20SK – Signals and Codes

Lecture 12 – Binary cyclic codes (2018/12/17)

Topics discussed:

- Relation between vectors and coefficients of polynomials
- Binary arithmetic modulo N
- Binary cyclic codes: properties, generator and parity-check polynomial, construction of generator polynomial, parity-check polynomial.
- Linear codes as binary cyclic codes.
- Relation between cyclic and linear codes.
- Encoding a cyclic code using a shift register.

The relevant literature is [1, chapter 3], [2, chapters 10 and 12] and [3, chapter 4].

Resources

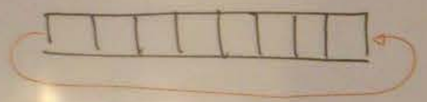
[1] Morelos-Zaragoza, R. H.: The Art of Error-Correcting Coding. 2nd edition, John Wiley & Sons, 2006, 263pp.

[2] Adámek, J: Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory. Wiley Interscience, 1991, 352 pp.

[3] Moon, T. K.: Error Correction Coding – Mathematical Methods and Algorithms. Wiley Interscience, 2005, 756 pp.

Binary cyclic codes

- a bit-rotated code-word is again a code-word



- bit vectors represented as polynomials
- all mathematical operations are performed as congruences $\bmod x^n \oplus 1$ where n is the length of the code-word

Ex: If $a = (0110)$ then also $(1100), (0011)$ and (1001) are code-words.

$\vec{a} \sim a(x) = x^2 \oplus x$

$\vec{a}^{(1)} \sim x\,a(x) = x^3 \oplus x^2$

$\vec{a}^{(-1)} \sim x^{-1} a(x) = x \oplus 1$

but:

$x^2 \cdot a(x) = x^4 \oplus x^3 \mod x^4 \oplus 1$

$= x^3 \oplus 1 \rightarrow (1001)$

why?

$x^4 \oplus x^3 : x^4 \oplus 1 = 1$

$x^4 \oplus 1$

$x^3 \oplus 1$ ... remainder

Construction

n ... length of the code $\Rightarrow x^n \oplus 1$

k ... number of information bits

$u(x) \cdot g(x) \rightarrow v(x)$

↳ generator polynomial

a) degree $n-k$

b) irreducible

c) divides $x^n \oplus 1$

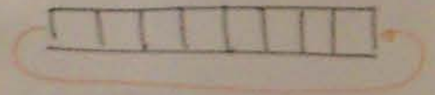
$v(x) \cdot h(x) = 0$

↳ parity check polynomial

$h(x) = \dfrac{x^n \oplus 1}{g(x)}$

Binary cyclic codes

- a bit-rotated code-word is again a code-word



- bit vectors represented as polynomials
- all mathematical operations are performed as congruences $\bmod x^n \oplus 1$ where n is the length of the code-word

Ex: If $a=(0110)$ then also $(1100), (0011)$ and (1001) are code-words.

$\vec{a} \sim a(x) = x^2 \oplus x$

$\vec{a}^{(1)} \sim x\,a(x) = x^3 \oplus x^2$

$\vec{a}^{(-1)} \sim x^3 a(x) = x \oplus 1$

but:

