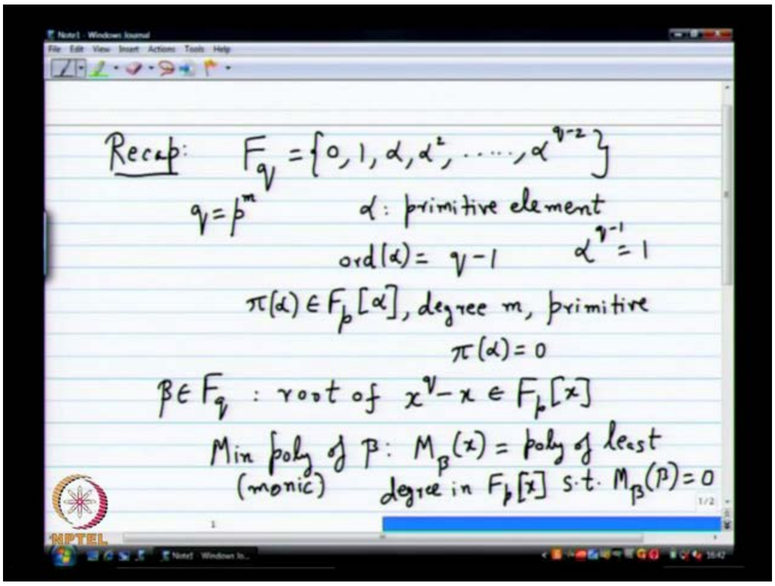
Coding Theory
Prof. Dr. Andrew Thangaraj
Department of Electronics and Communication Engineering
Indian Institute of Technology, Madras

Lecture - 12
BCH Codes

(Refer Slide Time: 00:16)



Recap: $F_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$

$q = p^m$ α : primitive element

$\text{ord}(\alpha) = q-1$ $\alpha^{q-1} = 1$

$\pi(\alpha) \in F_p[\alpha]$, degree m, primitive

$\pi(\alpha) = 0$

$\beta \in F_q$: root of $x^q - x \in F_p[x]$

Min poly of β: $M_\beta(x)$ = poly of least (monic) degree in $F_p[x]$ s.t. $M_\beta(\beta) = 0$

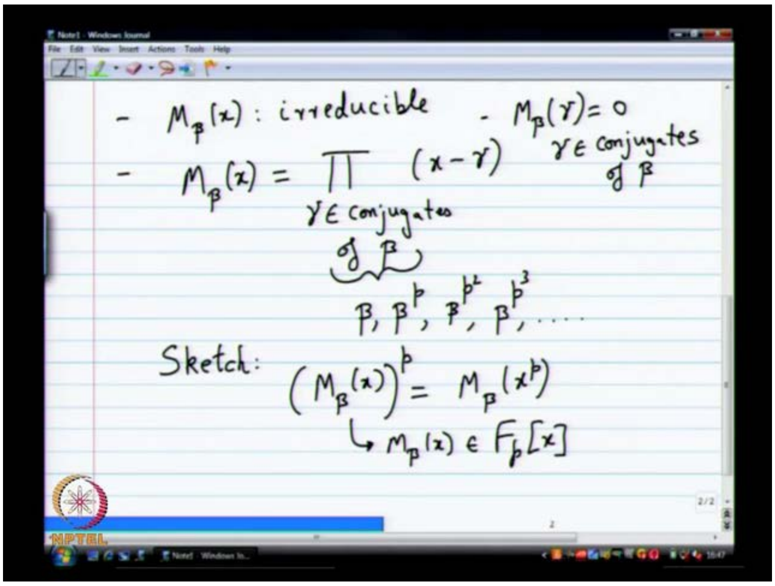
So, let us begin once again with the recap slightly longer recap, so we been talking about this finite field with q elements q is p to the power M and we know it can be written as alpha power q minus 2. There is one primitive element alpha is called primitive element so the multiplicative order of alpha is q minus 1. That is the property and what else to be known. So, alpha power q minus 1 is equal to 1 and then there is a primitive polynomial F alpha which is in F p alpha right and the degree m.

This is called as primitive and in this field pi of alpha would be 0, so that is one of the properties that alpha satisfies. So, once again do not ask what is alpha something which has all these properties and lets you do computation with field of q elements. So, it is all tied into together like that and then the latest thing we saw was this motion of minimum polynomial. So, we defined the minimum polynomial as something what it be defined a minimum polynomial would be, so if I have a beta in F q, I know for sure that beta is a route of route of what x to the power q minus x which is a polynomial with coefficient in F p.

So, I know there is some polynomial with coefficient F p for which beta is a route the question that the minimum polynomial tries to answer is what the minimum polynomial of alpha polynomial of beta. So, we need a notation for it, so I simply call it as M beta x capital M for minimal M beta x is the polynomial of least degree n F p x such that what M beta of beta equals 0. So, those points that Avinash was making that this does not quite uniquely define it why does not that uniquely defined polynomial.

So, I could take this M beta of x and multiplied by some element from F p say 2 or 3 or something, then I would still get a polynomial of least degree with these being beta as a route. So, you have to say something about the leading coefficient, so very standard to do is to say that this polynomial is monic, so that also should be there. So, monic is part of the definition, what does monic mean, the coefficient of the maximum degree term is 1, so that is the idea and this monic, so lot of interesting properties for M beta of x some properties.

(Refer Slide Time: 04:36)



- $M_\beta(x)$: irreducible
- $M_\beta(\gamma) = 0$ $\gamma \in$ conjugates of β
- $M_\beta(x) = \prod_{\underbrace{\gamma \in \text{conjugates of } \beta}_{\beta,\ \beta^{p},\ \beta^{p^2},\ \beta^{p^3},\ \ldots}} (x-\gamma)$

Sketch: $(M_\beta(x))^p = M_\beta(x^p)$

$\hookrightarrow M_\beta(x) \in F_p[x]$

I wrote down M beta of x is irreducible, so that is the first property, so reducible because if it were to be irreducible and you can write it as a product of two factors at least. Then beta would be a route of one of them at least one of them and then that would be polynomial of lower degree which would violate the least requirements. So, that makes it irreducible, what else did I write down, I must have written down some other properties, so that is something we come to later, so this let me write that down, then we will proceed.

So, we wrote down in fact an explicit formula for M beta of x, so this is going to be product of gamma conjugates of beta x minus gamma. So, what are the conjugates of beta, it is basically the set beta power p and then you rise beta power p to the power p. So, you would get beta power p square, and then you would get beta power p power 3 so on. This will repeat, so wherever it repeats, you just simply stop, you do not include the reputation also; it will come back to beta 1.

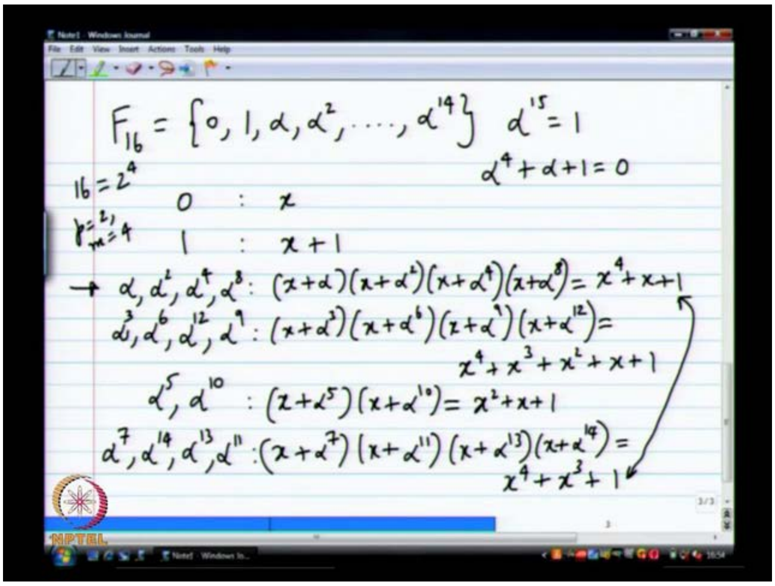
So, it stop where ever it repeats, so that is the that is the way you define conjugates, so I promised some kind of a pseudo proof, so it is the basis idea is to show. So, I will just simply sketch the proof, I do not want write down a proof like I said the books I am showing will have a proof. You can go look at it, I will sketch the general idea, so you will get how it works, so the basic idea is to do something like this, you can show M beta of x whole thing rise to the power p would work out to M beta x power p.

