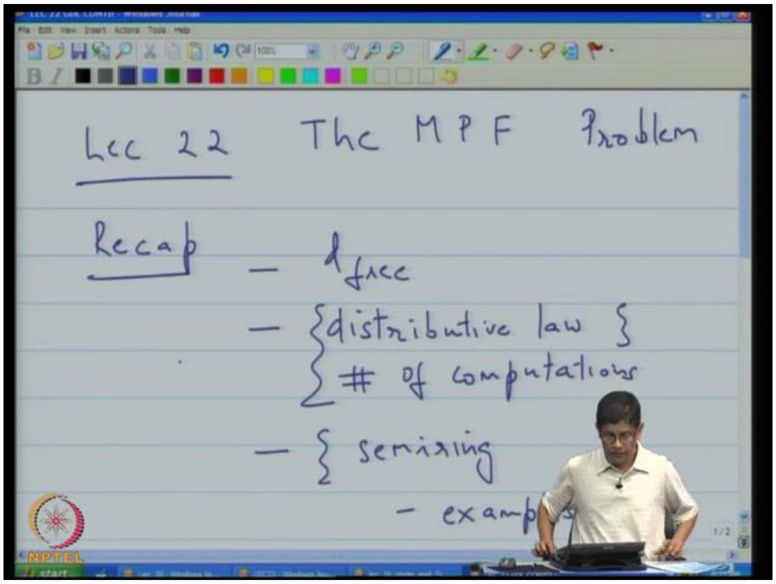
Error Correcting Codes

Prof. Dr. P Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore

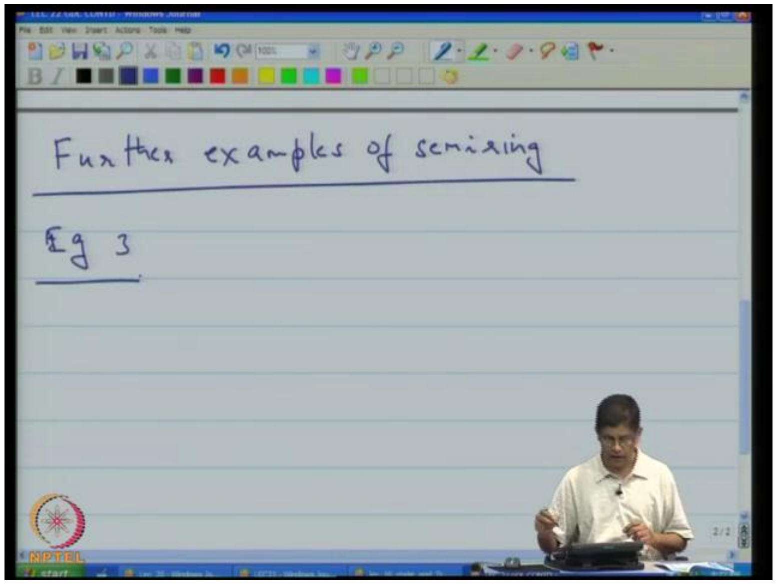
Lecture No. # 22
The MPF Problem

(Refer Slide Time: 00:30)



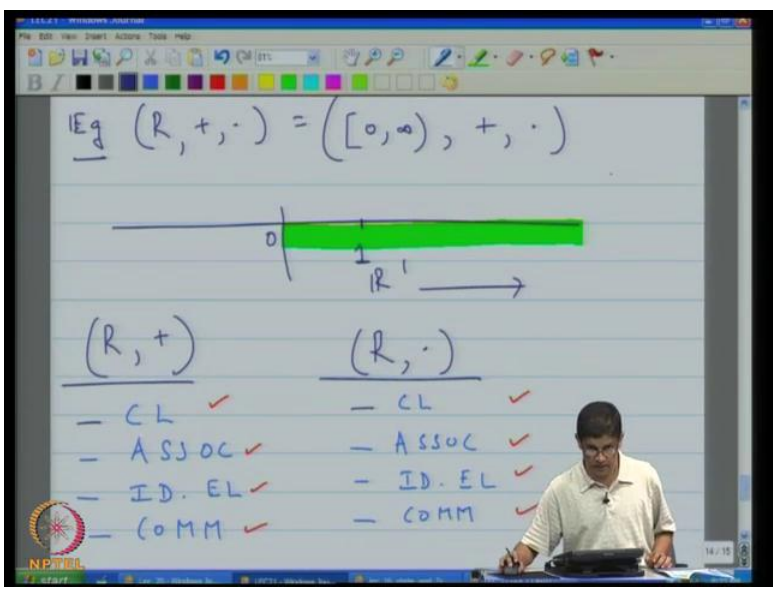
Welcome back; so, this is these are twenty second lecture, and is your title to your lecture I am going to call this is the MPF problem. So, as I mentioned last time, what you are basically going to do is continue discussion of the gdl. Now in the last class, what we did let us very quickly recap. So, I first explain what d free was, then I actually looked at how the distributive law could be used to reduce the number of computations. And then I said that to properly exploit the power of the gdl, it is a right setting a format set respective this setting of semi rings. So, we introduced the notion of semi ring, and we looked at some examples. Now, the way we are going to proceed is will continue our some more examples of semi rings; and after that we will define a general problem setting, which the distributive law can be used to attack. And that problem setting is the setting of the MPF, Marginalize the Product Function problem.

(Refer Slide Time: 02:58)



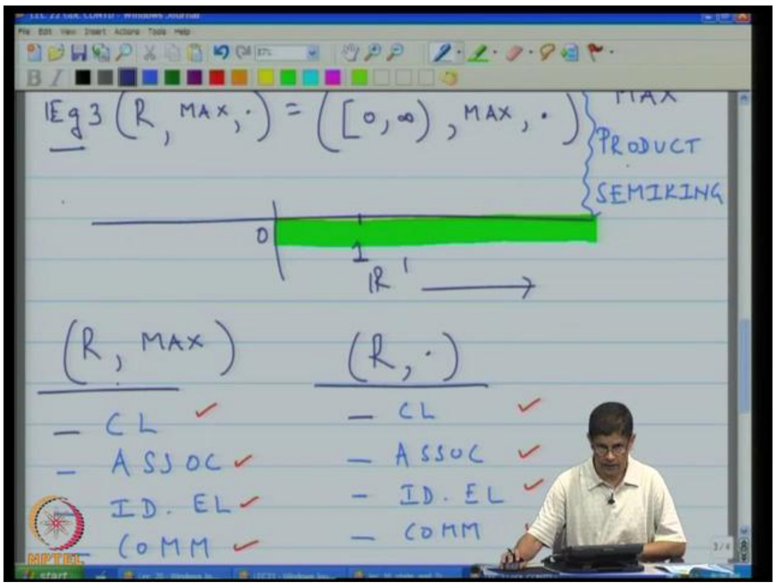
So, let us begin by calling these further examples of the semi ring. So, this would then example 3; example 1 was any commutative ring with identity; example 2 was the example from last time, and actually now the right come to think of it, I can give that need. So, let us do that.

