Spread Spectrum Communications and Jamming

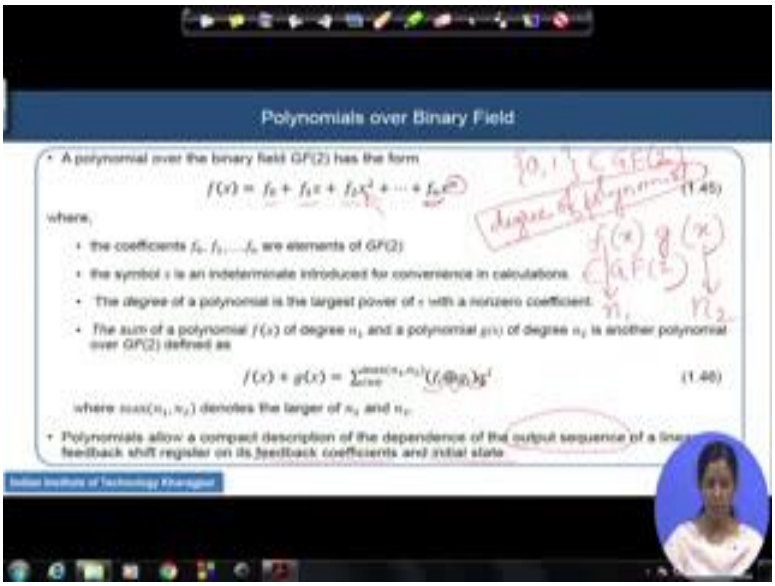
Prof. Debarati Sen
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

Lecture - 27
Polynomials over Binary Field

Hello students. Today our topic of discussion will be the Polynomials over Binary Field. In the last three modules we were concentrating in the Galois field mathematics, and we were trying to learn the different terms called the field, the ring and polynomials the polynomial ring, and we could not. Now we will learn how actually the all those terms are related in the context of our specific term communications. All this terms that will be heavily related in the code generation of direct sequences specific term as well as frequency hopping spectrum communication systems.

As we understand that codes are the heart of this kind of communication system design. So, it is really, means we need to have at least some basic idea, how those codes generation process, is heavily related with the Galois Field Mathematics. basically these are the polynomials where actually we will find the, there is a very deep understanding of between the generated code sequence as well, as the feedback circuit and the feedback input you are giving to the initial stages. And let us see how far we can proceed over the polynomials over the binary field concept, and how far we can relate these polynomials in the generation process of the different codes polynomials.

(Refer Slide Time: 02:17)



The polynomials allow a very compact description between the generated code sequence of a linear feedback shift register, with its feedback coefficients and the initial steps that we said for the m stage, for the m stage memories. Hope you will remember that long back we were discussing about the linear feedback shift registers which is the, re fundamental block of generating the pseudo random sequences, the p n sequences we also saw, the there are different kind of the structures, and some of them are also match filter based structure, and we also saw the derivations of how the output beets can be generated over through that structure.

We understood the periodicity of the generated codes, we understood what is the, how the feedback circuit needs to be generate needs to be design, how the feedback to the initial stage needs to be given, how they stored data in the stages, slowly proceed from the left most to the right most, based on the clock pulse arrival, and we also understood the periodicity of the generated codes. So, in the linear feedback shift register this output sequence what we have already generated, in the last few last classes. Those output sequences are having some deep relation, the way the feedback logic is designed, and the way the initial states are given.

So, polynomials are the bridge up compact description I would say, who will show us the dependence of these output generated sequence with the feedback coefficient as well as with the initial stage; that is why we are. So, interested about the polynomials, and as we

are dealing with the Galois field too, because all the stage values that are stored inside the linear feedback shift register, they belong to the value of either 0 or 1, they are basically the elements of the belongs to the Galois, basically the elements that belongs to the Galois field too. So, the polynomial today whatever we will be discussing; that is the polynomial over Galois field two.

