

Cyclic

George McNinch

2024-03-06 and 2024-03-11

Cyclic codes: definitions

Consider a linear code $C \subset \mathbb{F}_q^n$. Then C is said to be *cyclic* if

$$(c_0, c_1, \dots, c_{n-1}) \in C \implies (c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C.$$

Observe that there is an isomorphism of vector spaces

$$\mathbb{F}_q^n \rightarrow \mathbb{F}_q[T]/\langle T^n - 1 \rangle$$

given by the assignment

$$\phi(c_0, c_1, \dots, c_{n-1}) = \sum_{i=0}^{n-1} c_i T^i.$$

Here $\mathbb{F}_q[T]/\langle T^n - 1 \rangle$ denotes the quotient of the polynomial ring $\mathbb{F}_q[T]$ by the (principal) ideal generated by $T^n - 1$. Elements of $\mathbb{F}_q[T]/\langle T^n - 1 \rangle$ are additive cosets $f + \langle T^n - 1 \rangle$ for $f \in \mathbb{F}_q[T]$; we have

$$f + \langle T^n - 1 \rangle = g + \langle T^n - 1 \rangle$$

if and only if $f - g \in \langle T^n - 1 \rangle$; i.e. if and only if $T^n - 1 \mid f - g$.

We are going to identify C and its image in $\mathbb{F}_q[T]/\langle T^n - 1 \rangle$; from this point of view, each codeword in C is represented by a unique polynomial $f \in \mathbb{F}_q[T]$ with $\deg f < n$.

Let's write $A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$. Recall that an *ideal* of the ring A is a linear subspace $I \subseteq A$ with the property that

$$f \cdot I \subseteq I \quad \forall f \in A$$

i.e. $fg \in I$ for all $f \in A$ and all $g \in I$.

Remark The weight of a vector $f = \sum_{i=0}^n a_i T^i \in A$ is of course given by $\text{weight}(f) = \#\{j \mid a_j \neq 0\}$.

Lemma A subspace $I \subseteq A$ is an ideal if and only if $T \cdot I \subseteq I$.

Proof of Lemma Let $I \subseteq A$ be a linear subspace. If I is an ideal, then by definitions we know that $T \cdot I \subseteq I$.

Suppose on the other hand that $T \cdot I \subseteq I$. Fix $f = \sum_{i=0}^{n-1} a_i T^i \in A$ where $a_i \in \mathbb{F}_q$, and let $g \in I$. We have to argue that $fg \in I$.

By assumption we know that $Tg \in I$, and by an easy induction we see that $T^j g \in I$ for all $j \geq 0$. Now

$$fg = \sum_{i=0}^n a_i T^i g \in I$$

since I is a *linear subspace* of A .

Proposition The code C is *cyclic* if and only if C is an ideal when viewed as a subspace of $A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$.

Proof For a polynomial $f = \sum_{i=0}^{n-1} c_i T^i \in A$, notice that

$$T \cdot f = \sum_{i=0}^{n-1} c_i T^{i+1} = c_{n-1} + c_0 T + c_1 T^2 + \cdots + c_{n-2} T^{n-1}$$

since $T^n = 1$ in A .

Note that f corresponds to $(c_0, c_1, \dots, c_{n-1})$ and Tf corresponds to $(c_{n-1}, c_0, \dots, c_{n-2})$.

Thus C is cyclic iff $TC \subseteq C$; by the Lemma, this last condition is equivalent to the condition that C is an ideal of A .

We recall the important result:

Theorem Let F be a field

- a. The polynomial ring $F[T]$ is a principal ideal domain. Thus if I is an ideal of $F[T]$, there is $f \in I$ with

$$I = \langle f \rangle = \{fh \mid h \in F[T]\} = fF[T].$$

- b. For any ideal I of $F[T]$, the quotient ring $F[T]/I$ is also a principal ideal domain.
- c. In particular, $A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$ is a principal ideal domain.

Proof of b Recall that ideals of $F[T]/I$ are in one-to-one correspondence with ideals of $F[T]$ which contain I .

In fact, if $I \subseteq J \subseteq F[T]$ with J an ideal, the ideal of $F[T]/I$ corresponding to J is $J/I = \{h + I \mid h \in J\}$. Since $J = \langle f \rangle = fF[T]$ is principal, also $J/I = \langle f + I \rangle = (f + I)(F[T]/I)$ is principal.

Cyclic codes via polynomials

Let $C \subset A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$ be a cyclic code of length n . Since C is an ideal of A , there is a polynomial g with $\deg(g) < n$ for which $C = \langle g \rangle$.

We will always choose g to be *monic* and of minimal degree among polynomials in C .