(Refer Slide Time: 03:40)



So, I am going to go back in to the last lecture; so this is the setting for last lecture. So, since the operations are addition and multiplication are available to call this sum product semi ring. So, let us put that down, this is the sum product semi ring. And in fact, I am going to copy this over to the next current lecture. Let us see; so copy page let us see, if I can paste page here I go. So, I have reproduced an example here.

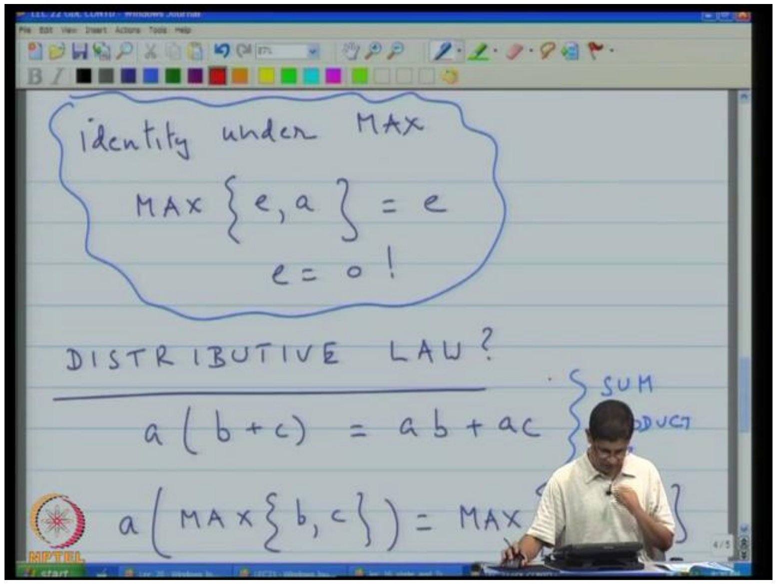
(Refer Slide Time: 05:34)



And I am going to now, because our third example is in a setting similar to our second example, there are certain differences. So, what I will point about. So, here two operations are max and product. So, just like we had sum and product; so, this is max and product. And again in this case, the ranges is going to be 0 to infinity, and again for the same reason, because the quantity is that varied valuating are going to be scaled probability. So, we will put down max and will put down product, and note surprising this semi ring is called the max product semi ring.

Again range is 0 to infinity, and if we check to see if all the axioms are satisfied, we go down the list; again let us correct is that we have max, under max it is close that is if you take max of two quantities, and each of two quantities is real number between 0 and infinity will there also be between a 0 and infinity; and that is obviously the case, so that property is satisfied. Similarly, you can check associative property is satisfied; how about the identity element.

(Refer Slide Time: 07:35)

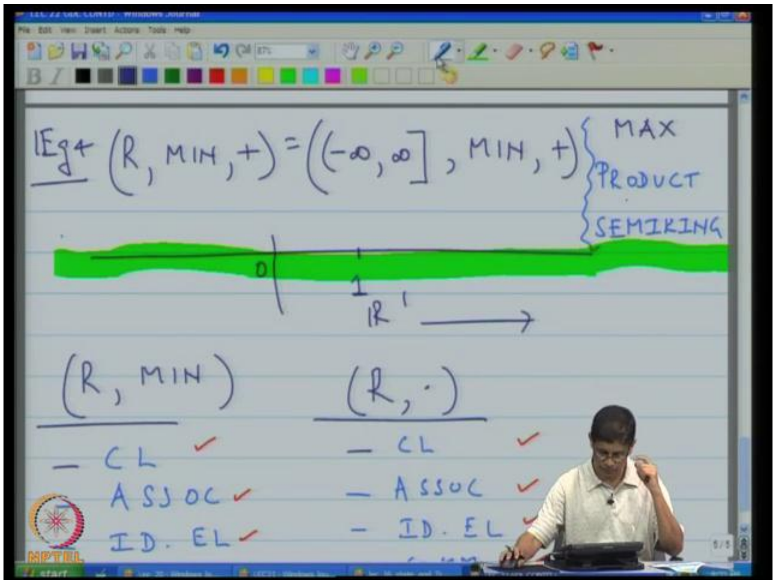


So, if we take the max of two elements and you want that the second elements always win then what should be first element for this to be happened, because that is the definition of an identity. So, select this right. So, the identity under max operation, because we want that max of e, a should always be equal to e. So, the question is, in this set from 0 to infinity, which real number can apply that role? And you can see that role played by 0; so it is same as additive identity, there is if you compare 0 with anything else, we have this number going to win in the max. So, that is means, it is preserved that means, zero serves as the identity element.

So, for this reason, we also have there is closed and addition in the max associative identity its commutated, because it does not matter, when you take max for it is a b or b. Under product we already see in these are conditions are satisfied; so and distributive law so those only remain to see is the distributive law hold. So, these are this that is identity element unless take how about the distributive law. So, what the distributive law would call for is that is it true that observe the way I find this convenient to handle is to actually write it way understand it in sum product semi ring. So, it is a times b plus c is equal to a b plus a c and this is in the sum product semi ring. So, s r stands for the sum product semi ring.

So, unambiguously the quantity that ambiguously to this would have asked, because addition is replaced by max. So, the question is asking here, is it true that a time the max of b c is that equal to now this addition is replaced by again by max is that equal to the max of a b and a c that is equation. And of course, that is true, because b and c are all a b c are all nonnegative real number and of course, we take real number maximum b and c multiplied by a then in precisely in max of a b a c. So, this is also satisfied. So, this is one example, of semi ring.

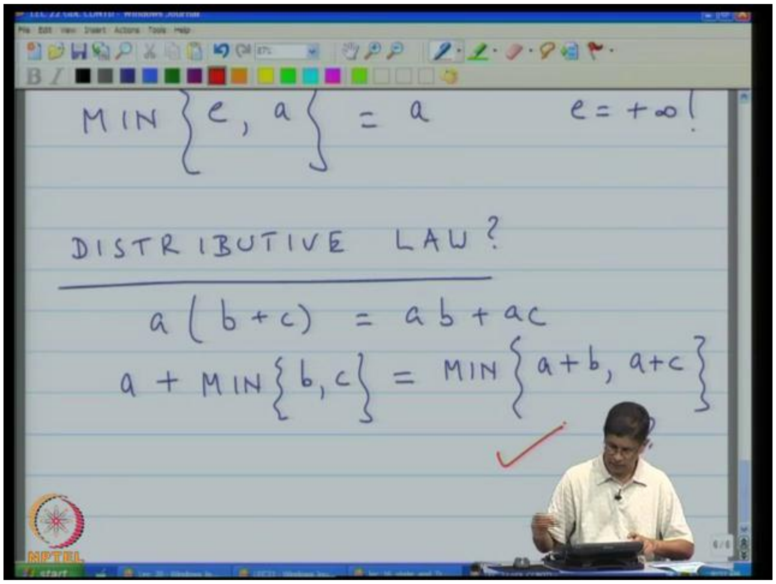
(Refer Slide Time: 12:03)



Now our last example, and later on I give you reference which has many other examples, of semi ring as well. So, last example is that and perhaps what I will do here, is once again since this has been helpful I am going to copy this, put that down here. So, this then they are example. So, and here the operations are here we going to work with R the min and plus, so this is R min plus. So, R is now and also this is change in the very definition of R itself. So, R is now the integral between minus infinity and plus infinity, but including plus infinity. So, R is now the integral from minus infinity to plus infinity inclusive of plus infinity. And so therefore, I should actually in extend this all the way and just too imprecise there includes plus infinity that mean, take it all the way to the edge which other page.

