Cyclic codes

Let us start with the motivating example for cyclic codes, the narrow sense Reed-Solomon codes. In this case, we take as the vector $\mathbf{a}$ the vector $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ for a primitive n-th root of unity α. With some algebra it can be seen that the dual code of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{1})$ is the code $\mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{a})$, so the parity check matrix is

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \\ & & \ldots & \ldots & \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \ldots & \alpha^{(n-k)(n-1)} \end{pmatrix}.$$

If a word $(c_0, c_1, \ldots, c_{n-1})$ is a codeword then it is orthogonal to each row of the parity check matrix. This can be described easily if we introduce the polynomial $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$. Using this, the orthogonality conditions simply mean that

$$c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{n-k}) = 0,$$

or in other words,

$$(x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{n-k}) | c(x).$$

So, to describe the polynomial $c(x)$ for codewords, we can simply say that they are of the form $g(x)f(x)$, where $\deg(gf) \leq n - 1$, and

$$g(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{n-k}).$$

This procedure can be generalized slightly, and using a different GRS code, one can show that for an appropriate GRS code we can have

$$c(\alpha^t) = c(\alpha^{t+1}) = \ldots = c(\alpha^{t+n-k-1}) = 0,$$

or in other words,

$$(x - \alpha^t)(x - \alpha^{t+1}) \ldots (x - \alpha^{t+n-k-1}) | c(x).$$

This leads us to the definition of Reed-Solomon codes in the polynomial setting.

Definition. Let $\alpha \in \mathrm{GF}(q)$ be a primitive n-th root of unity, $n|q-1$. Consider the polynomial $g(x) = (x-\alpha^t)(x-\alpha^{t+1})\dots(x-\alpha^{t+n-k-1})$ for a fixed t. Then $C = \{g(x)f(x) : \deg(f) \leq k-1\}$ is called the narrow sense Reed-Solomon code in the polynomial setting. We remark that they have parameters $[n, k, n-k+1]_q$, since they are GRS codes.

The more general definition of cyclic codes is the following. Using the polynomial associated to a codeword, we will show that cyclic codes always have a generator polynomial, similar to the polynomial $g(x)$ in the definition above.

Definition. A linear code C is called *cyclic* if the right shifts of codewords are also codewords. More formally, if $(c_0, c_1, \dots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. To a codeword $(c_0, c_1, \dots, c_{n-1}) \in C$ we can associate the polynomial $c_0 + c_1 x + \dots + c_{n-1}x^{n-1} = c(x)$ of degree at most $n-1$. The set of these polynomials will be denoted by $C(x)$.

In case of cyclic codes we will always assume that $(n, q) = 1$.

We may observe that the right shift is just $c(x) \mapsto xc(x) \pmod{x^n-1}$. Since using multiplication with x and taking linear combinations we can get $c(x)r(x)$ for any polynomial $r(x)$, we immediately see that $C(x)$ has to be an ideal.

Proposition. *C is a cyclic code if and only if $C(x)$ is an ideal in $\mathrm{GF}(q)[x]/(x^n-1)$.*

We can go a step further and describe cyclic codes explicitly.

Proposition. *C is a cyclic code if and only if $C(x) = (g(x))$ is the principal ideal generated by a monic polynomial (i.e. having leading coefficient 1) $g(x)$, which divides (x^n-1), so $C(x) = \{g(x)f(x) : \deg(gf) \leq n-1\}$.*

Such a polynomial C indeed generates an ideal that contains all the polynomials of the form $g(x)f(x)$ with $\deg(gf) \leq n-1$.

If $C(x)$ is an ideal in $\mathrm{GF}(q)[x]$, then consider its inverse image $I = \{c(x) + t(x)(x^n-1) : c(x) \in C(x), t(x) \in \mathrm{GF}(q)[x]\}$. I is an ideal in $\mathrm{GF}(q)[x]$. The polynomial ring is a principal ideal ring, so $I = (g(x))$ for a monic polynomial $g(x)$. The ideal contains x^n-1, hence $g(x)|x^n-1$. As $g(x)$ divides x^n-1, the multiples of $g(x)$ divided by x^n-1 are multiples of $g(x)$ themselves.

We may also note that $g(x)$ is unique, and it is the monic polynomial in $C(x)$ of smallest degree. If the code C has dimension k, then $\deg(g) = n-k$. The polynomial $g(x)$ is called the *generator polynomial* of C.

