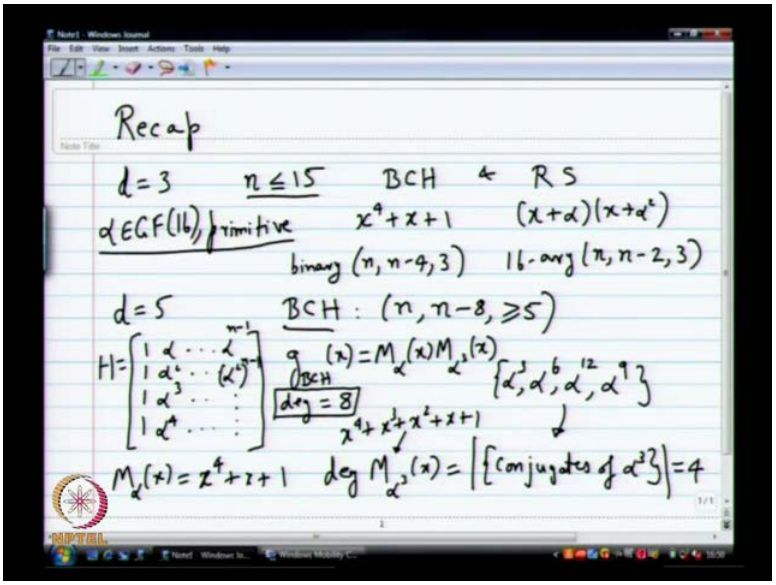
Coding Theory
Prof. Dr. Andrew Thangaraj
Department Of Electronics and Communication Engineering
Indian Institute of Technology, Madras

Lecture - 14
BCH and R S Codes II

(Refer Slide Time: 00:22)



So, let us do very quick recap, basically the last thing we say was d equals 3, n less than or equal to 15 constructions for BCH and resolve. So, basically you got the generator matrix as x power 4 plus x plus 1, here you get x plus alpha times x plus alpha squared and what is this alpha? This alpha is a primitive element in g is 16. So, this k give a n, n minus 4, 3 code, this is binary, so this gives you a 16 ary 15, no not 15 n, n minus 2, 3.

We also a draw two pictures to see what the difference between binary and 16 ary are and what it means impact is how you can think about this is various different ways. So, it is important to know these differences, so by now clearly I think you must have you must have convinced yourself that this generator polynomial means a lot of things about the code. So, it is critically controls all the properties of the code, actually you can, it is an interesting question, the question is does the concept of minimal polynomial.

When you deal with redolent codes in a way, so what is the minimal polynomial of alpha it is x plus alpha because I am allowed to take co efficient from g f 16 itself you can take coefficients from this itself. Then, simply x minus alpha will be the minimal polynomial

always so the same idea holds such that when you insist on coefficients from binary you have to do something. It is certain, it is always x minus alpha x minus alpha square, so for d equals 5 for BCH, what will be the generator polynomial you are going to get?

The rows of H if you want to think of H it is going to be one alpha so on and then alpha square and then alpha power 3 and then alpha power 4. Remember, it is just d minus 1, then it will end, I mean n means some n which is less than 15. So, you just take alpha power n minus n alpha r square rise to the power n minus 1 so on, I am going to leave it like that, so for the BCH, the generator polynomial using our formula is going to be the LCM of the minimal polynomial of alpha times.

Then, alpha square and then alpha power 3 and then alpha power 4, the minimal polynomial of alpha square and alpha power 4 are all the same and that is x power 4 plus x plus 1 what about the minimal polynomial of alpha power 3. This is separate alpha 3, so it is easy to find the degree of the minimal polynomial without doing any Galois field direct matrix. You can find the degree of the minimal polynomial what is the degree, so let us first find that question, so m alpha of x you give me a very simple answer that is correct x power 4 plus x plus 1.