So, this then R is the range of our semi ring. Now let us as before check to see if the axioms are satisfied under minimum; is it closed? There is if you take min of two elements and both them r m, the extended real line, the extended real line meaning there including I am including the point it in infinity, if I do that then is it closed in of course, it is. So, that is actually valid. So, that is fine associated you can check the identity element.

(Refer Slide Time: 14:28)

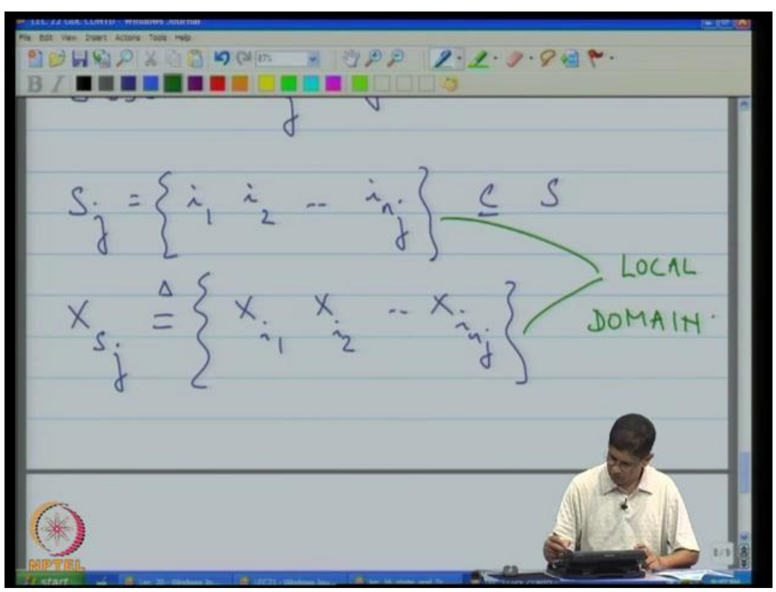


So, what would be the identity element? So, what we are looking for in an identity element is, we are looking for an element having the property that min of a excuse me min of e and any element will actually give you back that element. So, it is not hard to see the back role is played by plus infinity. So, plus infinity placed the role 0 played in the other semi rings, it is additive identity. So, that is one that we have to check; it is commutated, because it does not matter when which order you take, when you take the min operation. The second operation is sum; so this is not this is not this is not long other product sum. So, this for the reason, this ring is called min sum semi ring; the min sum semi ring and under addition is not have to see that you do have closure. In fact, very find that that is have the property of real number. So, all of this properties are immediate are the identity element under plus is still 0.

So, the two identity element which in sum product are 0 and 1 r here plus infinity and 0, but you still do have these then the question is as before is it true that distributive law holds. So, this is I am going to ask same question is before I am just going to copy from here. So, the question is, does it is distributive law hold and the form of distributive law is a little bit different in this case, because now we have the min sum, so the addition is the min and this is, so here this is going to look different. So, the addition is the min. So, we will put down min of b c, and instead of product sums. So, the question is it true that a plus the minimum of b and c is now this sum is the min, is it true that this is equal to the min. So, let me get rid of this, since this is going to come in the way; is it true that this is equal to min of a plus b, a plus c that is the question. And of course, once you have the question very clearly later it is immediate of course, that is true a plus the minimum of b and c is same as the minimum of a plus b and a c. So, the distributive law also holds. So, the answer is yes.

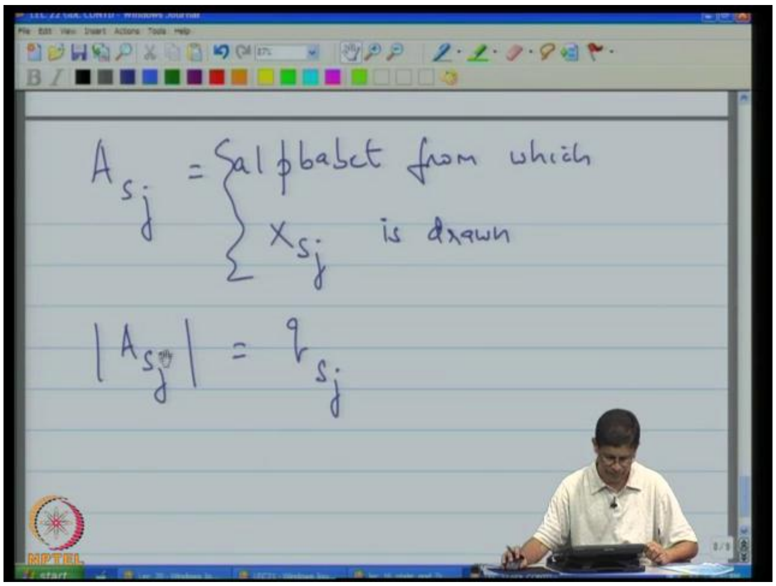
So, we have R third semi ring. So, now you seen three examples, of semi rings apart from the usual examples come out from rings, that is we look at the sum product semi ring, we will look at the max product semi ring and the min sum; these three are the ones that we will you depict encountered encoding theory. I think we in particular will make use of the first two that is we will make use of the sum product in the semi ring.

(Refer Slide Time: 21:28)