So, it is not too hard to show when you rise this to the power p something like this will happen, p is when you can think of in order. There will be some issue to take care of when you look at minus 1 bit p is mostly odd, only even prime is 2 and with 2 minus 1 or plus 1 does not matter. So, it is all the same, so you will get, you can show this quite easily, not quite easily, let me say with some work, you can show it. So, once you show this, you can argue from this that M beta of x belongs to F p x assume the coefficient of M beta x will be F p.

That is the main idea once you get that M beta of x has to be the minimum polynomial why is that because one of the other property is of M beta of x which I wrote down before I came to this was what M beta of gamma 0 for gamma being conjugate of beta. So, if I take any power of p power of beta and plug it into it is minimum polynomial that also has to be a route that is got to do with the way coefficients of M beta of x. So, all these have to, I mean they are all related, there are some dangerous sick lick kind of arguments here which we have to avoid very carefully.

So, it works out quite easily to be true, so there are other ways of proving this, you will get the answer. So, we also check this by example you know and I think for F 8, I asked you to check the example and for F 60, I wanted you to do it at home, I would not ask you to rise your hands if you did at home, but I believe that at least some of you tried it. It is a good exercise to try and convenience yourself, so let us do it real quick for F 16, I know the answer I have obtained.

(Refer Slide Time: 08:52)



$$F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\} \quad \alpha^{15} = 1$$

$$\alpha^4 + \alpha + 1 = 0$$

$16 = 2^4$

$p = 2, m = 4$

$0 : x$

$1 : x + 1$

$\rightarrow \alpha, \alpha^2, \alpha^4, \alpha^8 : (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) = x^4 + x + 1$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9 : (x+\alpha^3)(x+\alpha^6)(x+\alpha^9)(x+\alpha^{12}) = x^4 + x^3 + x^2 + x + 1$

$\alpha^5, \alpha^{10} : (x+\alpha^5)(x+\alpha^{10}) = x^2 + x + 1$

$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11} : (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14}) = x^4 + x^3 + 1$

So, I will just write it down without doing too much work so F sixteen is what is clear finite field its sixteen elements so you need a primitive element which have a order fifteen and then. You can take any primitive polynomial, this is one of them there is only one, other you can take for degree 4, we will just take a, so this is F 16. So, the way you have to do conjugates is you simply start at 0, 0 is very easy, 0 what are the conjugates of 0, just 0, nothing else. The minimal polynomial is very easy to write down what is the minimal polynomial is x and for 1 x minus x plus 1 plus 1 or minus 1 does not matter because characteristic is 2 and minus 1 is same as plus 1.

So, this is for 0 and 1, so beginning with alpha, you will have a non tribunal set of conjugates alpha, then what would be the next conjugate alpha square next one is alpha power 4, next one is alpha power 8, next one is alpha. So, we can stop there that you can stop, so these are the four conjugates, so the minimum polynomial for alpha will work out as x plus alpha and x plus alpha square x plus alpha power 4 and x plus alpha power 8. If you do the computation here, if you multiply look out what happens is the coefficient etc, you should get what x power 4 plus x plus 1, so this was done by you know the polynomial is alpha power 4 plus alpha plus 1. So, if you get the answer quite obviously, so it will work out too much, so next what you have to do is you have to look at what terms you have missed out here to find other minimal polynomial.

There is no point in looking at alpha square again, why is there no point in looking at alpha square again, you will get the same set of conjugates, so you do not have to repeat that once again. So, you can go to alpha power 3, what would you get next, so 16 is 2 power 4, so that means p is to M 4 M does not matter, but p is 2, so you have to rise the previous thing to the power p which means you have keep squaring. So, we will mostly in this course look a characteristic too, so do not worry about d being something else rather than 2, simply take d is 2 always square.

That is the rule to keep in mind always minus 1 is same as plus 1 will very rarely will be ever go out of characteristic 2, so let us say what would be the next one alpha power 6 alpha power 9, alpha power nine comes later. So, do not write with so much of own sight, I think we are into trouble, let us do alpha part well, next alpha power 9, then you have to multiply it out. So, if you do this calculation I know the answer of this calculation, but for those who do not know, it is a little bit more difficult to do. You will get this answer, so x power 4 plus x power 3 plus x square plus x plus 1, so that is the minimal polynomial corresponding to alpha particles.

So, you can check a lot of those things, it is irreducible, so it is one of those irreducible polynomial and you have to do some checking to figure out. This is this is irreducible, so you can plug in 0 plug in 1 and then you also have to divide by x square plus x plus 1. So, once you see that none of those things divide, you can control that is the irreducible, what is the next term that I can look at, alpha power 5. So, what about conjugates of alpha power five, alpha power 10. So, it is only these two, now who is going to tell me without doing the multiplication what is irreducible polynomial has to be, it has to be a x square plus x plus 1, you know it is a binary polynomial, you know it is irreducible.

So, degree 2 and that is just gives you one possibility you do not have anything else, so this has to work out to x square plus x plus 1. If it is not, then you are making some mistake and then competition, so you can go back and check that, so here is one more thing which is interesting about these finite fields. So, if you look at the complex field as an extension of the real field every real number, I mean how many conjugates can a complex number have, it is either 1 or 2. Either, its elements is its own conjugate and in this case its real or it would have one other conjugates, so here you are seeing more interesting situation elements can be its own conjugate.

Then, just that is the end of story or it can have multiple number of conjugates, you can have 4, you can two all kinds of interesting situations happen in finite fields. So, what is the next thing alpha power 7, 14, 13, 11, so once you do a lot of coding theory, all these sequence will be automatic. You know you just know exactly what has to happen, but first time you see it, you will be thinking what is going on, so this is 7, 11, 13 and 14 other conjugates. You can once again do the multiplication what do you think the answer will work out to, so there is an interesting way of doing this. If you do not notice, you can do you can put x equals x inverse in the first equation that I have here.

Then, you do some manipulation, we will see that this is basically the polynomial with the coefficients flipped around inverted. So, we will see this will be x power 4 plus, sorry sometimes this touch pad is a bit a little too sensitive x power 4 plus x power 3 plus 1. So, it is basically between these two polynomials, you put x equals x inverts and then multiplied by x power 4, so what it does in effect is you have a set of coefficient like this. You simply flipping it around that is what that does you might have studies some kind of something like this in DSP or something may be so simple little operation.