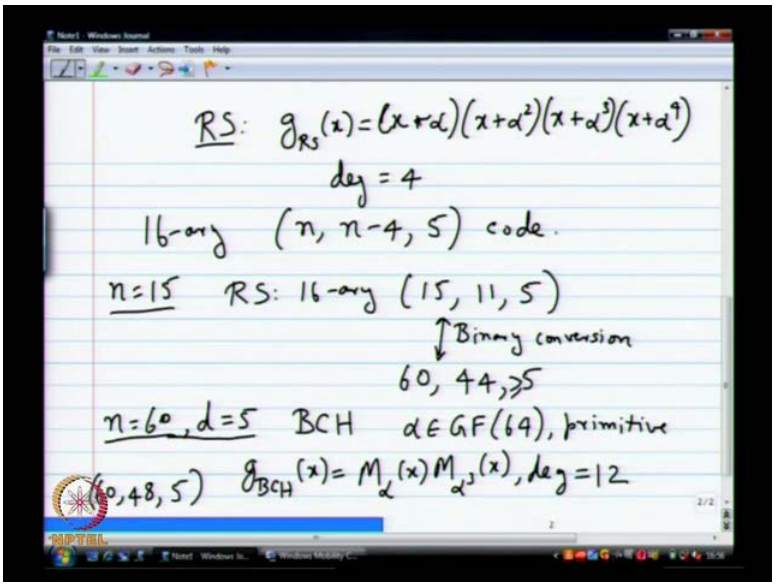
You know the entire polynomial, so degree is 4 what is the degree m alpha power 3 of x, this is basically the size of the set of conjugates of alpha power 3. So, what is the conjugates of alpha power 3 alpha power 3, you have to square it, so alpha power 6 square it again alpha power 12 square it again alpha power 9. Then, you square it again, then you will get 3 again, so the size of that is what 4, how did I get this result that it is the size of the conjugate, you have explicit formula.

For the minimal polynomial, what is the explicit formula x plus alpha power 3 times x plus alpha power 6 times x plus alpha power 12 times x plus alpha power 9. So, you can go back and check that, so that was the result one of the main result of the minimal polynomial take all the conjugates do x plus and multiply. You get the minimal polynomial, so in this case this minimal polynomial will work out to x power 4 plus x power 3 plus x square plus x plus 1. So, that is what this will work out to I know it before hands, so that is why I am writing it down, I did not do the multiplication and figure it out you can do that you will get this answer.

You will get x power 4 plus x power 3 plus x square plus x plus, but even without computing, I know the degree why is that crucial to know that degree. I want the degree of BCH of x, now g b c of x is going to be m alpha of x times m alpha power 3 of x. That is the least common multiple of all those things two different things and they are irreducible and they do not have any common factors etc. So, clearly you have to multiply these two things, so if you know exactly what m alpha of x is and m alpha power 3 of x is then you can do the multiplication and find out exactly what g BCH of x.

Even without finding the polynomial explicitly, you can easily find the degree because I know that the degree of m alpha of x is 4 degree of m alpha power 3 of x is 4, you multiply you are going to get degree 8. So, this is vital information sitting in the middle of all those computation, so once you have that computation the BCH code simply becomes an n comma n minus 8, n greater or equal to 5. I can only say greater or equal to 5, it is difficult to say anything beyond that unless you can explicit show the existence of a weight 5 code word or a weight 5 polynomial. You have to do that computation so that is what will happen in resole men picture much simpler.

(Refer Slide Time: 08:41)



So, it is really easy, what do you do for resole men of x, simply x plus alpha and x plus alpha square and x plus alpha power 3 and x plus alpha power 4. So, clearly degree is 4 and you have a n comma n minus 4 comma exactly equal to 5, so this would be a sixteen ary code remember that. So, just to just to keep things interesting, let us fix n equals 15

and look at the resplendent code the RS code is 16 ary, 15, 11, 5, it can correct two errors. So, what does it mean to say 15, 11, 5 the error correcting capability is to since two simple errors in 15 symbols can be correct.

