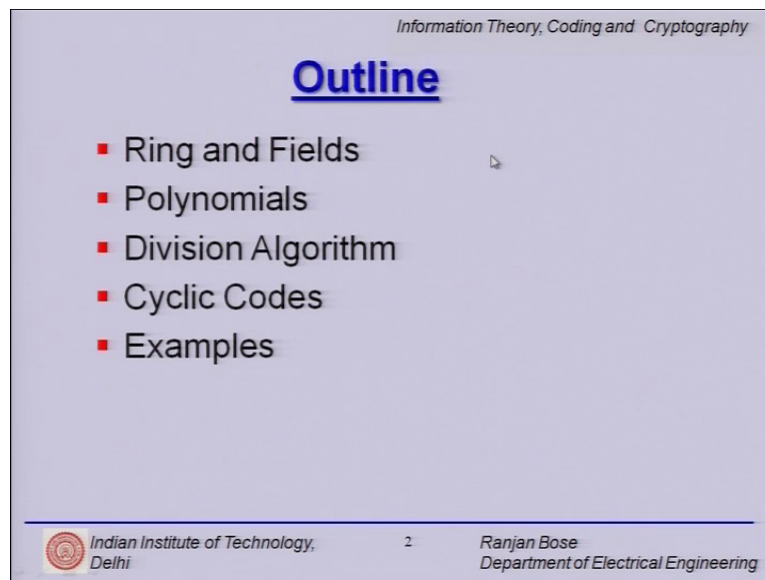


Information Theory, Coding and Cryptography
Dr. Ranjan Bose
Department of Electrical Engineering
Indian Institute of Technology, Delhi

Module - 20
Cyclic Codes
Lecture - 20

Hello, and welcome to our next lecture on Cyclic Codes.

(Refer Slide Time: 00:32)



The slide is titled "Information Theory, Coding and Cryptography" at the top right. The main title "Outline" is centered and underlined in blue. Below it is a bulleted list of topics: Ring and Fields, Polynomials, Division Algorithm, Cyclic Codes, and Examples. At the bottom, there is a footer with the IIT Delhi logo on the left, the number "2" in the center, and the name "Ranjan Bose" and "Department of Electrical Engineering" on the right.

Information Theory, Coding and Cryptography

Outline

- Ring and Fields
- Polynomials
- Division Algorithm
- Cyclic Codes
- Examples

Indian Institute of Technology, Delhi 2 Ranjan Bose
Department of Electrical Engineering

Let us look at a brief outline of today's talk. We would consider what is a ring and how they are related to fields, then we will look into polynomials and use them as building blocks for our cyclic codes. We will look at the division algorithm and then using these mathematical tools we would introduce the concept of cyclic codes. Finally, we will have some examples.

(Refer Slide Time: 00:59)

Information Theory, Coding and Cryptography

Recap

- Linear Block Codes
- Hamming Code
- LDPC Codes
- MDS Code
- Probability of Errors

Indian Institute of Technology, Delhi 3 Ranjan Bose
Department of Electrical Engineering

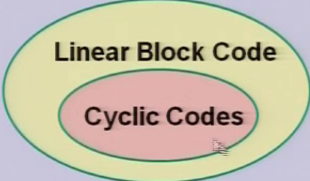
Let us look at a quick recap as to what we have done already. We have spent quite some time looking at linear block codes, we figured out why they work. We looked at some specific examples of Hamming code, the LDPC codes, MDS codes, and finally we looked at the probability of residual errors.

(Refer Slide Time: 01:23)

Information Theory, Coding and Cryptography

Cyclic Codes

- A code C is **cyclic** if
 - C is a linear code, and,
 - any **cyclic shift** of a codeword is also a codeword, i.e., if the codeword $a_0a_1\dots a_{n-1}$ is in C then $a_{n-1}a_0\dots a_{n-2}$ is also in C .



Indian Institute of Technology, Delhi 4 Ranjan Bose
Department of Electrical Engineering

Having said that we now move on to this new subclass of codes called cyclic codes. Now, let us define it first. So, code C is cyclic, if number one – C is a linear code. So, we are now looking at a subclass of linear block codes. Whatever theory we have learned so

far is applicable to cyclic codes because C is itself a linear block code, but what is more is that any cyclic shift of a codeword is also a valid codeword, all right. So, if a 0 a 1 a 2 up to a n minus 1 is a codeword contained in a cyclic code C , then if you put a n minus 1 in the beginning and then shift each one of them by 1 1 1 you would end up getting another codeword which is also valid. So, any cyclic shift is also a valid codeword, hence the name cyclic codes.

So, clearly the first bullet tells us that if you take this linear block code then cyclic codes are necessary a subset of linear block codes. So, all the techniques that we have learned so far are applicable to cyclic codes, but as we will see cyclic codes have tremendous error correcting capabilities in terms of burst error corrections also they are very hardware friendly.

So, these cyclic codes are a much more powerful class of linear block codes.

(Refer Slide Time: 02:59)

Information Theory, Coding and Cryptography

Example

- The binary code $C_1 = \{0000, 0101, 1010, 1111\}$ is a cyclic code.
- However $C_2 = \{0000, 0110, 1001, 1111\}$ is not a cyclic code, but is *equivalent* to the first code.
- Interchanging the third and the fourth components of C_2 yields C_1 .

Indian Institute of Technology,
Delhi

5

Ranjan Bose
Department of Electrical Engineering

So, let us look at a quick example, let us look at a binary code there are four codewords in this code 0000, 0101, 1010 and 1111. The first step is to verify whether it is a linear block code and then we will look at the cyclic shifts. So, if you see the all 0 codeword is contained the sum of any two codewords gives a valid codeword and therefore, we can say definitely this is a linear block code.

Now, we do the third check whether if you do a cyclic shift if you put the 0 1 this 1 here and the 0 here, you get this one and then any cyclic shift will give you back this one leads onto itself and so on and so forth. So, any of the four code words undergoing any number of cyclic shifts ends up being another valid code. So therefore, this is definitely a cyclic code, but if you look at a slightly different example where it is an equivalent code, but it is definitely not cyclic.

So, because the cyclic shift of this does not yield another valid codeword and therefore, you can verify that this is maybe a linear block code, but it is not a cyclic code and these two codes are equivalent in terms of the distance properties both of them have a minimum distance of 2.

(Refer Slide Time: 04:27)

Information Theory, Coding and Cryptography

Polynomials

- A **polynomial** is a mathematical expression

$$f(x) = f_0 + f_1x + \dots + f_mx^m,$$
 where the symbol x is called the indeterminate and the coefficients f_0, f_1, \dots, f_m are the elements of $GF(q)$.
- The coefficient f_m is called the leading coefficient.
- If $f_m \neq 0$, then m is called the **degree** of the polynomial, and is denoted by $\deg f(x)$.
- A polynomial is called **monic** if its leading coefficient is unity.
- **Example:** $f(x) = 3 + 7x + x^3 + 5x^4 + x^6$ is a monic polynomial over $GF(8)$.
- The degree of this polynomial is 6.