We can now write the generator matrix of $(g(x))$ by putting the coefficients of $g(x), xg(x), x^g(x), \dots x^{k-1}g(x)$ in the rows of a $k \times n$ matrix.

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k-1} & g_{n-k} & 0 & \dots & 0 \\ & & & \dots & & & & \dots & \\ 0 & 0 & 0 & \dots & g_0 & g_1 & g_2 & \dots & g_{n-k} \end{pmatrix}.$$

Definition. Let $C = (g(x))$ be a cyclic code. The *parity check polynomial* of C is $h(x) = (x^n-1)/g(x)$. Note that $\deg(h) = k$.

One can also find a parity check matrix of the code $C = (g(x))$, using $h(x)$. Let

$$H = \begin{pmatrix} 0 & \dots & 0 & h_k & \dots & h_1 & h_0 \\ 0 & \dots & h_k & \dots & h_1 & h_0 & 0 \\ 0 & \dots & & & \dots & & \\ h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \end{pmatrix}.$$

To prove that $GH^T = O$, we have to observe that the scalar product of row i of G and row j of H is the coefficient of $x^{n-i-j+1}$ in $g(x)h(x)$, which is zero. The important property here is that the coefficients of h are in reverse order. This implies the following.

Proposition. *Let $C = (g(x))$. Then $C^\perp = (x^k h(1/x))$, so the generator polynomial of the dual code is the reciprocal polynomial of the parity check polynomial.*

From what we saw before, it is clear that we have to factorize $x^n - 1$) over GF(q). If it is factorized into r different factors, then there are 2^r possibilities to choose $g(x)$. Of course, some of these codes are trivial.

Another way to describe a cyclic code is to specify the roots (or some of the roots) of $g(x)$ in a field extension of GF(q). If the roots $\alpha_1, \dots, \alpha_s$ are given, then $g(x)$ will be the least common multiple of the minimal polynomials of $\alpha_1, \dots, \alpha_s$.

Proposition (BCH bound)**.** *If α is a primitive n-th root of unity in* GF(q^m)*, and for the generator polynomial $g(x)$ of a cyclic code over* GF(q) *we have that $\alpha^t, \alpha^{t+1}, \dots, \alpha^{t+\delta-2}$ are roots of $g(x)$, then the minimum distance of $C = (g(x))$ is at least δ.*

Roughly speaking, the narrow sense RS code defined over GF(q^m) by t, δ contains the code C. The narrow sense RS code is MDS. Comparing the meaning of δ and $n - k$ in the definition of narrow sense RS codes, we can see that the minimum distance is at least δ. This implies that also C has minimum distance at least δ. For more details, see the notes on BCH codes.

As a special case, we can obtain the Golay code as cyclic codes. Let us start with the perfect binary Golay codes as cyclic codes. They have length 23, so we have to factorize

$$x^{23}+1 = (x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1).$$

Note that this is not a surprise, because the 23-rd roots of unity are contained in the field GF(2^{11}). If α is a primitive 23rd root of unity, then it is a root of one of the factors (say the second). Let us denote this factor by $g(x)$. Then

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^9, \alpha^{18}, \alpha^{36} = \alpha^{13}, \alpha^{26} = \alpha^3, \alpha^6, \alpha^{12}$$

are also roots of $g(x)$. The code $C = (g(x))$ is indeed a $[23, 12]$ code. Its minimum distance is at least 5, by the BCH bound. We also see that the parity check polynomial of C is the other factor, and it turns out to be the reciprocal

polynomial of $g(x)$. This implies that $C^\perp = (x+1)g(x)$, so $C^\perp \leq C$ and it has dimension 11. We may see that the all-1 vector belongs to C, since the polynomial $(x^{23}+1)/(x+1)$ is a multiple of $g(x)$.

Using these observations we can show that $\bar{C}$ is a self-dual. If we extend with the parity check bit the basis $g(x)xg(x), \ldots, x^{11}g(x)$, then we get a basis of $\bar{C}$ all of whose vector have weight 8. So, the code $\bar{C}$ is self-dual and doubly even, and by the above remark has minimum distance at least 5, proving $d = 8$. So $\bar{C}$ is the extended Golay code.