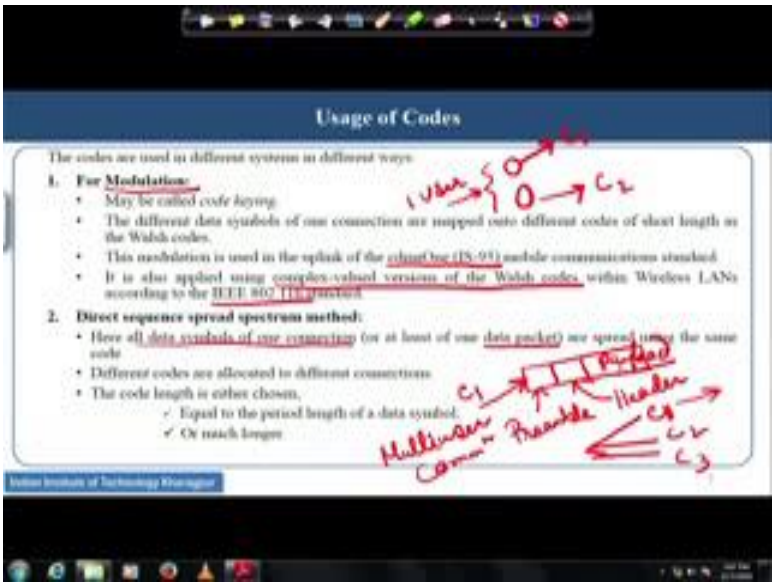
Spread Spectrum Communications and Jamming
Prof. Debarati Sen
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

Lecture - 14
Walsh Hadamard Code and Properties

Hello students, today we will discuss about the different codes that are used in spread spectrum communication systems, and there are several properties involved. We will also try to understand the interrelation of the different codes, the fundamental autocorrelation and cross correlation properties, and the key sense of a using those codes in different kind of the applications involved in practice. The first kind of the codes which is widely used in practical system design is the Walsh Hadamard code, and we will start with that. But before detailing about this kind of the code generation - Walsh Hadamard code generation, we would like to revisit the usage of the codes.

(Refer Slide Time: 01:19)



So, the codes spread spectrum communication systems, the way they are used may be broadly classified into two ways. Ones for the modulation, we call it the code keying when codes are used for modulation, then they are done that code keying is done in this way. You take each and every data symbol of any user or a single connection one user

and then each of this symbols are then mapped into different codes. So, this symbol will be utilized you will be utilizing the code 1 and he will be utilizing code 2. So, for several number of the symbols, you are having 1 1 dedicated codes for that, so it is the code modulation as if going on. So, it is the called code keying. We have utilize this kind of the code keying in a practical system design CDMA 1 or IS-95 mobile communication standard where in the uplink communication this code is utilized. The each and every symbol of a user is mapped into different kind of the codes.

Also the complex valued version that is used or completion of the Walsh code which is used in your WLAN especially in a 802 dot 11 B standard this is also an another example good example of the code keying. Another kind of the uses; so code utilize for the modulation is one application code can be utilized for spreading also for giving resilient against the jammers and the interferes, which we are discussing since beginning of these course. Here when code is used for the spreading the spectrum then all the data symbols of one connection there or at least the one data packet, they will be spread using the same code.

So, data what is the meaning of a data packet, if I see the structure of a packet, packet may be constituted by the number of the frames. So, let us understand that one packet is supposed having one frame. Then the package will have mainly the three sections one is actually the called preamble, where we sent the training sequences to synchronize the transmitter and the receiver. And there comes a we also utilize the sum sequences here for our channel estimation; we do AGC - automated gain control also during this period, so and also the frequency synchronization.

So, time frequency synchronization, channel estimation for all that is saying some known training sequence from the transmitter. And the bits associated to that operation we call it a preamble; and all the symbols were associated is second block is constituted of a header section which is basically the indication about what kind of the modulation you are utilizing for the next data coming or what kind of the coding you are utilizing for the next data coming. And the rest part of the packet is a payload. Here is the actual modulated data symbols are sending during this section. So, this is the whole packet for a

one data packet. So, one data packet does not mean you are only sending the data symbols is the constitution of the preamble header as well as the payload section.