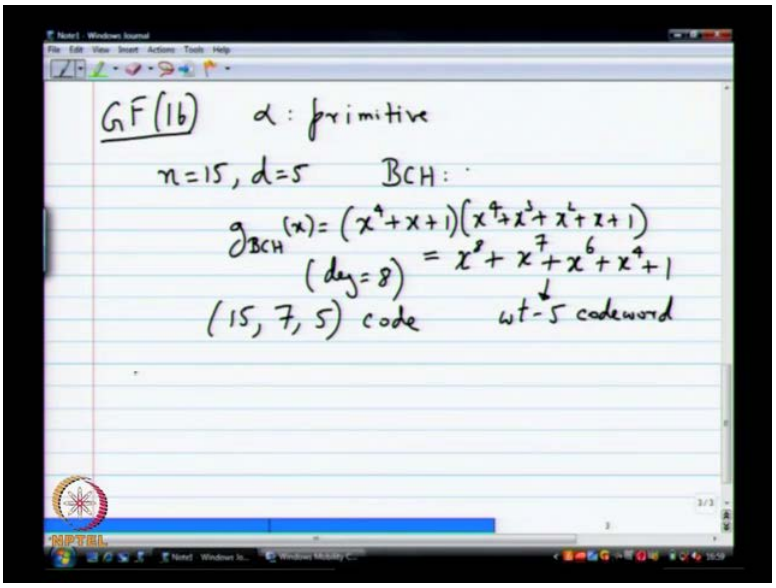
So, when you do an implementation if you do the binary conversion what do you get equivalently, it goes to 60, 44 again 5 well. At least 5, let us say at least 5, so it is five in case it will be equal to 5, you can show that sorry, no it will be greater than i equal to that i as only at least this. So, what is happening here, so this is the kind of situation you will have you will have to process 44 bits of a time put out 60 bits and within those 60 bits you guaranteed to correct any two errors.

So, that is the that is the correct guaranteed thing, so if you start with an n equals 60 BCH code, so what happens n equals 60 d equals five BCH will give you what. So, once again you will start with alpha belonging to g of 64 it is primitive construct everything with that and then what would be g BCH of x it would be the product of two minimal polynomials, minimal polynomials of alpha. Then, minimal polynomials of alpha power 3 of x, you can go through same expression as before you will have four rows in your paretic check matrix alpha square and alpha power 4.

This will have the same minimal polynomial alpha power 3 will be the other one, but what is the degree of each of these case remember that. So, it is 16, so alpha now is in g f 63, I am using the same alpha may be it is not a good idea, but hopefully. You can you can think of it something different it is a g f 64 which is primitive. So, it would have degree equals to 6, so how do you confirm for sure that it has degree equal to 6 m alpha's primitive again.

It is 6 what about alpha power 3, you have to write out all the conjugates you write it out you will see it has size 6, so I will just like we did before, so this would have degree equals 12. So, what is the dimensions that you get 60, 40, 8, 5, it is actually even in this case believe me it will be greater or equal to 5, but you can show that it is equal to 5. So, for the BCH code, you get slightly more if you seen, then the equivalent binary is u after resole men. So, that is the way to put it think it about it slightly carefully, so let us look at this 15, 11, 5, so 60 is little bit more complicated, so let us go back to this picture and I want to look at this code little bit more closely.

