Week 9

Cyclic codes

Version 2023-11-12. To accessible online version of this chapter

Synopsis. *Cyclic codes form a subclass of linear codes. Cyclic codes are easy to define, but to reveal their advantages, one needs to study them using polynomials. We identify $\mathbb{F}_q^n$ with the space R_n of polynomials in $\mathbb{F}_q[x]$ of degree less than n, so that a linear code of length n becomes a subspace of R_n. We prove that cyclic codes are subspaces of very special form: a cyclic code C consists of all multiples, in R_n, of its generator polynomial $g(x)$. We also define a check polynomial of C. We can classify cyclic codes of length n by listing all monic divisors of the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$. Theory and applications of cyclic codes are underpinned by the Division Theorem for polynomials and the long division algorithm, which we review here.*

Definition: cyclic shift, cyclic code

For a vector $\underline{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, we denote $s(\underline{a}) = (a_{n-1}, a_0, \ldots, a_{n-2})$ and call the vector $s(\underline{a})$ the **cyclic shift** of $\underline{a}$.
A **cyclic code** in $\mathbb{F}_q^n$ is a **linear** code C such that $\forall \underline{a} \in C$, $s(\underline{a}) \in C$.
Equivalently, a cyclic code is a linear code C such that $s(C) = C$.

Remark: We can iterate the cyclic shift, so if a cyclic code C contains $(a_0, a_1, \ldots, a_{n-1})$, then C also contains the vectors $(a_{n-2}, a_{n-1}, a_0, \ldots, a_{n-3})$, $\ldots$, $(a_1, \ldots, a_{n-1}, a_0)$.

Vectors as polynomials

To study cyclic codes, we will identify **vectors of length n** with **polynomials of degree $< n$** with coefficients in the field $\mathbb{F}_q$:

$$\underline{a} = (a_0, a_1, \ldots, a_{n-1}) \quad \mapsto \quad a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \quad \in \mathbb{F}_q[x]$$

Here $\mathbb{F}_q[x]$ is the **ring of polynomials** in one variable, x, with coefficients in $\mathbb{F}_q$.

Notation: the polynomial $a(x)$ and the vector $\underline{a}$

If n is given and $a(x)$ is a polynomial of degree less than n, $\underline{a}$ (same letter, underlined) will denote the vector which corresponds to $a(x)$ in $\mathbb{F}_q^n$.

Example: E_3 is a cyclic code

Show that the binary even weight code $E_3 = \{000, 110, 011, 101\} \subseteq \mathbb{F}_2^3$ is cyclic. List the **code polynomials** of E_3.

Solution. We know that E_3 is a linear code. It is closed under the cyclic shift: 000 is invariant under the cyclic shift, and $110 \xrightarrow{s} 011 \xrightarrow{s} 101$. Hence E_3 is a cyclic code:

Codevector	Code polynomial	Remark
000	0	
110	$1+x$	
011	$x+x^2$	$= x(1+x)$
101	$1+x^2$	$= (1+x)(1+x)$

We will soon explain the notable fact that all code polynomials of E_3 are multiples of $1+x$.

The Division Theorem for polynomials

In general we cannot divide $f(x)$ by $g(x)$ in $\mathbb{F}_q[x]$ and expect to get a polynomial. However, just as the ring $\mathbb{Z}$ of integers, the ring $\mathbb{F}_q[x]$ has an extra operation called **division with remainder**, as per the following

Theorem 9.1: Division Theorem for polynomials

For all $f(x) \in \mathbb{F}_q[x]$, $g(x) \in \mathbb{F}_q[x] \setminus \{0\}$, there exist unique $Q(x), r(x) \in \mathbb{F}_q[x]$ with

$$f(x) = g(x)Q(x) + r(x) \qquad \text{and} \qquad \deg r(x) < \deg g(x)$$

(possibly $r(x) = 0$). In this case the polynomial $Q(x)$ is the **quotient**, and $r(x)$ the **remainder**, of $f(x)$ when divided by $g(x)$.

We will **not** prove the Division Theorem but we will note and use the practical algorithm for finding the quotient and the remainder, known as **long division of polynomials**.

Example: long division of polynomials

Divide $x^5 + 1$ by $x^2 + x + 1$ in $\mathbb{F}_2[x]$, finding the quotient and the remainder.