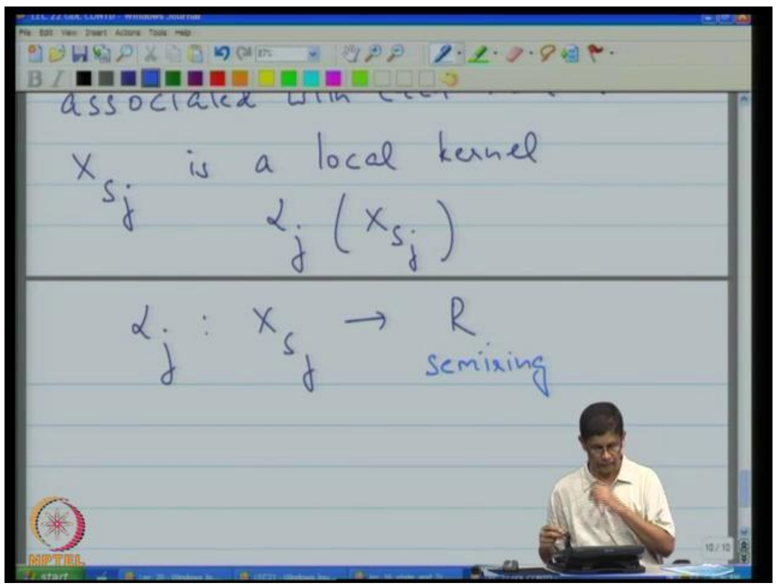
Now, I mention at the outset in fact, that was the title of lecture, the title of lecture the mpf problem; so, will get that now, the mpf problem. So, that is the mpf problem; so first of all mpf stands for Marginalize a Product Function. And the meaning will become clear once you look at some examples; so the setting is the following. There is a universal set S, which is 1 2 n, there is an associated set of variables, which will write as x s which will be x 1, x 2, x n; each x i will take on variables from alphabet a i. So, this is the alphabet of the variable x i. The size of this alphabet A i will be q and I could write q i and in fact, we will then so that is that in addition, we have subsets we have subsets s j of S. So, if you have for instance of particular S j, whose elements are let say i 1 i 2 the sum i base of n j, then this are subset of S. If you want to refer to the variables corresponding to this subsets will actually use this short form notation x base s j will mean we will mean x of i 1 x of i 2 x of i sub n j. So now, will be little back sloppy in our terminology, and will actually refer to both of this inter changeably as local, excuse me I think I needed dark colour here; so let us pick this. So we will refer interchangeably to this as local domains.

(Refer Slide Time: 23:26)



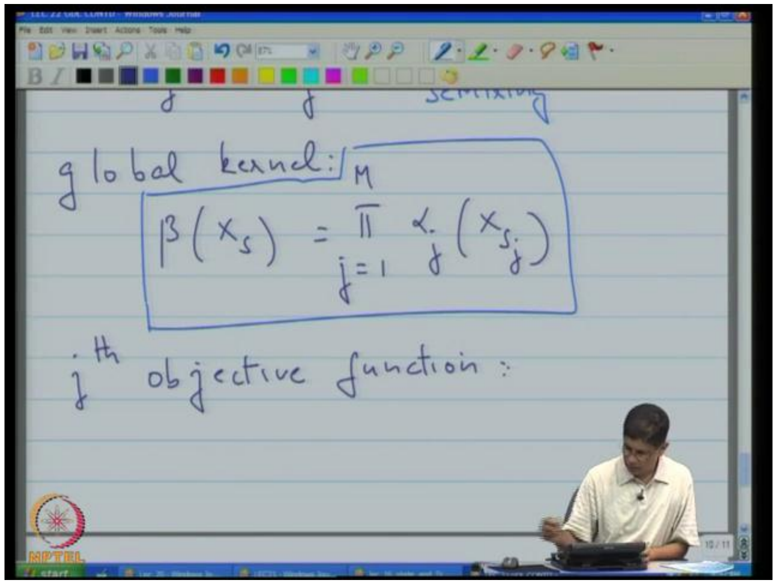
And if I want to refer to the alphabet associated to let say this local domain, then I will accordingly use the notation. So, A sub s sub j is the alphabet, from which X sub s sub j is drawn. Now, it may look at little bit confusing the notation, but as you look for examples, it will actually turn out that it is not complicated at all. And similarly, if you want to before to the size of this alphabet, we will simply write q sub s sub j. Now so let us just recap that; so what we have is universal set, and you can think of this as set of subscript, universal set of subscript, we have set of variables the sum sense is universal all variables, and there are m, little m variables in all; each alpha each variables takes on values from it shown alphabet the size of the alphabet is q i for the higher variable. Then there also have subsets of s, which we will call local domains; the total number of then is actually m, so let me put down here. So, j varies between 1 and m. So, there are m of this subset.

(Refer Slide Time: 25:44)



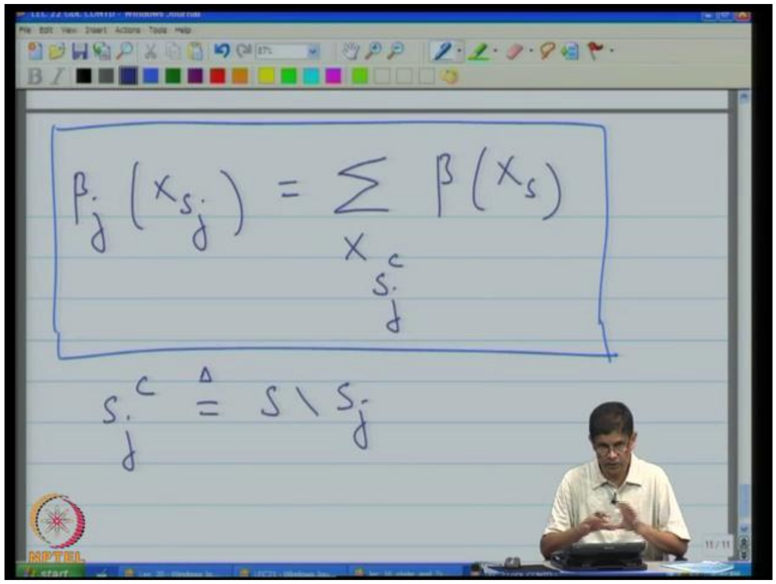
And we have introduced some notation to talk about the alphabet of associated subset of variables; we going to call them local domain. So, this is the alphabet of j eth, this is the alphabet of j eth local domain, and that alphabet has the size. We almost done with the description for setting; we also have what are called local kernels, associated with each local domain x s j is local kernel, is a local kernel, which we will call alpha sub j of x of sub j. So, that is the j th local kernel.

(Refer Slide Time: 27:14)



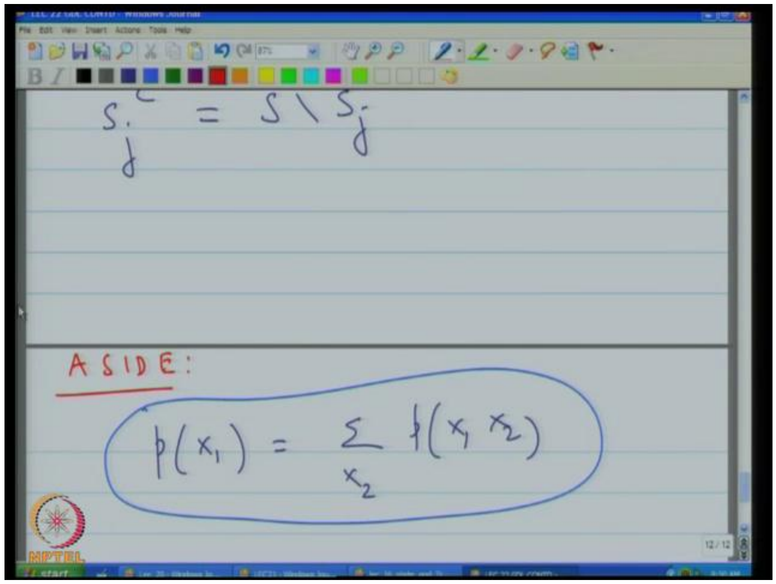
And what is this do? So, this alpha sub j maps x sub j on true R, what is R? Well, R is the semi ring comes in. So, the values of alpha are in some semi ring R. To begin with you can think of as max product semi ring there is this set of all non-negative real number; and the operation of semi ring R the usual addition and multiplication. Then there is something called global kernel. So, the global kernel is beta of x of s is the product j goes to one to m of alpha sub j x sub s sub j; since there are m local kernels you have a product of m terms there is called the global kernel.