$x^2 \cdot a(x) = x^4 \oplus x^3 \bmod x^4 \oplus 1$

$= x^3 \oplus 1 \rightarrow (1001)$

$x^4 \oplus x^3 : x^4 \oplus 1 = 1$

$x^4 \oplus 1$

$x^3 \oplus 1$

Construction

n ... length of the code $\Rightarrow x^n \oplus 1$

k ... number of information bits

$u(x) \cdot g(x) \rightarrow v(x)$

↳ generator polynomial

a) degree $n-k$

b) irreducible

c) divides $x^n \oplus 1$

$v(x) \cdot h(x) = 0$

↳ parity check polynomial

$$h(x) = \frac{x^n \oplus 1}{g(x)}$$

Ex: $n=7$

$g(x) = x^3 \oplus x \oplus 1$

$\deg(g(x)) = 3 \rightarrow k = 4$

$h(x) = x^7 \oplus 1 : x^3 \oplus x \oplus 1 = x^4 \oplus x^2 \oplus x \oplus 1$

$x^7 \oplus x^5 \oplus x^4$

$x^5 \oplus x^4 \oplus 1$

$x^5 \oplus x^3 \oplus x^2$

$x^4 \oplus x^3 \oplus x^2 \oplus 1$

$x^4 \oplus x^2 \oplus x$

$x^3 \oplus x \oplus 1$

a) encoding $\vec{u} = (0101)$

$u(x) = x^2 \oplus 1$

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

$= x^5 \oplus x^3 \oplus x^2 \oplus x^3 \oplus x \oplus 1 =$

$= x^5 \oplus x^2 \oplus x \oplus 1$

$\vec{v} = (0100111)$

b) decoding $v(x)$:

$(x^5 \oplus x^2 \oplus x \oplus 1)(x^4 \oplus x^2 \oplus x \oplus 1) =$

$= x^9 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^6 \oplus x^4 \oplus x^3 \oplus x^2 \oplus$

$\oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus x^4 \oplus x^2 \oplus x \oplus 1 =$

$= x^9 \oplus x^7 \oplus x^2 \oplus 1 \ \underline{\text{mod}} \ x^7 \oplus 1$

$= x^2 \oplus x^2 = 0$

$v(x)$ is a code word!

Generator polynomial $g(x) \rightarrow G$

For our (7,4) code:

$g(x) \sim (0001011)$

$xg(x) \sim (0010110)$

$x^2 g(x) \sim (0101100)$

$x^3 g(x) \sim (1011000)$

$$\rightarrow G = \begin{pmatrix} 0001011 \\ 0010110 \\ 0101100 \\ 1011000 \end{pmatrix}$$

Def: (n,k) bin. cyclic code with gen. poly. $g(x)$ can be transformed into generated bin. lin. code as

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k} \cdot g(x) \end{pmatrix}$$

Construction:

$$w(x) = u(x) \cdot g(x) \bmod x^n \oplus 1$$

n ... code length, k ... number of data bits

m ... number of parity bits

$g(x)$: generator polynomial

$\deg(g(x)) = m$

$g(x) \mid x^n \oplus 1$ (it divides $x^n \oplus 1$)

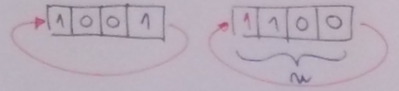
$\Rightarrow g(x) \cdot h(x) = x^n \oplus 1$

$h(x)$: parity check polynomial

$$w(x) \cdot h(x) = 0$$

BINARY CYCLIC CODES

- a bit rotation of a code word yields again a code word



Can be represented as polynomials of degree $n-1$

$\Rightarrow$ all operations performed in $\bmod x^n \oplus 1$

$\vec{w} = (1001) \Rightarrow w(x) = 1 \oplus x^3$

$\vec{w}' = (0110) \Rightarrow w'(x) = x \oplus x^2$

Ex $w = (1001) \Rightarrow w(x) = 1 \oplus x^3$

rotate one bit to the right:

$w'(x) = x \cdot w(x) = x \oplus x^4 \bmod x^4 \oplus 1$

$= 1 \oplus x$

$x^4 \oplus x : x^4 \oplus 1 = 1$ ← not interesting for us

$x^3 \oplus 1$

$x \oplus 1$ but this is

rotate 2 bits:

$w''(x) = x^2 \cdot w(x) = x^2 \oplus x^5 \bmod x^4 \oplus 1$

$= x \oplus x^2$

$x^5 \oplus x^2 : x^4 \oplus 1 = x$

$x^5 \oplus x$

$x^2 \oplus x$

Ex: $w = (1001)$ is a cyclic code

other code word are for sure: (0011), (0110), (1100)

001001

$\oplus 010001$

011000

CYCLIC CODES

parity check polynomial:

$$h(x) = \frac{x^n \oplus 1}{g(x)}$$

$$h(x) \cdot g(x) \equiv x^n \oplus 1 \equiv 0$$

Divison with reminder: $a(x) = q(x) \cdot (x^n \oplus 1) + r(x)$

How to construct $g(x)$?