Solution.

$$
\begin{array}{r|llll}
\multicolumn{1}{r}{} & x^3 + x^2 + 1 & & & \text{(quotient)} \\
\cline{2-4}
x^2+x+1 & x^5 & & +1 & \text{(dividend)} \\
 & -\;x^5+x^4+x^3 & & & \\
\cline{2-3}
 & \quad x^4+x^3 & & +1 & \\
 & \quad -\;x^4+x^3+x^2 & & & \\
\cline{2-4}
 & \qquad\quad x^2 & & +1 & \\
 & \qquad\quad -\;x^2+x+1 & & & \\
\cline{2-4}
 & \qquad\qquad\quad x & & & \text{(remainder)}
\end{array}
$$

Hence $x^5 + 1 = (x^2 + x + 1)Q(x) + r(x)$ in $\mathbb{F}_2[x]$, with $Q(x) = x^3 + x^2 + 1$ and $r(x) = x$.

This example shows long division of polynomials over $\mathbb{F}_2$. Division by a fixed binary polynomial is widely implemented in electronic circuits at hardware level, by means of shift feedback registers. We will soon see why such implementations are needed.

The generator polynomial of a cyclic code

In what follows, R_n denotes the space of polynomials of degree less than n.

Definition: generator polynomial

A **generator polynomial** of a cyclic code $C \subseteq R_n$, $C \neq \{0\}$ is a monic polynomial of least degree in C.
By convention, the generator polynomial of the null code $\{0\} \subseteq R_n$ is $x^n - 1$.

Recall that a polynomial $g(x)$ is **monic** if the coefficient of the highest power of x in $g(x)$ is 1.

Lemma 9.2: existence and uniqueness of a generator polynomial

Every cyclic code C has a unique generator polynomial $g(x)$.

Proof. If $C = \{0\}$, by definition $x^n - 1$ is the unique generator polynomial. Assume $C \neq \{0\}$.

Existence: take $g(x) \in C$ to be a non-zero polynomial of lowest degree in C. Make $g(x)$ monic by dividing it by its leading coefficient. This does not change the degree, so we now have a monic polynomial of least degree in C. Existence is proved.

Uniqueness: let $g_1(x) \in C$ be another generator polynomial, then by definition $g_1(x)$ is monic and has the same degree as $g(x)$. So $f(x) = g_1(x) - g(x)$ has degree less than $\deg g(x)$ (because the leading term $x^{\deg g}$ cancels due to subtraction). Note that $f(x) \in C$ because C is linear. If $f(x) \neq 0$, divide $f(x)$ by its leading coefficient and obtain a monic polynomial, again in C, of degree less than $\deg g$. This contradicts the choice of $g(x)$. Hence $f(x)$ must be 0, and $g_1(x) = g(x)$. Uniqueness is proved. $\square$

Theorem 9.3: properties of the generator polynomial

Let $C \subseteq R_n$ be a cyclic code with generator polynomial $g(x)$. Write $\deg g = n - k$. Then

1. $C = \{u(x)g(x) : u(x) \in R_k\}$, i.e., the code polynomials of C are all possible multiples of $g(x)$ of degree less than n.

2. $g(x)$ is a monic factor of the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$.

Proof. Both claims are trivially true when $C = \{0\}$ and $g(x) = x^n - 1$, so assume $C \neq \{0\}$.

1. Observe that, writing elements of C as vectors, we have

$$\underline{g} = (g_0, g_1, \ldots, g_{n-k}, \underbrace{0, 0, \ldots, 0}_{k-1 \text{ zeros}})$$

and, as long as $i \leq k - 1$,

$$\underline{x^i g} = (\underbrace{0, \ldots, 0}_{i \text{ zeros}}, g_0, g_1, \ldots, g_{n-k}, \underbrace{0, \ldots, 0}_{k-1-i \text{ zeros}}).$$

That is, $\underline{x^i g}$ is obtained from $\underline{g}$ by applying the cyclic shift i times. Since C is cyclic, this means that $xg(x), \ldots, x^{k-1}g(x) \in C$.

Now, every polynomial $u(x) \in R_k$ — that is, a polynomial of degree less than k — is written as $u_0 + u_1 x + \cdots + u_{k-1}x^{k-1}$ for some $u_0, \ldots, u_{k-1} \in \mathbb{F}_q$. Hence $u(x)g(x)$ is a linear combination of the polynomials $g(x), xg(x), \ldots, x^{k-1}g(x)$ which are in C, and, as C is linear, $u(x)g(x) \in C$. We proved that $C \supseteq \{u(x)g(x) : u(x) \in R_k\}$.

