

Error Correction Code (1)

Fire Tom Wada
Professor, Information
Engineering, Univ. of the Ryukyus

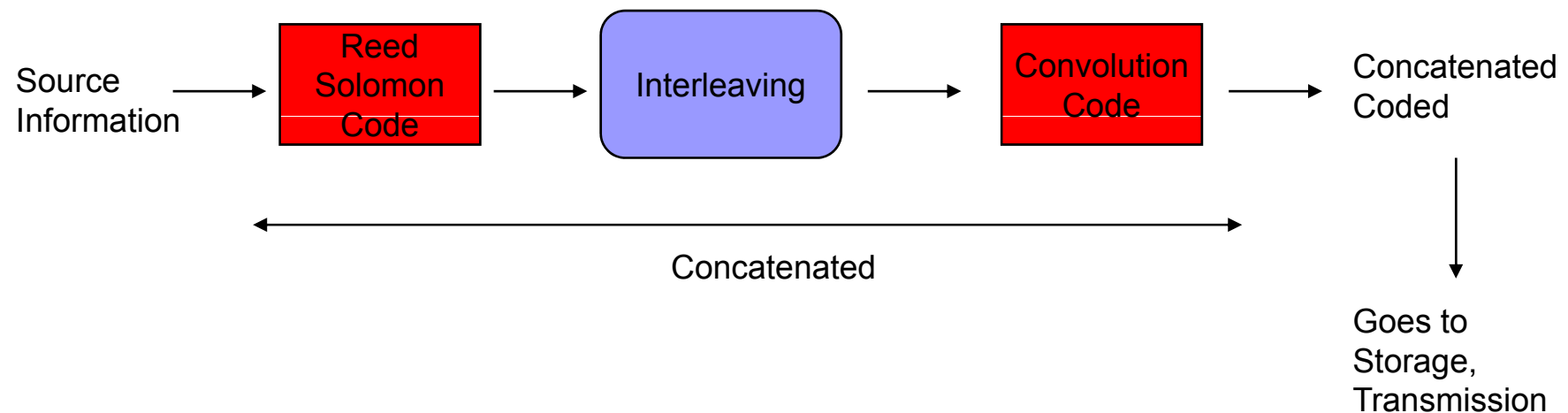


Introduction

- Digital data storage
- Digital data transmission
 - Data might change by some Noise, Fading, etc.
 - Such data change have to be corrected!
- Forward-Error-Correction (FEC) is need.
 - Digital Video (DVD), Compact Disc (CD)
 - Digital communication
 - Digital Phone
 - Wireless LAN
 - Digital Broadcasting

Two major FEC technologies

1. Reed Solomon code
2. Convolution code
3. Serially concatenated code





Reed Solomon Code

- Can correct Burst Error.
- Famous application is Compact Disc.
- Code theory based on Galois Field
 - For 8 bit = Byte information
 - Galois Field of 2^8 is used
- We will start from Galois Field in following slide.



Galois Field

- “Field” is the set in which +, -, x, / operations are possible.
 - e.g. Real numbers is Field.
 - -2.1, 0, 3, 4.5, 6, 3/2,
 - Number of Element is infinite (∞).
- Instead, 8 bit digital signal can represents $2^8=256$ elements only.
- Galois Field is
 - Number of element is finite. e.g. $2^8=256$.
 - +, -, x, / operations are possible.
 - GF(q) means q elements Galois Fields.
 - q must be a prime number (p) or p^n .

Example 1. GF(q=2)

■ GF(2)

- Only two elements {0,1}
- Add and Multiply : do operation and mod 2
- Subtract : for all $a \in \{0,1\}$, $-a$ exists.
- Division : for all a excluding {0}, a^{-1} exists.

