Problems 3 - GF(q), Reed-Solomon codes, BCH codes

Coding Technology

Illés Horváth

2025/10/17

Reminder: GF(q), Reed-Solomon codes

GF(q): finite field with q elements.

- q prime $\rightarrow$ mod q arithmetics
- $q = 2^m \rightarrow$ binary polynomials of degree $\leq m-1$, polynomial multiplication with reduction mod $p(y)$; primitive element is y

C(n, k) Reed-Solomon code generated by primitive element α over GF(q):

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \dots & \alpha^{(n-1)(k-1)} \end{bmatrix} \qquad H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-1)(n-k)} \end{bmatrix}$$

$n = q - 1$. RS codes are MDS $\rightarrow d_{\min} = n - k + 1$,

- detects $n - k$ errors;
- corrects $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors.

Problem 1

Solve the equation $6x + 5 = 2$ in GF(7).

Solution.

$$
\begin{aligned}
6x + 5 &= 2 \\
6x &= 2 - 5 \\
6x &= -3 \\
6x &= 4 \\
x &= 6^{-1} * 4 \\
x &= 6 * 4 \\
x &= 24 \\
x &= 3.
\end{aligned}
$$

Problem 2

Design an RS code over GF(7) that corrects every double error.

Solution. We compute the (n, k) parameters. First, $n = q - 1 = 6$. The error correcting capability is

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor = 2 \qquad \to \qquad n - k = 4,$$

so $k = 2$ and this is a C(6,2) code.

Any C(6,2) RS code over GF(7) is suitable; for example, for the RS code generated by the primitive element 5, we have

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{bmatrix}$$

Problem 3

Using the previous code, determine the codewords assigned to the message vectors $u = (4, 4)$, $u = (3, 5)$ and $u = (5, 1)$.

Solution.

$$(4\,4) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (1\,3\,6\,0\,5\,2)$$

$$(3\,5) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (1\,0\,2\,5\,6\,4)$$

$$(5\,1) \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} = (6\,3\,2\,4\,0\,1)$$

Problem 4

A C(10,4) RS code over GF(11) has generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \end{bmatrix}$$

(a) How many errors can the code correct?

(b) What is the primitive element used?

Problem 4

Solution.

(a) This is a RS code, so the code can correct $\left\lfloor \frac{n-k}{2} \right\rfloor = 3$ errors.

(b) The primitive element used is 6:

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \end{bmatrix}$$

Problem 5

A C(6,2) linear cyclic code over GF(7) can correct 2 errors.
(1,0,3,5,2,6) is one of the codewords.

(a) Is (5,2,6,1,0,3) a codeword?

(b) Is (2,0,6,3,4,5) a codeword?

(c) Is (2,0,1,3,5,6) a codeword?

Solution.

(a) Yes, because it is the cyclic shifted version of the given codeword (shifted 3 times).

(b) Yes, because it is equal to the given codeword multiplied by 2.

(c) No, because the code can correct 2 errors $\rightarrow$ $d_{\min} \geq 5$, but the (b) and (c) vectors have Hamming-distance 3.

Reminder: code polynomials

Cyclic linear codes can be generated by generator polynomial via

$$c(x) = u(x)g(x)$$

The RS code has generator polynomial

$$g(x) = \prod_{i=1}^{n-k}(x - \alpha^i)$$

Problem 6

Compute the generator polynomial of the cyclic C(6,4) RS code over GF(7) generated by the primitive element 3.

Solution.

$$g(x) = \prod_{i=1}^{n-k}(x - \alpha^i) = (x-3)(x-3^2) =$$
$$(x-3)(x-2) = x^2 - 5x + 6 = 6 + 2x + x^2.$$

Problem 7

Using the previous code, calculate the codeword for the message vector (1 1 0 0).

Solution.

$$c_1(x) = u_1(x)g(x) = (1 + x)(6 + 2x + x^2) =$$
$$6 + 8x + 3x^2 + x^3 = 6 + x + 3x^2 + x^3$$

$$\rightarrow\ c_1 = (6\,1\,3\,1\,0\,0)$$

Problem 8

A code over GF(8) has generator polynomial

$$g(x) = y^3 + y^4 x + x^2.$$

(a) Is this a RS code?

(b) What are the code parameters?

(c) What are the error detection and correction capabilities of the code?

(d) We use this code to transmit a message section over a q-ary channel ($q = 8$) with digit error $p = 0.02$. Compute the probability of a decoding error.

Problem 8

1	1	y^0
2	y	y^1
3	$y+1$	y^3
4	y^2	y^2
5	y^2+1	y^6
6	y^2+y	y^4
7	y^2+y+1	y^5

Solution.

(a) RS codes have generator polynomials of the form $\prod_{i=1}^{n-k}(x-y^i)$, so we need to decide if $g(x)$ is of this form.

The given $g(x)$ has degree 2 (we need to consider the exponent of x, the y terms are coefficients, 'numbers' from GF(8)).

The generator of the RS code with degree 2 is

$$g'(x) = (x-y)(x-y^2) = x^2 - (y+y^2)x + y^3 = x^2 + y^4x + y^3$$

so $g(x) = g'(x)$, and the original code is a RS code.

(b) The code parameters are:

- RS codes over GF(8) have $n = 8-1 = 7$, and
- $\deg(g(x)) = n-k = 2$, so $k = 5$.

Problem 8

(c) The code can detect

$$n - k = 2$$

errors, and correct

$$\left\lfloor \frac{n-k}{2} \right\rfloor = 1$$

error.