$$x^n \oplus 1 = \prod_{i=1}^{m} \varphi_i(x)$$ ... irreducible polynomials

$x^n \oplus 1 = \varphi_1(x) \cdot \varphi_2(x) \cdot \varphi_3(x)$

$g(x) = \varphi_1(x)$ $\quad h(x) = \varphi_2(x) \cdot \varphi_3(x)$

or $g(x) = \varphi_1(x) \cdot \varphi_3(x)$ $\quad h(x) = \varphi_2(x)$

$\vdots$

$g(x) = \varphi_2(x)$ $\quad h(x) = \varphi_1(x) \cdot \varphi_3(x)$ dual code

Ex: $n = 7$ $\quad x^7 \oplus 1 = (x \oplus 1)(x^3 \oplus x + 1)(x^3 \oplus x^2 \oplus 1)$

$\varphi_1(x)$ $\quad \varphi_2(x)$ $\quad \varphi_3(x)$

$g(x) = x^3 \oplus x \oplus 1$ Hamming!

$h(x) = \varphi_1(x) \cdot \varphi_3(x) = x^4 \oplus x^3 \oplus x \oplus x^3 \oplus x^2 \oplus 1$

$h(x) = x^4 \oplus x^2 \oplus x \oplus 1$

$g(x) = \varphi_2(x) \cdot \varphi_3(x)$ Parity!

$h(x) = x \oplus 1$

RELATION TO LINEAR CODES

$g(x) = g_{n-k} \cdot x^{n-k} \oplus \dots g_1 \cdot x \oplus g_0 \cdot 1$

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

Ex: $g(x) = x^3 \oplus x \oplus 1 \quad n=7, k=4$

$\Rightarrow \vec{g} = (1101) = (g_0\, g_1\, g_2\, g_3)$

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

non-systematic code

$x^6 : x^3 \oplus x \oplus 1 = x^3 \oplus x \oplus 1$

$x^6 \oplus x^4 \oplus x^3$

$x^4 \oplus x^3$

$x^4 \oplus x^2 \oplus x$

$x^3 \oplus x^2 \oplus x$

$x^3 \oplus x \oplus 1$

$x^2 \oplus 1$

$x^6 = (x^3 \oplus x \oplus 1) \cdot g(x) \oplus x^2 \oplus 1$

$x^6 = g(x) \cdot g(x) \oplus x^2 \oplus 1$

coincidence

→ systematic code?

parity sub-matrix:

$r_0(x) = x^{n-1} \bmod g(x) \rightarrow \vec{r}_0$

$r_1(x) = x^{n-2} \bmod g(x) \rightarrow \vec{r}_1$

$\vdots$

$r_{k-1}(x) = x^{n-k} \bmod g(x) \rightarrow \vec{r}_{k-1}$

$\Rightarrow P = \begin{bmatrix} \vec{r}_0 \\ \vec{r}_1 \\ \vdots \\ \vec{r}_{k-1} \end{bmatrix}$

Ex: $g(x) = x^3 \oplus x \oplus 1 \quad n=7 ; \boxed{k = 4 = n - \deg[g(x)]}$

$r_0(x) = x^6 \bmod g(x) = x^2 \oplus 1 \quad \vec{r}_0 = (101)$

$r_1(x) = x^5 \bmod g(x) = x^2 \oplus x \oplus 1 \quad \vec{r}_1 = (111)$

$r_2(x) = x^4 \bmod g(x) = x^2 \oplus x \quad \vec{r}_2 = (011)$

$r_3(x) = x^3 \bmod g(x) = x \oplus 1 \quad \vec{r}_3 = (110)$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

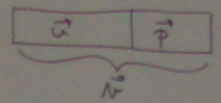
systematic!