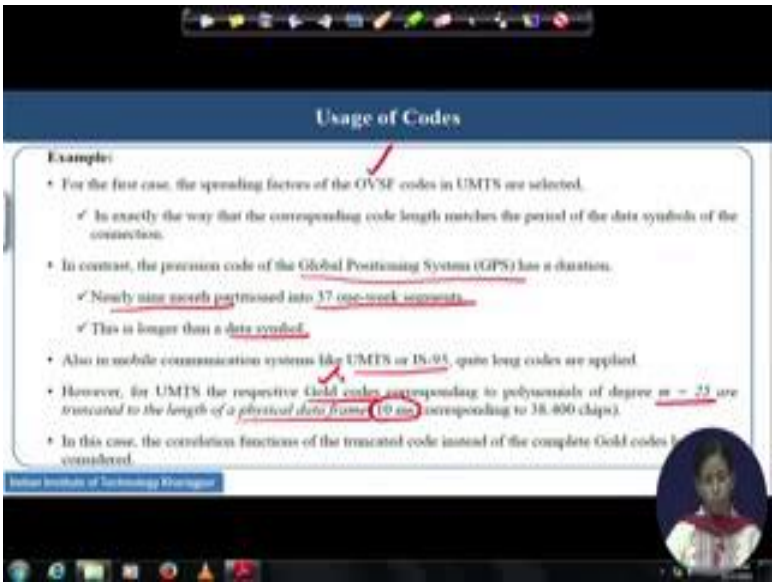
So, when we utilize a code to spread the data symbols at least one packet if we keep the spreading code sent then it is actually the spread spectrum. You usually we do not prefer to defer to use different kind of the codes to spread the same section of a one (Refer Time: 05:32) within a packet. We do not utilize a different kind of the codes for spreading for different section of the payloads within a packet. So, different codes maybe allocated and for spread spectrum communication you may utilize actually the different code for the different packets that is true. But usually when it is utilized for the segregating the users, then we utilize one dedicated code for one user; and for different users we prefer to align prefer to provide different kind of the codes to separate them out. So, as the codes we have understood that codes are required to be orthogonal to each other. So, the interference from one kind of the code to the next will be minimal even if actually they are transmission time is same. So, users will be differentiated by means of the orthogonal codes, they are uniquely utilized for each of them.

How the signals from the one user to the next will be differentiated out is such that you will be always a receiver will be always multiplying the combined signal combined received signal by means of his own known code. So, as the codes are orthogonal to each other I mentioned that its interference with the other set of the codes. I mean the cross correlation with the other set of the codes over the duration of the symbol duration will be perfectly 0, and you will be ending up with the signal to extract out, so that is the de-spreading procedure that we have already learned.

But this different codes, when they are allocated to different users, we call it is a codes are getting utilized for the multiuser communication. So, codes utilized for your spreading for one user to provide resilient against the interference and jamming is one usage. And then the at the same time different codes allocated to the different users not only they are giving the resilience to their from the interference the jammers, but also it is providing a very good kind of protection from the cross from the co-channel interference is kind of from the core users and the core network user kind of interferences. The code length in such a scenario, the way we choose it may be of two

types. Either you choose actually the period of the length of a data symbol or sometimes we choose the length of the code will be much, much longer than the duration of a data symbol, where we use which one is the next slide we will learn.

(Refer Slide Time: 08:26)