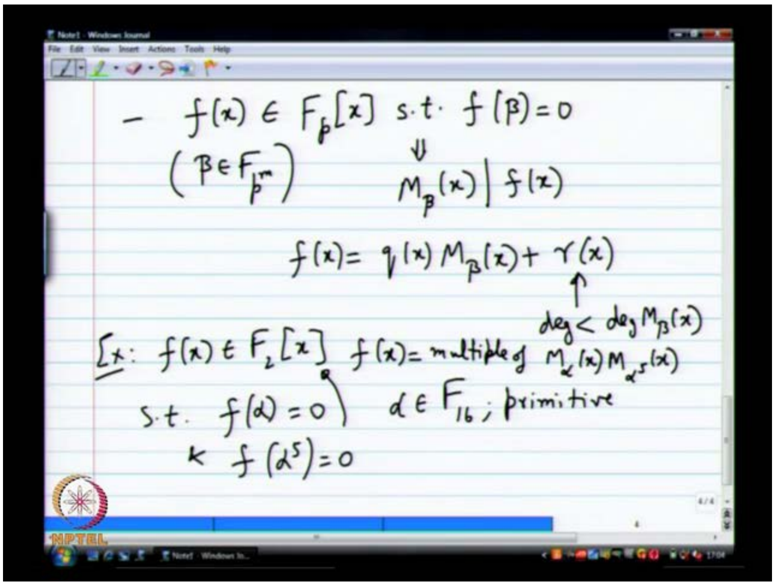
It is just a flipping around of things, so that is it, those are minimal polynomials of elements in elements in F 16. What will I get if I multiply all these minimal polynomials together x power 16 plus x, so you would get that, so that is also something we saw in last class. So, lot of queries results are true which we will not prove in this class, it is not too difficult to prove also, but we would not prove it for instance. If M is 4, the only degrees of minimal polynomials can be 1, 2 and 4, so basically the degree of minimal polynomial has to divide the exponential. It has to happen, so if you do some competition and you see you got the polynomial, minimal polynomial of degree 3 and M was 4.

It means you have made a mistake, so go back and check that something you can use in your examination if you like. So, the degree of the reducible polynomial you get as a minimal polynomial has to divide M and there has to be at least one which has degree equal to M. Also, you cannot have M not occurring, M will definitely occur and sorry that it will come whatever polynomial you use for generating the field. That itself will come, definitely there is lots of certain logics in using things careful way in which you have to build it, but these are results that are true.

You will get something which is degree 4 etc, so beyond that it is really difficult to say what it will be you know when you can get some reducible polynomial. Also, all kinds of results about in fact all the reducible polynomials of degree M will definitely show up in this list. There are also interesting things about this minimal polynomial, anyway that is not relevant for the course, but it is good to know these results, 1 plus 1, 2, 10, 12.

If we did not get x power 16, I made a mistake, theory is correct, you have to get x power 16 plus x, so I do not think I have made a mistake. Here, it works out correctly, so let us let us stop it with these minimal polynomials, so there is one more result I have to give you, I am sorry about that, so let us just finish that final result and then we will go other.

(Refer Slide Time: 18:58)



– $f(x) \in F_p[x]$ s.t. $f(\beta)=0$

$(\beta \in F_{p^m})$ $\Downarrow$

$M_\beta(x) \mid f(x)$

$$f(x) = q(x) M_\beta(x) + r(x)$$

$\uparrow$ deg < deg $M_\beta(x)$

Ex: $f(x) \in F_2[x]$ $f(x) =$ multiple of $M_\alpha(x) M_{\alpha^5}(x)$

s.t. $f(\alpha) = 0$ $\alpha \in F_{16}$; primitive

& $f(\alpha^5) = 0$

So, if you have a polynomial F of x which belongs to F p x such that say F of beta is 0, so remember beta is some element of F p power M. So, if beta is the route of some polynomial with coefficients in F p, then you can show without too much effort that M beta of x will divide F of x. It is not too difficult to show, you can show using several arguments, one very theoretically appealing argument is to divide F of x by M beta of x. Then what would you get if you divide F of x then M beta of x, you get q of x and then I remind a r of x, what would be the degree of r of x strictly less than degree of M beta of x.

Now, what can I do to claim my result, put x equals beta what happens to the left hand side goes to 0, what happens to the first term 0 goes to 0. So, what should happen to r of beta, go to 0 and that does give you any violation, it cannot be, you do not have degree of less than degree of the minimal polynomial that gives you violation.

This is one way using the division algorithm to prove it, another way to prove it is say if F of beta is 0 F of beta power p is also 0, so why is that you simply rise F of x to the power p and you will get the same answer. So, coefficient do not change, so it becomes x power p, you can use that to claim the result F of beta power p is also 0 and then a minimal polynomial is any way the product of all the conjugate. All these terms are they do not have any common factors, so when you multiply it out, it also has to divide F of x.

So, that is another way of arguing in, but this is also need little argument, so this is a little bit crucial because we will use this argument in our code construction. So, we will say try to start the little bit and make sure you understand what it means, so for instance if I have a polynomial that binary coefficients. Let us say F of x is an F 2 x and then I say F of beta 0 for some beta in F 16 such that this is true. Here, is an example just to illustrate say F of x is non zero for resistance, then what can I say about F of x, what can I say is there any information I can get about F of x.

Let us say beta is some, I do not know beta, let us say alpha is a primitive element, and so let me be a little bit more specific. So, that we get something more concrete out of it, so primitive element. So, what can be the degree of F of x, it has to be a at least 4, do you see that, so it cannot have degree 1 degree 2 and all it has to be degree at least 4, reason is the minimal polynomial of alpha which I know is the degree 4 polynomial has to divide F of x. It means F of x has to be multiple of that, which will have degree at least 4.

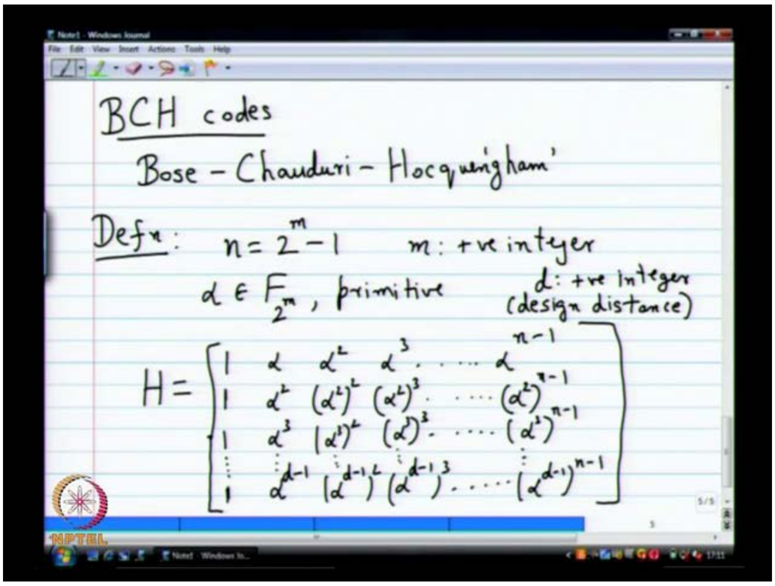
So, this is a interesting kind of idea if you have one route from a large field which is an extension of your field of coefficients. Then that one route means there are several other routes also from that same field, it is like saying if you have a polynomial with real coefficients, it has one complex route and it should also have conjugate as the route. So, this is just a small extension from real to complex, so have just 2, but when you have from F 2 to F 16, there is a large extension.

So, larger than 2 at least 4, so when you have one route, you can get up to three other routes depends on alpha. So, for instance if F of alpha power 5 is 0 and it can even be degree 2, it is a guaranteed one, another if you say, but if you say F of 1 is 0, then it can be anything. So, that is the idea, so very often we will also use this argument in reverse ways, so suppose I say both these things are true, so what should happen to F of x F of x has to be of the form some multiple of M alpha x times M alpha power 5 x.

In fact I should be a little bit careful here; we should say it is a multiple of LCM of M alpha x and M alpha power 5 of x, so the least common multiple is the product because there is no common factor between M alpha x and M alpha power 5. So, I mean as well multiplied out, but in case, so suppose I say for instance instead of alpha power 5 if I had alpha square, then I cannot say M alpha by x times M alpha square of it. Then if I do the LCM simply becomes a M alpha, so it is the only thing I can say, so this motion is used in our PCH code construction. So, tartaric for a while and make sure you are happy about it and come back and haunt you later.