Let us show that $C \subseteq \{u(x)g(x) : u(x) \in R_k\}$. Take $f(x) \in C$ and apply the Division Theorem for polynomials to write $r(x) = f(x) - g(x)Q(x)$ where $\deg r(x) < \deg g(x)$. We will get $\deg Q = \deg f - \deg g < n - (n - k) = k$ and so, by what has already been proved, $g(x)Q(x) \in C$. Then by linearity $r(x) \in C$. We have seen already that there cannot be a non-zero polynomial in C of degree strictly less than $\deg g$, so $r(x) = 0$ and $f(x) = g(x)Q(x)$ is a multiple of $g(x)$, as claimed. Part 1 of the Theorem is proved.

2. Continuing from the above, observe that

$$s(\underline{x^{k-1}g}) = (g_{n-k}, \underbrace{0, \ldots, 0}_{k-1 \text{ zeros}}, g_0, g_1, \ldots, g_{n-k-1})$$

where s is the cyclic shift. Hence the vector $s(\underline{x^{k-1}g})$ corresponds to the polynomial

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

which can be written as

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

as $g_{n-k} = 1$ given that $g(x)$ is monic. Since C is cyclic, $s(\underline{x^{k-1}g}) \in C$ and so $x^k g(x) - (x^n - 1) \in C$. Then by Part 1, $x^k g(x) - (x^n - 1) = u(x)g(x)$ for some polynomial $u(x)$, and so $x^n - 1 = (x^k - u(x))g(x)$ which shows that $g(x)$ is indeed a factor of $x^n - 1$. $\square$

Example: the generator polynomial of E_3

The code E_3 as a subspace of $\mathbb{F}_2[x]$ consists of polynomials 0, $1+x$, $x+x^2 = x(1+x)$ and $1 + x^2 = (1 + x)^2$. The generator polynomial of E_3 is $g(x) = 1 + x$ of degree 1.

As we have already noted, all the code polynomials of E_3 are multiples of $1 + x$.

Error detection by a cyclic code

Theorem 9.3 means that if C is a cyclic code, there is no need to store a check matrix for *error detection*. To determine whether the received vector $\underline{y}$ is a codevector, divide the polynomial $y(x)$ by the generator polynomial $g(x)$; the remainder is 0, if and only if $\underline{y} \in C$.

This is how error detection is implemented in practice for binary cyclic codes (e.g., in Ethernet networks). Long division by $g(x)$ is implemented by circuitry.

Nevertheless, for theoretical purposes we would like to have generator and check matrices for a cyclic code with a given generator polynomial.

The check polynomial

Definition: check polynomial

Let $g(x)$ be the generator polynomial of a cyclic code $C \subseteq \mathbb{F}_q^n$. The polynomial $h(x)$ defined by $g(x)h(x) = x^n - 1$ is the **check polynomial** of C.

Note that if $\deg g(x) = n - k$, then $\deg h(x) = k$, and h is monic.

Theorem 9.4: a generator matrix and a check matrix for a cyclic code

Let $C \subseteq \mathbb{F}_q^n$ be a cyclic code with generator polynomial $g(x) = g_0 + g_1 x + \ldots + g_{n-k}x^{n-k}$ and check polynomial $h(x) = h_0 + h_1 x + \ldots + h_k x^k$.
The vector $\underline{g}$ and its next $k-1$ cyclic shifts form a generator matrix for C:

$$G = \begin{bmatrix} g_0 & g_1 & \ldots & \ldots & g_{n-k} & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & \ldots & g_{n-k} & \ddots & 0 \\ \vdots & \ddots & \ddots & & & & & \ddots \\ 0 & \ldots & 0 & g_0 & \ldots & \ldots & & g_{n-k} \end{bmatrix} \qquad (k \text{ rows}).$$

The vector of the polynomial

$$\overleftarrow{h}(x) = h_k + h_{k-1}x + \ldots + h_0 x^k,$$

obtained from $h(x)$ by reversing the order of the coefficients, and its next $n-k-1$ shifts form a check matrix for C:

$$H = \begin{bmatrix} 1 & h_{k-1} & \ldots & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & & & & & \ddots & \\ 0 & \ddots & 1 & h_{k-1} & \ldots & \ldots & h_1 & h_0 & 0 \\ 0 & \ldots & 0 & 1 & \ldots & \ldots & & h_1 & h_0 \end{bmatrix} \qquad (n-k \text{ rows}).$$

Proof. The rows of G are linearly independent and the rows of H are linearly independent. Indeed, H is a matrix in a row echelon form with no zero rows, and so is G up to scaling of rows by a non-zero scalar g_0: note that $g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0$.

The linearly independent rows of G correspond to the polynomials $g(x), xg(x), \ldots, x^{k-1}g(x)$ and so they span $\{u(x)g(x) : \deg u(x) < k\}$ which by Theorem 9.3 is C. Thus, G is a generator matrix for C.