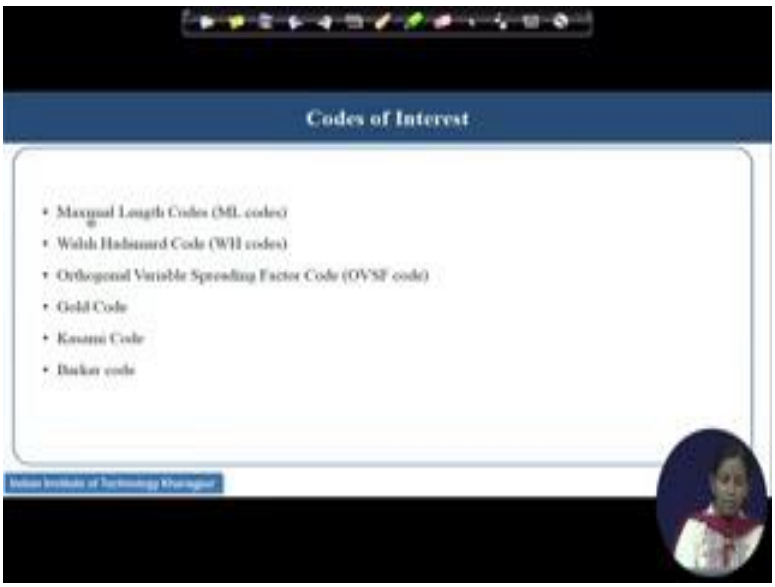
For example, the OVSF codes orthogonal the variable spreading factor codes, which we have to utilize in the UMTS system - universal mobile telecommunication system, they are exactly of the length of the code is exactly of the symbol duration. But in contrast, the precision code that we try to use in the global positioning system, it has a duration of 37 one-week segments, it is having a total period of a nine months which we have a partition for 37 one-week segments. And which is far, far longer than the duration of a data symbol. And this was necessary because you really do not reach it is a local it is a precision that you are asking for the localization in the GPS. We do not prefer anybody to hack the codes and that is why the length of the codes is chosen. So, long and we understand that if you are having a non-linear codes as well as a very long duration code, it will be very, very hard to track the code.

Though in the mobile communication system like UMTS or IS-95 a quite long codes are applied this kind of the codes like the GPS we also pay for to utilize. In UMTS, the Gold codes are utilized where actually the polynomials of M is equal to 25 are truncated. See,

if sometimes actually we generate a code of the very long length and then finally, we can truncate it physically to actually from the full form it is reusable format. And in UMTS, such kind of a Gold codes which is truncated with the length of the physical data frame approximately around the 10 milliseconds and that is utilized in practice.

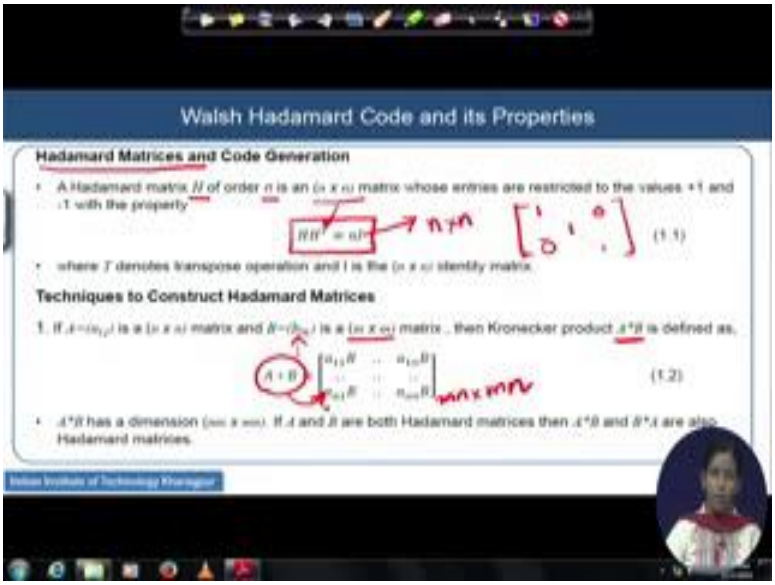
So, in this situation, the correlation function of the truncated codes they were ever will be equivalent to the complete Gold codes that we are utilizing. In this slide, already we have utilized we have talked about few some kind of the codes for example, OVSF is 1; Gold code is another. So, you now know that these are the name of the codes which are most popularly used in practice. We will slowly enter into the characteristics and the generation process of each of these codes today.

(Refer Slide Time: 11:01)



So, codes of our interest, there are maximal length sequence codes which we have already studied in detail. And the rest are the new to us the Walsh Hadamard code, orthogonal variable spreading factor code, Gold code, Kasami code and the barker code. We will learn all the remaining five types of the codes and with the fact that maximum length codes whatever is discussed is well understood.

