IERG6120 Coding for Distributed Storage Systems Lecture 10 - 20/10/2016

Decoding of primitive RS codes

Lecturer: Kenneth Shum *Scribe: Cao Qi*

Recall that two linear codes of the same length are said to be *equivalent* if we can obtain one of them from the other by (i) permuting the code coordinates and (ii) multiplying a code coordinate by a non-zero constant, or any combination of these two operations. In view of code equivalence, we define a generalized version of Reed-Solomon codes.

Definition. Let $\alpha_0, \dots, \alpha_{n-1}$ be distinct elements in a finite field $\mathbb{F}_q$, and $r_0, \dots, r_{n-1}$ be non-zero elements in $\mathbb{F}_q$. An (n, k) linear code with

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} r_0 & & & \\ & r_1 & & \\ & & \ddots & \\ & & & r_{n-1} \end{bmatrix},$$

as a generator matrix is called a *generalized Reed-Solomon code.* When $n = q - 1$, the RS code is said to be *primitive.*

See e.g. [2] for further details on generalized Reed-Solomon code. When r_i's are all equal to 1, the generalize RS code reduces to the RS code we considered before. In this lecture, we consider primitive RS code with all r_i's equal to 1. Every non-zero element in $\mathbb{F}_q$ appears as one of the α_i's. We let α be a primitive element of $\mathbb{F}_q$, and let $\alpha_i = \alpha^i$ for $i = 0, 1, 2, \dots, q - 2$. The corresponding generator matrix is shown as follows,

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix}.$$

Lemma 1. *Let α be a primitive element in $\mathbb{F}_q$, then we have*

$$\sum_{i=0}^{q-2} (\alpha^i)^j = \begin{cases} -1, & j \equiv 0 \mod q-1 \\ 0, & \textit{otherwise.} \end{cases}$$

Proof When $j \equiv 0 \mod q - 1$, we have that $(\alpha^i)^j = 1$ for all i. Then $\sum_{i=0}^{q-2} (\alpha^i)^j = \sum_{i=0}^{q-2} 1^i = -1$.

Otherwise, when $j \not\equiv 0 \mod q - 1$, we have that $\alpha^j \neq 1$. Then

$$\begin{aligned} \sum_{i=0}^{q-2} (\alpha^i)^j &= \frac{1 - \alpha^{(q-1)j}}{1 - \alpha^j} \\ &\overset{(a)}{=} \frac{1 - 1}{1 - \alpha^j} \\ &= 0 \end{aligned}$$

where (a) follows from $\alpha^{q-1} = 1$. □

By Lemma 1, we can obtain the parity-check matrix of a primitive RS code,

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-1-k} & \alpha^{2(q-1-k)} & \cdots & \alpha^{(q-2)(q-1-k)} \end{bmatrix}.$$

We note that the rows of the matrix H are orthogonal to the rows of G, i.e., $G \cdot H^T = \mathbf{0}$, and H has full rank.

Example 1 Let $\mathbb{F}_8$ be a finite field of size 8, and α be a primitive element in $\mathbb{F}_8$. Let $q-1 = n = 7$, $k = 3$ and $d = n - k + 1 = 5$. We can obtain the corresponding generator matrix and check matrix for primitive RS code.

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix}, \qquad H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}.$$

Definition. Let $\boldsymbol{c}$ be a transmitted codewords, and $\boldsymbol{y}$ be the received vector. Define the *error vector* as $\boldsymbol{e} \triangleq \boldsymbol{y} - \boldsymbol{c}$, and the *syndrome vector* $\boldsymbol{s} \triangleq \boldsymbol{y} \cdot H^T$. The components in the syndrome vector are called the *syndromes.*

The syndromes only depend on the error vector, but not on the transmitted codeword,

$$\boldsymbol{s} \triangleq \boldsymbol{y} \cdot H^T = (\boldsymbol{c} + \boldsymbol{e}) \cdot H^T = \boldsymbol{e} \cdot H^T.$$

Out task is to determine the number of errors, the locations of the errors, and the values of the errors from the syndromes. We illustrate a bounded distance decoding algorithm, called the Peterson-Gorenstein-Zierler decoder [1].

We will use Example 1 as a running example. In this example, we can correct up to $t = 2$ errors. We denote the syndrome vector as (s_0, s_1, s_2, s_3). We consider three cases.

(i) If there is no error, then $\boldsymbol{e} = 0$ and $s_0 = s_1 = s_2 = s_3 = 0$.

(ii) Suppose there is one error, and the i-th component of the error vector $\boldsymbol{e}$, denoted by e_i, is not 0, while the other components of $\boldsymbol{e}$ are 0. Then

$$\boldsymbol{s} = \boldsymbol{e} \cdot H^T = e_i H_i^T,$$

where H_i is the i-th column of H. There exists a common ratio in the syndromes

$$\frac{s_1}{s_0} = \frac{s_2}{s_1} = \frac{s_3}{s_2}, \tag{1}$$

and the common ratio determines the location of the error.