Proposition If $C = \langle g \rangle$ with g monic of minimal degree, then $g \mid T^n - 1$ in $\mathbb{F}_q[T]$.

Proof Working in the polynomial ring $\mathbb{F}_q[T]$, let $h = \gcd(g, T^n - 1)$. Thus

- $h \mid g$,
- $h \mid T^n - 1$, and
- for any polynomial f satisfying $f \mid g$ and $f \mid T^n - 1$, we have $f \mid h$.

It is an important fact that h may be written

$$(*) \quad h = a \cdot g + b \cdot (T^n - 1) \quad \text{for } a, b \in \mathbb{F}_q[T].$$

For clarity, I'm going to write (for the Lemma only) $[f]$ for the element of the quotient ring A represented by $f \in \mathbb{F}_q[T]$.

Now, if g does not divide $T^n - 1$, then $\deg h < \deg g$.

On the other hand, working in the quotient ring $A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$, $(*)$ shows that $[h] = a \cdot [g] \in \langle [g] \rangle$.

Thus h is a polynomial with $[h] \in C$ having strictly smaller degree than g , contradicting the fact that g has minimal degree among polynomials in C .

This contradiction shows that $g \mid T^n - 1$.

Example Let $0 \leq i < n$ and consider the ideal $\langle T^i \rangle$ of $A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$.

Notice that T^i (or more precisely, the element of A determined by the coset $T^i + \langle T^n - 1 \rangle$) is a *unit* in A , since

$$T^i \cdot T^{n-i} = 1 \quad \text{in } A$$

(i.e. $T^i \cdot T^{n-i} \equiv T^n \equiv 1 \pmod{T^n - 1}$).

Thus $1 \in \langle T^i \rangle$ so that $\langle T^i \rangle = \langle 1 \rangle = A$.

In particular, the minimal degree representative for the ideal $\langle T^i \rangle$ is $1 = T^0$.

Proposition Let F be any field, let $f, g \in F[T]$ and suppose that $g \mid f$. Form the quotient ring $B = F[T]/\langle f \rangle$. Then

$$\dim_F \langle g \rangle = \dim_F gB = \deg f - \deg g.$$

Proof Note that $g \mid f \implies \langle f \rangle \subseteq \langle g \rangle$. Now, basic properties of the polynomial ring tell us that $\dim B = \dim F[T]/\langle f \rangle = \deg f$.

(Indeed, the cosets $T^i + \langle f \rangle$ for $0 \leq i < \deg f$ form an F -basis).

One of the *Isomorphism Theorems* tells us that the quotient ring $B/gB = B/\langle g \rangle$ may be identified with $F[T]/\langle g \rangle$; indeed, the natural mapping

$$B/gB = \frac{F[T]/\langle f \rangle}{\langle g \rangle/\langle f \rangle} \rightarrow F[T]/\langle g \rangle$$

is a ring isomorphism. In particular, we see that $\dim B/gB = \deg g$.

Our goal is to compute the dimension of $gB = \langle g \rangle$. Of course, as *linear spaces*

$$B \simeq \langle g \rangle \oplus (B/\langle g \rangle);$$

this shows that

$$\dim \langle g \rangle = \dim B - \dim(B/\langle g \rangle) = \deg f - \deg g.$$

We get at once:

Corollary If $g \in \mathbb{F}_q[T]$ and g divides $T^n - 1$, then the ideal $\langle g \rangle \subset A = \mathbb{F}_q[T]/\langle T^n - 1 \rangle$ has dimension

$$\dim \langle g \rangle = \dim gA = n - \deg g.$$

In particular, we see that a polynomial $g \mid T^n - 1$ determines a code with parameters $[n, n - \deg g]_q$.

The Ternary Golay code.

Let $q = 3$ and consider $f = T^{11} - 1 \in \mathbb{F}_3[T]$.

We first look for $j \geq 1$ for which $\ell = \mathbb{F}_{3^j}$ contains a root of f ; the minimal j is 5:

```
[ (i, mod(3^i - 1, 11)) for i in range(6) ]
=>
[(0, 0), (1, 2), (2, 8), (3, 4), (4, 3), (5, 0)]
```

If we choose a generator z for the multiplicative group $\ell^\times = \mathbb{F}_{3^5}^\times$, then $a = z^{((3^5 - 1)/11)}$ is an element ℓ^\times of order 11.

```
a = z^((3^5-1)/11)
# confirming...
multiplicative_order(a) == 11
=>
True
```

Now, the minimal polynomial of a over \mathbb{F}_3 must have degree 5. What are its roots?

