32031 Feedback Quiz, 2022/23 S2, Week 09: Cyclic codes

Open books. Not for credit

Recall that a **cyclic** code is a code $C \subseteq \mathbb{F}_q^n$ which is **linear** and **closed under the cyclic shift**:

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Longrightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C.$$

When studying cyclic codes, the key tool is converting vectors to polynomials:

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

If a code C is cyclic, it has exactly one **generator polynomial** $g(x)$. This is the monic polynomial of least degree among the code polynomials of C; it is always a factor of $x^n - 1$ in $\mathbb{F}_q[x]$. All the code polynomials are $u(x)g(x)$ where $u(x) \in \mathbb{F}_q[x]$ and $\deg u(x)g(x) < n$. Thus, cyclic codes in $\mathbb{F}_q^n$ are in one-to-one correspondence with monic divisors of $x^n - 1$ in $\mathbb{F}_q[x]$.

You are given that $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$ in $\mathbb{F}_3[x]$, a factorisation into monic irreducible polynomials. (*Irreducible* means that they cannot be factorised any further.)

Question 1 ♣ What are the possible **dimensions** of cyclic ternary codes of length 8?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9

Question 2 How many cyclic ternary codes of length 8 are there?

○ 8 ○ 256 ○ 3^5 ○ 32 ○ 5

Question 3 ♣ Select the polynomials which are generator polynomials of cyclic ternary codes of length 8.

○ $x-1$ ○ x^2-1 ○ 1 ○ $1+x-x^2$ ○ x^4+1

An extra question about binary codes — attempt if you have done Q1–3.

Question 4 ♣ Various data transfer protocols such as USB, DECT (cordless phones), Bluetooth etc protect data from errors by using a binary cyclic code with the following properties: **length** $2^{15}-1$, **dimension** 32751, **can detect up to** 3 **bit errors** in a codevector. On the basis of these properties, select the polynomials that could be generator polynomials for such a code.

○ $x^{32751} + x^{32740} + 1$

○ $x^{16} + x^5 + 1$

○ $x^{32751} + x^{15} + x^2 + x$

○ $x^{16} + x^{10} + x^8 + x^7 + x^3 + 1$

○ $x^{16} + x^8 + x^7 + x$

○ $x^{16} + x^{15} + x^2 + 1$

○ $x^{32751} + x^8 + x^7 + 1$

CORRECTED

32031 Feedback Quiz, 2022/23 S2, Week 09: Cyclic codes

Open books. Not for credit

Recall that a **cyclic** code is a code $C \subseteq \mathbb{F}_q^n$ which is **linear** and **closed under the cyclic shift**:

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Longrightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C.$$

When studying cyclic codes, the key tool is converting vectors to polynomials:

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

If a code C is cyclic, it has exactly one **generator polynomial** $g(x)$. This is the monic polynomial of least degree among the code polynomials of C; it is always a factor of $x^n - 1$ in $\mathbb{F}_q[x]$. All the code polynomials are $u(x)g(x)$ where $u(x) \in \mathbb{F}_q[x]$ and $\deg u(x)g(x) < n$. Thus, cyclic codes in $\mathbb{F}_q^n$ are in one-to-one correspondence with monic divisors of $x^n - 1$ in $\mathbb{F}_q[x]$.

You are given that $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$ in $\mathbb{F}_3[x]$, a factorisation into monic irreducible polynomials. (*Irreducible* means that they cannot be factorised any further.)

Question 1 ♣ What are the possible **dimensions** of cyclic ternary codes of length 8?

☒ 0 ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8 ○ 9

Explanation: Cyclic codes in $\mathbb{F}_q^n$ are in 1-to-1 correspondence with monic polynomials $g(x)$ that divide $x^n - 1$, referred to as generator polynomials. The dimension of a cyclic code is $k = n - \deg g(x)$. From the factorisation of $x^8 - 1$ it is clear that one can form polynomials $g(x)$ of degrees $0, 1, \ldots, 8$ by multiplying some of the factors of $x^8 - 1$. Degree 0: $g(x) = 1$. Degree 1: $g(x) = x - 1$. Degree 2: $x^2 + 1$. Degree 3: $(x-1)(x^2+1)$. Degree 4: $(x+1)(x-1)(x^2+1)$. For each $g(x)$, the polynomial $(x^8-1)/g(x)$ is also a generator polynomial, of degree $8 - \deg g(x)$; this covers degrees 5,6,7,8. Dimension 9 is of course impossible if the length is 8. Special cases: 0-dimensional code is $\{00000000\}$, cyclic; 8-dimensional code is the trivial code $\mathbb{F}_3^8$, also cyclic.

Question 2 How many cyclic ternary codes of length 8 are there?

○ 8 ○ 256 ○ 3^5 ☒ 32 ○ 5

Explanation: A generator polynomial is a product of a subset of the five monic irreducible factors of $x^8 - 1$ which are all distinct. There are $2^5 = 32$ ways to choose a subset of a set of 5 elements.

Question 3 ♣ Select the polynomials which are generator polynomials of cyclic ternary codes of length 8.

CORRECTED

⊗ $x-1$ ⊗ x^2-1 ⊗ 1 ◯ $1+x-x^2$ ⊗ x^4+1

Explanation: From the factorisation we can see that $x-1$ and $x^2-1=(x-1)(x+1)$ divide x^8-1; they are monic, hence they are generator polynomials.
Trivially, 1 divides x^8-1, and 1 is a generator polynomial: 1 generates the trivial code $\mathbb{F}_3^8$.
The polynomial $1+x-x^2$ is not monic (leading coefficient is -1) so it is not a generator polynomial.
Note that x^4+1 is monic and divides x^8-1 as we have $x^8-1=(x^4-1)(x^4+1)$, so is a generator polynomial. Incidentally $x^4+1=(x^2+x-1)(x^2-x-1)$ in $\mathbb{F}_3[x]$.

An extra question about binary codes — attempt if you have done Q1–3.

Question 4 ♣ Various data transfer protocols such as USB, DECT (cordless phones), Bluetooth etc protect data from errors by using a binary cyclic code with the following properties: **length** $2^{15}-1$, **dimension** 32751, **can detect up to** 3 **bit errors** in a codevector. On the basis of these properties, select the polynomials that <u>could be</u> generator polynomials for such a code.
Explanation: Note that $\deg g(x)=n-k=(2^{15}-1)-32751=32767-32751=16$.

◯ $x^{32751}+x^{32740}+1$

Explanation: No: degree is not 16

◯ $x^{16}+x^5+1$

Explanation: No: the corresponding codevector 10000100000000001000... has weight 3 hence 3 undetected bit errors are possible — the code cannot detect 3 errors

◯ $x^{32751}+x^{15}+x^2+x$

Explanation: No: degree is not 16

⊗ $x^{16}+x^{10}+x^8+x^7+x^3+1$

Explanation: Yes; generates the CRC-16-DECT cyclic code. Although the generator polynomial is written as a vector of weight 6, the weight of the code is in fact 4 as there are codevectors of weight 4

◯ $x^{16}+x^8+x^7+x$

Explanation: No: is a multiple of x hence cannot divide x^n-1 which is not a multiple of x

⊗ $x^{16}+x^{15}+x^2+1$

Explanation: Yes; in fact, this generates the CRC-16-IBM cyclic code

○ $x^{32751} + x^8 + x^7 + 1$

Explanation: No: degree is not 16