Systematic encoding of cyclic code:

(n,k) code : $u(x)$: $\deg[u(x)] = k-1$

$\rightarrow v(x) = u(x) \cdot g(x)$

$= u(x) \oplus x^k \cdot p(x)$



Ex: $u(x) = x^3 \oplus x$ | $p(x) = x \oplus 1$ $\quad x^6 x^5 \dots x^0$

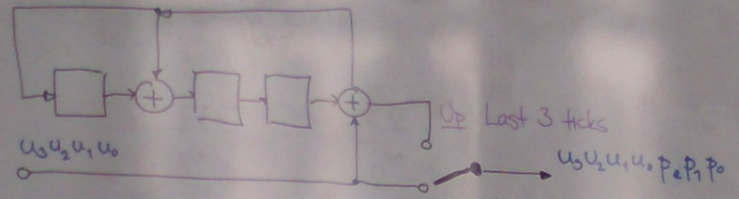
$k=4, n=7$ $\quad \vec{v} = (0101110)$

$v(x) = u(x) \oplus x^4 \cdot p(x) =$

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

$= x^5 \oplus x^4 \oplus x^3 \oplus x$

Ex: Systematic encoder for Hamming (7,4)



Decoder for cyclic codes

→ syndrome decoding

table : syndrom poly. $s(x)$ → error poly. $e(x)$

$v(x) = u(x) \cdot g(x)$

$w(x) = v(x) \oplus e(x)$

$w(x) \cdot h(x) \equiv 0 \mod x^n \oplus 1$

decoder : $w(x) : g(x) =$

$= v(x) : g(x) \oplus e(x) : g(x)$

$= 0 \oplus s(x)$

Ex: Mapping table for Hamming (7,4)

$e(x)$	$s(x)$
0	0
1	1
x	x
x^2	x^2
x^3	$x \oplus 1$
x^4	$x^2 \oplus 1$

↓ corrects single err

$e(x) = x^i$

not practical for high t

Trick : Maggit (1960)

$w(x) \rightarrow w^{(1)}(x) \equiv x \cdot w(x) \mod x^n \oplus 1$

$s(x) \rightarrow s^{(1)}(x) \equiv x \cdot s(x) \mod x^n \oplus 1$

⇒ a shift of $w(x)$ shifts also the $s(x)$

Maggit decoder

for cyclic code of length n, checks all n shifts of $w(x)$ against syndromes with $\deg[e(x)] = \max$.

↳ only $x^6 \Leftrightarrow x^2 \oplus 1$ for Hamming $(n=7)$

but $x^{14} \dots x^{13} \oplus x^{14} = e(x)$ for Golay $(n=15)$

Hoggat algorithm:

1. move all n bits of $w(x)$ into LSR
2. compute $s(x)$ while shifting by $w(x) : g(x)$
3. if $s(x) = 0 \Rightarrow$ do nothing
   else: check for $s(x)$ pattern
   if match: add $e(x)$ to the current $w(x)$
   $w'^{(i)} \leftarrow w^{(i)} \oplus e(x)$
4. continue shifting

$\Rightarrow$ most significant bit is the one that contains error

most sig. bit: $v = (0100101)$ MSB

Ex: $\vec{v} = (00100101)$

$\vec{w} = (00110101)$

1. 0 0 1 1 0 1 0 1 → $s(x) \neq 0$, no match
2. 1 0 0 1 1 0 1 0 → —"—
3. 0 1 0 0 1 1 0 1 → —"—
4. 1 0 1 0 0 1 1 0 → —"—
5. 0 1 0 1 0 0 1 1 → $s(x)$ matches
   0 1 0 1 0 0 1 0 Okay: 01011010
6. 0 0 1 0 1 0 0 1

⋮

etc

Can we construct a cyclic code with given t and k?

↑ number of corrected errors

BCH codes (Bose, Chaudhuri, Hocquenghem 1960)

given: $m, m \geq 3$; $t < 2^m - 1$

provides:
- block length $n = 2^m - 1$
- parity symbols $n - k \leq m \cdot t$
- min. dist. $d_{min} \geq 2 \cdot t + 1$
- generator polynomial

d_{min} may be higher!

Reed-Solomon codes (1960)

→ a BCH with s bit long symbols

widely used: cca since 1990 (decoding)

- storage (SSD, RAID) CD, DVD, BD
- wireless networks (WiMAX)
- satellite communications (DVB-S, NASA)
- bar-codes (QR)
- ADSL, xDSL