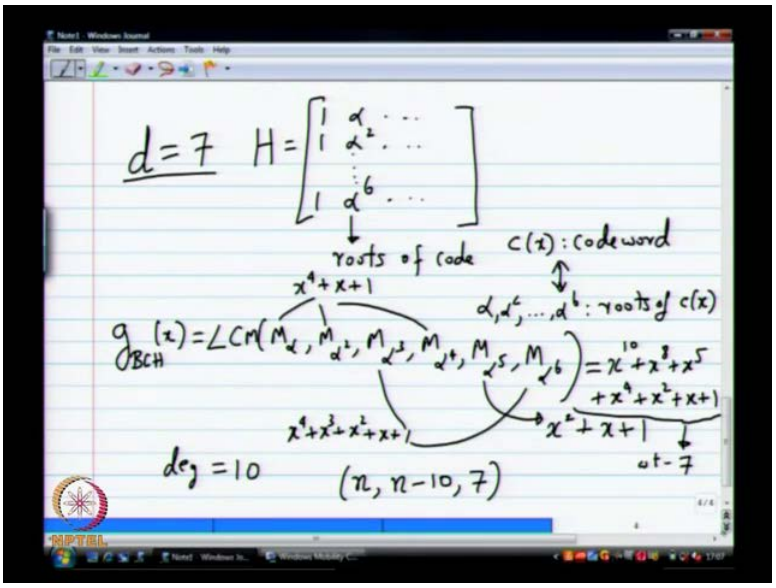
(Refer Slide Time: 14:02)



So, let us come back to g f 16 alpha is primitive, let us fix n equals 15 and d equals 5 and ask for the BCH code, you do that you are going to get the generator polynomial to be x power 4 plus x plus 1 times clearly degree is 8. So, what code I will have will be 15, 7, 5 code, you go ahead multiply this and tell me what you get this. So, simple exercise, but do the multiplication, everything 8, 7, 6, 4, 1, now do you have a proof for the exact minimum distance of this code.

It has to be equal to 5 why there is some staring at you write that, so you have to this you have to this. So, this is weight 5 code word, you give me any other weight 5 code word multiplied by x, it is an interesting, any other x square x plus v. All those things are interesting things, so remember when you multiply by x what you are doing shifting by shifts or what is happening. So, this is a code 15, 7, 5, now let us come back to this same old game we are playing here with this n and d.

(Refer Slide Time: 17:58)



So, let us say we go to d equals 7 that is the next step, so let us go to what is happening, so I think I have gone wrong with the pen, it is gone into a, it is come back. Let us go to d equals 7, so you can once again write down the matrix, if you want, but it is a little bit redundant. I do not have to write down a matrix, you know one alpha is going to be there alpha square, alpha power 3, alpha power 4, alpha power 5 and alpha power 6. So, crucial is what is the first or let us say second column of h, those that tells you exactly what you need to worry about.

So, any way the so those entry are called the roots of the code, but anything it is not so important to us. So, if you write it down you will see the paretic check matrix H would have 1 alpha 1 alpha square so on till alpha power 6. So, from here this column is tells you the roots of the code what do I mean by routes of code, so basically what it means is if you have a code word c of x if and only if alpha square so on till alpha power 6 are routes of c of x.

So, that is why that column is called the routes of the code, so if you think of your code words are a polynomial all those entries in those columns are routes of the code word polynomials. So, it is called routes, so any way the routes are important, so given a d you can simply list the routes once you list the routes the g. Also, you can write down generator polynomial, basically LCM of what m alpha m alpha square m alpha power 3

m alpha power 4 m alpha power 5 m alpha power 6. I am writing x, so compact these three guys are the same, they are basically x power 4 plus x plus 1.

What else can we say what about alpha 3 and 6, also will give you the same polynomial, so that will give you the x power 4 plus x power 3 plus x square plus x plus 1, what about alpha power 5. So, first of all the degree is important degree, you can quickly find without doing any Galois field arithmetic, so only have to look at the conjugates what are the conjugates of alpha power 5, alpha power 5, alpha power 10 and then it comes back to alpha power 5.

So, it is just the degree is simply two from that you can easily find out what the minimal polynomial will be why is 2 right degree and it is irreducible all minimal polynomials irreducible. So, it has to be x square x plus 1 right that is the only irreducible polynomial in binary right x square plus x plus 1. There is nothing else right that has to be x square plus x plus 1 degree 2, you can find very easily I mean this you can find what the LCM of all these gates is. It is simply the product of these three polynomials, so that will work out to something, so in general degree is going to be particular degree is going to be 10.