Indian Institute of Technology,
Delhi

6

Ranjan Bose
Department of Electrical Engineering

So, let us now foray into the world of polynomials which have a very strong linkage to cyclic codes. So, we are going to take a mathematical detour for the next few slides build up some mathematical tools and then use it for describing cyclic codes much more efficiently. So, let us look at a polynomial most of us already know this, but just for the sake of clarity f of x can be written as f_0 plus f_1x plus so and so forth up to f_mx^m and f_0, f_1 are the coefficients and the highest order will be the degree of the polynomial.

So, please note, if I define this polynomial over $GF(q)$; that means, the coefficients here are taken from $GF(q)$ they are the elements of $GF(q)$ and we already know Galois field with q elements we know the properties. So, this also means that if I can add subtract

multiply divide two polynomials because the coefficients get added subtracted multiplied hence and so and so forth. Therefore, I will follow the arithmetic of GF q to do those things. As I said f m is the leading coefficient here for the highest degree and m is the degree of the polynomial and it is often denoted by $\deg f$ of x .

Now, a polynomial is called monic if its leading coefficient is unity. So, f of m if it is 1 then this also becomes a monic polynomial. Please note in polynomials which are binary you do not have to worry about it because it is either a one or a 0 and 0 means it does not that term does not exist, but for a general case GF q you will need to have f m equal to one for a monic otherwise for example, GF 4 this f m can be either a 1, 2 or 3, but for monic it needs to be 1, the highest coefficient.

So, let us look at an example here a polynomial over GF 8. So, the valid coefficients could be 0 1 2 3 up to 7 and GF 8 is 2 raised power 3 is 8. So, it is a prime power and hence GF 8 exists if you look at this polynomial the highest power is x raised power 6 and the leading coefficient is 1, hence it is a monic polynomial the degree of this polynomial clearly is 6.

(Refer Slide Time: 07:12)

Information Theory, Coding and Cryptography

Polynomials

- Polynomials will play an important role in the study of cyclic codes, the subject of this chapter.
- Let $F[x]$ be the set of polynomials in x with coefficients in $GF(q)$.
- Different polynomials in $F[x]$ can be **added, subtracted and multiplied** in the usual manner.
- $F[x]$ is an example of an algebraic structure called a **ring**.
- $F[x]$ is **not a field** because polynomials of degree greater than zero do not have a multiplicative inverse.

Indian Institute of Technology, Delhi 7 Ranjan Bose Department of Electrical Engineering

Now, polynomials do play a very important role in the study of cyclic codes as we will see now if you say F of x be a set of polynomials. So, suddenly we are talking about a set of polynomials in x with coefficients in GF q . So, x is that indeterminate right and F capital F of x is the set of polynomials. Now, clearly this set of polynomials is a

collection and the polynomials in this set can be added subtracted or multiplied in the usual manner and the arithmetic will be carried over GF q.

So, $F[x]$ is an example of an algebraic structure called a ring. We will soon see; what are the properties of a ring and whether it is a field or not is what we will have to verify and check under what condition this collection becomes a field.

(Refer Slide Time: 08:13)

Information Theory, Coding and Cryptography

Polynomials

- It can be seen that if $f(x), g(x) \in F[x]$, then $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.
- However, $\deg(f(x) + g(x))$ is not necessarily $\max\{\deg f(x), \deg g(x)\}$.
- For example, consider the two polynomials, $f(x)$ and $g(x)$, over $GF(2)$ such that $f(x) = 1 + x^2$ and $g(x) = 1 + x + x^2$.
- Then, $\deg(f(x) + g(x)) = \deg(x) = 1$.
- This is because, in $GF(2)$, $1 + 1 = 0$, and $x^2 + x^2 = (1 + 1)x^2 = 0$.

Indian Institute of Technology, Delhi

8

Ranjan Bose
Department of Electrical Engineering

So, look at some properties of the polynomials some of them we know and we use them without even realizing then if you see $f(x)$ and $g(x)$ are two polynomials contained in this set of polynomials $F[x]$ then degree of the product is a sum of the degrees we know all of this. But, please note that degree of $f(x)$ and $g(x)$ when you add them up is not necessarily the maximum of degree of $f(x)$ and degree of $g(x)$ for a simple reason that if both of them are monic, then they will cancel each other out possibly.


So, if you see $1 + x^2$ is my polynomial $f(x)$ and $g(x)$ is $1 + x + x^2$ and if you add them up look the degree has actually gone down. So, this is what we know, because if you do binary arithmetic GF 2 then $1 + 1 = 0$ and $x^2 + x^2$ cancels out. And therefore, the highest power of x is 1.

(Refer Slide Time: 09:18)

Information Theory, Coding and Cryptography

Example

- Consider the polynomial $f(x) = 1 + x$ over $GF(2)$.
 $(f(x))^2 = 1 + (1+1)x + x^2 = 1 + x^2$
- Again consider $f(x) = 1 + x$ over $GF(3)$.
 $(f(x))^2 = 1 + (1+1)x + x^2 = 1 + 2x + x^2$

 Indian Institute of Technology,
Delhi

9

Ranjan Bose
Department of Electrical Engineering

Let us look at another example these are basically refreshing our memory we know most of these stuff consider a simple polynomial f of x $1 + x$ and defined over $GF(2)$.

So, all the arithmetic that we do will be over $GF(2)$. So, we can square it how does it look. So, $f(x)$ square is you take this and multiply it over and $1 + 1$ gives 0 and therefore, $1 + x + x + x^2$ is nothing but $1 + x^2$, but just consider $1 + x$ as the polynomial over $GF(3)$. So, I am now going to square this, but not over $GF(2)$, but $GF(3)$. Now, $GF(3)$ can have coefficients $0, 1$ and 2 my polynomial happens to have just one coefficient as 1 . So, I would like to square it. So, $1 + x + x + x^2$ is what you get by squaring it, simple multiplication by itself and now you end up with $1 + 1 + 2x + x^2$ and if you look at the table $GF(3)$ which is also modular 3 arithmetic because 3 is a prime number I get $1 + 2x + x^2$.


So, same polynomial squared over $GF(2)$ and $GF(3)$ gave different results. So, this is important to observe that the field is important.