(Refer Slide Time: 28:50)



And finally, we have something called the j eth objective function, so j eth objective function is beta sub j of x sub s sub j. What is that? This is simply the marginalization; so think that is cramped that, so let me write dotted on next page. So, the j eth objective function is the marginalization, so that is given by the sum over x sub S sub j compliment of beta of x of S what is S sub j compliment means, this is simply set of all elements in S. So, their sets theoretic compliment S. So, it is all the elements in the universal set as apart from those in S of j. Now why this called as marginalization is called marginalization, because just like when we deal with probability.

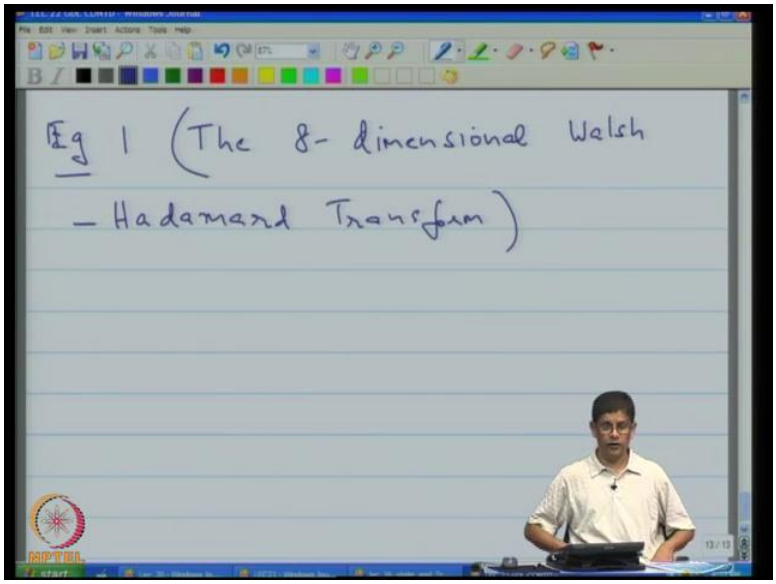
(Refer Slide Time: 30:47)



So, let me just make as slight detour. So, in probability when we write that p of x 1 is equal to sum over x 2 of p of x 1 x 2, then that is an instance of marginalization in probability theory. So, since elements let me do one think, since this is really an aside, period an next page, we say put this down as in a side. So, marginalization used in the sense of probability theory that is you wants to use sum over variables. So, that what is left function in the remaining variables. So, now now the meaning of mpf should become clear, because you are trying to marginalize is the product function right.

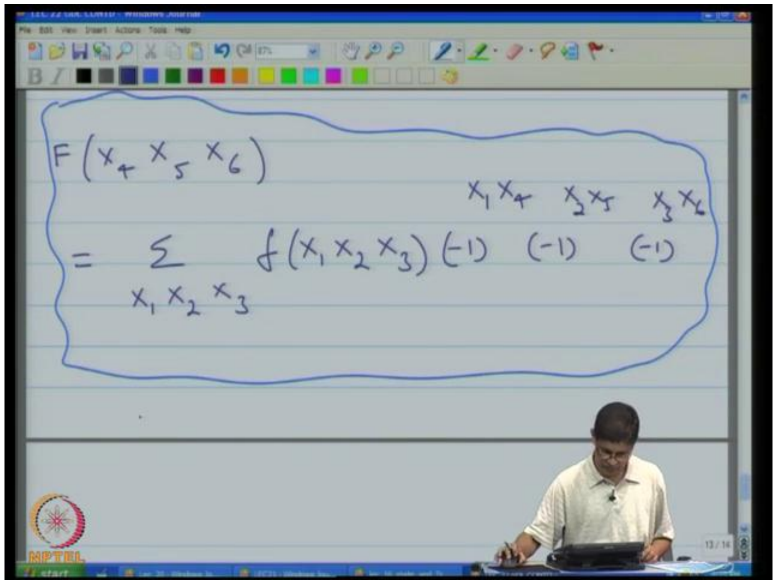
So, in our case, the product function is the global kernel is our product function, which is also of global kernel, and marginalizing because you are summing over subset of the variables. And again you have as many objective functions has there are local kernel; so there are this many objective functions. Now that might seem like a lot to absurd terms of notations, and there is true that I think once you get examples that will all become clear.

(Refer Slide Time: 32:37)



So, these are first example, one the 8-dimensional Walsh Hadamard transform. Now the once Hadamard transform is similar in nature to the discrete Fourier transform it is little bit difference, because I have the different set of functions are involved, but the well function is do turn up in a service anything for example, in your CDMA, you know that whenever you take Fourier transform with discrete Fourier transform basically what discrete Fourier transform does is that it takes time function multiplies it, the unitary matrix which is the Fourier transform. So, here you dealing with different unitary matrix, and as you all know that if the rows or columns of unitary matrix are paired as orthogonal.

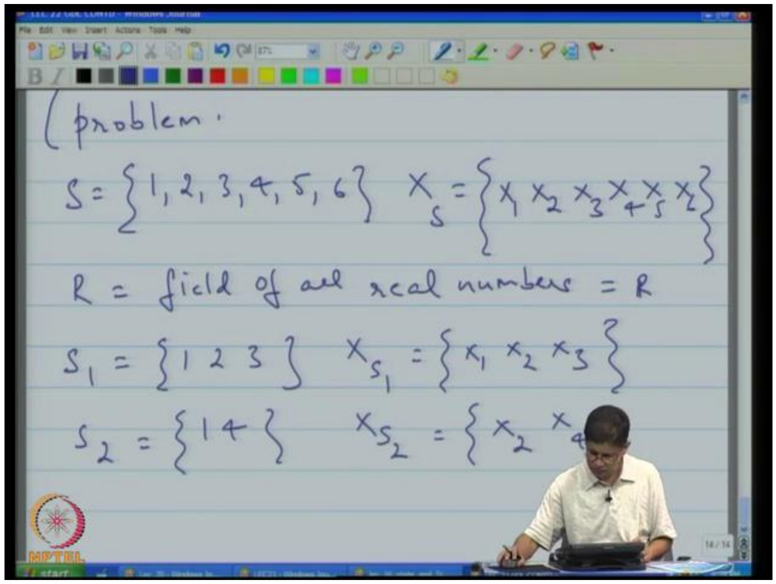
(Refer Slide Time: 34:52)



So, the word transform is also defined in terms of unitary matrix, and the rows of matrix are also pair as orthogonal. The matrix is particularly simple in nature, because it consists of only plus minus ones; and in its these functions there actually show up in the higher 95 cdma, original higher 95 cdma system, because there these function well write kept separate the channels of the different users on the down link. So, that is devotion. Let me write down expression for walsh transform. So, that transforms carries out the following computation. It says that f of x 4, x 5, x 6 is the sum over x 1, x 2, x 3 of little f of x 1 x 2 x 3 times minus 1 to the x 1 x 4 minus 1 to the x 2, x 5 minus 1 to the x 3 x 6. So, this is the computation there it actually carries out.