+	0	1
0	0	1
1	1	0

Same as XOR operation

a	-a
0	0
1	1

- operation is same as +

X	0	1
0	0	0
1	0	1

Same as AND operation

a	a^{-1}
0	-
1	1

Example 2. GF(5)

- Elements = $\{0, 1, 2, 3, 4\}$
- Use mod 5 operation

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

a	-a
0	0
1	4
2	3
3	2
4	1

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a	a ⁻¹
0	-
1	1
2	3
3	2
4	4

- So far $q=2, 5$ are prime numbers.

Example 3. GF(4)

- Here 4 is NOT a prime number.
- Use mod 4
- 2^{-1} does NOT exist.

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

a	a^{-1}
0	-
1	1
2	-
3	3

- GF(4) with integer elements does NOT exist!
- The elements can be polynomial.



GF with polynomial elements

- Polynomial such as aX^2+bX^1+c
- Those coefficient $a, b, c = GF(2) = \{0, 1\}$
 - Can be added
 - Can be subtracted
 - Can be multiplied
 - Can be divided
 - And Can be modulo by other polynomial
- GF with polynomial elements is possible
- $GF(4) = \{0X+0, 0X+1, X+0, X+1\}$
 - Use $\text{mod}(X^2+X+1)$

Example 4. GF(2²) with polynomial (1)

- Elements={0, 1, x, x+1}
- Use Modulo(x²+x+1)
- Each coefficient is GF(2)

+	0	1	x	x+1
0	0	1	x	x+1
1	1	2=0	x+1	x+2=x
x	x	x+1	2x=0	2x+1=1
x+1	x+1	x+2=x	2x+1=1	2x+2=0


a	-a
0	-
1	1
x	x
x+1	x+1

Example 4. GF(2²) with polynomial (2)

- Use Modulo(x^2+x+1)
- $\text{mod}(x^2+x+1)$ is equivalent to use $x^2=x+1$ assignment


X	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	$x^2=x+1$	$x^2+x=$ $2x+1=1$
x+1	0	x+1	$x^2+x=$ $2x+1=1$	$x^2+2x+1=$ $x^2+1=$ $x+2=x$

a	a ⁻¹
0	0
1	1
x	x+1
x+1	x



Let's calculate $(x^2+x)\text{mod}(x^2+x+1)$

$$\begin{array}{r} x^2 + x + 1 \overline{) x^2 + x + 0} \\ \underline{x^2 + x + 1} \\ 1 \end{array}$$

- 
- $(x^2+x+1)\bmod(x^2+x+1)=0$
 - Then $x^2+x+1=0$
 - Now consider the root of $x^2+x+1=0$ is α
 - Then $\alpha^2 + \alpha + 1 = 0$
 - $\alpha^2 = -\alpha - 1$

Example 5. $GF(2^2)$ with polynomial α is the root of $x^2+x+1=0$

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

a	-a
0	0
1	1
α	α
α^2	α^2

X	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	α
α^2	0	α^2	1	0

a	a^{-1}
0	-
1	1
α	α^2
α^2	α

- Previous page's GF is made by polynomial $x^2+x+1=0$
- This polynomial is generation polynomial for GF.

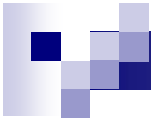
Bit representation	Polynomial representation	Root index representation
00	0	$\alpha^{-\infty}$
01	1	$\alpha^0=1$
10	α	α^1
11	$\alpha+1$	α^2

- $\alpha^3 = \alpha^2 \times \alpha = (\alpha+1) \alpha = \alpha^2 + \alpha = 1$

Example 6. $GF(2^3)$ with polynomial α is the root of $x^3+x+1=0$

Bit representation	Polynomial representation	Root index representation
000	0	$\alpha^{-\infty}$
001	1	$\alpha^0=1$
010	α	α^1
100	α^2	α^2
011	$\alpha+1$	α^3
110	$\alpha^2 + \alpha$	α^4
111	$\alpha^2 + \alpha+1$	α^5
101	$\alpha^2 + 1$	α^6

■ $\alpha^7 = \alpha^3 \times \alpha^3 \times \alpha = (\alpha+1) (\alpha+1) \alpha = \alpha^3 + \alpha = 1$