(iii) There are two errors whose positions are denoted by i_1 and i_2, and the corresponding error values are denoted by e_{i_1} and e_{i_2} respectively. We have

$$s_j = e_{i_1} \alpha^{(j+1)i_1} + e_{i_2} \alpha^{(j+1)i_2}, \text{ for } j = 0, 1, 2, 3.$$

Define the *error-locator polynomial*

$$\Lambda(z) \triangleq (1 - \alpha^{i_1} z)(1 - \alpha^{i_2} z) = 1 + \Lambda_1 z + \Lambda_2 z^2. \tag{2}$$

By construction, the reciprocals of α^{i_1} and α^{i_2} are the roots of the error-locator polynomials. The relationship between the coefficients Λ_1 and Λ_2 and the syndromes can be obtained through the equations

① $0 = \Lambda(\alpha^{-i_1}) = 1 + \Lambda_1 \alpha^{-i_1} + \Lambda_2 \alpha^{-2i_1}$,

② $0 = \Lambda(\alpha^{-i_2}) = 1 + \Lambda_1 \alpha^{-i_2} + \Lambda_2 \alpha^{-2i_2}$.

We linearly combine the above two equations and get

$$0 = ① \cdot e_{i_1} \alpha^{3i_1} + ② \cdot e_{i_2} \alpha^{3i_2} = s_2 + \Lambda_1 s_1 + \Lambda_2 s_0,$$

$$0 = ① \cdot e_{i_1} \alpha^{4i_1} + ② \cdot e_{i_2} \alpha^{4i_2} = s_3 + \Lambda_1 s_2 + \Lambda_2 s_1.$$

These two equations can be written as follows,

$$\begin{bmatrix} s_1 & s_0 \\ s_3 & s_2 \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \end{bmatrix} = - \begin{bmatrix} s_2 \\ s_4 \end{bmatrix}. \tag{3}$$

By this equation, we can obtain $\Lambda(z)$.

Given the received vector $\mathbf{y}$, the decoder runs as follows.

Step 0 Compute the syndromes by $(s_0, s_1, s_2, s_3) = \mathbf{y}H^T$.

Step 1 If $s_0 = s_1 = s_2 = s_3 = 0$, then declare that there is no error and return $\boldsymbol{y}$.

Step 2 If there exists a common ratio in syndrome as in (1), then we say that an error occurs at position $i = \log_\alpha \frac{s_1}{s_0}$. The error value is the unique field element e_i such that

$$(s_0, s_1, s_2, s_3) = e_i \cdot (\alpha^i, \alpha^{2i}, \alpha^{3i}, \alpha^{4i}).$$

At the i-th position of vector $\mathbf{y}$, subtract e_i, and return the resulting vector.

Step 3 If the determinant of the matrix in (3) is zero, declare that there is a decoding error. Compute Λ_1 and Λ_2 by solving (3). Find the roots of $\Lambda(z)$ in (2). If $\Lambda(z)$ fails to have two distinct nonzero roots, declare that there is a decoding error. Otherwise, let β_1 and β_2 be the roots of $\Lambda(z)$, and let $\alpha^{i_1} = 1/\beta_1$ and $\alpha^{i_2} = 1/\beta_2$. Obtain the error values by solving

$$\begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} \\ \alpha^{2i_1} & \alpha^{2i_2} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \end{bmatrix}.$$

Finally, subtract e_1 at the i_1-th position of $\mathbf{y}$, subtract e_2 at the i_2-th position, and return the resulting vector.

We give a few examples of decoding the RS code in Example 1. The field arithmetic can be facilitated by the following correspondence between the powers of primitive element α and the polynomials in α.

i	α^i
0	$\alpha^0 = 1$
1	$\alpha^1 = \alpha$
2	$\alpha^2 = \alpha^2$
3	$\alpha^3 = \alpha + 1$
4	$\alpha^4 = \alpha^2 + \alpha$
5	$\alpha^5 = \alpha^2 + \alpha + 1$
6	$\alpha^6 = \alpha^2 + 1$

Example 1. Suppose that the received vector is

$$\mathbf{y} = (\alpha^2, \alpha^2, \alpha^4, \alpha^7, \alpha^3, \alpha^4, \alpha^3)$$

We compute the syndrome vector.

$$\mathbf{s} = \mathbf{y}H^T = (0, 0, 0, 0)$$

Since the syndromes are all zero, $(\alpha^2, \alpha^2, \alpha^4, \alpha^7, \alpha^3, \alpha^4, \alpha^3)$ is a valid codeword.