Any polynomial in the Galois field two in general can be written as f x f 0 plus f 1 x plus f two x square dot dot dot fn x to the power n, where the term f 0 f 1 f 2 dot dot dot f n we call them the coefficients. The x introduced here are called inter determinate, and this inter determinate are introduced for the convenience in the calculation. See that there is a term called degree of polynomial. The degree is the highest order of x, provided that its coefficient value nonzero. So, the highest coefficient; so the highest order of x, or the highest degree of the x, highest power of x, I should say the power of x, where actually the nonzero coefficients are belonging ,those powers are called those power that highest power is called the degree of the corresponding polynomial.

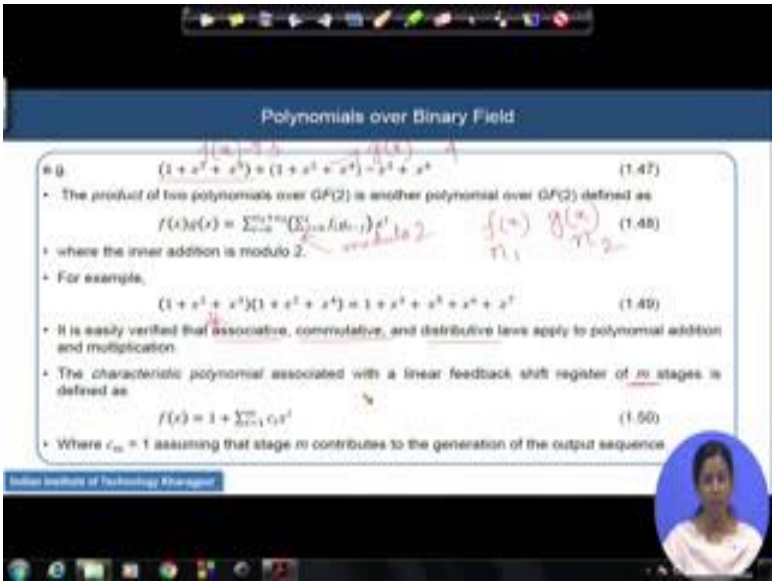
So, these are the terms, this degree will be repeatedly called, because there is several relation of this degree, with the generation polynomial and the generation function and the corresponding generating function as well as the characteristic polynomial, and degree will play repeated, repeatedly degree will be called to define several characteristics of the generated polynomial in Galois field too, in the context of linear feedback shift register.

Now let us consider that we have two polynomials; one is f x and another is g x. Let us also consider that both f x and g x, they belong to Galois field two. Let us also assume that the degree associated with f x is equal to n 1, and the degree associated with g x is equal to n 2. Now given this situation we will be interested to know, how the expression will look like if we add this two polynomial, and if we multiply this two polynomial.

For addition we write that f x plus g x will be given by the modulo 2 operation growing on the bit by bit, and that can go, the addition will run with the maximum degree of n 1 comma n 2, max n 1 comma n 2 says up to the largest value, whoever is the larger one the (Refer Time: 07:53) the summation will go up to that. If n 1 is larger than n 2 the sum will go up to n 2 and vice versa, and this inner summation, to understand that actually

how does it go, in the next slide we will take an example to have a clear idea about the summation of two polynomials over Galois field two.

(Refer Slide Time: 08:10)



Here is the example let us have 1 f x suppose be 1 plus x square of plus x to the power cube, who is having the degree of equal to 3 and this is my another polynomial g x, with the maximum polynomial value is equal to 4, n value is equal to 4 degree is equal to 4. If you add these two, as I described in the last slide, that this addition is the, another Galois feild is modulo 2 operations going on. So, hence it is an Exon operation if 1 plus 1, it will yield 0 x 2 plus x 2 will yield 0 and you will be left with terms called x 3 and plus x 4. Hence the addition of f x plus g x in this example will yield the result x 3 plus x 4.