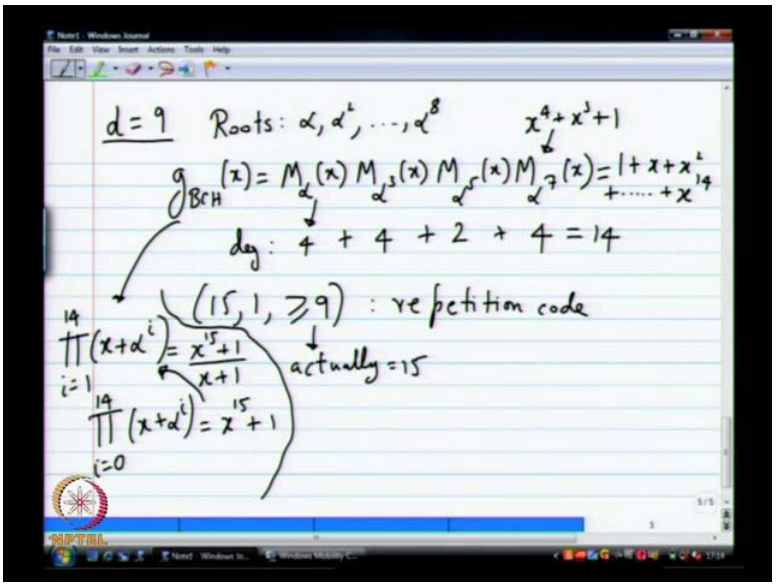
So, I want you to go ahead and do that multiplication and tell me what this polynomial is it is easy, I mean you have already done the part of the multiplication. You only have to multiply with one plus x plus x square, so let us see what will be the final answer n 8, what else this is it, so even all these information what the various parameters of my code are.

I have n and then I have what is dimension n minus 10, so clearly this code is meaningful only when n is at least n. So, you cannot have n smaller then n whether n is you cannot have d equals 7, so that is what it means if you want d equals 7 should have n at least n. So, n equals to 15 is the good thing to have, so think of it as 15 and 15 minus 10 and then what about minimum distance, what do I know it is equal to 7 if there is there is weight seven code words, so this guy is the weight 7 code words.

So, if you specifically if you pick n equals fifteen you would get 15, 5, 7, so I can also write down the corresponding resole man code, how will that look is something you can write down. I am not going to do it is very easy the resole code is easy, what will the generator polynomial alpha square so on till be x plus alpha power 6. It will be n comma

n minus 6 comma 7 code, you can do the BCH comparison and find out how many more bits the BCH gives you if you get some similar answer the next thing is d equals 9.

(Refer Slide Time: 24:56)



Let me give you about 2 3 minutes to scribble something in your note books and then I will write down the final answer here same thing. I am not changing, so instead of writing out the paretic check matrix, I am simply going to write out routes what are the routes alpha square so on till alpha power 9. These are the these are the routes, so if you want to write out g BCH it will the LCM of all these things, basically if you look at it very closely it is m alpha of x times m alpha 3 of x times m alpha power 5 of x times alpha power 7 of x. So, this is got degree 4 if you count the degrees this is got degree 2 power 4, I am sorry 2 4 for 7.

Also, you will get 4, you get 7, 14, 13 and 11, so 4 that works out to 14, so basically you are expecting of 15 comma 1 greater than or equal to 9 code. So, I know where better 15 comma 1 got, this is what the reputation got, so in fact it will turn out that this is also the reputation. So, what will happen when you actually do the multiplication, I told you all the other minimal polynomials this guy is x power 4 plus x power 3 plus 1. You can take the previous one and multiply with this you will see that you I will get 1 plus sorry once again there is you will get everything you will get 1 plus you will get 1 plus x plus x square plus so on till x to the power 14.

So, you will get all the powers of x plus x square plus x power 3 plus x power 4, you can test it out if you like you will get this so in fact what is the minimum distance of this code actually 15, do not just go by the weight of the generator polynomial. In this case, you can I mean there are some exceptions to this rule, be very careful happily, I mean there are reasons why we got those answers here it works out it is actually 15. You have basically the reputation code you cannot any other n, so you cannot n less than 15, it does not make any sense, you have to take only n equals to 15.