(Refer Slide Time: 11:28)

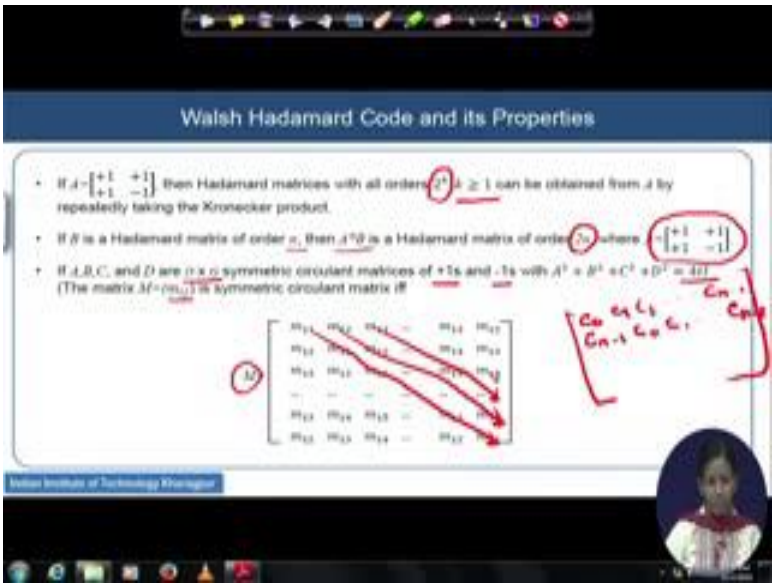


Let us start with the Walsh Hadamard code. Before entering into the generation and the properties of a generation mechanism and their properties of a Walsh Hadamard code, let us start with the Hadamard matrix, because the key part of this code generation is a matrix is a Hadamard matrix. The matrix is a suppose it is a matrix is called H, and its order is n, then it is an n cross n matrix, whose all the entries will be either plus 1 or minus 1. And it has a very unique property that H into H transpose will give you small n into I, I is the identity matrix and as it is an n cross n matrix. So, this I will also be an n cross n identity matrix. So, the construction will be like this; with an call an identity matrix. And the T here it denotes the transpose operation on the matrix. So, H into H transpose, it should boils down to a identity matrix multiplied by the order number. There are several mechanisms; and the way, we can construct the Hadamard matrix; we will learn them one-by-one and finally, we will enter into Walsh Hadamard code.

See the suppose A is the matrix which is having its elements a i j, and he is an n cross n matrix. Suppose there is another matrix B, which is having his entries with b l k and this is also an m cross m matrix then the Kronecker product of this A and B given by A dot B like this can be given as this all the coefficients of this a multiplied with the matrix B n given by the format written in equation 1.2. The dimension of these guy will be always m n cross m n.

If now this A and this B both are the Hadamard matrix, so the property says that A dot B which is the Kronecker product of A and B and also the B is star A whatever be the way you construct it will be also raising an another Hadamard matrix. So, this is the first property of the matrix Hadamard matrix by means of each from two Hadamard matrix you can generate the third Hadamard matrix. So, the first this is the first generation mechanism of a Hadamard matrix from two are there other two Hadamard matrix of different sizes or different orders.

(Refer Slide Time: 14:25)



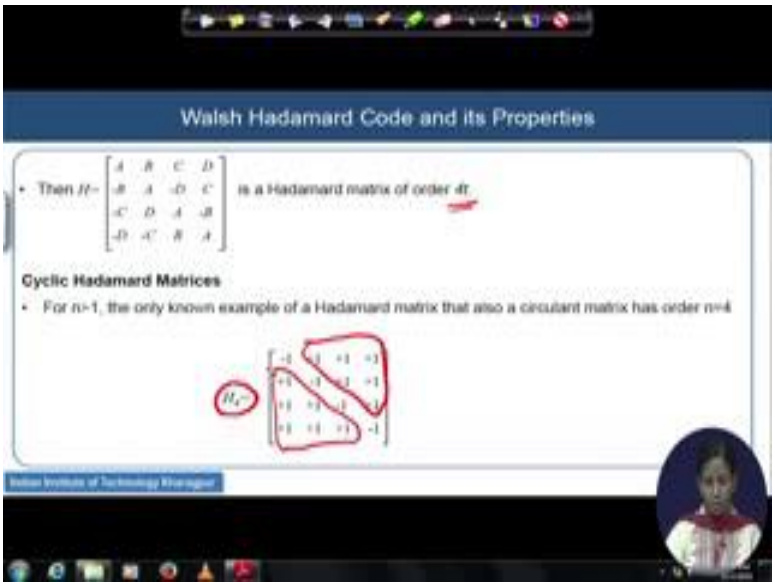
So, the suppose A given by this plus 1 plus 1 plus 1 minus 1, it is an Hadamard matrix with all orders 2 to the power k, where k is always greater than or equal to 1. It can be obtained from a repeatedly taking the Kronecker product. So, if A is this and you can generate the several Hadamard matrices from A, by actually simply increasing the order to the power of 2. If k is equal to greater than or equal to 1 by the Kronecker product of that the way we have shown earlier. If B is an Hadamard matrix which is having an order of n and then we understand that A star B is will be an Hadamard matrix, where A will be given by this and this Hadamard matrix will have power of 2 n.