The product we will start again with the same two polynomial f x and g x, both belong to the Galois field two, and one is having the polynomial degree n 1, another is having the degree n 2, if we multiply this two polynomial. The multiplication will be governed by the equation written in 1.48. Here this inner multiplication, this is in the summation basically modulo two operations going on. remember unlike the addition, unlike the addition of two polynomials here the outer summation for over I will be going with the sum of both the orders, for some of both the degrees n 1 plus n 2, it is not the maximum of n 1 and n 2, it will go up to the summation of n 1 plus n 2.

We will take again another example the 1 plus x 2 plus x 3 and 1 plus x 2 plus x 4; like our earlier case if we keep on multiplying. So, 1 multiply 1 multiplied by 1 will give you

1, you will generate actually 1 x square term here, another x square term, because of the multiplication of this two terms and because of the summation operation is the modulo 2 operation going on; that will boil down on to 0 that will boil down to 0 and you will be having the term independent, again independent term of x 3.

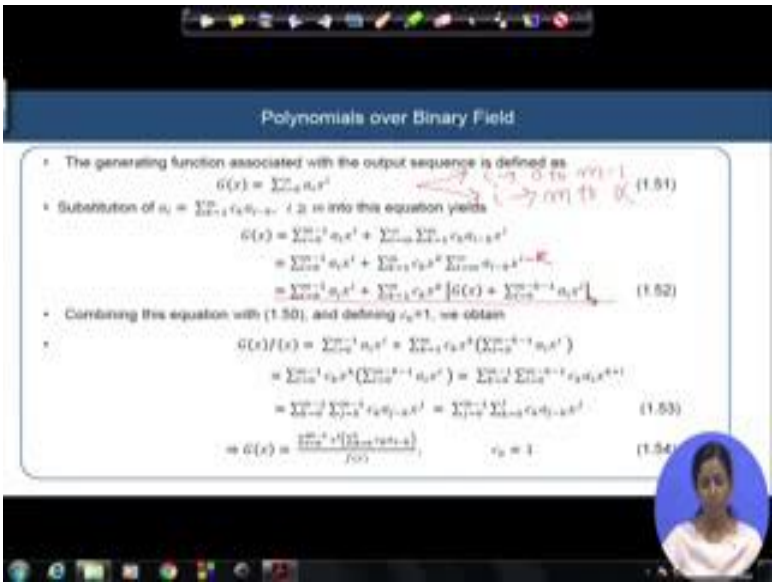
For x 4 I will have 1 x 4 terms here and another x 4 term will be generated by the multiplication of x square b, x square and addition modulo 2 operation of this 2 x 4 term will lead us to 0. So, hence going by this pattern these are the independent terms which are which will be left with x to the power 6 plus x to the power 7 x to power 5 6 and 7, and this is the result of the multiplication of two polynomials.

You can easily verify that the rule of association, it is associative commutative and distributive laws. All the three laws they apply heavily over this multiplication as well as the addition operation of two polynomials over Galois field two. So, this is very important property that if you are having a polynomial for Galois field two, addition of two polynomials and the multiplication of two polynomials over the field, will always follow the associative commutative and distributive laws now we come to a point which is called a characteristic polynomial.

Characteristic polynomial is such polynomial, which always helps to give the equation of generating polynomial of a typical code. we will see how does it go for our linear feedback shift register, which is having a stage of m, the characteristic polynomial is given as 1 plus, sum of all the stages where inside the summation there is a multiplication term of c i into x to the power i. c i we understand that these are all the feedback switches that we have earlier discussed.

The value of the c i equal to 1, signifies that this typical stage is contributing, output of that typical stage is contributing in the feedback process otherwise it is not if slides value equal to 0 means it is not that typical stage, is not contributing to the feedback logic. and definitely we have also discussed earlier that the value of cm if it is 1, it should be 1 such that the last stage the mth stage of the feedback shift register, contribute to the feedback logic. If it is not equal to 1, then that structure in the last stage will not have any contribution and then the last stage will simply give a 1 delay, simply give a delay of the generative sequence by n minus 1 stage given this characteristic polynomial.