And and let me just show that let us do one think first; I first want to actually point out that this falls into the setting of marginalize the product function twice that is not have to see, because here what you have is the product of several function. So, these are the local kernels, you multiplying the local kernels, and then you are marginalizing with respect to certain set of variables. So, this is an example of an mpf problem. So, let us make note down that; this is thus an example, of the mpf problem. So, how is it an example?

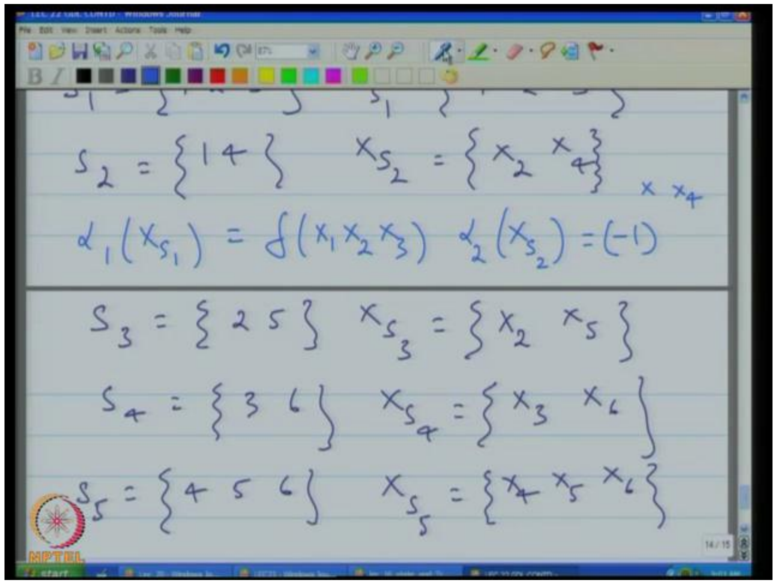
(Refer Slide Time: 36:29)



So, here there universal set is s to 1, 2, 3, 4, 5, 6. So, X of s is therefore, X 1 X 2 X 3 X 4 X 5 X 6; so this is your universal set in the corresponding local domain. The semi ring; so this is the sum product semi ring have to be little back careful here I am sorry. So, here in fact, this is not quite some product semi ring, because the value some take on negative values so in fact, this semi ring is just the field of all real numbers of all then as. So, this is here nothing but R with double vertical bar. And then so it remains be identify the local domains; so going back to this expression here you can see the local domains.

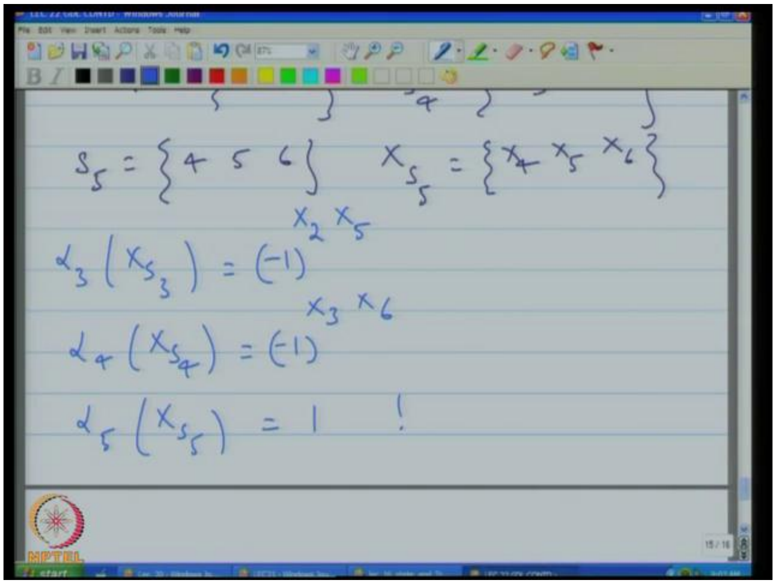
So, one domain is, so this is typically what do you do in practicing. You have presented with certain computation, and then what would have to do is, you would have to actually translate to the certain of the mpf problem, and then go back solving it. Now we have come to the part may be actually try to solve. So, we are trying to now make the connection between this and the mpf setting. So, this is marginalization; this is product function. So, therefore, this must be the local kernels. This kernel x 1 x 2 x 3 x 1 x 4 x 2 x 5 x 3 x 6.

(Refer Slide Time: 39:39)



So, let us put those down. So, you can say that S 1 is 1 2 3; x s 1 is x 1 x 2 x 3; S 2 is 1 4 x of s 2 is x 2 x 4 s 3 is 2 5. So, if x of S 3 is x 3 x 5; S 4 is 3 6; x of S 4 is sorry that should be 2 here; this is x 3 x 6. So, we have got four local domains right now. So, we have the local domains that correspond to 1 2 3, 1 4, 2 5, 3 6, but we are not done; the reason for that, you go back here and look is because we needed in the problem setting to be evaluating certain objective function again at a local domain. So, even the variables that appear on the left hand side must correspond to local domain. So, that forces us introduce in other local domain, which will be S 5, which will be 4, 5, 6 associated to x 4, x 5, x 6, but now, so that then next question is well, what are the local domains. So, let us put that down here. So, alpha 1 x of s 1 is f of x 1, x 2, x 3 and similarly, alpha 2 of x s 2 is minus 1 to the x 2, x 4.