Suppose A, B, C and D, they are the t cross t symmetric circulant matrix is the circulant matrix always look like this. Suppose, you have c 0 to c 0, c 1, c 2 dot dot dot say

suppose c n minus 1 elements in the matrix. If it is say so it will to be a circulant matrix then in the next row, you should be able to see that c n minus 1 is there, c 0 is there, c 1 is there dot dot dot, you are ending with c n minus 2. And this is the way we will be able to see that this is 0, the all the locations it is circularly all the elements of the matrix they are circularly rotating. So, if this is a property, this property is observed, then we will say this is asymmetric circulant matrix.

And suppose you are calling that we are having four matrices which are t cross t symmetric circulant matrices, and their entries are restricted to be plus 1 and minus 1. Such a way that if you square them up and add them up, you will be ending up with 4 t i. And then the matrix bigger matrix capital M, who is having this entries as m i j, he will be actually a symmetric and circulate matrix if and only if this is a matrix construction going on. And you see that all these elements, who are having the, each and every element is having a symmetric circulant property, and see the way they are moving.

(Refer Slide Time: 17:18)

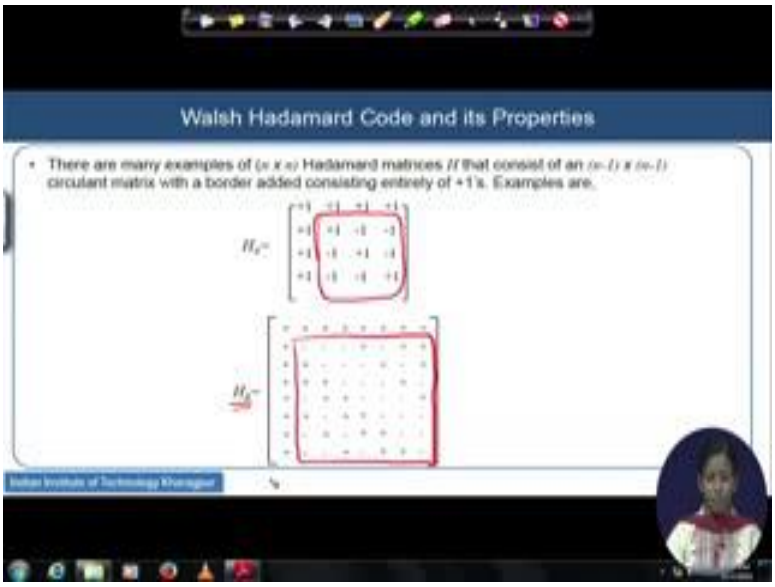


So, if this is the situation they will be having a symmetric circulant matrix if and only if that happens and then we can construct Hadamard matrix from all those four symmetric matrices combining them in this way. So, first row consists of all those t cross t symmetric matrix. Second row will be taken as the in as minus of this B and then A

minus B C. Third construction will be like this. So, fundamentally you are doing something, here it is actually the A, B, C, D the matrices it is a symmetric 2 cross 2 asymmetric matrix and here all are the transpose and then you are constructing the fundamental matrix A shift A. So, you are shifting the fundamental matrix as well as you are taking the transpose of them. And this Hadamard matrix the way it is constructed here from a four different matrices which are having a circular symmetry property as well as a typical dimension given in the last slide. The Hadamard matrix we are ending up with it will have a order of 4 t.

