# Information and Coding Theory MA41024/ MA60020/ MA60262 

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

> Lecture 18
> March 27,2023

## Cyclic codes <br> Question Does the reverse shifting give a cyclic code?

## Cyclic codes

Question Does the reverse shifting give a cyclic code?
The reverse code $C^{[-1]}$ of a cyclic code $C$, reversing each codeword, is still cyclic:

$$
\left(c_{0}, \ldots, c_{i}, \ldots, c_{n-1}\right) \in C \longleftrightarrow\left(c_{n-1}, \ldots, c_{n-1-i}, \ldots, c_{1}, c_{0}\right) \in C^{[-1]}
$$

## Cyclic codes

Question Does the reverse shifting give a cyclic code?
The reverse code $C^{[-1]}$ of a cyclic code $C$, reversing each codeword, is still cyclic:

$$
\left(c_{0}, \ldots, c_{i}, \ldots, c_{n-1}\right) \in C \longleftrightarrow\left(c_{n-1}, \ldots, c_{n-1-i}, \ldots, c_{1}, c_{0}\right) \in C^{[-1]}
$$

In polynomial notation, this becomes

$$
c(x) \in C \longleftrightarrow x^{n-1} c\left(x^{-1}\right) \in C^{[-1]}
$$

## Cyclic codes

Question Does the reverse shifting give a cyclic code?
The reverse code $C^{[-1]}$ of a cyclic code $C$, reversing each codeword, is still cyclic:

$$
\left(c_{0}, \ldots, c_{i}, \ldots, c_{n-1}\right) \in C \longleftrightarrow\left(c_{n-1}, \ldots, c_{n-1-i}, \ldots, c_{1}, c_{0}\right) \in C^{[-1]}
$$

In polynomial notation, this becomes

$$
c(x) \in C \longleftrightarrow x^{n-1} c\left(x^{-1}\right) \in C^{[-1]}
$$

Reciprocal polynomial For a polynomial $p(x)$ of degree $d$, the reciprocal of $p(x)$ is given by

$$
p^{[-1]}(x)=\sum_{i=0}^{d} p_{d-i} x^{i}=x^{d} p\left(x^{-1}\right)
$$

## Cyclic codes

Proposition If $g(x)$ generates a cyclic code $C$ then $g_{0}^{-1} g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of $G$

## Cyclic codes

Proposition If $g(x)$ generates a cyclic code $C$ then $g_{0}^{-1} g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of $G$

## Observation

$\rightarrow$ Let $C$ be a cyclic code of length $n$ with generator polynomial $g(x)$ of degree $r$ and check polynomial $h(x)$ of degree $k=n-r=\operatorname{dim}(C)$.

## Cyclic codes

Proposition If $g(x)$ generates a cyclic code $C$ then $g_{0}^{-1} g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of $G$

## Observation

$\rightarrow$ Let $C$ be a cyclic code of length $n$ with generator polynomial $g(x)$ of degree $r$ and check polynomial $h(x)$ of degree $k=n-r=\operatorname{dim}(C)$.
$\rightarrow$ Since $h(x)$ is a divisor of $x^{n}-1$, it is a generator polynomial for a cyclic code $D$ of length $n$ and dimension $n-k=n-(n-r)=r$

## Cyclic codes

Proposition If $g(x)$ generates a cyclic code $C$ then $g_{0}^{-1} g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of $G$

## Observation

$\rightarrow$ Let $C$ be a cyclic code of length $n$ with generator polynomial $g(x)$ of degree $r$ and check polynomial $h(x)$ of degree $k=n-r=\operatorname{dim}(C)$.
$\rightarrow$ Since $h(x)$ is a divisor of $x^{n}-1$, it is a generator polynomial for a cyclic code $D$ of length $n$ and dimension $n-k=n-(n-r)=r$
$\rightarrow$ We have

$$
C=\left\{q(x) g(x) \mid q(x) \in F[x]_{k}\right\}, \quad D=\left\{p(x) h(x) \mid p(x) \in F[x]_{r}\right\}
$$

## Cyclic codes

Let $c(x)=q(x) g(x) \in C$ so that $\operatorname{deg}(q(x)) \leq k-1$, and let $d(x)=p(x) h(x) \in D$, so that $\operatorname{deg}(p(x)) \leq r-1$.