(Refer Slide Time: 10:48)

Information Theory, Coding and Cryptography

Addition and Multiplication

- Consider the polynomials
 $f(x) = 2 + x + x^2 + 2x^4$ and $g(x) = 1 + 2x^2 + 2x^4 + x^5$ over $GF(3)$.
- Then,
 $f(x) + g(x) = (2+1) + x + (1+2)x^2 + (2+2)x^4 + x^5 = x + x^4 + x^5$.
 $f(x) \cdot g(x) = (2 + x + x^2 + 2x^4)(1 + 2x^2 + 2x^4 + x^5)$
 $= 2 + x + (1+2 \cdot 2)x^2 + 2x^3 + (2+2+2 \cdot 2)x^4 + (2+2)x^5$
 $+ (1+2+1)x^6 + x^7 + 2 \cdot 2x^8 + 2x^9$
 $= 2 + x + (1+1)x^2 + 2x^3 + (2+2+1)x^4 + (2+2)x^5 + (1+2+1)x^6 +$
 $x^7 + x^8 + 2x^9$
 $= 2 + x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6 + x^7 + x^8 + 2x^9$
- Note that the addition and multiplication of the coefficients have been carried out over $GF(3)$.

 Indian Institute of Technology,
Delhi
10
Ranjan Bose
Department of Electrical Engineering

Now, let us quickly go over this addition and multiplication. So, you can take two examples it is best to show by examples I have got $f(x)$ and $g(x)$ over $GF(3)$. So, please note the coefficients are from 0, 1 and 2. So, $g(x)$ and $f(x)$ and their degrees are also different, but I can always add these two polynomials and we can do it like this explicitly. So, this is a coefficient of x raised power 0, I add them up and then I add the coefficients of x , there is a missing x here, there is an x here only x and so and so forth and you get an answer like this.

Similarly, I can multiply them it is a long multiplication and I carry it out and again use the arithmetic for the $GF(3)$ table and if I do this I can simply get an answer as a product and product highest power is 5 highest power is 4 and it is no surprise that the product has the highest power x raised power 9. So, the degrees have added, ok. So, this is a simple example that you can carry out addition and multiplication, but each time I do the sum or the product I take care of the table belonging to the correct Galois field.


(Refer Slide Time: 12:10)

Information Theory, Coding and Cryptography

The field is important !

- Consider the polynomial $f(x) = 1 + x$ over $GF(2)$.
 $(f(x))^2 = 1 + (1+1)x + x^2 = 1 + x^2$
- Again consider $f(x) = 1 + x$ over $GF(3)$.
 $(f(x))^2 = 1 + (1+1)x + x^2 = 1 + 2x + x^2$

The field is important !!!

 Indian Institute of Technology, Delhi 11 Ranjan Bose
Department of Electrical Engineering


So, we have already established that field is important and if you square over GF 2 and GF 3 the same example, but we are trying to emphasize that the same operation over different fields will give a different answer. So, field is indeed very important.

(Refer Slide Time: 12:31)

Information Theory, Coding and Cryptography

Division Algorithm

- The **division algorithm** states that, for every pair of polynomial $a(x)$ and $b(x) \neq 0$ in $F[x]$, there exists a unique pair of polynomials $q(x)$, the quotient, and $r(x)$, the remainder, such that $a(x) = q(x) b(x) + r(x)$, where $\deg r(x) < \deg b(x)$.
- The remainder is sometimes also called the **residue**, and is denoted by $R_{b(x)}[a(x)] = r(x)$.
- **Two important properties of residues are**
- $R_{f(x)}[a(x) + b(x)] = R_{f(x)}[a(x)] + R_{f(x)}[b(x)]$, and
- $R_{f(x)}[a(x) \cdot b(x)] = R_{f(x)}\{R_{f(x)}[a(x)], R_{f(x)}[b(x)]\}$
where $a(x)$, $b(x)$ and $f(x)$ are polynomials over $GF(q)$.

 Indian Institute of Technology, Delhi 12 Ranjan Bose
Department of Electrical Engineering

Now, let us look at the remaining part which is the division algorithm. What does it say? Well, it states that for every pair of polynomial $a(x)$ and $b(x)$ contained in $F[x]$. So, what is this capital F of x it is nothing but a collection it is a set of polynomials, all right. We have already seen that we can add subtract multiply.

Now, the question is can we divide? So, clearly division by $0 \neq 0$ is not acceptable. So, I have got $b(x)$ not equal to 0 and then what we would like to do is they we say that this algorithm states that there exists a unique pair of polynomials $q(x)$ which is called the quotient; and $r(x)$ called the remainder such that $a(x)$ which is one of the first polynomials is nothing but quotient into $b(x)$ which is the divisor plus $r(x)$ which is the remainder and degree of $r(x)$ must be less than the degree of $b(x)$ which is the divisor. So, it is stated as an algorithm it is more like a simple theorem.

So, the remainder is also called as the residue and residue succinctly it is written as R_b of x . So, I am dividing with $b(x)$ what am I dividing $a(x)$. So, if you divide $a(x)$ by $b(x)$ the remainder or the residue is called $r(x)$. How is it written? $a(x)$ is equal to quotient times $b(x)$ plus residue. So, we will use this notation many many times during the subsequent slides.

So, let us look at some important properties of residues since I can add two polynomials the residue of $a(x)$ plus $b(x)$ for $f(x)$ is nothing but the residue of $a(x)$ when divided by $f(x)$ plus the residue of $b(x)$ when divided by $f(x)$. So, this is nice, it can help us solve some of the properties and solve some of the theorems that we will encounter in the future and the product also holds true. So, if I have a product $a(x)$ into $b(x)$ and I will take the residue with respect to $f(x)$ it is nothing but the product of the residues and the residue with respect to $f(x)$. So, that is how we get. We will use these two properties over and over again, alright.

(Refer Slide Time: 15:04)


Information Theory, Coding and Cryptography

Example

- Let the polynomials, $a(x) = x^3 + x + 1$ and $b(x) = x^2 + x + 1$ be defined over $GF(2)$.
- We can carry out the long division of $a(x)$ by $b(x)$ as follows

$$\begin{array}{r}
 \begin{array}{l} b(x) \longrightarrow x^2 + x + 1 \end{array} \quad \begin{array}{r}
 \begin{array}{r}
 \begin{array}{r}
 x + 1 \longleftarrow q(x) \\
 x^3 + + x + 1 \longleftarrow a(x) \\
 \hline
 x^3 + x^2 + x \\
 \hline
 x^2 + + 1 \\
 \hline
 x^2 + x + 1 \\
 \hline
 x \longleftarrow r(x)
 \end{array}
 \end{array}
 \end{array}
 \end{array}$$

- Thus, $a(x) = (x+1) b(x) + x$.
- Hence, we may write $a(x) = q(x) b(x) + r(x)$, where $q(x) = x + 1$ and $r(x) = x$.
- Note that $\deg r(x) < \deg b(x)$.