So, cyclic Hadamard matrix, now we will enter into; and say for n greater than 1 the only main example that you may have for the circularly symmetric Hadamard matrix, which is a order of 4 basically and this denoted as H 4. See, the way the matrix is circularly symmetric is, this was the first element first rows say that first row elements are Hadamard matrix. And if I rotate it, then it will form the symmetrically shifting symmetrical form is given, and it is shift all the elements as cyclically shifted. So, it is a symmetric; the symmetric nature comes from the fact that you see the upper portion of the matrix, which is exactly the similar to the lower section. So, this is the way the symmetric property holds good, and that is why we are calling it also circular matrix and it has an order n is equal to 4.

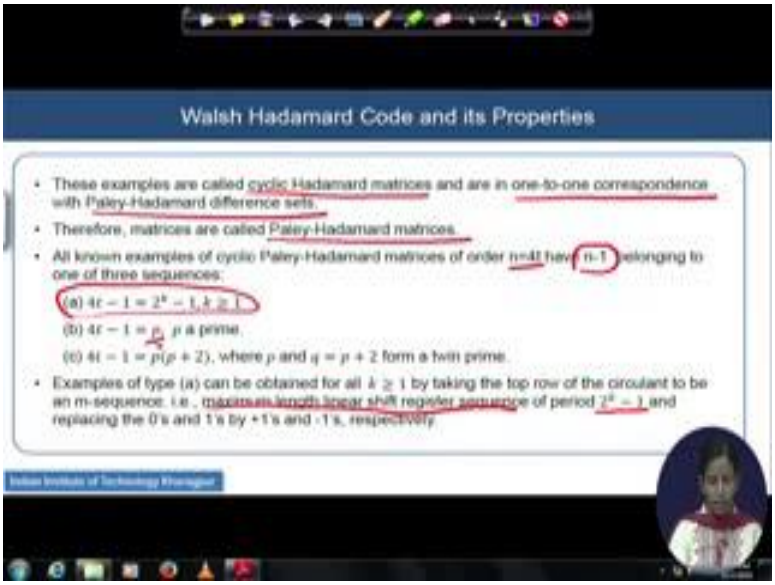
(Refer Slide Time: 19:47)



There are a many examples of this n cross n Hadamard matrices H that consists of this n minus 1 cross minus 1 circulant matrix. See, there is an example. Actual matrix and in that if you are getting an n minus 1 cross n minus 1 circulant matrix; and if you add the border of plus 1, you will be able to get you an n cross n Hadamard matrix inside which there is a n minus 1 cross n minus 1 circulant matrix. Let us take an example of another H 4. See, this H 4, this is the fundamental n minus 1 n cross n minus 1 matrix circulant matrix. See, the property this is plus 1 minus 1 minus 1 it rotated once this minus 1 came here plus 1 and then minus 1; you rotate one with more and then this minus 1 one more you rotate it one more and then it will be shifted. So, plus 1 is getting shifted slowly and then this minus 1 first came here, and then this is shifting here. and the last minus 1 is there. So, this section is showing the circulant property, and the Hadamard matrices is constructed by giving a border of the plus 1 on the top and towards the left.

Another example good example is H 8. Inside H 8, you see this section. These are pluses written because I have just because of the size of the matrix, we have not written the ones. We basically minus says that actually minus 1, and plus says the plus 1. And the way it is moving, you see that it is a circulant, so this plus 1 is moved, this minus 1 are moving slowly shifted one time, you do one more shift, and then actually this will be moved for two places, similar, the 3 plus shift, 4 plus shift like that this is going on. And you can construct Hadamard matrix by adding a border of the plus ones on the top row and to the leftmost row. So, like that you can check several Hadamard matrix where you we will see the matrix is basically is constituted of the n minus 1 cross n minus 1, where n is the order of the Hadamard matrix; and he is consisting of n minus 1 cross n 1 circulant matrix inside that.