If you did not get the true meaning of how you go from polynomial with coefficients in binary, but having some route from F 16 or some other larger field and what it means about that polynomial if you have multiple routes from F 16 what it means for that polynomial so on. So, should I break the substance and define the BCH code or should I torture you for little bit more some time. You know BCH code everybody wants BCH code, I think you are hesitating because you know what is done?

(Refer Slide Time: 26:20)



BCH codes

Bose – Chauduri – Hocquenghem'

Defn: $n = 2^m - 1$ m: +ve integer

$\alpha \in F_{2^m}$, primitive d: +ve integer (design distance)

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & (\alpha^{d-1})^3 & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}$$

Today is included in the syllabus with coefficient, may be you want me to wait for a while, anyways it does not matter. I am going to define BCH code, anybody is having second, now no chance this is very simple. So, let me expand BCH, first thing you should do in BCH code first name is Bose, second name is Chaudhuri. These two I can spell quite easily, but third one is difficult to spell, so I might make a mistake, go back and check it with your book, I think this is correct. So, the last part could be my own spelling Hocquenghem, go back and check that there would be some mistake here.

Bose and Chaudhuri are quite standard, so this is codes one of the earliest codes that showed up and a very interesting from. So, many different points of view they used to theoretical computer science they used in coding of codes and practice in theory. So, it is very interesting elegant, some might even say beautiful construction of codes and what I I should say, let me justify that and we will do it. So, couple of parameters that go into the definition of these codes first is the block length.

You know codes usually mean any I have to tell you what the block length is i have to tell what the dimension is or basically I have to generator matrix or the parity check matrix. Some such thing I have to give you or I should define the code using some other meaning, I will do some two or three types of definition just to convince you that all of them are equivalent. Then we will find look at how to find them, the first is going to be a parity check matrix definition, so let us say we will begin with 9, so there is something wrong with the display. So, do not get confused by some balloons coming up from here and there they may not work trying not to do it, but somehow it decides and so on.

So, we will pick n equals 2 to the power n minus 1, so n is my block length, I am going to pick it in this form, it is not very special, we will see later on. I can relax this very easily, but for start is I will start with this for the definition is simple and nice and for this particular n the code has several other interesting properties which make it very interesting. So, that is why I am picking this, but there is nothing very special about this choice, so n equals 2 power M minus 1 what is M, M is some positive integer, take it as positive integer. Then we need this extract alpha equivalent what is alpha, it is strange, alpha you need for this construction.

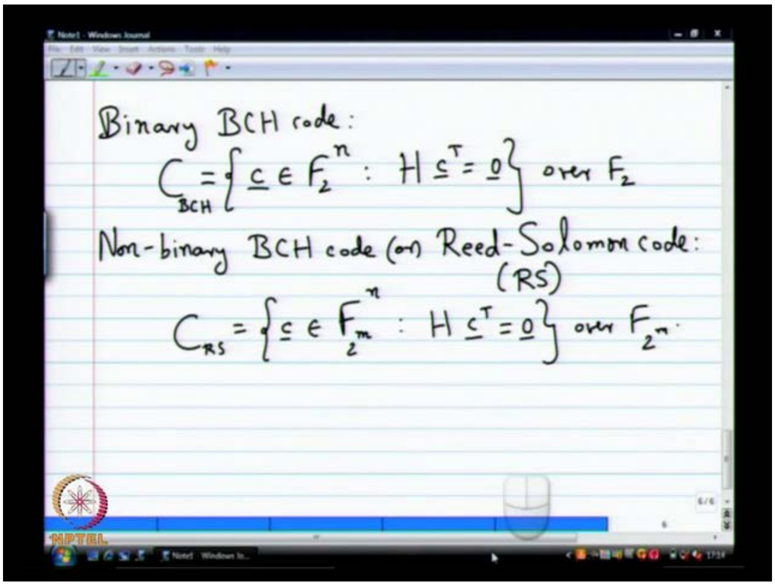
So, we will take F in alpha in F 2 power M to be a primitive element, so I am going to give you a parity check matrix which has a n 3 from F 2 power M. So, that itself is a slightly strange notion that it really define a code, what kind of code does it defines; we have to look at it very closely. So, let us do this alpha n F 2 power M and here is the parity check matrix, I just give you the parity check matrix and worry about other things later, parity check matrix will look like this. The first row will have one alpha square, let us I will alpha power 3 on till alpha power n minus 1 that is the first row, second row is 1.

So, just thinking if I run out of this room here, write it first and then draw the brackets second row is going to be 1 alpha square alpha square whole square alpha power 3 whole square so on. So, I think I am going to write it the other way round, I think that is better alpha square to whole power 3 alpha square whole power n minus 1. So, what will be the third row, alpha power 3 alpha power 3 square alpha power 3 raise to the power 3 so on till alpha power 3 raise to the power n minus 1. We have to stop somewhere, so for that we need another parameter, so that parameter is common to take it as d minus 1, so d is sum positive integer, it has some constraints.

It cannot be any positive integer, think of it as a small positive integer 3, 5, 7 something like that, small compared to n. It cannot be very large and we will stop at d minus 1 alpha power d minus 1 square why d minus 1 etcetera will become clearer. Can somebody guess why d minus 1, so we will be able to later lower bond the minimum distance by B.

So, the obvious stop at d minus 1, so the obvious notation d for this all the way here quick terminology. So, n is called the block length of course d is called the designed distance, I am going to define two different codes with this one parity check matrix. Both of them you can call them BCH code, but usually the binary, so one of them is called BCH, so I am going to first take the binary BCH code.

(Refer Slide Time: 32:34)



Binary BCH code:

$$C_{BCH} = \{ \underline{c} \in F_2^n : H\underline{c}^T = \underline{0} \} \text{ over } F_2$$

Non-binary BCH code (or Reed-Solomon code:
(RS)

$$C_{RS} = \{ \underline{c} \in F_{2^m}^n : H\underline{c}^T = \underline{0} \} \text{ over } F_{2^m}.$$

So, we need a notation here, so what notation can we use, I simply say C for now, we say C later on, and we will see what to do, C is set of all vectors in F 2 n such that H C transpose is 0. So, this is the binary BCH code of block length n and design distance d block length n equals 2 power n minus 1 and design distance d, there is also a non binary BCH code that I can define. It is more popularly known as the emolument code RS code, here what I would change in case I want a non binary code. I should have seen being F 2 n and simply make a F 2 power M n, any way my parity check matrix is defined over F 2 power M as well do both.

So, that is the non binary BCH code or emolument code very popular abbreviation, again may be I will put C BCH here, it is distinguished between C RS. So, M should be better spelt, so first of all notice that this h C transpose is a very well defined operation, there is nothing wrong with that. In both these definition why is that very well defined, even though h has elements from F 2 power M, I know it also contains F 2 inside it and it is a proper extension of that.

So, there this properly contains F 2 inside it, so I can definitely do H C transpose, after all I know 0 and 1 are in F 2 power M. Also, I might assume that F belonging F 2 power M and do the computation, so no problem in that and definitely if I say C belongs F 2 power M. Also, its very well defined we did see some examples for F four right in general F 2 power M sounds like a very large quantity, we saw for F 4, how these examples works, so I can have a code over F 2 power M.

So, this code is clearly over F 2, it is binary, this is over F 2 power M, the code words are vectors where each co ordinate is a symbol from F 2 power M. So, the element of F 2 power M, so we would not look at non binary BCH codes for a while we will look at binary BCH codes, but some of the proofs are very similar for either of these properties. So, I do not have to really repeat each of proofs separately over and over again, I can just simply do one common proof of both because after all they share the same parity check matrix. For instance, the rank properties that define the minimum distance it is going to be very similar.