Example 2. Suppose that the received vector is

$$\mathbf{y} = (0, \alpha^3, \alpha^4, \alpha^2, \alpha^2, \alpha^3, \alpha^5)$$

The syndrome vector is

$$\mathbf{s} = \mathbf{y}H^T = (\alpha^6, \alpha, \alpha^3, \alpha^5)$$

The syndromes are non-zero, but they form a geometric sequence

$$s_0 = \alpha^4\alpha^2, \ \ s_1 = \alpha^4\alpha^4, \ \ s_2 = \alpha^4\alpha^6, \ \ s_3 = \alpha^4\alpha^8.$$

There is an error at the position associated with α^2, and the error value is α^4. The decoder's output is

$$\mathbf{y} - (0, 0, \alpha^4, 0, 0, 0, 0) = (0, \alpha^3, 0, \alpha^2, \alpha^2, \alpha^3, \alpha^5)$$

Example 3. Suppose that the received vector is

$$\mathbf{y} = (\alpha^5, \alpha^7, \alpha, 0, \alpha^5, \alpha^3, \alpha^7)$$

The syndrome vector is

$$\mathbf{s} = \mathbf{y}H^T = (\alpha^6, \alpha^3, \alpha^4, \alpha^3)$$

The syndromes are not zero and do not form a geometric sequence,

$$\frac{s_1}{s_0} = \alpha^4 \neq \frac{s_2}{s_1} = \alpha.$$

We solve for Λ_1 and Λ_2 from

$$\begin{bmatrix} \alpha^3 & \alpha^6 \\ \alpha^4 & \alpha^3 \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \end{bmatrix} = - \begin{bmatrix} \alpha^4 \\ \alpha^3 \end{bmatrix}.$$

We can apply Cramer's rule to get

$$\Lambda_1 = \frac{\begin{vmatrix} \alpha^4 & \alpha^6 \\ \alpha^3 & \alpha^3 \end{vmatrix}}{\begin{vmatrix} \alpha^3 & \alpha^6 \\ \alpha^4 & \alpha^3 \end{vmatrix}} = \frac{1 + \alpha^2}{\alpha^6 + \alpha^3} = \frac{\alpha^6}{\alpha^4} = \alpha^2,$$

$$\Lambda_2 = \frac{\begin{vmatrix} \alpha^3 & \alpha^4 \\ \alpha^4 & \alpha^3 \end{vmatrix}}{\begin{vmatrix} \alpha^3 & \alpha^6 \\ \alpha^4 & \alpha^3 \end{vmatrix}} = \frac{\alpha^6 + \alpha}{\alpha^6 + \alpha^3} = \frac{\alpha^5}{\alpha^4} = \alpha.$$

Find the roots of $\Lambda(z)$ by exhaustive search

i	0	1	2	3	4	5	6
$\Lambda(\alpha^i)$	α^5	α^7	0	α^5	0	α^4	α^4

Polynomial $\Lambda(z)$ has two distinct roots, namely $\beta_1 = \alpha^2$ and $\beta_2 = \alpha^4$. The reciprocal roots are $\beta_1^{-1} = \alpha^5$ and $\beta_2^{-1} = \alpha^3$. There are errors at the 6-th and the 4-th coordinates.

Compute the error values by solving

$$\begin{bmatrix} \alpha^5 & \alpha^3 \\ \alpha^{10} & \alpha^6 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} \alpha^6 \\ \alpha^3 \end{bmatrix}.$$

By Cramer's rule again, we can obtain the error values e_1 and e_2,

$$e_1 = \frac{\begin{vmatrix} \alpha^6 & \alpha^3 \\ \alpha^3 & \alpha^6 \end{vmatrix}}{\begin{vmatrix} \alpha^5 & \alpha^3 \\ \alpha^{10} & \alpha^6 \end{vmatrix}} = \frac{\alpha^5 + \alpha^6}{\alpha^4 + \alpha^6} = \frac{\alpha}{\alpha^3} = \alpha^5,$$

$$e_2 = \frac{\begin{vmatrix} \alpha^5 & \alpha^6 \\ \alpha^{10} & \alpha^3 \end{vmatrix}}{\begin{vmatrix} \alpha^5 & \alpha^3 \\ \alpha^{10} & \alpha^6 \end{vmatrix}} = \frac{\alpha + \alpha^2}{\alpha^4 + \alpha^6} = \frac{\alpha^4}{\alpha^3} = \alpha.$$

Therefore, the error vector is equal to $\mathbf{e} = (0, 0, 0, \alpha, 0, \alpha^5, 0)$. The decoder return the codeword

$$\mathbf{y} - \mathbf{e} = (\alpha^5, \alpha^7, \alpha, 0, \alpha^5, \alpha^3, \alpha^7) - (0, 0, 0, \alpha, 0, \alpha^5, 0) = (\alpha^5, \alpha^7, \alpha, \alpha, \alpha^5, \alpha^2, \alpha^7).$$

References

[1] W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes,* 2nd edition, MIT Press, 1972.

[2] R. M. Roth, *Introduction to coding theory,* Cambridge University Press, 2006.