(Refer Slide Time: 22:13)



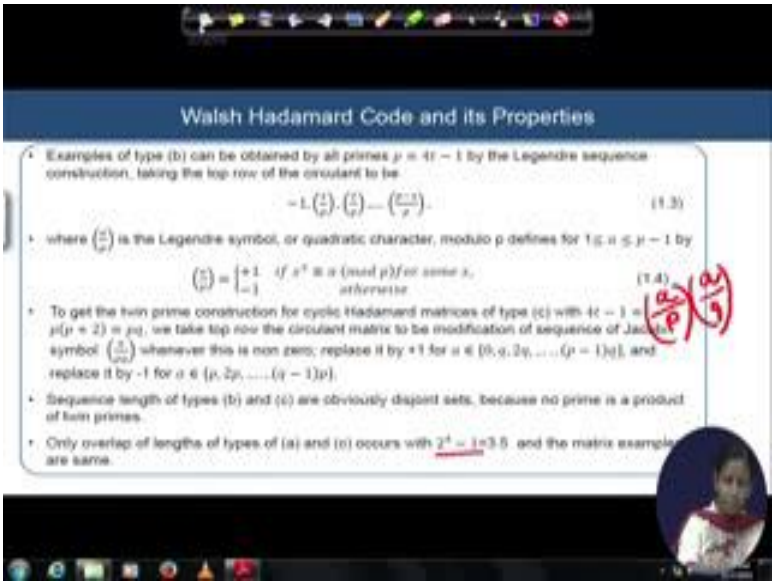
So, this example so which we are calling as a cyclic Hadamard matrix, and they are having basically a one-to-one correspondence with the Paley Hadamard difference sets, so that is why we are having so sometimes we call with the Paley Hadamard matrices also. So, all the cyclic Hadamard matrices are basically the Paley Hadamard matrices. And very good well known examples of the cyclic Paley Hadamard matrices of the order n is equal 4 t; and 4 t, they are having n minus 1 belongings inside; and then the n 1 minus belonging to only have any one of these three sequences involved in that.

For case number one, see that 4 t, if you have a order is n is equal to 4 t. So, 4 t minus 1 is equal to 2 to the power k minus 1 will be either type. So, in order to generate this first type of the Paley Hadamard matrices, we have to have that k should be always greater than or equal to 1, and we start from a maximum length sequence. So, maximum length linear shift register sequence, we keep it as a top row. And then we try to go ahead with the circulant of those all m sequences. And this period of the maximum length sequence that you are taking this is having a relation with k is equal to 2 to the power k minus 1.

But remember the maximum length sequence is really consisting of 0s and 1s. So, you have to replace all the 0s by minus 1 and all the plus 1s with the plus 1 only. So, 1s and 1s will be presented by the ones and minus 1s so respectively; and the way you are

constructed for the Paley Hadamard matrices will be ending up with Paley Hadamard matrices with this with this typical relation. So, say the for second type of the situation, to generate the Paley Hadamard matrix of type p ,where p is considered to be p is called a prime number that will be generated like this.

(Refer Slide Time: 24:23)



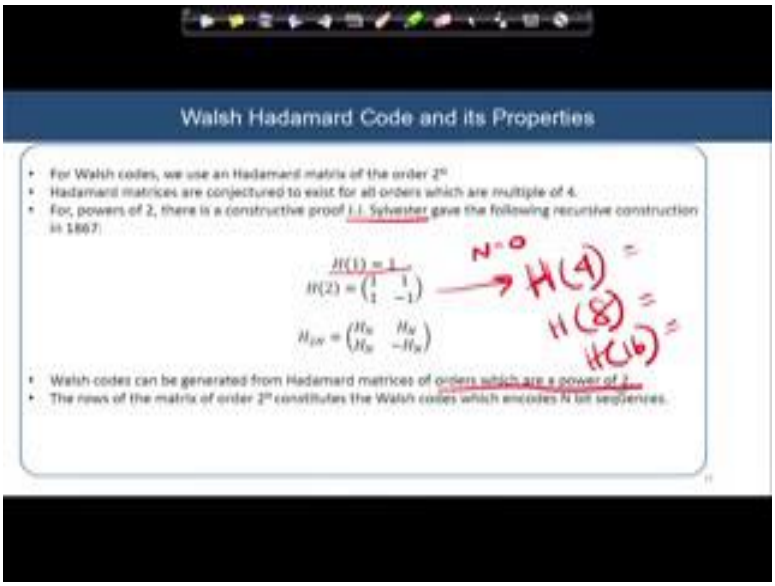
So, for a second type of the Paley Hadamard matrix for all primes to be 4 t minus 1, we will start with the Legendre sequence. The Legendre symbol where actually 1 by p or each and every one is called Legendre symbol of quadratic character for modulo two which defines that for a belonging to 1 to p minus 1 by this relation, where each and every Legendre symbol should have either plus 1 or minus 1. For plus 1, it will have the plus 1 if the x square the quadratic character is coming actually modulo p operation is obtained equal to the value obtained by the module p operation for some x. And it starts with this by taking the top row to be the Legendre sequence and then start the generation.