(d) $p = 0.02$. The probability of a block error is

$$1 - \left((1-p)^7 + \binom{7}{1} p^1 (1-p)^6 \right) \approx 0.00786.$$

Reminder: BCH codes

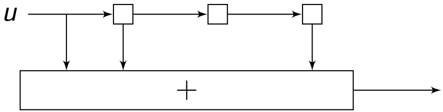
Nonzero elements of $GF(2^m)$ can be grouped into conjugate groups with the same minimal polynomial.

For the $C(n, k)$ binary BCH code with generator polynomial $g(x)$:

- $n = 2^m - 1$
- we start from $GF(2^m)$
- $y^1, \ldots, y^{2t}$ are roots of $g(x) \rightarrow$ the code can correct t errors
- entire conjugate groups are included, and $g(x)$ is the product of the corresponding minimal polynomials

Problem 9

The following shift register architecture is used to generate a linear cyclic code over GF(8).



(a) What is the generator polynomial $g(x)$ of the code?

(b) What are the parameters of the code?

(c) What are the error correction capabilities of the code?

Problem 9

Solution.

(a) The given shift register architecture is multiplication by a polynomial. It contains no constant factors, so all coefficients of the polynomial are either 0 or 1, depending on whether the corresponding coefficient is included in the sum or not.

Altogether, the architecture is multiplication by the polynomial $g(x) = x^3 + x + 1$, so the generating polynomial of the code is $x^3 + x + 1$.

(b) Over GF(8), generator polynomials with 0-1 coefficients are typical for BCH codes. Let's check whether this polynomial is the generator polynomial of a BCH code.

The conjugate groups and minimal polynomials over GF(8) are

$$\{1\} \to x - 1$$
$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

Problem 9

Solution (cont.)

(b) We need to check whether the generator polynomial is a product of some of the minimal polynomials. Actually, $g(x)$ is equal to the minimal polynomial of the group $\{y, y^2, y^4\}$, so yes.

So this is a BCH code; the parameters are $n = 8 - 1 = 7$ and the degree of the generator polynomial is $n - k = 3$, so $k = 4$, and this is a C(7,4) code.

(c) The roots of $g(x)$ contain y^1 and y^2 (along with their entire conjugate group), but not y^3, so this code can correct $t = 1$ error.

Problem 10

Can the following polynomial be the generator polynomial of a BCH code over GF(8)?

$$g(x) = x^4 + yx^3 + y^3x^2 + yx + 1$$

Solution. No, because the generator polynomial of a BCH code over GF(8) must have coefficients from GF(2), so each coefficient must be either 0 or 1.

Problem 11

(a) Determine the parameters of the BCH code correcting every double error over GF(8).

(b) Calculate the generator polynomial.

(c) Determine the codeword belonging to the message vector in which each component is 7.

Solution.

(a) Due to $t = 2$, the generator polynomial $g(x)$ must have roots y, y^2, y^3, y^4. We need to include the entire conjugate groups:

$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

so

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

Problem 11

(a) $g(x)$ has degree $n - k = 6 \;\rightarrow\; n = 7, k = 1$.

($g(x)$ has roots $y^1, \ldots, y^6$, so this code can actually correct 3 errors, not just 2.)

(b)

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

Side remark. The generator matrix of this code is

$$G = [1\,1\,1\,1\,1\,1\,1].$$

(c) $u = (7) \;\rightarrow\; c = (7\,7\,7\,7\,7\,7\,7)$

Problem 12

A C(15,5) BCH code that can correct 3 errors is used to transmit a 5-bit message through a channel with bit error probability $p_b = 0.01$. Compute the probability of a decoding error.

Solution. Decoding will be correct if there are 0, 1, 2 or 3 errors out of 15 bits, so

$$\begin{aligned} P(\text{correct decoding}) = & (1-p_b)^{15} + \binom{15}{1}(1-p_b)^{14}p^1 + \\ & + \binom{15}{2}(1-p_b)^{13}p^2 + \binom{15}{3}(1-p_b)^{12}p^3 \\ & \approx 0.9999875, \end{aligned}$$

and

$$P(\text{decoding error}) \approx 1 - 0.9999875 = 1.25 \times 10^{-5}.$$

Problem 13

Using the facts that in GF(2^m), α and α^2 belong to the same conjugate group, and also that $y^{63} = y^0 = 1$, map out all the conjugate groups of GF(64) (the minimal polynomials are not required).

Solution. Instead of $y^0, y^1, y^2, \ldots$, only the exponents $0, 1, 2, \ldots$ will be displayed.

{0}	(always a standalone group)
{1,2,4,8,16,32}	{3,6,12,24,48,33}
{5,10,20,40,17,34}	{7,14,28,56,49,35}
{9,18,36}	{11,22,44,25,50,37}
{13,26,52,41,19,38}	{15,30,60,57,51,39}
{21,42}	{23,46,29,58,53,43}
{27,54,45}	{31,62,61,59,55,47}

Problem 14

Using the previous problem, design a code that can correct 5 errors.

Solution. The generator polynomial of the code needs to contain $y^1, y^2, \ldots, y^{10}$. To include all of these, 5 groups are necessary, with a total of $4 \times 6 + 3 = 27$ elements.

The code parameters are $n = 64 - 1 = 63$, and from the fact that the groups contain a total of 27 elements, $n - k = 27$ and $k = 36$ follows.

So this is a C(63,36) BCH code. (Without the minimal polynomials, we cannot derive the generator polynomial, but that's OK.)