(Refer Slide Time: 13:22)



Now we would look into the generating function. The generating function of a linear feedback shift register is given by g x. It is directly related with the output. So, output is, a i is the output which is directly the output coming from the stage is mi, and he is actually getting, the summation of the outputs that is coming from the last stage, over the clock pulses that is starting from i equal to 0 to the very high infinity value. So, continuously the sequence is getting generated.

we understand that this output a i is having linear recurrence in relation, given by the fact that ck into a i minus k from this sum over sum over k is equal to 1 to the stage number m can generate my output sequence a i. This equation we have established earlier, when we have we have declared and we have discussing the linear feedback shift register architecture. Remember this expression holds good if and only if the clock pulse value exceeds the number of the stages involved in the linear feedback shift register .For i less than equal to m minus, for i less than equal to m, less than m; that means, up to m minus 1 you will get only the output coming equal to the initial stage values stored, initial stage value stored inside the stages.

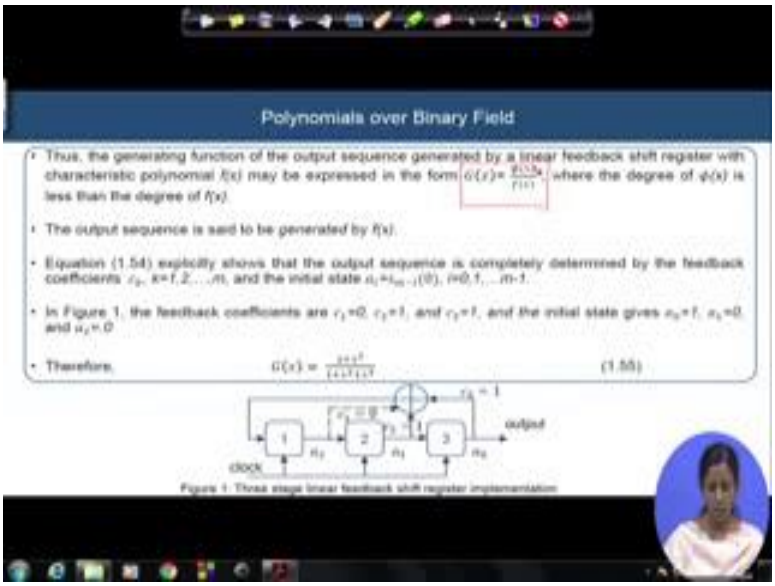
So, now re recap having the remembrance of that fact we understand that this expression i is equal to 0 to infinity is basically having two components. The situation one when the value of i is varying between 0 to m minus 1, where m is the number of stages. Another stage: this process number two where i is having the value from m to infinity. So, the

value of a i for both the cases are not same. For i equal to 0 to m minus 1 it is directly whatever actually, you have stored in a initial stage given by the expression a i x to the power i, but once you are crossing that value m minus 1 from m to infinity he will be governed by the a i will be substituted by this expression. So, we have just broken this initial generating function by this expression.

Now, if I change the order of summation here, I will be ending up with ck and some x k i have taken out. So, this will go x, if say I have taken x k out then that guy will be x a i minus k and it will be x i minus k also. Please check that this will be not x i it will be a x i minus k. Now if I try to see this expression which is written inside, this is basically I can re write in the form of this g x, if I include the term which are coming in between 0 to m, and here i is not exactly i which is equal to i minus k, if I substitute that it will go up to m minus k minus 1 and all those guys will come down to a i x to the power i i is varying from 0 to this zone. So, this is a classic equation that we are ending up here with 1.52, where this is the generating function who will finally help us to generate the final code sequences. Now, if I take the expression, if I clap this expression of the generating function, with that of the initial f x characteristic polynomial I, we have discussed here and if I take the multiplication of this g x and f x.

