Math 525

Chapter 6: Reed-Solomon Codes (Sections 6.1–6.3)

December 4, 2020

- Reed-Solomon (RS) codes are non-binary linear codes; they were invented in 1960 by Irving S. Reed and Gustave Solomon at MIT.

- The first ever use was aboard the Voyager 2 spacecraft that was launched in 1977. On April 5, 1985, the Voyager 2 captured the first image of Uranus from 200 million miles away.
- They became very popular in the early Eighties, being used for burst-error correction on compact discs. Today, they are the standard coding scheme used on CDs, DVDs, and Blu-ray discs.
- RS codes form a subclass of non-binary BCH codes.
- The theory of RS codes forms the basis for understanding more advanced codes that are object of current research, e.g., algebraic-geometry codes.
- The standard decoding algorithm consists of five main steps. It was developed by Peterson, Gorenstein, and Zierler (PGZ algorithm).
- Two key steps of the decoding algorithm, namely, determination of the number of the errors and their locations, can be performed very efficiently via the Berlekamp-Massey algorithm.

Codes over $\mathrm{GF}(2^r)$

Definition

Let r be a positive integer. An (n, k) linear block code over $\mathrm{GF}(2^r)$ is a k-dimensional subspace of $(\mathrm{GF}(2^r))^n$ (i.e., the $\mathrm{GF}(2^r)$-vector space consisting of all n-tuples whose entries are in $\mathrm{GF}(2^r)$).

- Observe that a k-dimensional code of length n over $\mathrm{GF}(q)$ contains q^k codewords (n-tuples over $\mathrm{GF}(q)$). We refer to a code over $\mathrm{GF}(q)$ as a q-ary code. Throughout this presentation, $q = 2^r$.
- Just like codes over $K = \mathrm{GF}(2)$, (n, k) linear block codes over $\mathrm{GF}(q)$ have generator and parity-check matrices.
- The theory we developed for binary cyclic codes can be extended to q-ary cyclic codes with no difficulties.

- A q-ary (n, k) cyclic code is generated by a polynomial of degree $n - k$ over $\mathrm{GF}(q)$,

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k-1} x^{n-k-1} + x^{n-k},$$

  with $g_0 \neq 0$ and $g_i \in \mathrm{GF}(q)$, for $i = 0, 1, \ldots, n - k - 1$.
- We also have: $g(x) \mid x^n - 1$, and $v(x) \in \mathrm{GF}(q)[x]$ of degree $\leq n - 1$ is a code polynomial if and only if $g(x) \mid v(x)$.
- The proofs for the above facts are quite similar to those presented in Chapter 4, so we will omit them.
- If $\alpha_1, \alpha_2, \ldots, \alpha_s$ are distinct non-zero elements of $\mathrm{GF}(q)$, then

$$g(x) = (x + \alpha_1)(x + \alpha_2) \cdots (x + \alpha_s)$$

  generates a linear cyclic code of length $q - 1 = 2^r - 1$ over $\mathrm{GF}(q)$.

Definition

Let $\beta \in \mathrm{GF}(2^r)$ be primitive, let m be an integer, and let δ be a positive integer. A Reed-Solomon code $RS(2^r, \delta)$ of length $n = 2^r - 1$ is a cyclic code over $\mathrm{GF}(2^r)$ with generator polynomial

$$g(x) = (x + \beta^{m+1})(x + \beta^{m+2}) \cdots (x + \beta^{m+\delta-1}).$$

Theorem

For the $RS(2^r, \delta)$-code C above, we have:

(a) *Dimension:* $k = 2^r - \delta$;

(b) *Distance:* $d = \delta$;

(c) *Size:* $|C| = (2^r)^k$.

Corollary

RS codes are maximum distance separable (MDS) codes.

Proof of Theorem: Note that $\deg g(x) = \delta - 1$. Since $n = 2^r - 1$, it follows that $k = (2^r - 1) - (\delta - 1) = 2^r - \delta$. This proves (a). Part (c) is immediate. As for Part (b), notice that a parity-check matrix for $RS(2^r, \delta)$ is

$$H = \begin{bmatrix} 1 & 1 & & 1 \\ \beta^{m+1} & \beta^{m+2} & & \beta^{m+\delta-1} \\ (\beta^{m+1})^2 & (\beta^{m+2})^2 & \cdots & (\beta^{m+\delta-1})^2 \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{n-1} & (\beta^{m+2})^{n-1} & \cdots & (\beta^{m+\delta-1})^{n-1} \end{bmatrix}.$$

Now consider a $(\delta - 1) \times (\delta - 1)$ sub-matrix H' of H, formed by rows $0 \le j_1 < j_2 < \ldots < j_{\delta-1} \le n - 1$ of H:

$$H' = \begin{bmatrix} (\beta^{m+1})^{j_1} & (\beta^{m+2})^{j_1} & \cdots & (\beta^{m+\delta-1})^{j_1} \\ (\beta^{m+1})^{j_2} & (\beta^{m+2})^{j_2} & \cdots & (\beta^{m+\delta-1})^{j_2} \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{j_{\delta-1}} & (\beta^{m+2})^{j_{\delta-1}} & \cdots & (\beta^{m+\delta-1})^{j_{\delta-1}} \end{bmatrix}.$$