## Cyclic codes

Let $c(x)=q(x) g(x) \in C$ so that $\operatorname{deg}(q(x)) \leq k-1$, and let $d(x)=p(x) h(x) \in D$, so that $\operatorname{deg}(p(x)) \leq r-1$.

Then

$$
\begin{aligned}
c(x) d(x) & =q(x) g(x) p(x) h(x)=q(x) p(x)\left(x^{n}-1\right)=s(x)\left(x^{n}-1\right) \\
& =s(x) x^{n}-s(x)
\end{aligned}
$$

where $s(x)=q(x) p(x)$ with

$$
\operatorname{deg}(s(x)) \leq(k-1)+(r-1)=r+k-2=n-2<n-1 .
$$

## Cyclic codes

Let $c(x)=q(x) g(x) \in C$ so that $\operatorname{deg}(q(x)) \leq k-1$, and let $d(x)=p(x) h(x) \in D$, so that $\operatorname{deg}(p(x)) \leq r-1$.

Then

$$
\begin{aligned}
c(x) d(x) & =q(x) g(x) p(x) h(x)=q(x) p(x)\left(x^{n}-1\right)=s(x)\left(x^{n}-1\right) \\
& =s(x) x^{n}-s(x)
\end{aligned}
$$

where $s(x)=q(x) p(x)$ with

$$
\operatorname{deg}(s(x)) \leq(k-1)+(r-1)=r+k-2=n-2<n-1 .
$$

Therefore, the coefficient of $x^{n-1}$ in $c(x) d(x)$ is 0 .

## Cyclic codes

If $c(x)=\sum_{i=0}^{n-1} c_{i} x^{i}$ and $d(x)=\sum_{j=0}^{n-1} d_{j} x^{j}$ then in general the coefficient of $x^{m}$ in $c(x) d(x)$ is $\sum_{i+j=m} c_{i} d_{j}$

## Cyclic codes

If $c(x)=\sum_{i=0}^{n-1} c_{i} x^{i}$ and $d(x)=\sum_{j=0}^{n-1} d_{j} x^{j}$ then in general the coefficient of $x^{m}$ in $c(x) d(x)$ is $\sum_{i+j=m} c_{i} d_{j}$
In particular, the coefficients corresponding to $x^{n-1}$ in $c(x) d(x)$ gives us

$$
\begin{aligned}
0 & =\sum_{i+j=n-1} c_{i} d_{j}=\sum_{i=0}^{n} c_{i} d_{n-1-i} \\
& =c_{0} d_{n-1}+c_{1} d_{n-2}+\ldots+c_{i} d_{n-i}+\ldots+c_{n-1} d_{0} \\
& =\mathbf{c} \cdot \mathbf{d}^{*}
\end{aligned}
$$

where

$$
\mathbf{c}=\left(c_{0}, c_{1}, \ldots, c_{i}, \ldots, c_{n-1}\right), \mathbf{d}^{*}=\left(d_{n-1}, d_{n-2}, \ldots, d_{n-i}, \ldots, d_{0}\right)
$$

## Cyclic codes

If $c(x)=\sum_{i=0}^{n-1} c_{i} x^{i}$ and $d(x)=\sum_{j=0}^{n-1} d_{j} x^{j}$ then in general the coefficient of $x^{m}$ in $c(x) d(x)$ is $\sum_{i+j=m} c_{i} d_{j}$

In particular, the coefficients corresponding to $x^{n-1}$ in $c(x) d(x)$ gives us

$$
\begin{aligned}
0 & =\sum_{i+j=n-1} c_{i} d_{j}=\sum_{i=0}^{n} c_{i} d_{n-1-i} \\
& =c_{0} d_{n-1}+c_{1} d_{n-2}+\ldots+c_{i} d_{n-i}+\ldots+c_{n-1} d_{0} \\
& =\mathbf{c} \cdot \mathbf{d}^{*}
\end{aligned}
$$

where

$$
\mathbf{c}=\left(c_{0}, c_{1}, \ldots, c_{i}, \ldots, c_{n-1}\right), \mathbf{d}^{*}=\left(d_{n-1}, d_{n-2}, \ldots, d_{n-i}, \ldots, d_{0}\right)
$$

Thus each codeword $\mathbf{c}$ in $C$ has dot product 0 with the reverse of each codeword d of $D$, which further implies $C^{\perp} \subseteq D^{[-1]}$.