We will lead here, and with some simple mathematical calculation derivation we will come down to this value, where actually finally, this g x this generating function, it will be an equivalent to this like where this j is replaced by I, it will be given by this expression divided by f x, while deriving this expression you will have to consider that the c 0 is equal to 1 initially, and c 0 is 1 in the throughout the expression , and does I told already mention that this j is replaced by the i. Hence this two are the similar kind of expression that we are getting, and this xi is taken out. So, your expression will look like the generating function in terms of the characteristic polynomial is given by 1.54.

(Refer Slide Time: 18:59)



Now, the key part and the key learning from this expression is. See if the numerator of this generating function is nothing, but another polynomial say ix, and we will if we consider that and then the generating function can be written like g x equal to phi x divided by f x. It is the indication basically that linear feedback shift register sequence, the output sequence can be generated by the characteristics polynomial f x, and the degree, to do that the degree of this phi x should be less than the degree of this f x. This output sequence that can be generated by f x if it is generating function, this characteristic polynomial actually can generate the generating function if you know f x; that is one point, and if you do that actually should there should be the existence of another polynomial, where this polynomial will be completely divisible by this f x in such a way that the degree of that polynomial, is at least less than one degree than that of f x.

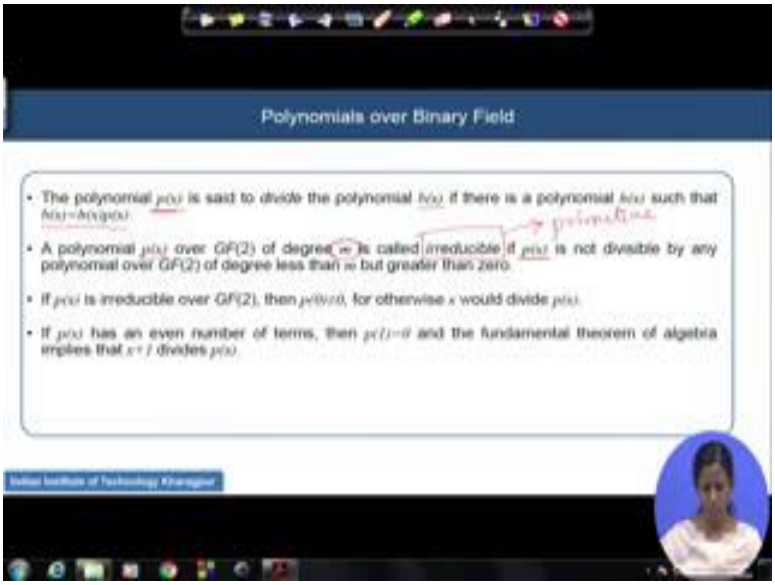
Now, this equation that we have shown in the last slide; 1.54 it clearly indicates, what it clearly indicates that, the generating function or the generating function which is generating the output as well. He is completely describable by you c k values; that means the feedback coefficient logic, and also the initial conditions that are coming up, and we will take a good example to find out how does it go with a practical example. In this figure let us consider a figure where we are having three stages of, to generate the linear feedback shift register clocks are driving the stages, and the c 1 is equal to 0. So, he is not contributing to the feedback logic, but c 2 and c 3 are on equal to 1 and. So, this is a

XOR logic only in the feedback path, where actually the contribution from the output of the two stage number two and the stage number three, they are logically combined to give the feedback to the stage number one.

We understand that if we follow the equation of f x given in the given here. So, my value of the c 1 is equal to 0. So, x to the power 1 is also not existing for that x next to c 2 and x square it will be a term. So, c 2 equal to 1. So, the term will be x square, and the c three also c 1 c 3 is equal to 1 and x to the power q. So, I will be ending up with for f x equal to 1 plus x square plus x 3, which is exactly coming in the denominator here. So, the generating function will be given by, similarly you can put find out the value of the phi x following the equation number 1.54, you substitute there, and this is coming from the expression of this characteristics function f x, which is given by one plus your equation that written earlier; c k and c i into x to the power ii is moving from 0 to infinity.

So, where i is moving from 0 to infinity; so like this actually. Now if I divide these two polynomials now, the generating function will be obviously known to us.