It is nothing is going to change for those things, so all those things are similar, so we will do some of the proofs and I will simply say the same proofs holds for it, so that is why I defined both of them together, but usually in a codes in a book. For instance, they would do BCH first and then take a lot of time before they do that, so you used to get that also, let us start at this parity check matrix. Once again, it is important that you start at an assimilated, it is quite easy to remember, and so one alpha square all the way till alpha power d minus 1.

Then, you square, then raise it to the power 3, go on all the way till n minus 1, now suppose I picked n to be let us say 2 power M minus 2 or 2 power M minus 3 or some number lesser than 2 power M minus 2 not equal to 0. That can I do the same definition, I mean I can do, but you must say the same definition without losing too much. So, that is why I said n equals 2 power M minus 1 does not matter, so if because I picked it to be equal to 2 power M minus 1, I can happily write alpha belonging to F 2 power M primitive. If it was something lesser, then I have to say how I find the 2 power M, the smallest 2 power M greater than n or something.

I have write that down very clearly is it is bit more painful, so I simply wrote n equals 2 power M minus 1, another thing you notice is I have picked alpha to be primitive what will happen if alpha is not primitive in this choice. This columns will start repeating and I would have gone only up to n minus 1, I did not got to n if I go to n what will happen, I simply get all 1 s columns which is the reputation of the first one which means the minimum distance is 2. So, that will just kill everything, so I cannot allow this reputation to happen.

So, the only crucial property is the element that you pick from F 2 power M should have should have what should have something at least n as long as you pick something of order at least n. This parity check matrix would be a very well defined parity check matrix without any reputation and it would give you the minimum distance property that we are going to get. So, what I am trying to say this that I have several very simple generalizations from this definition, but we will mostly stick to this choice of parameters in the proof just because it is simple to write it down.

There is no other reason, but in general there are other obvious extensions for which the same kind of proof or minimum distance holds as you can imagine the most crucial thing is the proof of minimal distance. Nothing else is important here, so as long as you know that this is a minimal distance you get here, so do you want to study different ways of viewing this or defining this code first or do you want to see the minimum distance proof first. So, to find out more about k or like k is the x parameter of interested what is k, the dimension of the code for which of these codes is k very easy.

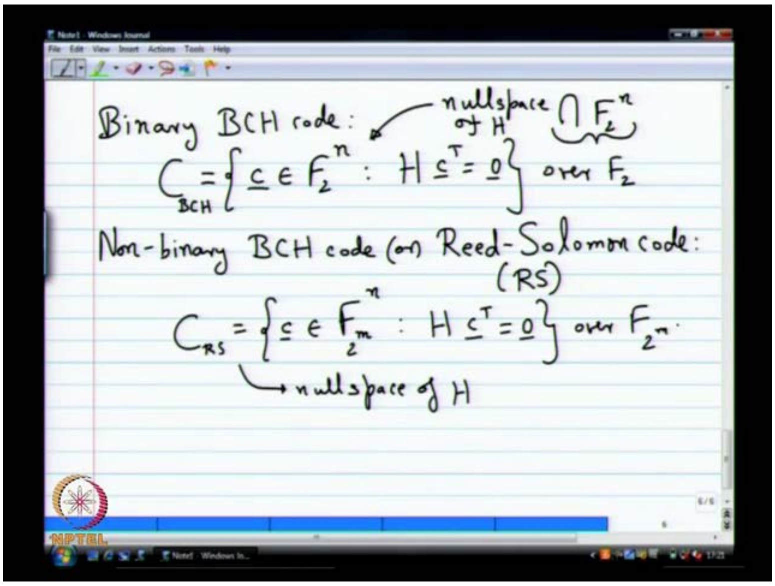
It is without too much thinking you can do k first one or second one, I think in my opinion, the second one is slightly easier. All the elements are from one field, I can do Gaussian elimination to find out what, so all I have to do is Gaussian elimination on H to find out the row rank of H because I have a properly well defined code over F 2 power M. It is just its coefficient from F 2 power M, I do Gaussian elimination over F 2 power M, I find out if this is got full rank or not.

If you pick d suitably small, I have not really told you what choice of d is good, but d is something small, let say and this will have full rank. In fact, it will always have a full rank in many cases, so it will have full rank and then you can easily find k.

Why cannot I not use the same definition same idea for the first code, can I use the same kind of idea, suppose I find that this is full rank in F 2 power M, can I say n minus k will be b 1 d minus 1 for this second, first code can I say that F 2. That is the problem because I am saying C is restricted to F 2 n, I cannot allow code words from F 2 power M.

Remember, all my vector space all the Gaussian elimination works only in F 2 power M when I have elements from F 2 power M in H. Suddenly, I am putting this artificial restriction that the solution the null space I am looking for is not in F 2 power M. It is only F 2, so that is the artificial restriction I have to resolve that somehow let say resolved that I cannot be sure about my game, see this is basically null space of H.

(Refer Slide Time: 40:56)



Binary BCH code: nullspace of H $\cap \underbrace{F_2^n}$

$$C_{BCH} = \{ \underline{c} \in F_2^n : H\underline{c}^T = \underline{0} \} \text{ over } F_2$$

Non-binary BCH code (or) Reed-Solomon code: (RS)

$$C_{RS} = \{ \underline{c} \in F_{2^m}^n : H\underline{c}^T = \underline{0} \} \text{ over } F_{2^m}.$$

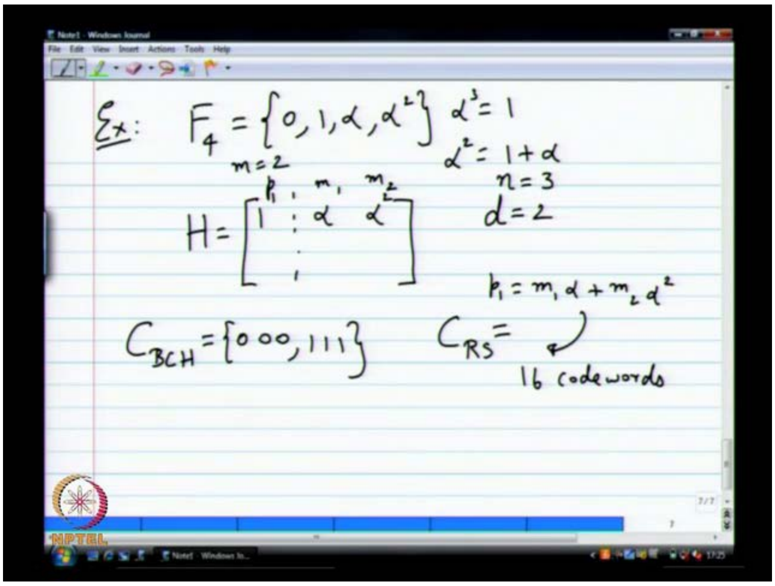
nullspace of H

If this is also null space, I do not need two different definitions, if both of them would be the same, this is not null space what is this this is the null space of h what should I do to the null space of h to get this.

I should intersect it with something, what I should intersect it with, F 2 n, so that is an artificial intersection that I am introducing intersected with F 2 n. Now, this is not a very linear algebraic type of intersection, it is not a rank or any row space or something, it is something else I am doing totally different. It is what to do how the fields work; in fact it is got to do with how minimal polynomial works.

So, that is why we saw minimal polynomial, so this is all what this intersection does to the dimension k. So, that is where we were looking at minimal polynomial etc is that, so the first thing you have to appreciate is the difference between these two definition. So, let us see very simple example to convince ourselves of this difference at least first and then we will go on to minimum distance proof etcetera.