## Cyclic codes

If $c(x)=\sum_{i=0}^{n-1} c_{i} x^{i}$ and $d(x)=\sum_{j=0}^{n-1} d_{j} x^{j}$ then in general the coefficient of $x^{m}$ in $c(x) d(x)$ is $\sum_{i+j=m} c_{i} d_{j}$
In particular, the coefficients corresponding to $x^{n-1}$ in $c(x) d(x)$ gives us

$$
\begin{aligned}
0 & =\sum_{i+j=n-1} c_{i} d_{j}=\sum_{i=0}^{n} c_{i} d_{n-1-i} \\
& =c_{0} d_{n-1}+c_{1} d_{n-2}+\ldots+c_{i} d_{n-i}+\ldots+c_{n-1} d_{0} \\
& =\mathbf{c} \cdot \mathbf{d}^{*}
\end{aligned}
$$

where

$$
\mathbf{c}=\left(c_{0}, c_{1}, \ldots, c_{i}, \ldots, c_{n-1}\right), \mathbf{d}^{*}=\left(d_{n-1}, d_{n-2}, \ldots, d_{n-i}, \ldots, d_{0}\right)
$$

Thus each codeword $\mathbf{c}$ in $C$ has dot product 0 with the reverse of each codeword d of $D$, which further implies $C^{\perp} \subseteq D^{[-1]}$. Also

$$
\operatorname{dim}\left(C^{\perp}\right)=n-\operatorname{dim}(C)=n-k=r=n-\operatorname{deg}\left(h^{[-1]}(x)\right)=\operatorname{dim}\left(D^{[-1]}\right)
$$

## Cyclic codes

Conclusion If $C$ is the cyclic code of length $n$ with check polynomial $h(x)$, then $C^{\perp}$ is cyclic with generator polynomial $h_{0}^{-1} h^{[-1]}(x)$

## Cyclic codes

Conclusion If $C$ is the cyclic code of length $n$ with check polynomial $h(x)$, then $C^{\perp}$ is cyclic with generator polynomial $h_{0}^{-1} h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let $C$ be a cyclic code. Then there is a unique codeword $c(x)$ which is an identity element for $C$

## Cyclic codes

Conclusion If $C$ is the cyclic code of length $n$ with check polynomial $h(x)$, then $C^{\perp}$ is cyclic with generator polynomial $h_{0}^{-1} h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let $C$ be a cyclic code. Then there is a unique codeword $c(x)$ which is an identity element for $C$
Proof
Let $g(x)$ be the generator polynomial of $C$, and $h(x)$ the check polynomial i.e. $g(x) h(x)=x^{n}-1$

## Cyclic codes

Conclusion If $C$ is the cyclic code of length $n$ with check polynomial $h(x)$, then $C^{\perp}$ is cyclic with generator polynomial $h_{0}^{-1} h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let $C$ be a cyclic code. Then there is a unique codeword $c(x)$ which is an identity element for $C$
Proof
Let $g(x)$ be the generator polynomial of $C$, and $h(x)$ the check polynomial i.e. $g(x) h(x)=x^{n}-1$
Since $x^{n}-1$ has no multiple zeros, we have $\operatorname{gcd}(g(x), h(x))=1$ and hence there exist polynomials $a(x)$ and $b(x)$ such that

$$
a(x) g(x)+b(x) h(x)=1
$$

## Cyclic codes

Conclusion If $C$ is the cyclic code of length $n$ with check polynomial $h(x)$, then $C^{\perp}$ is cyclic with generator polynomial $h_{0}^{-1} h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let $C$ be a cyclic code. Then there is a unique codeword $c(x)$ which is an identity element for $C$
Proof
Let $g(x)$ be the generator polynomial of $C$, and $h(x)$ the check polynomial i.e. $g(x) h(x)=x^{n}-1$
Since $x^{n}-1$ has no multiple zeros, we have $\operatorname{gcd}(g(x), h(x))=1$ and hence there exist polynomials $a(x)$ and $b(x)$ such that

$$
a(x) g(x)+b(x) h(x)=1
$$

Define $c(x)=a(x) g(x)=1-b(x) h(x)$, which is a codeword in $C$

## Cyclic codes

If $p(x) g(x)$ is any codeword in $C$ then

$$
\begin{aligned}
c(x) p(x) g(x) & =p(x) g(x)-b(x) h(x) p(x) g(x) \\
& =p(x) g(x) \bmod \left(x^{n}-1\right)
\end{aligned}
$$