(Refer Slide Time: 22:59)



So, the key understanding is that you need to find out the characteristic polynomial over a Galois field two, to understand that what will be the generating function for a typical kind of the code that we are trying to generate. So, generating function and the characteristic polynomial, they are the two parts, they are the key essential and the true

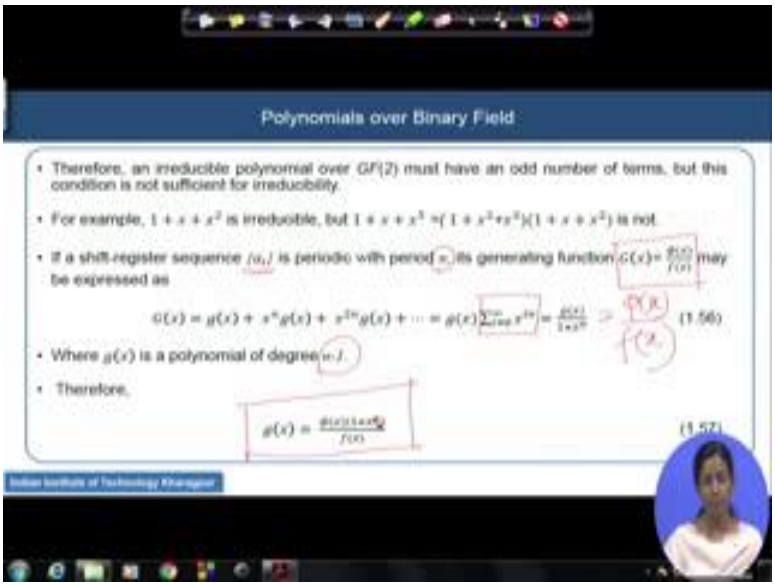
essential parts of generation code generation a for your specific spectrum communication system.

Now, let us go ahead with few more characteristics of these polynomials. So, that we are discussing now over the binary field. Suppose there is a polynomial called p x. The p x is called, it said to be, is said to divide another polynomial b x remember p x and b x both are belonging to the same field, and p x is said to divide b x if and only if there exists another polynomial h x on the same field; such that the b x is equal to h x into p x

So, we understood about the addition of two polynomials over the field multiplication of two polynomials over the field, this is the condition of division of the two polynomials. now think a situation that if a polynomial p x over this Galois field two, is having a degree of m than he said be irreducible, if and only if it is not divisible by any other polynomial who is having some degree less than small m, but greater than 0 . So, why we are so interested about the irreducible polynomial, because we will see that it has some connection later on, with the primitive polynomial.

So, it is required to understand what is the meaning of irreducible polynomial, I repeat (Refer Time: 25:04) polynomial is having degree of small m, and if there is, if it is not divisible by any other polynomial over the same field, who is having the degree less than small m, but greater than 0 , then we will declare that p x is primitive polynomial, it is not irreducible. if it is irreducible over a Galois field two, then it is obvious that if p x is irreducible then it is obvious that for p 0 p 0 is not equal to 0; otherwise that x would have divide this p x. So, for example, if p x, we find that it has an even number of the terms, then the p 1 which is equal to 0, these are the fundamental theorem of the algebra is shows that x plus 1 should also divide the p x, because p x is a at least one even number is that. So, it is not the x, it is x plus 1 should divide p x.

(Refer Slide Time: 26:22)