Well, if a is a root, also a^3 is a root since the mapping $\alpha \mapsto \alpha^3$ is in the Galois group of \mathbb{F}_{3^5} over \mathbb{F}_3 . Similarly, $a^{(3^i)}$ is a root for every natural number i .

But of course $a^{(3^5)} = a$ since 11 divides $3^5 - 1$.

```
# let's display the roots of the minimal polynomial of a:
[( f"a^(3^{i})=" , a^(3^i) ) for i in range(5) ]
=>
[('a^(3^0)=', 2*z^3 + 2*z^2 + z + 1),
 ('a^(3^1)=', z^4 + z^3 + 2*z^2 + 2),
 ('a^(3^2)=', z^3 + 2*z + 1),
 ('a^(3^3)=', 2*z^4 + 2*z^3 + z),
 ('a^(3^4)=', 2*z^2 + 2*z + 1)]
```

In fact, the monic minimal polynomial is the product of the linear factors corresponding to these roots. Namely:

```
g = product([T - a^(3^i) for i in range(5)])
g
=>
T^5 + T^4 + 2*T^3 + T^2 + 2
```

Note that this polynomial has coefficients in \mathbb{F}_3 !

In addition to the trivial root 1, there are still another 5 roots to $T^{11} - 1$ in $\ell = \mathbb{F}_{3^5}$ to account for.

Well, the roots of $T^{11} - 1$ in ℓ are precisely the elements of the multiplicative subgroup $\langle a \rangle$.

So what we really need is a good description of the roots of f .

So we need to describe the set of exponents $1, 3, 3^2, 3^3, 3^4$ modulo 11.

```
S1 = [ mod(3^i,11) for i in range(5) ]
S1
=>
[1, 3, 9, 5, 4]
```

This shows that the roots of f are exactly a^i for i in $S1 = [1, 3, 9, 5, 4]$

The set $S1$ is called a *cyclotomic coset*.

Note that a^2 is a root of $T^{11} - 1$ but is not a root of f . So we need to consider the cyclotomic coset $S2$ containing 2, namely:

```
S2 = [ mod(2*3^i,11) for i in range(5) ]
S2
=>
[2, 6, 7, 10, 8]
```

This shows that the minimal polynomial a^2 has roots a^j for j in $S2$.

```
h = product([T - a^j for j in S2])
h
=>
T^5 + 2*T^3 + T^2 + 2*T + 2
```

Again, this polynomial has coefficients in \mathbb{F}_3 .

Together, $S1$ and $S2$ account for all numbers $[1 \dots 10]$, and it follows that $(T - 1) \cdot g \cdot h = T^{11} - 1$.

We can check this via Sage:

```
(T-1)*g*h == T^11 -1
=>
True
```

To compute the *minimal distance* of the codes $C_1 = \langle g \rangle$ and $C_2 = \langle h \rangle$, we can use the following code in Sage to construct the codes as vector subspaces of \mathbb{F}_3^{11} .

We construct the codes by vectorizing the bases

$$\{T^i g \mid 0 \leq i \leq 5\} \quad \text{and} \quad \{T^i h \mid 0 \leq i \leq 5\}$$

```

V = VectorSpace(k,11)
#S = V.subspace([ (T^i * g).coefficients(sparse=False) for i in range(5) ])

def pad(ll,n):
    # pad the list ll with 0's to make it have length n
    x = len(ll)
    if x < n:
        return ll + (n-x)*[0]
    else:
        return ll[0:n]

def vectorize(p,n):
    # make a vector of length n out of a polynomial
    coeffs = p.coefficients(sparse=False)
    return V(pad(coeffs,n))

def mkCode(p):
    # vectorize the polynomial T^i * p and use the vectors as a basis for the code C
    # I'm assuming deg p = 5...
    return V.subspace([ vectorize( T^i * p, 11) for i in range(6) ])

C1 = mkCode(gg)
C2 = mkCode(hh)

C1
=>
Vector space of degree 11 and dimension 6 over Finite Field of size 3
Basis matrix:
[1 0 0 0 0 0 2 0 1 2 1]
[0 1 0 0 0 0 1 2 2 2 1]
[0 0 1 0 0 0 1 1 1 0 1]
[0 0 0 1 0 0 1 1 0 2 2]
[0 0 0 0 1 0 2 1 2 2 0]
[0 0 0 0 0 1 0 2 1 2 2]

C2
=>
Vector space of degree 11 and dimension 6 over Finite Field of size 3
Basis matrix:
[1 0 0 0 0 0 2 2 1 2 0]
[0 1 0 0 0 0 0 2 2 1 2]
[0 0 1 0 0 0 2 2 0 1 1]
[0 0 0 1 0 0 1 0 1 1 1]
[0 0 0 0 1 0 1 2 2 2 1]
[0 0 0 0 0 1 1 2 1 0 2]

```

Now we can just compute the minimal distance of each code using a *brute force* computation:

```

def weight(v):
    r = [x for x in v if x != 0]
    return len(r)

def min_distance(D):
    # brute-force computation of minimal distance of D
    return min([ weight(v) for v in D if v != 0])

```

```
[min_distance(C) for C in [C1,C2]]
=>
[5, 5]
```

Thus we see that each of C_1 and C_2 is a $[11, 6, 5]_3$ -code.