(Refer Slide Time: 43:00)



Ex: $F_4 = \{0, 1, \alpha, \alpha^2\}$ $\alpha^3 = 1$

$m = 2$ $\alpha^2 = 1 + \alpha$

$n = 3$

$$H = \begin{array}{c} \begin{array}{ccc} p_1 & m_1 & m_2 \end{array} \\ \begin{bmatrix} 1 & \vdots & \alpha & \alpha^2 \\ & \vdots & & \\ & , & & \end{bmatrix} \end{array}$$

$d = 2$

$p_1 = m_1 \alpha + m_2 \alpha^2$

$C_{BCH} = \{000, 111\}$ $C_{RS} =$ 16 codewords

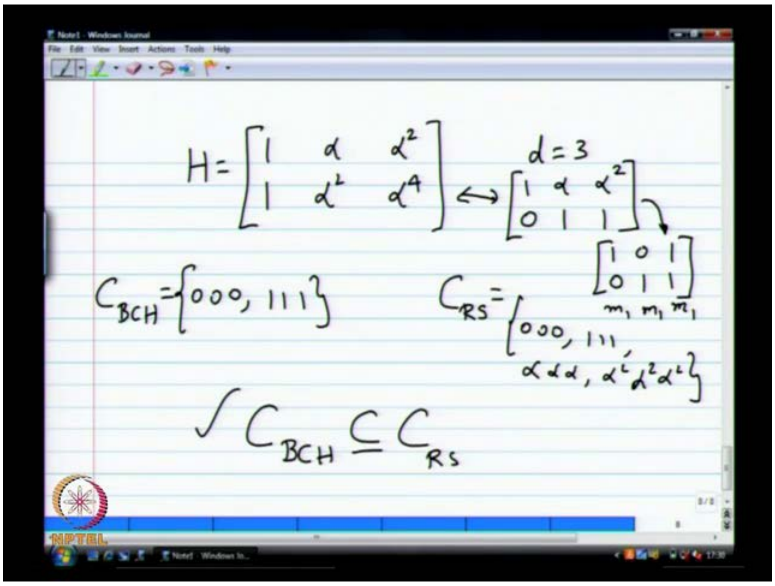
The easiest examples come from which field, so it is too simple, but any way I mean let us see the example does not heard too much if it is too trivial. Then we will go to F 8, then you guys have to do all the work alpha power 3 is 1 alpha square is 1 plus alpha. So, let us define what is the n that I can have here 3, I cannot go 3 can I go up to 3, you can go up to 3, everybody is looking at me, so alpha has got order 3. So, I can go up to n equals 3, so order n, so the first row would be one alpha square, then what about d, let me say d equals 2, I pick d equals 2, let me not say what do u mean, you cannot pick, I can pick, no you can pick let us say d equals 2. So, I will say n is equal to 2, remember so M is 2, I take n is 3, so alpha is I will take d is 2, so then H has simply only one row.

So, this is a nice and nice enough thing I mean you might think it is too trivial, it is not so simple, so let us say just got one row what is BCH and what is CRH, let me see take some time and try and figure out the code words of these two codes. I mean I want you to write down all the code words, should I write down all, may be not all at least a few, so C BCH definitely all for CRS may be a few.

I would have quickly answered, let us see we will wait for everybody for BCH the quick way to do. It is to exhaust all possibilities for c, after all we have only eight possibilities right, there are eight different vectors for F 2, 3 you exhaust all possibilities, you will see only two of them will qualify. It will be 0, 0, 0 and 1, 1, 1. There will be no other code words, what about RS, the same this union more really I do not want to get any marks in the exams. For that, you have to do just a proper null space step of operation, take a look at this is your I part and what is your p part, you can take this to be your I, this is identity matrix.

So, you have a clarity p 1 here you have two messages M 1 and M 2, both of them from F 4, so you will have sixteen different code words in CRS how will you compute p 1, p 1 is M 1 times alpha plus M 2 times alpha squares. So, that will give you all CRS 16 code words is that, see what should you do to find CRS, you have to do Gaussian elimination, here there is only one row, I mean is very trivial Gaussian elimination. You can simply go on, you have already done Gaussian elimination and you already know what the parity is, you write it down, it allows 16 different code words is that seems simple enough.

(Refer Slide Time: 47:32)



$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 0 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$d = 3$

$m_1 \; m_1 \; m_1$

$C_{BCH} = \{000, 111\}$

$C_{RS} = \{000, 111, \alpha\alpha\alpha, \alpha^2\alpha^2\alpha^2\}$

$\checkmark \; C_{BCH} \subseteq C_{RS}$

Now, the next example slight twist on this you are still in the same F 4, but I am going to throw in one more row to this, basically I am going to pick d equals 3, remember alpha power 4 is the same as alpha. Let us keep it like that, now what will be c BCH what will be CRS. Now, we can write down all the code words for both codes C BCH remains the same, so interesting or not interesting, slightly interesting, you have to check what you have to do, Gaussian elimination doing CRS that is the easiest way of doing.

Let me do it, if you are not so interested in doing it, I will show you how to how that is done, so you do first you do pivoting, so you get first element to be 1 and then make all the elements below at 0. So, how do you make the element below at 0, you have to subtract which is the same as adding 0 what is alpha square plus alpha 1, what is alpha power 4 plus alpha square, 1 again. What is the next step to make it, I multiply the bottom row with alpha and then add it to the top, so that would give you an I, here 0 alpha power 3 plus alpha is what alpha square and the alpha power 3 is how did this become alpha power 3.

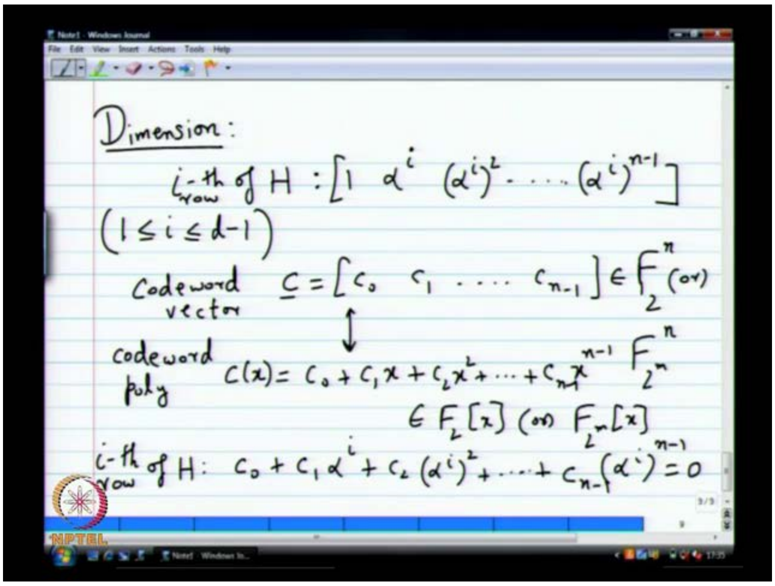
It is alpha square something is wrong this is one and what you get here 0, 1 and 1, so this is the parity check matrix, after you have done row reduction, why cannot I not do this row reduction when I am working with C BCH, what was wrong with that. The first step I only added the first two rows that was clearly a binary coefficient operation and then for the next step what did I have to do, I have to multiply by alpha and that is clearly not permitted.

If I am only working with F 2, so as long as you do only F 2 row operations, you are there is no problem when you start multiplying by alpha. You are clearly going to a F 4 row operation and that clearly violates my definition of BCH code. I am not contained within the space I defined it to be so that is the problem so that is why only the r s code is the proper way I mean only Gaussian elimination applies only for the RS code definition. So, here code is easy to write down F 2 parity bits p 1, p 2 parity symbols, sorry p 1, p 2 and then one message with M and what is p 2, p 2 equals M 1, p 2 equals M 1.