So, you get 15 comma 1 comma 15 code, so there are also several other ways of quickly seeing that this product has to be equal to this how do you see that the reason is this g BCH is basically worked out to product x plus alpha power i, i equals 1, 2, 14. I know this product i equals 0 to 14 x plus alpha power i is what is x power 15 plus 1 minus 1 or plus 1 x power 15 plus 1. It is actually usually you multiply with x also and say it is x power 16 plus x, so you do not include x you go to x how do I go from here to here i equals 0 which is the x plus 1 term.

So, I have to simply divide x power 15 plus 1 by x plus 1 and that will give you that answer it is like g p formula plus and minus, you will this is another way saying how this answer is not very surprising. If you come in a come along the wrong direction, it may be surprising, but in right direction. It is very simple answer, so people have done this kind of exercises for all Galois fields not just 16, 32, 64, I mean it is not a very difficult exercise the algorithm is really simple. If you only interested in the degree, but if you also want the generator polynomial it is a little bit more work, but if you pick up a standard book in coding most probably towards the end at least a older books linen costal instance.

So, it will have a table of all generator polynomial so you can go there and look it up then you get the answer. So, you do not have to do this work yourself, but finding the degree like I pointed out is a trivial task, you can do it very easily, so n and k you can find and the bound on the degree. You can find on that the minimum distance you can find, but if you want the accurate minimum distance and all it is a lot of work, but even if you want a generator polynomial. It is some work to multiply the polynomial can get some answer one more thing.

I want to warn you this thing of looking at the generator polynomial and finding the minimum distance is special it does not happen all the time there are exception and a very notable exception, but in many cases that is a good rule that is a good starting point. There are exceptions also be warned of that it is not always a it is not a full proof methods of ending minimum positions. So, I can also write this is most interesting is many computer memories and other things hard drives what code would be what 200 and 55 comma 239, 17 code and we have a really compact description of this code generator matrix gives you a complete description.

So, let us do the binary conversion you will see that this is impressive you will be a little bit scared it is not so easy to do this, suppose you do a binary conversion what do you get here 2040 this would be what. Somehow 2,000 is strict in my head does the memory I mean it is correct the multiplication; you are all starring at it like what is this. So, it is easy to can subtract also, 16 times 8 is what you have to subtract what is 16 times 8, 20, 8 divided by subtract from here that should be 1, 9, 1, 2 and then greater than or equal to 17.

Let us say its equal to 17, so this is after the binary conversion just pause for a second to think of this object what is this code, I am now dealing with the binary vector space with dimension 2040 bits sequences, how many of them are there 2 power 2040. So, it is probably bigger than the number of electrons in the universe itself, so it is huge from that huge set. I am able to give you how many 2 power 1912 and once again a huge number, you cannot even fact them how big that number is, so it is huge 2 power 1912 vectors. I can tell you I can give you very compact description for each one of those not just some very rare thing that there exists or something.

I can give you exactly how to generate each and every one of those, so that too very simple polynomial multiplication method and what am I guaranteed that any two vectors differ at least in 17 bits. If I told the beginning the class, you will do something like this you might not have believed right today you know how to do this. So, there a quite non trivial task, if you think about it this huge number of vectors, you can find another huge sub set or sub space be specific any two vectors in that space are at least 17 bits.