We are going to explain why C is a *perfect* code. Recall that *perfect* means that C meets the *sphere-packing bound*.

Recall that

$$\delta(m) = \sum_{i=0}^m \binom{n}{i} (q-1)^i$$

The sphere-packing bound says that a $[n, k, d]_q$ code satisfies

$$|C| \cdot \delta(t) \leq q^n$$

where $t = \lfloor (d-1)/2 \rfloor$.

so that C is a perfect code provided that

$$|C| \cdot \delta(t) = q^n.$$

```
def delta(n,q,m):
    return sum([ binomial(n,i)*(q-1)^i for i in range(m+1) ])

t = floor((5-1)/2)

delta(11,3,t).factor()
=>
3^5
```

Finally, we can check that the codes defined by g and by h are perfect

```
3^6 * delta(11,3,t) == 3^11
=>
True
```

The main unsatisfying part of the above account is that we found the minimal distance of the codes via a brute force computation (we just made a list of the weights of the non-zero vector, and found the minimum of this list).

A nicer approach to finding the minimal distance is as follows.

Let G be the generator matrix for (say) C_1 whose rows correspond to the polynomial $T^i g$ for $i = 0, 1, \dots, 5$.

```
G = MatrixSpace(k,6,11).matrix([ vectorize( T^i * g, 11) for i in range(6) ])
G
=>
[2 0 1 2 1 1 0 0 0 0 0]
[0 2 0 1 2 1 1 0 0 0 0]
[0 0 2 0 1 2 1 1 0 0 0]
[0 0 0 2 0 1 2 1 1 0 0]
[0 0 0 0 2 0 1 2 1 1 0]
[0 0 0 0 0 2 0 1 2 1 1]
```

Adding a column of 1's to G determines a $[12, 6]_3$ code which we can check to be *self-dual*:

```
GG = MatrixSpace(k,6,12).matrix([ list(row) + [1] for row in G ])
GG
=>
[2 0 1 2 1 1 0 0 0 0 0 1]
[0 2 0 1 2 1 1 0 0 0 0 1]
```

```
[0 0 2 0 1 2 1 1 0 0 0 1]
[0 0 0 2 0 1 2 1 1 0 0 1]
[0 0 0 0 2 0 1 2 1 1 0 1]
[0 0 0 0 0 2 0 1 2 1 1 1]
```

```
GG * GG.T
=>
[0 0 0 0 0 0]
[0 0 0 0 0 0]
[0 0 0 0 0 0]
[0 0 0 0 0 0]
[0 0 0 0 0 0]
[0 0 0 0 0 0]
```

If CC denotes the code with generator matrix GG , then the computation $GG * GG.T$ shows that CC is contained in the dual code CC^{\perp} ; since the dimension of CC^{\perp} is $12-6 = 6$, we conclude $CC = CC^{\perp}$.

Now we have

Lemma If C is a self-dual code of length n over the field \mathbb{F}_3 , then the weight of any codeword is a multiple of 3.

Proof We first note that 1 is the only non-zero square in \mathbb{F}_3 , since $1^2 = 2^2 = 1$.

Let $\mathbf{v} = (v_1, \dots, v_n) \in V$ and let $J = \{j \mid v_j \neq 0\}$.

Then $\text{weight}(\mathbf{v}) = |J|$.

Since C is self-dual we have in particular

$$\langle \mathbf{v}, \mathbf{v} \rangle = 0.$$

Now on the other hand

$$\langle \mathbf{v}, \mathbf{v} \rangle = \sum_{j \in J} (v_j)^2 = \sum_{j \in J} 1 = |J| \pmod{3}.$$

Thus we indeed find that $\text{weight}(\mathbf{v}) = |J| \equiv 0 \pmod{3}$.

Now, looking at the generator matrix, CC evidently contains codewords of weight 6, e.g.

```
( GG[5], weight(GG[5]))
=>
([0 0 0 0 0 2 0 1 2 1 1 1], 6)
```

We claim that CC has minimal distance 6. According to the Lemma it will suffice to show that CC has no codewords of weight 3.

Once we establish this fact, then the minimal weight of a codeword in C must be 5.

Bibliography