So, in fact what do you actually have here is the reputation code that is why we have M 1 M 1 M 1, so what are the four code words. If you want more experience which I will strongly suggest that you try going to F 8 or F 16, if you are really brave and try the same thing for different d s. So, you see how it looks like but of course the number of code words will suit up a lot, but you will learn something, I think there something is there valuable.

It will give you good idea for that anyways, so couple of quick things that you can figure out just by the definition is you will always have C BCH contained in CRS is this is true. So, F 2 is contained in F 2 power n, so clearly C BCH will also be contained in CRS always, so if you doing a computation and you find that this is not true something has gone wrong, may be you can go back and check. So, before we go to the proof of minimum distance I want to show you something about k, so I think it is reasonable that we do that I have to find out the dimension first before.

(Refer Slide Time: 52:40)



Dimension:

i-th row of H : $[1 \quad \alpha^i \quad (\alpha^i)^2 \cdots\cdots (\alpha^i)^{n-1}]$

$(1 \le i \le d-1)$

Codeword vector $\underline{c} = [c_0 \quad c_1 \quad \cdots\cdots \quad c_{n-1}] \in F_2^n$ (or)

$\updownarrow$

codeword poly $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$ $F_{2^m}^n$

$\in F_2[x]$ (or $F_{2^m}[x]$

i-th row of H: $c_0 + c_1 \alpha^i + c_2 (\alpha^i)^2 + \cdots + c_{n-1} (\alpha^i)^{n-1} = 0$

We find out minimum distance, so I have always being saying dimension of codes are easy minimum distance is a hard problem. So, we will do the minus, we will do the dimension first. So, dimension remember what was my let us say the i th row of h for i between 1 d minus 1 what was the i th row of h 1 alpha power i alpha power I square, so on till alpha power i to the power n minus 1. So, this is interesting, it almost looks like x power 0, x power 1, x square so on till x power n minus 1 and I am simply putting x equals alpha power i from i between 1 and d minus 1.

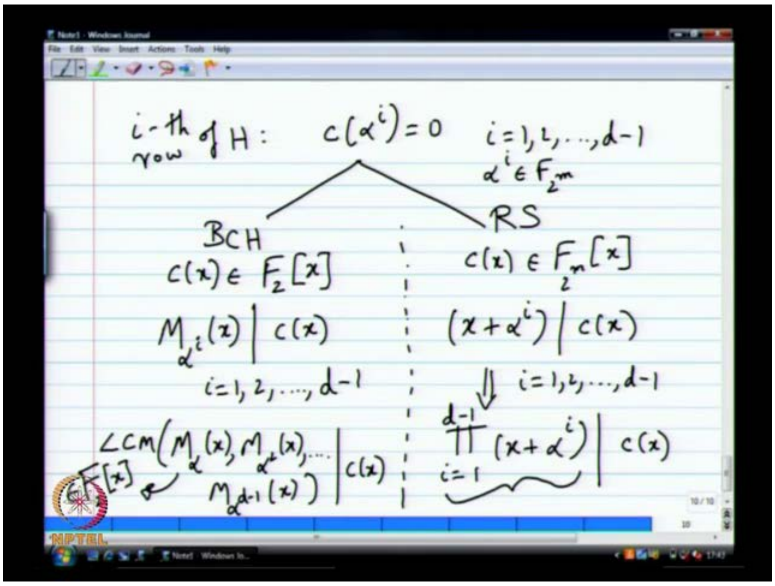
So, if you think of a vector C let us say c 0 c 1 all the way till c n minus 1 which you say in F 2, let us say something you know let us say F 2 power n or F 2 power M to the n one of those two things that I would do for BCH codes. This I would do for RS codes, I can associate with these vector a polynomial which is just a formally equivalent polynomial. It would looks something like this c 0 plus c 1 x plus c 2 x square plus so on till c n minus 1 x to the power n minus 1. This would be a polynomial which belongs to either F 2 x for p c h or F 2 power M x for its all.

So, the i th row of h is imposing a sudden constraint on this vector, what is it saying it is basically saying the i th row of h is saying i th row I forgot to write row i th row of h.

Basically, saying what c 0 times 1 plus plus c 1 times alpha power i plus c 2 times alpha power i square plus so on till c n minus 1 times alpha power i n minus 1 equals what 0.

So, let us start c of x and the condition imposed by the i th row of h for a while and see if we notice something. What can we notice instead of saying my code word has to be orthogonal to the i th row of which I can equivalently say my code word polynomial. So, this my code word vector which has to be orthogonal to the i th row of h, I can equivalently say my code word polynomial should do what should have alpha power i as a route. So, both of them are perfectly equivalent statements it is formally exactly equivalent nothing more to worry about it.

(Refer Slide Time: 56:24)



i-th row of H: $c(\alpha^i) = 0$ $\quad i = 1, 2, \ldots, d-1$

$\alpha^i \in F_{2^m}$

BCH

$c(x) \in F_2[x]$

$M_{\alpha^i}(x) \mid c(x)$

$i = 1, 2, \ldots, d-1$

$LCM(M_\alpha(x), M_{\alpha^2}(x), \ldots, M_{\alpha^{d-1}}(x)) \mid c(x)$

$\in F[x]$

RS

$c(x) \in F_{2^m}[x]$

$(x + \alpha^i) \mid c(x)$

$\Downarrow \quad i = 1, 2, \ldots, d-1$

$\underbrace{\prod_{i=1}^{d-1} (x + \alpha^i)} \mid c(x)$

So, basically the i row of h imposes the constraint that c of alpha power i equals 0, now you will have two different situations for the BCH code and the resole men code. So, I am going to branch out two BCH on the left and two resole men on the right, so for the resole men codes remember C of x belongs to F 2 power M x. So, if I say c of alpha power i is 0 for i is 1, 2 to d minus 1 what can I conclude about this c of x, it should have some factor what should be that factor. It is a F of x to some polynomial which is a real coefficients, when I say for a real number alpha F of alpha is 0, what can I say will be a factor of F of x x minus alpha, but real number real coefficients have a real number as a route.

So, what do I know x minus alpha will be a factor same thing is happening here c of alpha power i is 0 c of x as coefficients from F 2 power M alpha power i belongs to F 2 power M. Remember, alpha power i belongs to F 2 power M, so I do not really have a complicated situation when I deal with resole men code. I have a polynomial with coefficients over a certain field and I have a route from that very same field, it is not a smaller field or a larger field or any such things. So, very same field then I know for sure that x plus alpha power i why can i write alpha plus here.

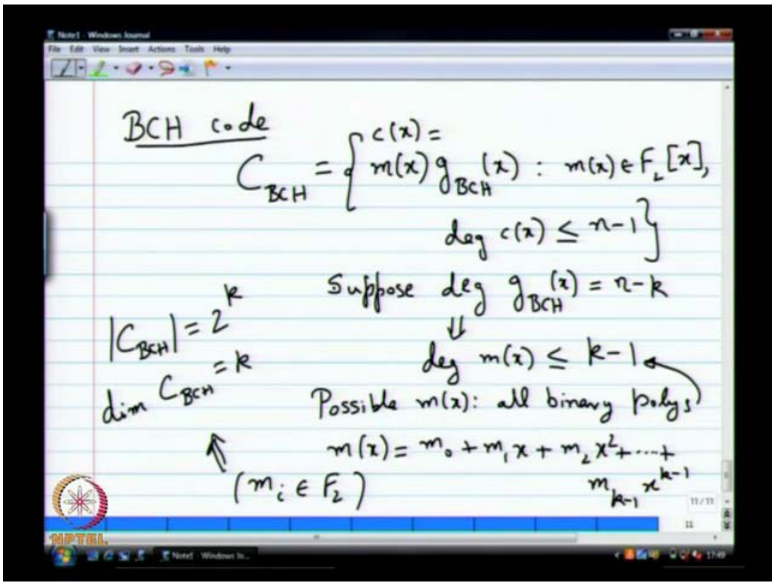
Otherwise, I have to write minus this will divide c of x for i equals 1, 2 to d minus 1, usually you pick d to be less than n. So, like I said it is usually much smaller than n and most codes in fact let us say theoretically you pick it to be less then n which means you do not have any reputations in the alpha power i. Then x plus alpha power i an x plus alpha power j are really no common factor we do in those two. So, this will implies product i equals 1 to d minus 1 x plus alpha power i divides 0, 5, everybody is happy very simple, not very simple, you know inacceptable is simple.