+	0	1	α	α^2	$1+\alpha$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$
0	0	1	α	α^2	$1+\alpha$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$
1	1	0	$1+\alpha$	$\alpha^2 + 1$	α	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	α^2
α	α	$\alpha + 1$	0	$\alpha^2 + \alpha$	1	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha + 1$
α^2	α^2	$\alpha^2 + 1$	$\alpha^2 + \alpha$	0	$\alpha^2 + \alpha + 1$	α	$\alpha + 1$	1
$1+\alpha$	$1+\alpha$	α	1	$\alpha^2 + \alpha + 1$	0	$\alpha^2 + 1$	α^2	$\alpha^2 + \alpha$
$\alpha^2 + \alpha$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	α^2	α	$\alpha^2 + 1$	0	1	$1+\alpha$
$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + 1$	$\alpha + 1$	α^2	1	0	α
$\alpha^2 + 1$	$\alpha^2 + 1$	α^2	$\alpha^2 + \alpha + 1$	1	$\alpha^2 + \alpha$	$1+\alpha$	α	0



Example 7. Simple Block Code

- 4bit information : 1011 (also shown as x^3+x+1)
- Make a simple block code as follows
 1. Shift 2 bit left 101100 ($x^5+x^3+x^2$)
 2. Calculate modulo by primitive polynomial x^2+x+1
 - **Ans=1**
 3. Add the modulo to 1. 101101 ($x^5+x^3+x^2+1$)
 - Now this code modulo(x^2+x+1)=0
- Send the 3. instead of 4bit information
- If received code's modulo(x^2+x+1) is 0,
It is thought that No ERROR HAPPENED!

- In this example, the coefficient of the polynomial is 0 or 1, But, Reed Solomon code can handle more bits!

Example 7. Simple Block Code

1011

Information
 $A(x) = x^3 + x + 1$

primitive polynomial
 $G(x) = x^2 + x + 1$

$$\frac{A(x) \cdot x^2}{G(x)} = \frac{(x^3 + x + 1) \cdot x^2}{x^2 + x + 1} = \frac{x^5 + x^3 + x^2}{x^2 + x + 1} = \frac{(x^2 + x + 1)(x^3 + x^2 + x + 1) + 1}{x^2 + x + 1}$$

$R(x) = 1$

101101

Information parity

Code
 $W(x) = x^k A(x) + R(x) = G(x)Q(x) = x^5 + x^3 + x^2 + 1$

Transmission

**If the received code can be divided by G(x),
 It is thought that No Error Happed.**

Example 8. RS(5,3) code with GF(2³)

- Remember GF(2³) has 8 elements in Example 6.
- One element can handle 3bits.
- Reed Solomon (5,3) code has 3 information symbol + 2 parity symbol.
 - 3x3= 9bit information + 2x3=6bit parity
- Assume Information = (1, α, α²)=(001 010 100)
 - I(x)=x²+αx+α²
 - G(x)=x²+α³x+α -> x²=α³x+α
- R(x)=(x²I(x))moduloG(x)=(x⁴+αx³+α²x²) moduloG(x)
=α⁴x+1
- W(x)=x²I(x)+R(x)= x⁴+αx³+α²x² +α⁴x+1
- RS(5,3) code = (1, α, α², α⁴, 1)=(001 010 100 110 001)



Calculation of R(x)

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



RS code parameters

- Code length n ; $n \leq q-1$, q =number of elements
- Information symbol length k : $k \leq n-2t$
- Parity symbol length $c \leq q-1-n+2t$
- Correctable symbol length = t

- Then, $q=2^3=8$
- Max $n=7$, when $t=3$, $k=1$, $c=6$
- $R(5,3)$ case
 - $n=5$, $q=8$, $k=3$, Then max $t = 1$ only one symbol error correctable.



RS code error correction

- Error correction Decoding is more tough!
- Decoding is not covered in this lecture.



HW-4

- According to the example 8,
- What is the RS(5,3) code for information= $(\alpha, \alpha^2, 1)$)