 Indian Institute of Technology, Delhi
13
Ranjan Bose
Department of Electrical Engineering

So, let us look at a simple example. Let us take $a(x)$ is equal to a polynomial $x^3 + x + 1$ and I have got $b(x)$ is equal to $x^2 + x + 1$ and I am going to carry out all of this arithmetic over $GF(2)$. So, it is a long division. I write $x^3 + x + 1$ this is the dividend, this is the divisor and I just multiply it out when I multiply it with x , I get another polynomial because product of polynomials is defined I subtract it out and I get an residue $r(x)$.


So, this simple example shows that we have got with us this quotient and the remainder and we can clearly write your $a(x)$ the dividend equal to $q(x)$ quotient into $b(x)$ divisor plus the remainder other residue $r(x)$, ok. So, this will be required many many times when we do cyclic codes because please remember we are taking a mathematical detour we are still trying to study cyclic codes, but these tools that we are revising or gathering with us will help us solve cyclic code problems much more easily please note one thing the degree of $r(x)$ must necessarily be less than the degree of $b(x)$ otherwise I could have divided one more time I keep doing till the degree is less than $b(x)$, strictly less than.

(Refer Slide Time: 16:38)

Information Theory, Coding and Cryptography

Congruent Modulo

- Let $f(x)$ be a fixed polynomial in $F[x]$.
- Two polynomials, $g(x)$ and $h(x)$ in $F[x]$ are said to be **congruent modulo** $f(x)$, depicted by
$$g(x) \equiv h(x) \pmod{f(x)},$$
if $g(x) - h(x)$ is divisible by $f(x)$.
- Let the polynomials $g(x) = x^9 + x^2 + 1$, $h(x) = x^5 + x^2 + 1$ and $f(x) = x^4 + 1$ be defined over $GF(2)$.
- Since $g(x) - h(x) = x^5 f(x)$, we can write $g(x) \equiv h(x) \pmod{f(x)}$.

 Indian Institute of Technology, Delhi 14 Ranjan Bose
Department of Electrical Engineering

We talked about this term called congruent modulo. So, let $f(x)$ be a fixed polynomial within this collection or set F of x . Now, two polynomials $g(x)$ and $h(x)$ both contain in $F[x]$ are said to be congruent modulo $f(x)$ if $f(x)$ was a fixed polynomial in $F[x]$ and capital F of x . So, if this is true if $g(x) \equiv h(x) \pmod{f(x)}$ and we have this $g(x) - h(x)$ is divisible by $f(x)$. So, let us look at this example. Please note we are trying to define congruent modulo $f(x)$.

So, I am taking this $h(x)$ and do modulo $f(x)$ that is you divided by $f(x)$ and whatever remains and that should be $g(x)$ then they are called congruent modulo. So, let us look at a quick example let us say $g(x)$ is $x^9 + x^2 + 1$ and $h(x)$ is $x^5 + x^2 + 1$ and my fixed polynomial is $x^4 + 1$ and I will do all the arithmetic over $GF(2)$.

Now, you can see that if $g(x) - h(x)$ we saw this earlier is divisible by $f(x)$ then they are written congruent modulo.


(Refer Slide Time: 18:19)

Information Theory, Coding and Cryptography

Ring of Polynomials

- If $a(x)$ and $b(x)$ belong to $F[x]/f(x)$, then the sum $a(x) + b(x)$ in $F[x]/f(x)$ is the same as in $F[x]$.
- This is because $\deg a(x) < \deg f(x)$, $\deg b(x) < \deg f(x)$ and therefore $\deg (a(x) + b(x)) < \deg f(x)$.
- The product $a(x)b(x)$ is the unique polynomial of degree less than $\deg f(x)$ to which $a(x)b(x)$ (multiplication being carried out in $F[x]$) is congruent modulo $f(x)$.
- $F[x]/f(x)$ is called the *ring of polynomials* (over $F[x]$) modulo $f(x)$.

▶

 Indian Institute of Technology, Delhi 15 Ranjan Bose
Department of Electrical Engineering

Now, we quickly go to rings of polynomials and then eventually fields of polynomials. Again, let us be patient and we will quickly link to cyclic codes, but this is interesting stuff. So, if $a(x)$ and $b(x)$ belong to $F[x]/f(x)$, then the sum $a(x) + b(x)$ in $F[x]/f(x)$ is the same as in $F[x]$. What does it mean? Well, we are looking with looking at two polynomials, right and we are going to look at the sum of these polynomials, but every time we do so, we are taking it modulo $f(x)$. So, what is critical is this very interesting polynomial.

Student: (Refer Time: 19:11).

$F[x]$ we are still going to do operations of addition and multiplication contained in this set $F[x]$, but now all the operations will be done modulo $f(x)$ that is whatever is the residual remainder after dividing with $f(x)$ is the answer. And this you can check degree of $a(x)$ is less than degree of $f(x)$ why because we are taking modulo $f(x)$ similarly, degree of $b(x)$ less than $f(x)$ and therefore, degree of $a(x) + b(x)$ is less than degree of $f(x)$.

Similarly, the product $a(x)b(x)$ is a unique polynomial of degree less than degree of $f(x)$, right to which $a(x)b(x)$ is congruent modulo $f(x)$. So, what are we trying to do? We are looking at a ring of polynomials. What is a ring? Ring is a set of elements with certain properties including additive inverse, associativity and distributive properties 0 and 1 being contained in the set and so and so forth it follows the first eight

of first seven of the eight properties required for a Galois field. So, we are not talking about this ring.

So, this capital F of x divided by f of x this is this shows that everything taken modulo f of x, this is a notation because the numerator is a set. So, this is called the ring of polynomials over f of x modulo small f of x, this is the notation and we will be using this notation. Now, under some special conditions for f of x the small f of x this ring actually translates to a field.

(Refer Slide Time: 21:15)

Information Theory, Coding and Cryptography

Example

- Consider the ring $F[x]/(x^2 + x + 1)$ defined over $GF(2)$.
- This ring will have polynomials with highest degree = 1.
- This ring contains $q^n = 2^2 = 4$ elements (each element is a polynomial).
- The elements of the ring will be 0, 1, x and x + 1.
- The addition and multiplication tables can be written as follows.

+	0	1	x	x+1	.	0	1	x	x+1
0	0	1	x	x+1	0	0	0	0	0
1	1	0	x+1	x	1	0	1	x	x+1
x	x	x+1	0	1	x	0	x	x+1	1
x+1	x+1	x	1	0	x+1	0	x+1	1	x

Indian Institute of Technology,
Delhi

16

Ranjan Bose
Department of Electrical Engineering

So, let us consider this ring again capital F of x divided by this polynomial x squared plus x plus 1 again our arithmetic will be over GF 2. So, this ring will have polynomials with highest degree 1. Why? Because whatever be your collection of polynomials where you take modulo x square plus x plus 1 the highest power can be at best x raised power 1. So, what are the polynomials possible here? Well, there are only four possible polynomials here.