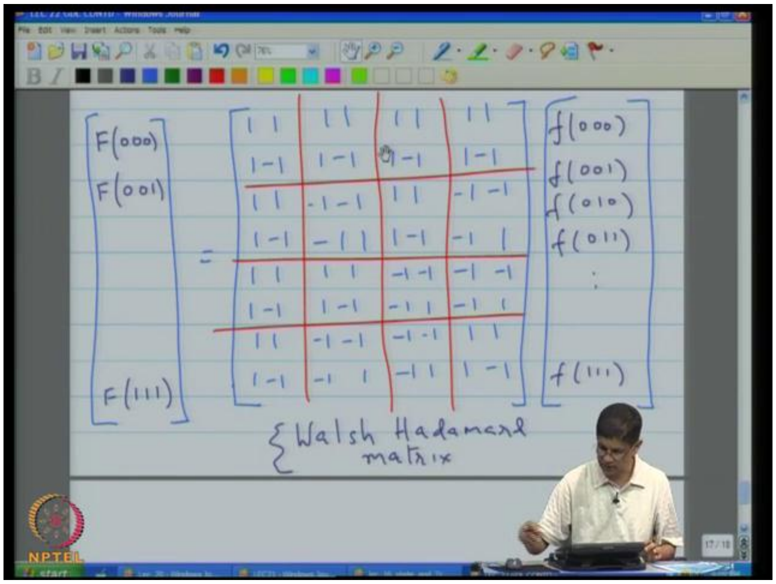
(Refer Slide Time: 42:21)



So, well looking at this computation and write now we looking at x 1 x 4 sorry. So, that should be this should be x 1 x 4 that is your second one and similarly we can write down the other alpha 3 x s 3 is minus 1 to the x 2 x 5, alpha 4 x s 4 is minus 1 to the x 3 x 6, but then here we have these other local domain, but kernel should be associated, but because if you go back to the expression here, there is no local kernels that present here yet the mpf problem, you do need, you do need to be multiplying all the local kernels together, before to proceed the marginalize.

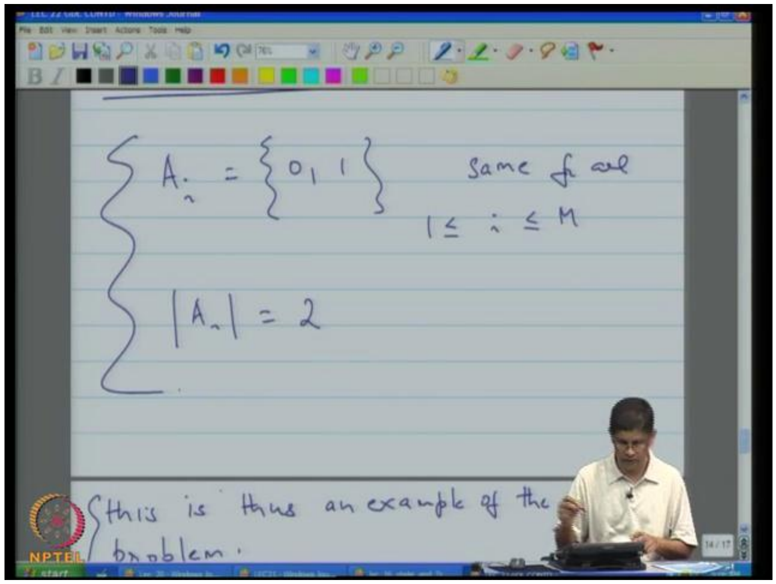
So, the answer is quite simple, you just introduced artificially, somewhat artificially local kernel, and you say that alpha five of x S 5 is just 1. So now, so this way having to effect to product in yet it map satisfies the property that you have the left hand side variables also, collection of variables also local domain. Now it is perfectly in the setting of an mpf problem, and again in going through this examples, my work may doing right now objective write now is little bit limited all the bit going to do is just take computation arising it whatever origin and put it in the settings an mpf problem. Later on and will actually go head on see how one will, one will solve it just to give a slightly that a feel for the watch transform let me put down in its metric format. So, it is metric format it would look like this it would actually would have the hard would have in 8 by 8 matrix in its I can do that. So, kept I can put it here. So, that would work.

(Refer Slide Time: 44:49)



So I have, so it would be a computation like this; just so that I, so never minds, so in the right hand side, I will have the various values of function f. So, I will have f of 0 0 0 f of 0 0 1 f of 0 1 0 f of 0 1 1, all the way down to f of 1 1 1, and that remains that I forgot to tell you something that was important mainly that these variables the alpha took that of the variables, something that I forgot to actually tell you. So let see, if I can insert a page, and fit that in theorem.

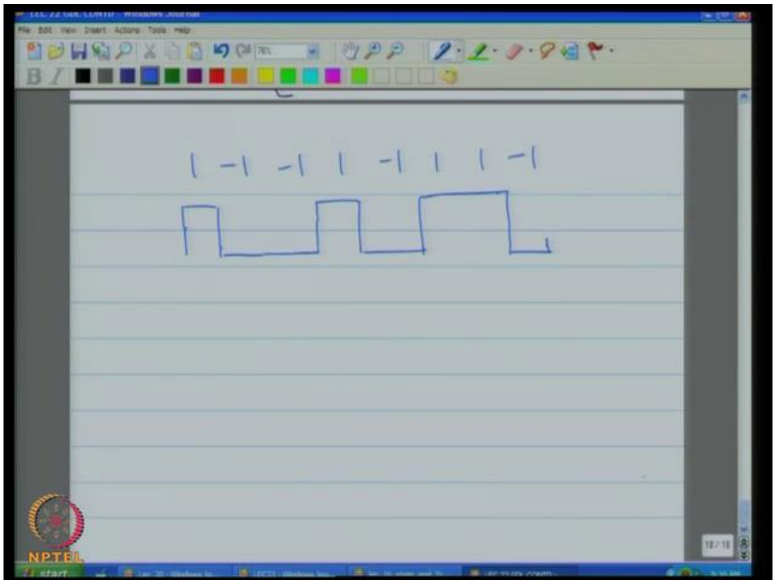
(Refer Slide Time: 46:23)



So, for as alphabets go, the alphabets a i; so each alphabet a i is just the binary alphabet 0 1. So, this same, the alphabet is the same for all i between 1 and M and of course, size of each of this alphabet is 2. So, that is for as alphabets score. So, that is the reason, when I am writing down matrix version on this computation, I have all the 0s and 1s over here. And here on the left hand side, what I am going to become computing are f of 000 f of 0 0 1 down to f of 1 1 1; in the middle I have what is called the Walsh matrix or Hadamard matrix and entry of this matrix or simply this is specific hard term is follow. So, I am going to ask on dividing line which makes it easier. So, it terms out these entries are 1 1 1 minus 1 1 1 minus 1 1 1 minus 1 minus 1 minus 1 minus 1 1 and so on and here again.

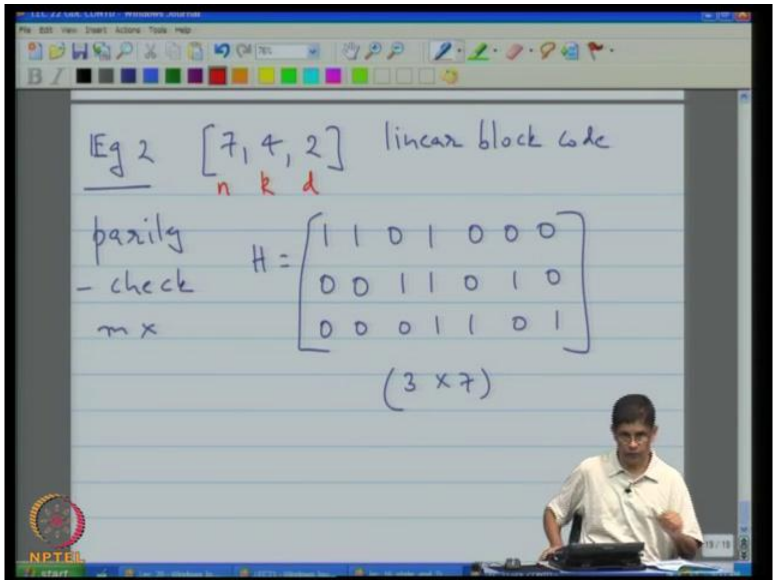
So, never mind; however, actually obtained these entries, this is simply part time if you stare at till if you figure it out. The reason I just want to introduce this simply because if you replace each 1 with a pulse strain, with a pulse strain pulse with positive height in minus 1 with a pulse of negative amplitude. Then you will get the Walsh function there employed in cdma. So, for example, so this is purely for motivation, we will not be using this.