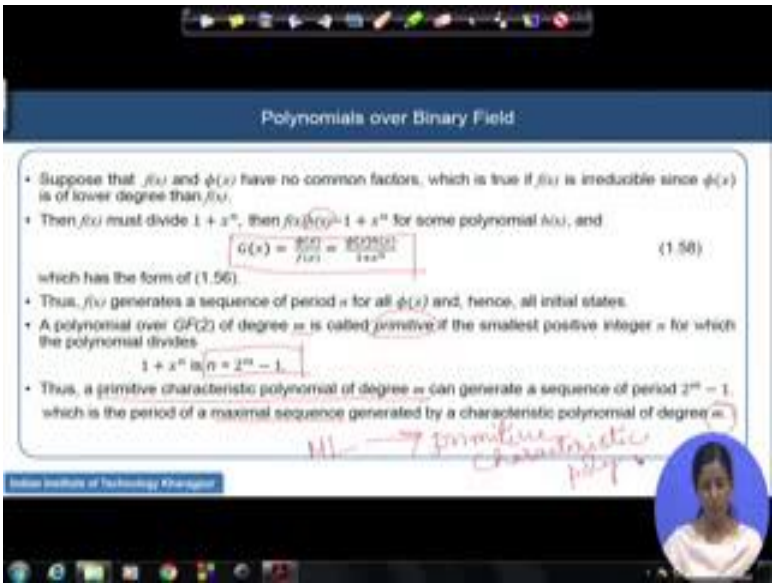


Another important consideration that if p x is having an odd number of the terms, then an irreducible polynomial Galois field should have am always an odd number of the terms, always by default, because if it is having even number of the terms then x plus 1 will divide that polynomial, but remember that it is not sufficient condition to prove the irreducibility. Here is an example suppose 1 plus x plus x x square, they are having the odd number of the terms, but it is irreducible fine, but there is another polynomial 1 plus x plus x to the power 5, we cannot see that, we cannot declare that as it is having a odd number of the terms. So, it is irreducible, because this polynomial is reducible by this two other polynomials.

Hence, by just checking the polynomial is having odd number of the terms, we cannot declare that it is irreducible, but if a polynomial is irreducible, definitely you will end up with the conclusion that it is continuing the odd number of the terms. Now next if I am having shift register sequence a i which is periodic, and which is having a periodic of n, then this generating function that we have just now learnt, which is the form of phi x by f x, where f x is the characteristic polynomial that we can be expressed like this, where actually this g x plus g n x o the power n g x plus x to the power 2 n g x, these are the combination of all this, and where is this and hence it can be written as g x summation of all these x to the power in i is going from 0 to infinity. And what is this? this is nothing a series of 1 by x x to the 1 by 1 plus x to the power n 1 by 1 x to the power n. now if g x is having a, this g x its polynomial should have a degree of n minus 1 obviously.

Therefore if I write down this expression in terms of your, and substitute its value from here then (Refer Time: 28:49) end up with this, this is equal to my phi x by f x, and so small g x will be is equal to nothing, but my phi x into 1 plus x to the power n by f x. This is another important conclusion in the context of the code design. What does it mean you know, that see if f x and phi x there is no greatest common divisor between these two polynomials, and which is obvious not to have, because your phi x is having degree less than the f x. So, you may not be able find the greatest common divisor between phi x and f x.

(Refer Slide Time: 29:43)



If you do not find it, then in order to hold this equation it should happen, that f x should divide 1 1 plus x to the power n. So, with this understanding, when f x is dividing my 1 plus x to the power n, then there must be having in the exist there must exist, another kind of the polynomial, over the same Galois field two say its value is h x, and such that this f x into h x will now be equal to 1 plus x to the power n.