(Refer Slide Time: 22:07)

$$\begin{aligned}
 & \boxed{F[x]} \div \underbrace{(x^2+x+1)}_{f(x)} \\
 & \quad \downarrow \\
 & \quad ()x + ()x^0 \\
 & = ()x + () \\
 & \quad \downarrow \quad \downarrow \\
 & \text{GF}(2) \quad 0,1 \quad 0,1 \quad \text{GF}(2) \\
 & \begin{array}{l} 1x+1 \\ 1x+0 \\ 0x+1 \\ 0x+0 \end{array} \rightarrow \begin{array}{|c|} \hline x+1 \\ x \\ 1 \\ 0 \\ \hline \end{array}
 \end{aligned}$$

So, let us look at it with a small example what we are trying to do is take this F of x and take all the polynomials modulo this. So, we have not put any restrictions on how big this set is. You can have infinite number of polynomials here you can make them as large as possible, but I will take each one of them and divide by $x^2 + x + 1$ and whatever is the residue is the set which I am looking at. And if you look at this the residue will be some polynomial with a coefficient times x plus another coefficient times x raised power 0 which is nothing but x plus.

Now, since we are looking at $GF(2)$ we will have two possibilities for this location either a 0 or a 1 again two possibilities 0 or a 1. So, we can have at most four distinct polynomials here which are they $1x + 1$, $1x + 0$, $0x + 1$, $0x + 0$ and if you write it out clearly, we are looking at the polynomials $x + 1$, x , 1 and 0 . Now, this is a finite set. So, from an infinite set just because we took this modulo F of x operation we are we ended up with only four distinct polynomials.

Now, they can be added multiplied subtracted as we want provided we are following this rule. Now, if you go back to the slides we see that this ring contains 2^2 is equal to 4 elements and each element is a polynomial. Please remember that elements can be anything and here we chose them to be polynomials 0 , 1 , x and $x + 1$ like we just saw and we can try to build the addition and multiplication table for this one. So, I can add and multiply. So, this is the addition table and this the multiplicative

multiplication table and you can check that there is a 0 in every row and column which shows that there is an additive inverse for each of the four elements, but if you try to see for one there is a problem because a multiplicative inverse is not necessarily present.

So, in therefore, what we would like to do is go to another example.

(Refer Slide Time: 25:21)

Information Theory, Coding and Cryptography

Example

- Next, consider $F[x]/(x^2 + 1)$ defined over $GF(2)$.
- The elements of the ring will be 0, 1, x and $x + 1$.
- The addition and multiplication tables can be written as follows.

+	0	1	x	$x+1$	·	0	1	x	$x+1$
0	0	1	x	$x+1$	0	0	0	0	0
1	1	0	$x+1$	x	1	0	1	x	$x+1$
x	x	$x+1$	0	1	x	0	x	1	$x+1$
$x+1$	$x+1$	x	1	0	$x+1$	0	$x+1$	$x+1$	0

- It is interesting to note that $F[x]/(x^2 + x + 1)$ is actually a field as the multiplicative inverse for all the non-zero elements also exists.
- On the other hand, $F[x]/(x^2 + 1)$ is *not* a field because the multiplicative inverse of element $x + 1$ does not exist.

Indian Institute of Technology, Delhi
17
Ranjan Bose
Department of Electrical Engineering

So, now we look at another example F of x divided by this polynomial x squared plus 1 again defined over $GF 2$ and again the elements will be 0, 1, x and x plus 1 and again I can write the addition and multiplication tables for these two and what we look at it is that the first example of $F x$ divided by x squared plus x plus 1 was actually field. Whereas, this one is just a ring because of the absence of a multiplicative inverse, if you see this multiplicative table x plus 1 does not have a multiplicative inverse whereas, every other one has a multiplicative inverse. So, each element 0 is of course, excluded from a multiplicative inverse, but x plus 1 element does not have a multiplicative inverse.

On the other hand, if you look at this ring each one so, x is a multiplicative inverse of x plus 1 and 1 is a multiplicative inverse of 1 and x is a multiplicative inverse of x plus 1 and so on and so forth. So, you have additive inverse and multiplicative inverse for every element and therefore, this ring is actually a field whereas, this ring remains a ring. So, what is interesting is this f of x small f of x sometimes ends up giving us a ring and


sometimes ends up giving us a field. So, $F[x]$ divided by $x^2 + 1$, this is not a field where $F[x]$ divided by $x^2 + x + 1$ is also a field.

(Refer Slide Time: 27:14)

Information Theory, Coding and Cryptography

Ring and Field

- It is interesting to note that $F[x]/(x^2 + x + 1)$ is actually a field as the multiplicative inverse for all the non-zero elements also exists.
- On the other hand, $F[x]/(x^2 + 1)$ is *not* a field because the multiplicative inverse of element $x + 1$ does not exist.
- It is worthwhile exploring the properties of $f(x)$ which makes $F[x]/f(x)$ a field.
- Condition: The polynomial $f(x)$ must be *irreducible* (*non-factorizable*).

 Indian Institute of Technology, Delhi 18 Ranjan Bose
Department of Electrical Engineering


So, now it come and connect these two concepts about why one gives a field and the other one does not give a fields. So, let us explore what properties of this $f(x)$ lead us to generating a field. So, the condition that we will soon see is that this polynomial f of x must be irreducible which is in Layman's language non-factorizable, we cannot factorize it but, let us see what do we mean by that.

(Refer Slide Time: 27:49)

Information Theory, Coding and Cryptography

Irreducible

- **Definition:** A polynomial $f(x)$ in $F[x]$ is said to be **reducible** if $f(x) = a(x) b(x)$, where $a(x)$, $b(x)$ are elements of $f(x)$ and $\deg a(x)$ and $\deg b(x)$ are both smaller than $\deg f(x)$.
- If $f(x)$ is not reducible, it is called **irreducible**.
- A monic irreducible polynomial of degree at least one is called a **prime polynomial**.

 Indian Institute of Technology, Delhi 19 Ranjan Bose
Department of Electrical Engineering

So, we define a polynomial f of x in capital F of x which is a set of polynomials is said to be reducible if f of x can be written as a product of two polynomials where a x and b x are elements of f of x right.

So, now if f of x is not reducible then it is called irreducible. So, if it is not factorizable then it is means that it is irreducible. Over and above if with this non factorizable irreducible polynomial happens to be a monic, the leading coefficient is 1 then it is also called as a prime polynomial, ok. So, monic additional condition of being a monic makes it a prime polynomial. So, a monic irreducible polynomial is a prime polynomial.


(Refer Slide Time: 28:46)

Information Theory, Coding and Cryptography

Factorization

- A polynomial $f(x)$ has a linear factor $(x - a)$ if and only if $f(a) = 0$ where a is a field element.
- A polynomial $f(x)$ in $F[x]$ of degree 2 or 3 over $GF(q)$ is irreducible if and only if $f(a) \neq 0$ for all a in $GF(q)$.
- Over any field,

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1).$$
 The second factor may be further reducible.