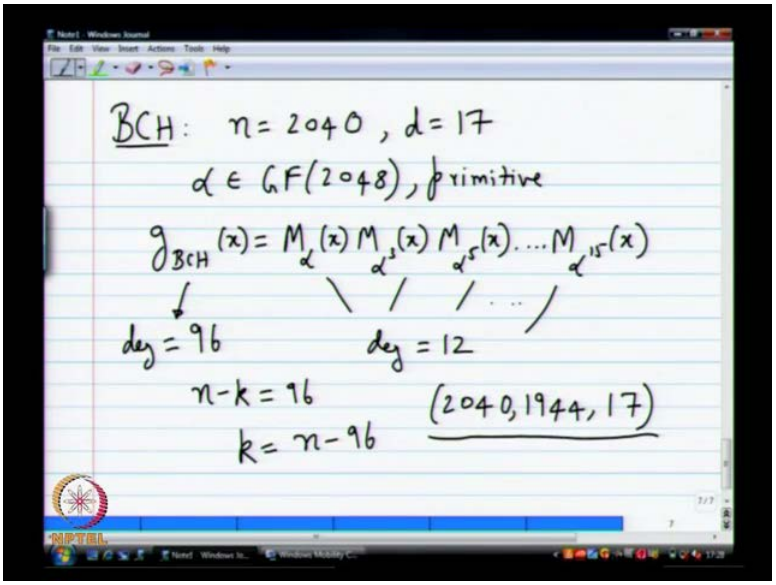
So, that is how where a 2 power 12, so you have to go 2048 m equals 12, so this 2048 BCH codes are also quite popular in quite a few application mostly preparatory

application people use these codes. You can see it is it is powerful see for a long time also velocity technology was not so advanced, so g f 256 was kind of the limit that you could go today. You can go to like g f whatever two part well is nothing, you can go 2 power 20 if you want right it is not it is not much of a limitation from real message.

So, people are going to larger and larger field and when larger and larger fields are possible you know it is to for an advantage, you to go to BCH code, we will be seeing that all along. So, instead of doing resole man if the only problem is not being able to go to a larger field, then you can just go to a larger field and get better efficiency for the same minimum distance or other way around same efficiency get larger minimum distance. So, let us try to ask the same question for 2048, now again g f 2048, this is a scary big field, but you it is not difficult in real today.

Remember that even in software you can write like a program which will do operations in g f 2048 and do encoding and decoding very fast. I mean it is possible it is not so difficult, so it is not so scary today but in the class room it is a bit scary when I say g f 2048. You will see without doing too much you can quickly find a linear n and k for BCH even for 2048, you do not all you have to know is multiplication and modular.

(Refer Slide Time: 40:17)



You can find the dimension very easily, so let us do the same thing with BCH, let us say we say n equals 2047 so you can 47. So, as well go to 47 and d equals 17, it is a bit weird it is a bit more difficult, it was computation, but I want to keep the same. I will give you

a simple argument for we can do it not worry about it, so d equals 17. So, you have to have an alpha which is in g f 2048 which is primitive and then what will happen to my g BCH of x what are the routes the routes are alpha through alpha power 16 alpha square all the way alpha power 16.

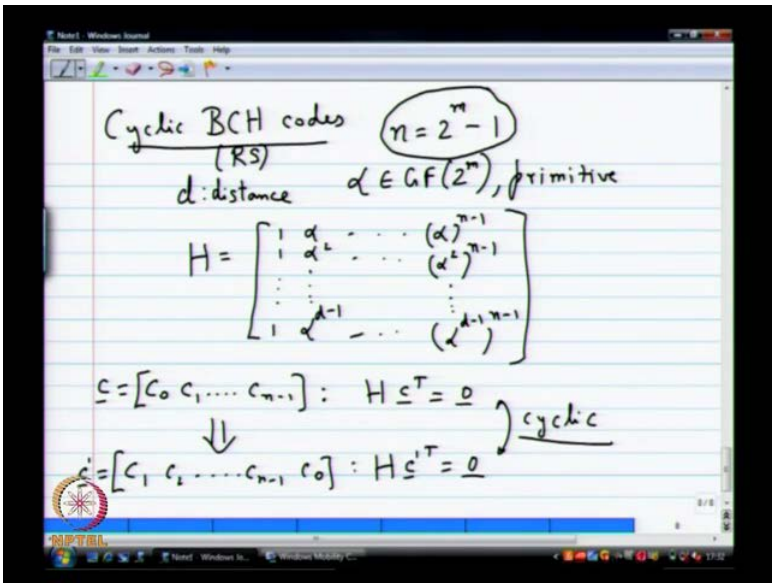
So, g BCH will be the product of m alpha x alpha power 3 x alpha power 5 x so on till alpha power 15 x assuming all of them are distinct believe they are distinct. So, you believe me or not you do not believe me if you do not believe me you have to prove me wrong. I know none of you are going to be ready to that it is easy. You know I mean at least conceptually, it is a very trial thing to check these things, I do not have to worry about the even powers of alpha why they are covered in odd.