Since the number of rows of H is $n - k = \dim C^\perp$ and the rows are linearly independent, to show that H is a check matrix it is enough to show that $HG^T = 0$, same as in the proof of Theorem 7.1.

We express the inner product of vectors in terms of polynomials: if $\underline{a}, \underline{b} \in \mathbb{F}_q^n$, then

$$\underline{a} \cdot \underline{\overleftarrow{b}} = \text{coefficient of } x^{n-1} \text{ in } a(x)b(x).$$

Indeed, with $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\underline{\overleftarrow{b}} = (b_{n-1}, \ldots, b_1, b_0)$ one has $\underline{a} \cdot \underline{\overleftarrow{b}} = a_0 b_{n-1} + \cdots + a_{n-1}b_0$ which is exactly the coefficient of x^{n-1} in the product of the polynomials $a(x)$ and $b(x)$.

Number the rows of G from 0 to $k-1$, the rows of H from 0 to $n-k-1$. The rows of G are $\underline{x^i g}$, and the rows of H are the vectors of $x^j h$ written backwards. So an entry of HG^T, which as we know is an inner product of a row of G and a row of H, is the coefficient of x^{n-1} in $x^i g(x) x^j h(x) = x^{n+i+j} - x^{i+j}$. But since $n+i+j > n-1$ and $i+j < n-1$, this coefficient is zero, proving $HG^T = 0$. $\square$

Remark: this is not the only generator matrix (resp., check matrix) for C. As we know, a generator matrix is not unique. Moreover, these matrices are not usually in standard form. Note that a generator polynomial of C is unique.

Corollary 9.5: generator polynomial of $C^\perp$

$C^\perp$ is also a cyclic code with generator polynomial $h_0^{-1}\overleftarrow{h}(x)$. (Scaling by h_0^{-1} is necessary because the generator polynomial must by definition be monic.)

Example: cyclic binary codes of length 3

Use Theorem 9.3 and Theorem 9.4 to find all the cyclic binary codes of length 3.

Solution. Generator polynomials are **monic factors of** $x^n - 1$ **in** $\mathbb{F}_q[x]$. The first step is to factorise $x^n - 1$ into **irreducible monic polynomials** in $\mathbb{F}_q[x]$. A polynomial is irreducible if it cannot be written as a product of two polynomials of positive degree.

Note that the polynomial $x^n - 1$ is **not** irreducible in $\mathbb{F}_q[x]$. Indeed, $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$.

We work over the field $\mathbb{F}_2$ and observe:

$$x^3 - 1 = (x-1)(x^2 + x + 1).$$

The polynomial $x - 1 = x + 1$ is irreducible, because it is of degree 1.

Can we factorise the polynomial x^2+x+1 in $\mathbb{F}_2[x]$? If we could, we would have a factorisation $(x+a)(x+b)$. But then $ab = 1$ which means $a = b = 1$ in $\mathbb{F}_2$. Note that $(x+1)^2 = x^2 + 1$ in $\mathbb{F}_2[x]$. We have shown that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

So the possible monic factors of $x^3 - 1$ in $\mathbb{F}_2[x]$ are:

$$1; \qquad 1 + x; \qquad 1 + x + x^2; \qquad 1 + x^3.$$

We now list every cyclic code in $\mathbb{F}_2^3$, giving its generator matrix G, minimum distance d and a well-known name of the code, and point out its dual code (which is also cyclic).

- $g(x) = 1$, $G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ which corresponds to the **trivial binary code** of length 3: $C = \mathbb{F}_2^3$ with $d = 1$. The dual code of $\mathbb{F}_2^3$ is the null code (see below).

- $g(x) = 1 + x$, $G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$. This is $\{000, 110, 011, 101\} = E_3$, the binary even weight code of length 3 which has $d = 2$. The dual of E_3 is $Rep(3, \mathbb{F}_2)$ (see below).

- $g(x) = 1 + x + x^2$, $G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$. This is $\{000, 111\} = Rep(3, \mathbb{F}_2)$, the binary repetition code of length 3 with $d = 3$. This code is $(E_3)^\perp$.

- $g(x) = 1 + x^3$. Theorem 9.4 returns matrix G with $k = 3 - 3 = 0$ rows, $G = [\quad]$. And indeed, by definition $1 + x^3$ is the generator polynomial of the null code $\{000\}$, which has empty generator matrix. It is a useless code but formally it is a linear and cyclic code, so we have to allow it for reasons of consistency. The minimum distance of the zero code is undefined. This code is $(\mathbb{F}_2^3)^\perp$.