 Indian Institute of Technology,
Delhi

20

Ranjan Bose
Department of Electrical Engineering


So, factorization as some of the facts we know and we can quickly go over it. So, polynomial f of x is a linear factor x minus a , if f of a is 0, this we know and then polynomial f of x in capital F of x set of polynomials of degree 2 and 3 over GF q is irreducible if and only if f of a is not equal to 0 for all a in GF q . So, we can quickly test these out and over any field we have this general expansion x raised power n minus 1 is x minus 1 times x raised power n minus 1 plus x raised power n minus 2 up to x plus 1, ok.

(Refer Slide Time: 29:30)

Information Theory, Coding and Cryptography

Field

- The ring $F[x]/f(x)$ is a field if and only if $f(x)$ is a prime polynomial in $F[x]$.
- **Proof:** To prove that a ring is a field we must show that every non zero element of the ring has a multiplicative inverse.
- Let $s(x)$ be a non zero element of the ring.
- We have, $\deg s(x) < \deg f(x)$, because $s(x)$ is contained in the ring $F[x]/f(x)$.
- It can be shown that the greatest common divisor (GCD) of two polynomials $f(x)$ and $s(x)$ can be expressed as
- $\text{GCD}(f(x), s(x)) = a(x)f(x) + b(x)s(x)$,
- where $a(x)$ and $b(x)$ are polynomials over $GF(q)$.
- Since $f(x)$ is irreducible in $F[x]$, we have $\text{GCD}(f(x), s(x)) = 1 = a(x)f(x) + b(x)s(x)$.

 Indian Institute of Technology, Delhi
21
Ranjan Bose
Department of Electrical Engineering


So, what we do is we quickly go over the next two slides and looking at that this ring of polynomials $F[x]$ divided by $f(x)$ is a field if and only if $f(x)$ is a prime polynomial, that is a monic irreducible polynomial, it cannot be factorized over the $GF(q)$ we are working at and the proof is pretty simple we to prove that a ring is a field we must show that every non zero element of the ring has a multiplicative inverse and that is what we do here. And we can show that the greatest common divisor GCD of two polynomials $f(x)$ and $s(x)$ can be written as follows and then we show that since $f(x)$ is irreducible in $F[x]$, we can write the GCD of $f(x)$ and $s(x)$ as 1.

(Refer Slide Time: 30:34)

Information Theory, Coding and Cryptography

Field

- Now, $1 = R_{f(x)}[1] = R_{f(x)}[a(x)f(x) + b(x)s(x)]$
 $= R_{f(x)}[a(x)f(x)] + R_{f(x)}[b(x)s(x)]$
 (property (i) of residues)
 $= 0 + R_{f(x)}[b(x)s(x)]$
 $= R_{f(x)}\{R_{f(x)}[b(x)] \cdot R_{f(x)}[s(x)]\}$
 (property (ii) of residues)
 $= R_{f(x)}\{R_{f(x)}[b(x)] \cdot s(x)\}$
- Hence, $R_{f(x)}[b(x)]$ is the multiplicative inverse of $s(x)$.

 Indian Institute of Technology, Delhi
22
Ranjan Bose
Department of Electrical Engineering

Now, we invoke the properties of residue and we do some basic maths and we can easily verify that you can indeed have the condition of a multiplicative inverse.

(Refer Slide Time: 30:54)

Information Theory, Coding and Cryptography

Field

- Next, let us prove the *only if* part of the theorem.
- Let us suppose $f(x)$ has a degree of at least 2, and **is not a prime polynomial** (a polynomial of degree one is always irreducible).
- Therefore we can write $f(x) = r(x)s(x)$ for some polynomials $r(x)$ and $s(x)$ with degrees at least one.
- If the ring $F[x]/f(x)$ is indeed a field, then a multiplicative index of $r(x)$, $r^{-1}(x)$ exists, since all polynomials in the field must have their corresponding multiplicative inverses.
- Hence, $s(x) = R_{f(x)}\{s(x)\} = R_{f(x)}\{r(x)r^{-1}(x)s(x)\}$
 $= R_{f(x)}\{r^{-1}(x)r(x)s(x)\} = R_{f(x)}\{r^{-1}(x)f(x)\} = 0.$
- However, we had assumed $s(x) \neq 0$.
- Thus, there is a **contradiction**, implying that the ring is not a field.

Indian Institute of Technology,
Delhi

23

Ranjan Bose
Department of Electrical Engineering

So, the theorem had if and only if so, the only if part can be proven like if you have f of x has a degree 2 at least 2 and is not a prime polynomial this is the assumption and then we will contradict this assumption, ok.


So, we know that a polynomial of degree 1 is always irreducible. So, we can write this f of x as some r of x plus s of x for some polynomial r of x , and then we look at this ring F of x divided by small f of x then a multiplicative inverse r inverse x exists. Since all the elements other than 0 should have a multiplicative inverse and then we substitute this here. So, r of x r inverse s , s of x here and we do some basic maths and we have assume s of x is not equal to 0 which leads to a contradiction implies that the ring is not a field. Therefore, we get this proof for a reducibility.

(Refer Slide Time: 32:07)

Information Theory, Coding and Cryptography

Example

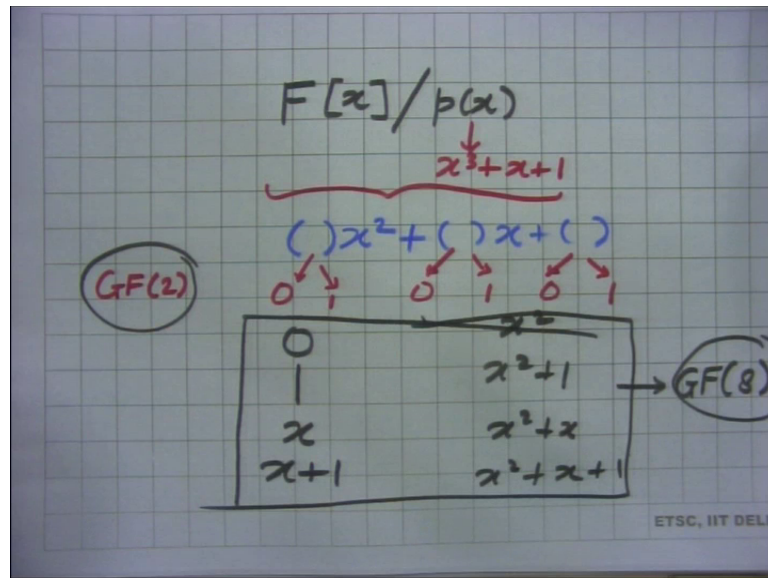
- Consider the polynomial $p(x) = x^3 + x + 1$ over $GF(2)$.
- Since, $p(0) \neq 0$ and $p(1) \neq 0$, the polynomial is irreducible in $GF(2)$.
- Since it is also monic, $p(x)$ is a prime polynomial.
- Here we have $n = 3$, so we can use $p(x)$ to construct a field with $2^3 = 8$ elements, i.e., $GF(8)$.
- The elements of this field will be $0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$, which are all possible polynomials of degree less than $n = 3$.
- It is easy to construct the addition and multiplication tables for this field.

