}, \underbrace{u_0, u_1, \ldots, u_{k-1}}_{message})$$

7. Example

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

Two factors of degree 3.

Each factor generates a $(7, 4)$ cyclic code.

8. Generator Matrix

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & \dots & \dots & \dots & g_{n-k} & \dots & 0 \\ \vdots & & & & & \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & \dots & \dots & g_{n-k} \end{bmatrix}$$

Generally, G not in systematic form

8. Parity-check Matrix

Consider polynomial $h(x)$ of degree $k \to x^n + 1 = g(x)h(x)$

Define *reciprocal* of $h(x)$ as:

$$x^k h(x^{-1}) \triangleq h_k + h_{k-1}x + h_{k-1}x^2 + \ldots + h_0 x^k.$$

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \ldots & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & 0 & h_k & h_{k-1} & \ldots & \ldots & \ldots & h_0 & \ldots & 0 \\ \vdots & & & & & \vdots & & & & \vdots \\ 0 & 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & \ldots & h_0 \end{bmatrix}.$$

H obtained from $h(x) \to h(x)$ - parity polynomial of C.

8. Parity-check Matrix

Dual Code of C

$C \rightarrow g(x)$

Dual code $\rightarrow x^k h(x^{-1})$, $h(x) = (x^n + 1)/g(x)$

Dual code of C is also cyclic

9. The generator matrix of a cyclic code in systematic form

Divide x^{n-k+i} by $g(x)$ for $i = 0, 1, 2, \dots, k-1$

$x^{n-k+i} = a(x)g(x) + b_i(x)$, with
$b_i(x) = b_{i0} + b_{i1}x + b_{i2}x^2 + \dots + b_{i,n-k-1}x^{n-k-1}$

$b_i(x) + x^{n-k+i}$ is a codeword in C.

9. The generator matrix of a cyclic code in systematic form

$b_i(x) + x^{n-k+i}$ is a codeword in C.

$$G = \begin{bmatrix} b_{00} & b_{01} & b_{02} & \dots & b_{0,n-k-1} & 1 & 0 & 0 & \dots & 0 \\ b_{10} & b_{11} & b_{12} & \dots & b_{1,n-k-1} & 0 & 1 & 0 & \dots & 0 \\ b_{20} & b_{21} & b_{22} & \dots & b_{2,n-k-1} & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & & & & & & \\ b_{k-1,0} & b_{k-1,1} & b_{k-1,2} & \dots & b_{k-1,n-k-1} & 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

9. The generator matrix of a cyclic code in systematic form

Corresponding parity-check matrix for C is

9. The generator matrix of a cyclic code in systematic form

Corresponding parity-check matrix for C is

$$H = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & b_{00} & b_{10} & \dots & b_{k-1,0} \\ 0 & 1 & 0 & \dots & 0 & b_{01} & b_{11} & \dots & b_{k-1,1} \\ 0 & 0 & 1 & \dots & 0 & b_{02} & b_{12} & \dots & b_{k-1,2} \\ & \vdots & & & & \vdots & & \vdots & \\ 0 & 0 & 0 & \dots & 1 & b_{0,n-k-1} & b_{1,n-k-1} & \dots & b_{k-1,n-k-1} \end{bmatrix}$$

10. Example

$(7,4)$ cyclic code generated by $g(x) = 1 + x + x^3$.

Calculate the ith basis vector v_i of G by dividing x^{3+i} by $g(x)$.

10. Example

$(7,4)$ cyclic code generated by $g(x) = 1 + x + x^3$.

Calculate the ith basis vector v_i of G by dividing x^{3+i} by $g(x)$.

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

10. Example

$$
\begin{aligned}
v_0(x) &= 1 + x + x^3 \\
v_1(x) &= x + x^2 + x^4 \\
v_2(x) &= 1 + x + x^2 + x^5 \\
v_3(x) &= 1 + x^2 + x^6,
\end{aligned}
$$

10. Example

$$G = \begin{bmatrix} \overline{v}_0 \\ \overline{v}_1 \\ \overline{v}_2 \\ \overline{v}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

11. Syndrome computation and error detection

Syndrome calculation

$r(x) = a(x)g(x) + s(x)$

$n - k$ coefficients of $s(x) \to$ syndrome $\bar{s}$.

Go through proof on own time

Syndrome of cyclically shifted vector

$s(x)$ syndrome of $r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}$.

Remainder $s^{(1)}(x) \to$ dividing $xs(x)$ by $g(x) =$ syndrome of $r^{(1)}(x)$

Go through proof on own time

12. Error Correction

Syndrome decoding method is used to decode cyclic codes.

13. Error Correction - Example

$(7,4)$ cyclic code C generated by $g(x) = 1 + x + x^3$.

$d_{min} = 3$

$2^7 = 128$ vectors in $\mathbb{Z}_2^7$

$2^4 = 16$ codewords in $C \rightarrow 128/16 = 8$ cosets for C.

The seven single-error patterns and the all-zero vector form the coset leaders of the decoding table.

13. Error Correction - Example

Table: Error patterns and the corresponding syndromes

Error pattern	Syndrome

13. Error Correction - Example

Table: Error patterns and the corresponding syndromes

Error pattern	Syndrome
$e_0(x) = x^0 = 1$	$s(x) = 1$
$e_1(x) = x^1$	$s(x) = x$
$e_2(x) = x^2$	$s(x) = x^2$
$e_3(x) = x^3$	$s(x) = 1 + x$
$e_4(x) = x^4$	$s(x) = x + x^2$
$e_5(x) = x^5$	$s(x) = 1 + x + x^2$
$e_6(x) = x^6$	$s(x) = 1 + x^2$

$$r(x) = 1 + x + x^4.$$
$$r(x) = xg(x) + x^2 + 1 \rightarrow s(x) = x^2 + 1 \rightarrow e_6(x)$$
$$c(x) \rightarrow r(x) + e_6(x) = 1 + x + x^4 + x^6.$$

Cyclic codes are very effective for detecting random as well as burst errors.

Burst error

An error pattern $\overline{e}$ where all the errors are contained in l consecutive positions is called a burst error of length l.

Example: error pattern (0 1 0 1 0 1 0 0) $\rightarrow$ burst error of length 5.

End-around burst

For a cyclic code, an error pattern with errors confined to i high-order positions and $l - i$ low-order positions is also regarded as a burst of length l and is called an *end-around burst*.

Example: error pattern (0 1 0 1 0 0 1) $\rightarrow$ end-around burst of length 5.

Burst error length

An (n, k) cyclic code is capable of detecting any error bursts of length $n - k$ or less, including the end-around bursts.
NB: Proof

bursts of length $n-k+1$

The probability of an undetected error burst of length $n-k+1$ is $2^{-(n-k-1)}$.
(No Proof)

14. Error Detection

bursts longer than $n - k + 1$

The probability of an undetected error burst of length $l > n - k + 1$ is $2^{-(n-k)}$.
(No Proof)