(Refer Slide Time: 49:38)



So, let me take this last Walsh function that I have here. Then this should be associated with a pulse strain that pulse strain will go positive, then negative, and then again go for positive, negative, positive, positive and negative. So, this is the pulse strain that this particular string of symbols represents, then these functions there are used to keep the different users in cdma forward or downlink separate. But this is again I said purely motivational getting interested in the computation. So, that is one some kind of an example that the gdl can actually compute.

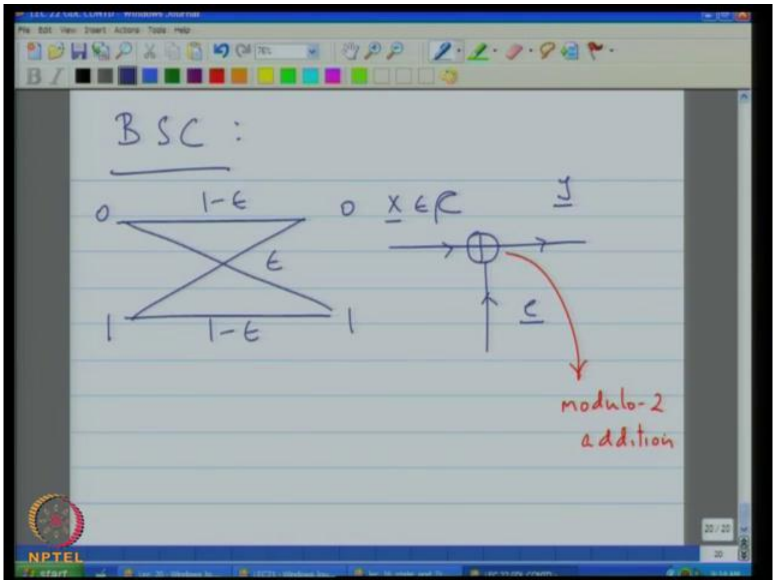
(Refer Slide Time: 51:54)



So, let us move to example 2; example 2 is an example from coding theory. So, will look at specific error correcting code; we will look at 7, 4, 2 linear block code, and will specified in terms of parity check matrix. So, the parity check matrix, each of this code will be given like this. So, this is the parity check matrix, and so you can see that this is the 3 by 7 matrix as required. Recall that whenever we write 7, 4, 2 linear code, what we mean is that the code has block length n, dimensional k and minimum distance d equal to 2. Now if still remember that some of the example, codes we look at earlier on you might say, this is 7, 4, 2 code, but don't have remembered you telling is or showing is a hamming code, which whose parameters are 7, 4 and 3 which means that the hamming code the relation this code, which I am showing your now has the same block link 7, the hamming code has the same dimension which is 4, the minimum distance here which is 2 whereas, the minimum distance of the hamming code is 3.

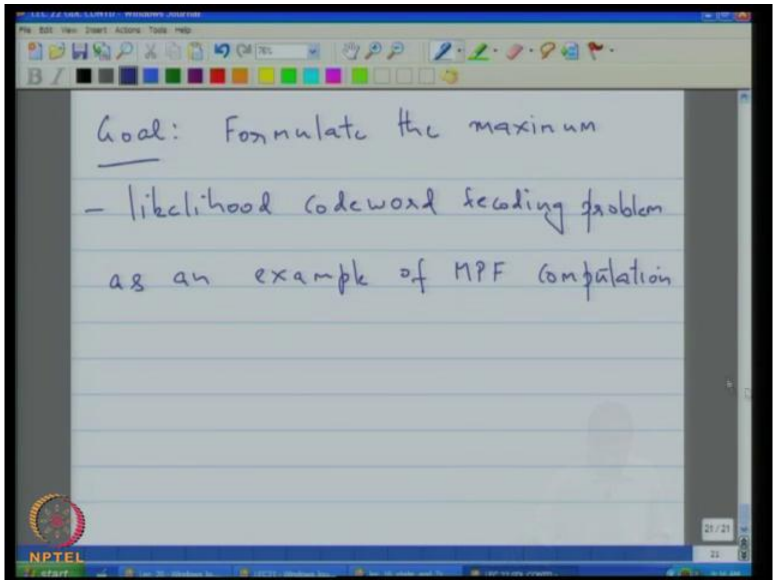
So, (( )) have why this code interesting; it have minimum distance which is less than that of the hamming code. And in fact, that is is vertical of this of of the wave coding theory as gone in recent years, because emphasis gone wave from trying to find the code, that is structurally have the best to one that easier to decode. So, this code by being modest code is hamming code, it does have break advantage over hamming code mainly that advantage of being easier to decode. So, this is very typical.

(Refer Slide Time: 53:56)



Now also setting in which we are going to look at this code is that of the binary symmetric channel. So, we are going to assume binary symmetric channel, which we can view in one of two ways either we can view it like this, input 0 1 output 0 1 with cross over probability epsilon or we can also view it as 1 in which you transmit a code word x, receive y and channel introduced an error vector e and this addition is of course, modulo 2, and addition here is modulo 2; and it is component by component. And this x actually is belongs drawn from over code, see step is transferred over code.

(Refer Slide Time: 55:27)



What we like to do is formulate the problem of carrying out maximum likelihood decoding, code word decoding in this code as an mpf problem. So, that will be here goal formulate the maximum likelihood decoding, and I should say perhaps I shall let me write spell this out, just to eliminate any confusion, formulate the maximum likelihood code word decoding problem, as an example, of mpf competition.

So I think, we just have a couple of minutes left summarize. So, what we have done is, I have defined what something called an mpf problem, and which turns from marginalize product function, and our goal actually show that problem of interesting decoding of codes of interest can be formulated as mpf problem. And that the generalize distributive law can be used to solve this problem. We began the lecture, further examples of semi rings that is have your left of in a previous lecture; and then after that I gave you the general setting of mpf problem, introduced all the notation. And then started at example the first example, that we look at is the 8-dimensional Walsh Hadamard transform, and then we just move to discuss it second example, which had do it maximum likelihood code word decoding of a block code. We will continue next time, thank you.