 Indian Institute of Technology, Delhi 24 Ranjan Bose
Department of Electrical Engineering

So, let us look at the example which helps us understand the theorem a slightly better. So, let us consider this polynomial p of x which is x cubed plus x plus 1 over $GF(2)$. Now, this is a prime polynomial, but we would rather verify that with is a prime or not. So, it is very easy let us see whether there are any linear factors. So, just substitute 0 and 1, because there are the two elements if you substitute $p(0)$ you get a non zero answer same with $p(1)$ non zero answer. So, there are no linear factors of the type $x - 1$ or x and this is monic and therefore, p of x is a prime polynomial.

So, now what we can do is we will shortly learn to construct extension fields using subfields. For example, we have $GF(2)$ and we can construct $GF(8)$ using this prime polynomial. Please note that: if you have capital f of x divided by p of x then the highest power is 2. So, let us look at this example.

(Refer Slide Time: 33:33)



if we look at F of x and we divided by p of x please note that p of x is nothing but x cubed plus x plus 1. So, anytime I take the residue the highest power can at most be a square. So, all polynomials are some coefficient square plus some coefficient x plus some coefficient. Now, we are working over $GF(2)$ consequently this is a 0 or 1, 0 or 1, 0 or a 1 and therefore, you have got these 8. So, you can have these places filled up right from 0, 1, x , x plus 1 and then you have x square x square plus 1 x square plus x and x square plus x plus 1. So, you have got these eight elements. These eight elements basically form elements of $GF(8)$ and we will show that we migrated from $GF(2)$ to $GF(8)$.


Now, we come back to the slides and we say that it is easy to construct the addition multiplication tables for this field.

(Refer Slide Time: 35:18)

Information Theory, Coding and Cryptography

Observations

- $x^n = 1 \pmod{x^n - 1}$.
Hence, any polynomial, modulo $x^n - 1$, can be reduced simply by replacing x^n by 1, x^{n+1} by x and so on.
- A codeword can *uniquely* be represented by a polynomial.
We can use a polynomial to represent the locations and the values of all the element in the codeword.
- For example, the codeword $c_1c_2\dots c_n$ can be represented by the polynomial $c(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n$.
- As another example, the codeword over $GF(8)$, $c = 207735$ can be represented by the polynomial $c(x) = 2 + 7x^2 + 7x^3 + 3x^4 + 5x^5$.

 Indian Institute of Technology, Delhi 25 Ranjan Bose
Department of Electrical Engineering

Now, we do a few observations because we should not forget an end goal which is to link it to cyclic codes and we are almost there just a few more mathematical tools and then we are ready to go. So, please note that x raised power n is equal to actually 1 modulo $x^n - 1$. So, this x raised power n minus 1 will become a very interesting polynomial for us.

Now, we first make our link any codeword can be uniquely represented by a polynomial and how do we do that well suppose my codeword is c_1, c_2, c_3 up to c_n then we can write it very easily as $c_0 + c_1x + c_2x^2 + \dots + c_nx^n$; so here of course, I did not start with a c_0 which is missing, but if I remove this c_0 here. So, $c_1x + c_2x^2$ and so and so forth up to c_nx^n , there are total n elements here, here $n + 1$. So, we can choose to either go from c_0 up to x raised power n minus 1 or c_1 to x raised power n either which way we will have n elements n coefficients corresponding one to one to the elements of the code.


So, if you have for example, over $GF(8)$ the codeword c equal to 207735 well you can always write it one to one for this. So, here there are n equal to 6 the block length is 6 the highest power I need to go is n minus 1 and clearly this is the unique representation of this codeword in terms of a polynomial. So, from this point onwards we will refer to codewords as codeword polynomials because for cyclic codes it is very easy to say that.

(Refer Slide Time: 37:24)

Information Theory, Coding and Cryptography

Observations

- Multiplying any polynomial by x corresponds to a single cyclic right-shift of the codeword elements.
- More explicitly, in R_n , by multiplying $c(x)$ by x we get
$$\begin{aligned}x \cdot c(x) &= c_0x + c_1x^2 + c_2x^3 + \dots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \dots + c_{n-2}x^{n-1}.\end{aligned}$$
- Recall $x^n = 1 \pmod{x^n - 1}$.
Hence, any polynomial, modulo $x^n - 1$, can be reduced simply by **replacing x^n by 1, x^{n+1} by x and so on.**

 Indian Institute of Technology, Delhi 26 Ranjan Bose
Department of Electrical Engineering

Now comes the most important link why are we talking about polynomials for the past so many minutes. Firstly, multiplying any polynomial by x corresponds to a single cyclic right shift of the codeword element because simply you are increasing the power by of x by 1 and so, it results in a cyclic shift right more explicitly in R_n by multiplying $c(x)$ by x we get so, c_0 which did not have a x now I have c_0x c_1 was coupled with x raised power 1, now it get x squared. So, you just simply shift and this R_n means take modulo $x^n - 1$ x raised power $n - 1$ the moment you do x raised power $n - 1$ this highest power which became n goes back to the front.

So, it is a cyclic shift this is the property of doing modulo x raised power $n - 1$ please recall that x^n is equal to 1 if you take mod $x^n - 1$. So, this will be our staple for the next few slides all operations all products additions would be done modulo $x^n - 1$, because that puts us in the domain of cyclic codes.

So, any polynomial modulo $x^n - 1$ can be reduced simply by replacing the x^n by 1 x^{n+1} by x and so on and so forth. This is the critical observation.


(Refer Slide Time: 39:18)

Information Theory, Coding and Cryptography

Back to Cyclic Codes

- A code C in R_n is a cyclic code if and only if C satisfies the following conditions: $F[x]/f(x)$ is R_n

$$a(x), b(x) \in C \Rightarrow a(x) + b(x) \in C$$
$$a(x) \in C \text{ and } r(x) \in R_n \Rightarrow a(x)r(x) \in C.$$

 Indian Institute of Technology, Delhi 27 Ranjan Bose
Department of Electrical Engineering

So, now we are back to cyclic codes a code C in R_n . So, R_n means we will take modulo $x^n - 1$ is a cyclic code if and only if C satisfies the following condition F of x divided by $f(x)$ is in R_n . So, $a(x), b(x)$ if are two elements of C . What does it mean? Well, C is a code. Code is a set of codewords.