The third type to get the twin prime construction of this cyclic Hadamard matrix of the type c which says that it should have a 4 t minus 1 equal to p into p plus 2 equal to p into q, where this p and q these are actually the prime. These are the twin prime numbers. They are the twin prime numbers. And then we take the top row of the circulant matrix to start with to be a from the Jacobi symbols, where this Jacobi symbols a divided by p into

q whenever this is nonzero element, and they will be replaced by plus 1 for a, when a is moving from 0 to p minus 1 into q. And it will replace minus 1 for all the values of the a which belong to p twice the p to it q minus 1 into p.

Remember actually here, if symbols are say to be completely independent, this p and q they are independent and they are not having any kind of their GCD is equal to 1. In that situation, actually there is a Jacobi symbol it can also written as a by p into a by q, I mean the multiplication of the two Legendre symbols. And the sequences that we have generated by the type b and type c they are obviously, disjoint. As said because there is no prime product no prime is a product of the 2 prime numbers. So, they can never be another prime number. And hence B and C are completely disjoint, the generation process itself. Some overlapping may be possible because in the generation type one and the generation type c sorry a and c; for say example when the 2 to the power 4 k value is equal to 4, and you are getting it is 15. So, 3 cross 5 is the example where actually c can be generated by means of this and also the by type a, our c you will get a 15 length sequence.

(Refer Slide Time: 27:45)



Now, this is the time with this understanding of different methods of generating the Hadamard sequence, let us see that how Walsh Hadamard sequence is generated. For

Walsh code, we use the Hadamard matrix always which is having the order of 2 to the power of capital N. And this Hadamard matrices are conjectured to exist for all the orders which are multiple of the 4. And for the powers of the 2, there is a consecutive proof given by J.J. Sylvester who showed that the higher order Hadamard matrices Walsh Hadamard matrix, Walsh Hadamard codes can be generated from the lower codes, lower order codes. So, this recurring relation we will be using for generation of the Walsh Hadamard code.

See, suppose first two Hadamard matrix, which we are starting is equal H 1 where capital N value is equal to 0, and you are having one element inside the matrix. So, from here the higher order matrix H 2 will be generated like this, where these are the same one H 1 repeated in the first column and the first row first row. And the last element will be the conjugate of this. And if I generalize this rule then for H 2 n it will be look like this H n. If it tries in the corresponding situations, and the last material the last symbol and the last element of the matrix will be the conjugate of that.

So, Walsh Hadamard codes can be generated from the Hadamard matrix only when actually this can be generated this way when the order of the Hadamard is only the power of the 2. And the rows of the matrix of the order 2 to the power N constitutes of Walsh code which can encodes the capital N bit sequences. So, you can pick up actually the rows of this matrix as a Walsh Hadamard code. So, 1 1 such rows will be picked up to develop; and we utilize as a code and spreading code and they can be actually utilize to spread and capital N bit sequence.

And we can do a very nice exercise at home. So, from H 2 onwards, we will proceed to construct the structure of say H 4 and H 8, and try to find out find some kind of the similarities H 8 and H 16 onwards. And you may try to find out some similarities actually about the fundamental properties of the Hadamard matrix that we have already discussed whether all those properties and holding good for when it is constructed as a Walsh Hadamard code. Because Walsh Hadamard code is a restrictive usage are there, it is a specially constructed kind of the matrices, which has the fundamental rules on the Hadamard matrix. So, all the properties of the Hadamard matrices that we have already discussed all should be hold good, once the Walsh Hadamard code is generated. So, you

may actually try to have a look of all those properties once constructed the higher order values of this higher order Walsh Hadamard codes.