We have:

$$\det H' = \begin{vmatrix} (\beta^{m+1})^{j_1} & (\beta^{m+2})^{j_1} & \dots & (\beta^{m+\delta-1})^{j_1} \\ (\beta^{m+1})^{j_2} & (\beta^{m+2})^{j_2} & \dots & (\beta^{m+\delta-1})^{j_2} \\ \vdots & \vdots & & \vdots \\ (\beta^{m+1})^{j_{\delta-1}} & (\beta^{m+2})^{j_{\delta-1}} & \dots & (\beta^{m+\delta-1})^{j_{\delta-1}} \end{vmatrix} =$$

$$\beta^{(m+1)(j_1+j_2+\cdots+j_{\delta-1})} \begin{vmatrix} 1 & \beta^{j_1} & \dots & (\beta^{j_1})^{\delta-2} \\ 1 & \beta^{j_2} & \dots & (\beta^{j_2})^{\delta-2} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{j_{\delta-1}} & \dots & (\beta^{j_{\delta-1}})^{\delta-2} \end{vmatrix}.$$

The latter determinant is always different from zero because it is a Vandermonde determinant (and the β^{j_i} are all distinct). In conclusion, any $\delta - 1$ rows of H are linearly independent, which proves that $d \geq \delta$. On the other hand, by the Singleton bound, $d \leq n - k + 1 = (\delta - 1) + 1 = \delta$. Thus, $d = \delta$. □

Example

Consider the field $\mathrm{GF}(2^4)$ whose elements are listed on page 114 of the textbook, Table 5.1. Find the generator polynomial of $RS(2^4, 4)$.

- We can take $m = -1$ in the definition on page 5. Then

$$g(x) = (x + 1)(x + \beta)(x + \beta^2) = x^3 + \beta^{10}x^2 + \beta^{11}x + \beta^3.$$

- The codeword corresponding to $g(x)$ is:

$$(\beta^3, \beta^{11}, \beta^{10}, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

- The dimension of $RS(2^4, 4)$ is $k = 12$.
- $RS(2^4, 4)$ can be described as:

$$\{a(x) \cdot g(x) \mid a(x) \in \mathrm{GF}(2^4)[x] \text{ and } \deg a(x) \leq 11\}.$$

Example (Cont'd.)

- For instance, let $a(x) = x^8 + x + \beta$. Then $a(x) \cdot g(x) =$

$$x^{11} + \beta^{10}x^{10} + \beta^{11}x^9 + \beta^3 x^8 + x^4 + \beta^8 x^3 + \beta^{10}x + \beta^4$$

is a code-polynomial in $RS(2^4, 4)$. The corresponding 15-tuple is:

$$(\beta^4,\ \beta^{10},\ 0,\ \beta^8,\ 1,\ 0,\ 0,\ 0,\ \beta^3,\ \beta^{11},\ \beta^{10},\ 1,\ 0,\ 0,\ 0).$$

Additional Definitions and Results

Definition (Subfield Subcode)

Let C be a cyclic code of length n over $\mathrm{GF}(q)$ where $q = 2^r$. The set $C_K = C \cap K^n$ is a binary cyclic code of length n, called the subfield subcode of C.

Example

Construct $\mathrm{GF}(4)$ from $h(x) = x^2 + x + 1$. We have

$$\mathrm{GF}(4) = \{0, 1, \beta, \beta^2\},$$

where β is a primitive element and $\beta^2 = \beta + 1$. Now let C be the cyclic code of length 3 over $\mathrm{GF}(4)$ with generator polynomial $g(x) = \beta + x$. One has:

$$\begin{aligned} C &= \{a(x) \cdot g(x) \mid a(x) = a_0 + a_1 \cdot x \text{ with } a_0, a_1 \in \mathrm{GF}(4)\} \\ &= \{(000), (10\beta), (\beta 0 \beta^2), (\beta^2 01), (\beta^2 1\beta), (\beta 10), (111), (01\beta^2), (0\beta 1), \\ &\quad (1\beta\beta^2), (\beta\beta\beta), (\beta^2\beta 0), (\beta^2\beta^2\beta^2), (\beta\beta^2 1), (1\beta^2 0), (0\beta^2\beta)\}. \end{aligned}$$

The subfield subcode C_K is given by

$$C_K = C \cap K^3 = \{(000), (111)\}.$$

Its generator polynomial is $g_K(x) = 1 + x + x^2 = m_\beta(x)$.

Remarks

- C_K is the largest binary cyclic code contained in C.
- Notation as above, let $g(x) = (x + \alpha_1) \cdots (x + \alpha_s)$ and $g_K(x)$ be the generator polynomials of C and C_K, respectively, where $\alpha_1, \ldots, \alpha_s$ are distinct non-zero elements of $\mathrm{GF}(q)$.
- Since $g(x)$ divides $g_K(x)$, $\alpha_1, \ldots, \alpha_s$ are roots of $g_K(x)$. Therefore, $g_K(x)$ equals the product of the *distinct* minimal polynomials of $\alpha_1, \ldots, \alpha_s$ over K.

Additional Definitions and Results (Cont'd).

Example

Let β be a primitive element of $\mathrm{GF}(2^3)$ as constructed below using $1 + x^2 + x^3$. Let $g(x) = (1 + x)(\beta + x)(\beta^2 + x)$ be the generator polynomial of a cyclic code C of length over $\mathrm{GF}(2^3)$. Determine $g_K(x)$, the generator polynomial of the subfield subcode C_K.

word	polynomial in x (modulo $h(x)$)	power of β
0 0 0	0	–
1 0 0	1	1
0 1 0	x	β
0 0 1	x^2	β^2
1 0 1	$1 + x^2 \equiv x^3$	β^3
1 1 1	$1 + x + x^2 \equiv x^4$	β^4
1 1 0	$1 + x \equiv x^5$	β^5
0 1 1	$x + x^2 \equiv x^6$	β^6

Field $\mathrm{GF}(2^3)$ constructed from $h(x) = 1 + x^2 + x^3$.