Now, my codewords are now codeword polynomials. So, $a(x)$ is one codeword polynomial, $b(x)$ is another codeword polynomial. Sum of two codewords is also valid codewords. Not a surprise because C is a linear block code and if $a(x)$ is a codeword and $r(x)$ is some polynomial then $a(x)r(x)$ is also a valid codeword, ok.

(Refer Slide Time: 40:24)

Information Theory, Coding and Cryptography

Back to Cyclic Codes

- A code \mathbf{C} in R_n is a cyclic code if and only if \mathbf{C} satisfies the following conditions:
 - $a(x), b(x) \in \mathbf{C} \Rightarrow a(x) + b(x) \in \mathbf{C}$
 - $a(x) \in \mathbf{C}$ and $r(x) \in \mathbb{R}_n \Rightarrow a(x)r(x) \in \mathbf{C}$.
- **Proof:** (i) Suppose \mathbf{C} is a cyclic code in R_n .
- Since cyclic codes are a subset of linear block codes, the first condition holds.
- (ii) Let $r(x) = r_0 + r_1x + r_2x^2 + \dots + r_nx^n$.
- Multiplication by x corresponds to a cyclic right-shift.
- But, by definition, the cyclic shift of a cyclic codeword is also a valid codeword.
- That is, $xa(x) \in \mathbf{C}$, $x(xa(x)) \in \mathbf{C}$, and so on.
- Hence
- $r(x)a(x) = r_0a(x) + r_1xa(x) + r_2x^2a(x) + \dots + r_nx^na(x)$ is also in \mathbf{C} since each summand is also in \mathbf{C} .

 Indian Institute of Technology,
Delhi28Ranjan Bose
Department of Electrical Engineering

So, let us understand this thing. So, the first part is very simple sum of any two codewords is also a valid codeword. The second part can be understood simply as follows; well, if you look at multiplication of a valid codeword with $r(x)$ then it is nothing but $r(x)$ is nothing but a polynomial given by this. So, individually when I multiply I can say ok, first we take a x and I multiply with r_1x . Well, what is multiplication with r_1x 1 cyclic shift, but we know cyclic shift our valid codeword is another valid codeword and then I multiply this valid codeword a x with r_2x^2 x^2 means two cyclic shifts. Well, two cyclic shifts is also a valid codeword and so and so forth. So, r_nx^n pertains to n cyclic shifts and multiplication by a scalar.


So, each of these operations is leading to a cyclic shift of a x which is a valid codeword. So, each of this operation is transforming ax into another valid codeword and some of all these codewords is a valid codeword because some of any two codewords should be a valid codeword for a linear block code. Consequently, the product of a x into $r(x)$ should be a valid codeword. Hence, should be an element of \mathbf{C} that is the proof.

(Refer Slide Time: 42:01)

Information Theory, Coding and Cryptography

Generating Cyclic Codes

- The following steps can be used to generate a cyclic code:
- Take a polynomial $f(x)$ in R_n .
- Obtain a set of polynomials by multiplying $f(x)$ by all possible polynomials in R_n .
- The set of polynomials obtained above corresponds to the set of codewords belonging to a cyclic code.
- The blocklength of the code is n .

 Indian Institute of Technology, Delhi29Ranjan Bose
Department of Electrical Engineering


So, now we have a very simple way to generate cyclic codes because in the previous slide we observed that this product of some valid codeword with any arbitrary polynomial is a valid codeword. So, can we have a notion of a generator polynomial which when multiplied with an information polynomial gives a valid polynomial that is the basic idea. So, how do we generate cyclic codes? Take a polynomial f of x in R_n , obtain a set of polynomials where multiplying $f \cdot x$ by all possible polynomials in R_n . Remember R_n is modulo x raised power n minus 1. The set of polynomials obtained above correspond to the set of codewords belonging to a cyclic codes of block length n .

(Refer Slide Time: 43:00)

Information Theory, Coding and Cryptography

Example

- Consider the polynomial in R_3 defined over $GF(2)$.
- In general a polynomial in $R_3 (= F[x]/(x^3 - 1))$ can be represented as $r(x) = r_0 + r_1x + r_2x^2$, where the coefficients can take the values 0 or 1 (since defined over $GF(2)$).
- Thus, there can be a total of $2 \times 2 \times 2 = 8$ polynomials in R_3 defined over $GF(2)$, which are $0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2$.
- To generate the cyclic code, we multiply $f(x)$ with these 8 possible elements of R_3 and then reduce the results modulo $(x^3 - 1)$:
- $(1 + x^2) \cdot 0 = 0, (1 + x^2) \cdot 1 = (1 + x^2), (1 + x^2) \cdot x = 1 + x, (1 + x^2) \cdot x^2 = x + x^2,$
- $(1 + x^2) \cdot (1 + x) = x + x^2, (1 + x^2) \cdot (1 + x^2) = 1 + x, (1 + x^2) \cdot (x + x^2) = (1 + x^2),$
- $(1 + x^2) \cdot (1 + x + x^2) = 0.$
- **Thus there are only four distinct codewords:**
 $\{0, 1 + x, 1 + x^2, x + x^2\}$ corresponding to $\{000, 110, 101, 011\}$.

 Indian Institute of Technology, Delhi30Ranjan Bose
Department of Electrical Engineering

So, let us take a simple example. So, let us take $r(x)$ is equal to $r_0 + r_1 x + r_2 x^2$ and we are doing it over $GF(2)$. So, we have got a total of 8 polynomials since we are taking $F[x]$ divided by $x^3 - 1$ which means that the highest power of this residue can be squared. So, there are 8 possible polynomials, and then we can multiply each one. So, if you say $x^2 + 1$ you multiply by 0 you get a 0 by 1 by x and so and so forth you can try out all the possible combinations and then you get only four distinct codewords coming out of it. So, just now you generated your first cyclic code using this notion of multiplication of a polynomial over R_3 . What are these four distinct codewords? The four distinct codewords as we just now saw are 0 1 plus x 1 plus x^2 and $x^2 + x$.

So, these can correspond to these four codewords as we know in terms of the binary digits and you can check whether they are linear block codes and whether they follow the cyclic property.

(Refer Slide Time: 44:42)

Information Theory, Coding and Cryptography

Summary

- Ring and Fields
- Polynomials
- Division Algorithm
- Cyclic Codes
- Examples

Indian Institute of Technology, Delhi

31

Ranjan Bose
Department of Electrical Engineering

So, with that we come to the end of today's lecture. We have understood what do we mean by a ring specifically a ring of polynomials and how and when a ring becomes a field. Then, we had a detour into polynomials how do we add multiply subtract and divide and then we linked it up to cyclic codes. Well, we just have scratched the surface, now that we have these mathematical tools ready we are ready to explore this domain of cyclic codes; we have first looked at a few examples.

With that, we come to the end of this module.