So, just put it that way, something like x plus alpha is a factor x plus alpha square is a factor x plus alpha power 3 is a factor. So, the product that the total degree is less than n minus 1, so what can be the degree of the other polynomial minus d plus 1, so degree I can take, so that any multiple of that you can go back and show will satisfy will be of orthogonal to every row of h and that will give you a valid code word. So, not only you go this way you can also go reverse can I do the same thing here, I mean I can do the same thing here.

So, you take any multiple of the LCM of this case all of them will have definitely alpha power i the route, but remember when I say any multiple I pick the other polynomial to be from F 2 M x, I have to take it only from F 2 x. I cannot take F 2 power M, then what will happen then c of x will not be will not be in F 2 x and that is not, I mean you cannot do that. You want c of x to be in F to x, so this polynomial is definitely in F 2 x, let me see why is this polynomial in F 2 x.

All of these not because c is in F of x, all the minimal polynomials are in F 2 x clearly if you take where LCM, you will also get an F 2 x only. So, that is go beyond anything beyond this, so just do it in F 2 itself LCM and F 2, so it is important, so what you should do when you do that c F x there have to be multiple of that and the other polynomial which you multiply, this with should also be in F 2 x 1. So, you can on the reverse way also I know you did not write all the steps of the proof, so you can fill it and if you like. You can look at the text books there will have a very clear explanation of this, so what do we have now for BCH code and resole men codes.

(Refer Slide Time: 01:06:03)



BCH code

$$C_{BCH} = \left\{ \overset{c(x)=}{m(x) g_{BCH}(x)} : m(x) \in F_2[x], \deg c(x) \leq n-1 \right\}$$

Suppose $\deg g_{BCH}(x) = n-k$

$\Downarrow$

$\deg m(x) \leq k-1$

Possible $m(x)$: all binary polys

$m(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}$

$|C_{BCH}| = 2^k$

$\dim C_{BCH} = k$

$\Uparrow$

$(m_i \in F_2)$

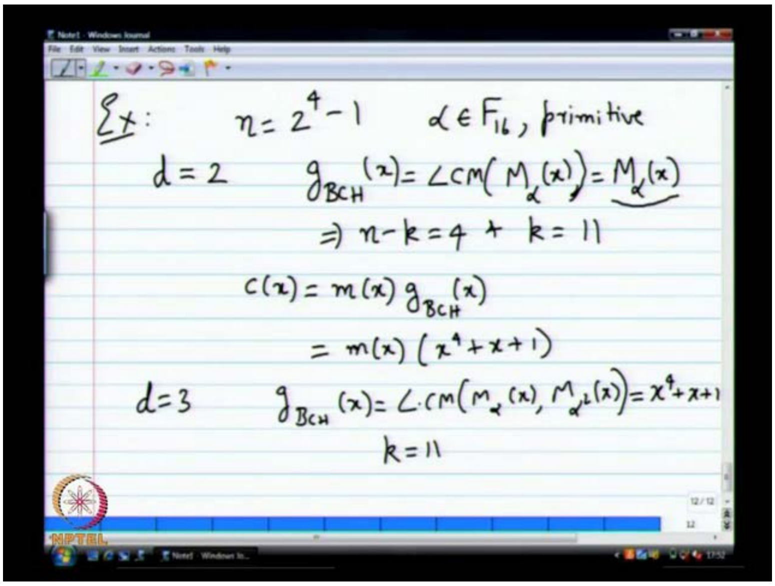
We have interesting characterization of the code words the code word polynomials, so if you look at the BCH code, so let us have a notation, so it is otherwise confusing this polynomial. I will call as G BCH x what can we call this polynomial. Once I call those two polynomials with some name the BCH code can be very easily characterized in terms of code word polynomials not in terms of code word vectors but in terms of well in terms of code word vector.

In terms of coded polynomials can be very easily characterized, so what is c BCH set of all polynomials of this form g BCH x, so let me write c of x equals degree of c of x is less than or equal to n minus 1. Then M of x belongs to F 2 x, so if I say that degree of g BCH is something, so let us say it is some it is n minus k whatever I said n minus k because I know what will happen. So, let us say suppose degree of G BCH is n minus k G BCH is the give polynomial, you know what it is given as a certain d, you can find g BCH.

You cannot change that suppose its degree is n minus k what can be the degree of M of x degree of M of x is less than or equal to k minus 1 and M of x is all polynomials of degree less than or equal to k minus 1. So, the possible M of x all binary polynomials with degree less than or equal to k minus 1, notice there is a one to one correspondence if I have a code word, then it has to be a multiple of g BCH of x. If it is a multiple of G BCH of x it is also code word. So, the only code words are multiples of g BCH of x i do not have to look at look at anything else, so once I have that I have this result.

Now, what is M of x then M of x is M 0 plus M 1 x plus M 2 x square plus so on till M k minus 1. I am running out of room, so I will write it on a next line M k minus 1 x to the power k minus 1. So, the question is given n and d how will you find k that is the question, so the answer is hidden in this result what should you do given n and d how will you find k? First step is to F i G BCH of x, once you find G BCH of x, what will you look for, the degree of G BCH and that is simply n minus k, you simply do n minus that you will get k.

(Refer Slide Time: 01:10:54)



Ex: $n = 2^4 - 1$ $\alpha \in F_{16}$, primitive

$d = 2$ $g_{BCH}(x) = LCM(M_\alpha(x)) = \underbrace{M_\alpha(x)}$

$\Rightarrow n - k = 4$ + $k = 11$

$c(x) = m(x)\, g_{BCH}(x)$

$= m(x)\,(x^4 + x + 1)$

$d = 3$ $g_{BCH}(x) = L.CM(M_\alpha(x), M_{\alpha^2}(x)) = x^4 + x + 1$

$k = 11$

So, let us do that with F 16, so I will take n to be 2 power 4 minus 1 and remember we wrote out the list of conjugates for this, so that will be useful, so we will see how to do this. So, let us look at d equals 2 is where we have to start right d equals 2 is where we have to start. So, let us start at d equals 2 in this case G BCH is what, so alpha belonging F 16 is primitive G BCH of x is LCM of what M alpha x just that. So, it is equal to M alpha of x, so what is the degree 4 implies n minus k equals 4 and k equals 11.

If you want find the code word corresponding to a message in actual hardware, you want to get out the code word you better know what g of x is it will give you a very simple way of doing it. All you have to do is simply take M of x and then multiply with G BCH of x, so in this case it is M of x times x power 4 plus x plus 1 which is a very easy multiplication. That you can do M of x is of maximum degree what degree 10 you take polynomial and multiply how to implement it very easily.

I am running out of time, so let me quickly do d equals 3 for d equals 3, you will G BCH of x to be what LCM of M alpha x and M alpha squared x which in case in this case is exactly equal to the same thing as before x power 4 plus x plus 2. So, you again get k equals 11 in fact you get the same exact code whether you pick d equals 2 or d equals 3, it is not a problem. So, d equals 4 you will start getting something interesting, so in fact you can show that show very general result. We will come back to it, I am really out of time, I do not want to do anything now, so we will come back and pick up here after how many weeks, 2 weeks.

Thank you.