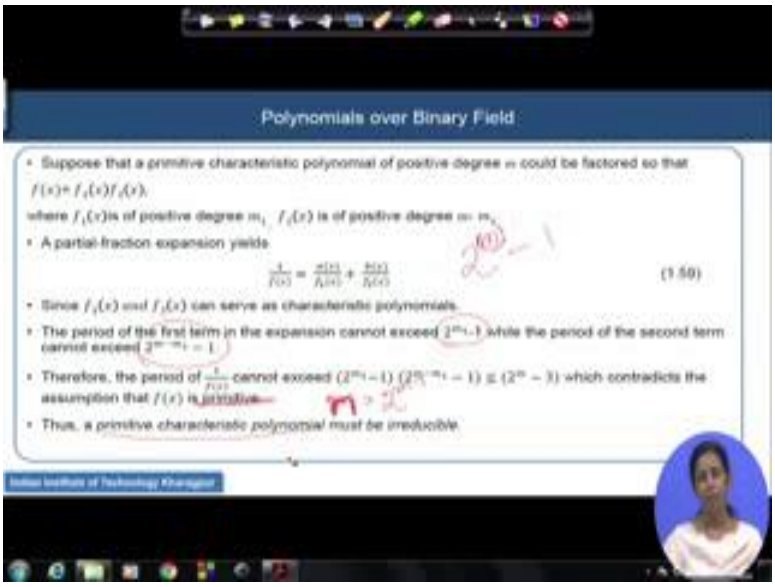
So, if I substitute this value here in the phi x by f x, where this f x is now is equal to my 1 plus x to the power n by h x, and we are ending up with another very nice expression, that the generating polynomial will be given by phi x into h x divided by always 1 plus x to the power n. So, thus this characteristic polynomial effects, it generates sequence who is having a period n for all the kind of that phi x, and hence all initial sates also, it will keep on creating that.

Now, polynomial we is having, we is over the Galois field two having a degree m, we will call it a primitive polynomial for what. if a when the smallest positive integer for which it is the polynomial divides, this 1 plus x to the power n, is given by n is equal to 2 to the power m minus 1, what I said repeat. So, polynomial there; suppose there exist a polynomial over Galois field two who is having degree of small m, and this polynomial has a smallest integer n, for which it is dividing this 1 plus x to the power n in such a way, that with this value of n is related to the degree of the polynomial by this relation.

If this happens then we call that this polynomial is a primitive polynomial. Now remember one thing a primitive characteristic polynomial. It is not a primitive polynomials only, which is a primitive characteristic polynomial also, because characteristic, this is the characteristics polynomial who is dividing 1 plus x to the power n, so this primitive characteristic polynomial of this degree m.

So, it can now generate also a sequence who is having period of small n or equivalent to period of two to the power m minus 1, but we understand that characteristic polynomial who is generating 2 to the power m minus 1 sequence, that sequence should be a maximal length sequence, and that polynomial who generous the maximal length sequence that characteristic polynomial always have a degree is equal to small m. So, it is just opposite proves that a ml sequence, the characteristic polynomial who generates an ml sequence, always is a primitive characteristic polynomial.

(Refer Slide Time: 33:05)



Now, suppose to prove whether these primitive polynomials are reducible or not. In order to check that let us consider that the polynomial of the positive degree m, can be factorized and. So, hence this f x is equal to given by f 1 into f 2, f 1 x into f 2 x. suppose the degree of this f 1 x is equal to m 1 and the degree of f 2 x is equal to of course, m minus small m minus m 1, because total degree is equal to m. If I do the partial fraction expansion then i yields that 1 by f x, will have something called ax by f 1 x plus b x by f 1 x, and they can serve as, both of them serve as the characteristic polynomials individually.

So, hence the period of this first term of this expansion can never have actually a period which goes beyond 2 to the power m minus 1 and whereas, for the second case it can never have a period that exceeds more than to 2 power m minus m 1 minus 1, because both of the m are characteristic polynomial and they are supposed to generate period which is equal to 2 to the power their corresponding 2 to the power m, which is the corresponding degree of the m minus 1. Here 1 is having the degree of m 1, another is having degree of m minus m 1.

So, actually the generated sequence can never have a period more than this and. So, in there for the period of 1 by f x cannot exceed this value. So, if it cannot exceeds this value. So, which contradicts with the assumption ,that is a primitive, because if it is supposed to be the primitive then its value m should be is equal to, its primitive than its order m, then its period, period n generated sequence period n it should have actually 2 to the power m minus 1, or the value the degree of the characteristics 1 plus x to the power n, that n should have a relation with 2 to the power m minus 1, which is not holds good, which is does not hold good, which is not holding good here.

If it does not hold good here, then what the conclusion is the conclusion that the assumption that we did, that it can be factorized is wrong. Hence the final decision is that the primitive characteristic polynomial is always irreducible.