All the odds will be distinct in this case, I think quite sure if you want you can go and check the distinct and in fact all of them will have degree equal to any two code words will have at least 17 bits. So, the advantage with resole man code is about a four bytes or something 32 bits, so finally when you get when you do all these it is you see the simplicity of the whole thing to know exactly why everything was known. You need a little bit of math and all that, but ultimately it is really quite simple what you need is only multiplication and addition integer multiplications inter addition.

I did not do anything beyond that and like I said today you go to mat lab mat lab will give you all these polynomials and you can ask it to multiply and you will get the generator polynomial. Then, you can implement the n code, you know exactly how to do it, so it is very simple to come up with BCH and resole man codes any questions.

I think everybody is busy thinking, there is question the most important question, now we can encode we can do 2 power 2040 to power 1914 all that is impressive, but what do you do at the decode. So, that is the most crucial and difficult problem, if you think about it right the encoding was tough we did not know how to generate codes with arbitrary minimum distance. Now, we know how to do that any error correcting capability we can come up with linear codes.

(Refer Slide Time: 47:42)



You can come over paretic check matrices, no problem you know that, but equally important is the problem on the other side. It is been quite something since we set the de coder the last time we visited that was syndrome d code. That is the idea that we say, so we saw that syndrome decoder is complex, it is not quite, so simple if you want to correct many errors it is complex.

So, that is the part which is a little bit more non trivial, so let me let me may be do, so the next class which is tomorrow. We will pick up from here and do the decoder in some more serious thing, but should I point out anything more the only thing. I want to point out in the next 2 minutes that we have left is the following. So, one of the properties there is a special cyclic BCH code, so usually when people say BCH codes they always mean n equals 2 power m minus 1.

So, this is the standard convention for BCH code you will always n to be equal to 2 power m minus 1, so in this class you have been saying n can be less than 2 power m minus 1, but usually n is taken as equal to 2 power m minus 1. You take alpha belonging to g f 2 power m to be a primitive element, and then you define a paretic check matrix suppose designed distance is d.

You go ahead and does this alpha square alpha power d minus 1, I let you complete it you know what it means then the final thing would be alpha power n minus 1 alpha square power n minus 1. Remember, n is equal two power n minus 1, so again resole

man codes also, also resole man I said BCH, but resole men also when n is equal to 2 power m minus 1, both of them have the same paretic check matrix. What you can show is this cyclic property what is cyclic property, if you have a vector c which is let us say c 0, c 1 to c n minus 1 is if it is such that H times c transpose 0.

Then, this implies if you look at this vector, let us say shifted left by one position, but make it cyclic shift in this 0 all the way the other side. This will also satisfies, let us say this is c prime this will be c prime transpose will also be 0. So, this is the cyclic property of these codes and it is valid only for n equals 2 power m minus 1. So, the other n clearly it is not be valid, but n equals 2 power m minus 1 where people study cyclic codes in detail then approach BCH and resole men codes.

From that angle, if you take the book for instance, I am pretty sure that is the angle that the view should be, but somehow I like this thing of giving paretic check matrix. Then, going finally and showing that any way guess what this is also cyclic both approaches are possible encourage you to read this second approach. Also, in the book for instance book by linen coastal read that and you get some interesting ideas, we will stop here break up.

Thank you.