## Cyclic codes

If $p(x) g(x)$ is any codeword in $C$ then

$$
\begin{aligned}
c(x) p(x) g(x) & =p(x) g(x)-b(x) h(x) p(x) g(x) \\
& =p(x) g(x) \bmod \left(x^{n}-1\right)
\end{aligned}
$$

So $c(x)$ is an identity element for $C$, and hence it is unique

## Cyclic codes

If $p(x) g(x)$ is any codeword in $C$ then

$$
\begin{aligned}
c(x) p(x) g(x) & =p(x) g(x)-b(x) h(x) p(x) g(x) \\
& =p(x) g(x) \bmod \left(x^{n}-1\right)
\end{aligned}
$$

So $c(x)$ is an identity element for $C$, and hence it is unique Since $c^{2}(x)=c(x)$, this codeword is called the idempotent. Since every codeword $v(x)$ can be written as $v(x) c(x)$, i.e. as a multiple of $c(x)$, we see that $c(x)$ generates the ideal $C$

## Cyclic codes

Maximal and minimal cyclic code Let $x^{n}-1=f_{1}(x) f_{2}(x) \ldots f_{t}(x)$ be the decomposition of $x^{n}-1$ into irreducible factors.

The cyclic code generated by $f_{i}(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by $M_{i}^{+}$

## Cyclic codes

Maximal and minimal cyclic code Let $x^{n}-1=f_{1}(x) f_{2}(x) \ldots f_{t}(x)$ be the decomposition of $x^{n}-1$ into irreducible factors.

The cyclic code generated by $f_{i}(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by $M_{i}^{+}$
The code generated by $\left(x^{n}-1\right) / f_{i}(x)$ is called the minimal cyclic code, denoted by $M_{i}^{-}$

## Cyclic codes

Maximal and minimal cyclic code Let $x^{n}-1=f_{1}(x) f_{2}(x) \ldots f_{t}(x)$ be the decomposition of $x^{n}-1$ into irreducible factors.

The cyclic code generated by $f_{i}(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by $M_{i}^{+}$
The code generated by $\left(x^{n}-1\right) / f_{i}(x)$ is called the minimal cyclic code, denoted by $M_{i}^{-}$
Observation(Homework)
$\rightarrow$ Let $g(x)=\left(x^{n}-1\right) / f_{i}(x)$, where $\operatorname{deg}\left(f_{i}(x)\right)=k$ be a generator of the minimal code $M_{i}^{-}$
$\rightarrow$ If $a(x)$ and $b(x)$ are two codewords in $M_{i}^{-}$such that $a(x) b(x)=0$, then one of them must be divisible by $f_{i}(x)$ and it is therefore 0

## Cyclic codes

Maximal and minimal cyclic code Let $x^{n}-1=f_{1}(x) f_{2}(x) \ldots f_{t}(x)$ be the decomposition of $x^{n}-1$ into irreducible factors.

The cyclic code generated by $f_{i}(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by $M_{i}^{+}$
The code generated by $\left(x^{n}-1\right) / f_{i}(x)$ is called the minimal cyclic code, denoted by $M_{i}^{-}$
Observation(Homework)
$\rightarrow$ Let $g(x)=\left(x^{n}-1\right) / f_{i}(x)$, where $\operatorname{deg}\left(f_{i}(x)\right)=k$ be a generator of the minimal code $M_{i}^{-}$
$\rightarrow$ If $a(x)$ and $b(x)$ are two codewords in $M_{i}^{-}$such that $a(x) b(x)=0$, then one of them must be divisible by $f_{i}(x)$ and it is therefore 0
$\rightarrow$ Since $M_{i}^{-}$has no zero divisors, it is a field

