Error Correcting Codes

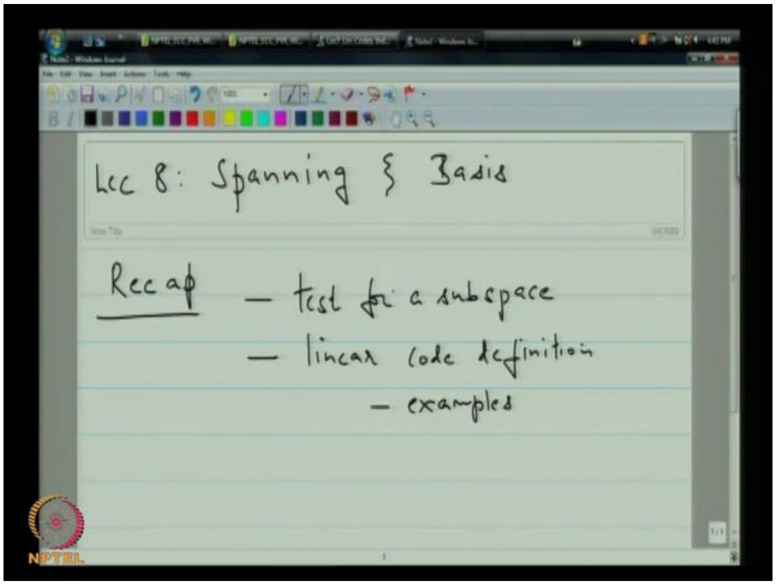
Prof. Dr. P .Vijay Kumar
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore

Lecture No. # 08
Spanning and Basis

Good afternoon, we will continue our lecture series on error correcting codes. So, in the last lecture, we began by looking at subspaces, how one would test subspaces with the examples. And then after finishing our discussion on subspaces, we went on to talking about, we made a comment that there was in a particular instance, there was no difference between a subgroup and a subspace, and that is the case which applies to linear codes. So, linear codes were introduced as examples of subspaces, but they also turned out to be examples of subgroups.

We briefly defined linear codes next, and then I went on to the linear algebraic notion of linear independence. And we went through a discussion by the saying what is it mean; and looking at examples. Then we went on talking about spanning, and we are just got started talking about what it means for set of vectors to spanner space. So, we will look at a examples and then we will put the two notions of linear dependence and spanning together and come up with the basis. So, that is the direction in which we are headed.

Refer Slide Time: 01:46)

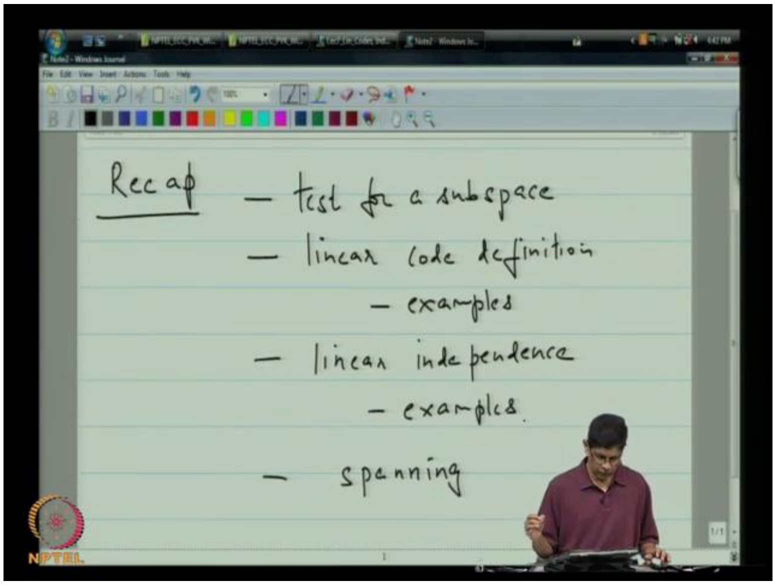


Lec 8: Spanning & Basis

Recap
- test for a subspace
- linear code definition
  - examples

Excuse me, so I have put down (( )) a title for our lecture. Let me just put down a quick recap, what we have done. So, we looked at test for a subspace. Then we looked at linear codes, linear code definition. We looked at examples.

(Refer Slide Time: 02:28)



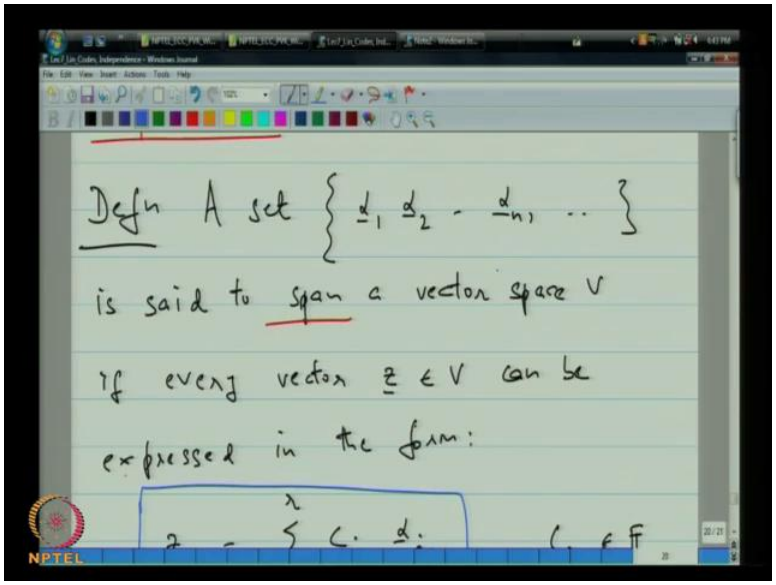
Recap
- test for a subspace
- linear code definition
  - examples
- linear independence
  - examples.
- spanning

So, we looked at linear code definition and examples. And after this, we went on to talking about the notion of linear independence. We looked at examples and towards the end of the last lecture, we talked about the notion of spanning. Let me just quickly go over our last lecture. So, I will actually kind of zoom out. Since, the intension is just to give a quick overview.

So, we began by talking about linear codes and linear independence. Testing for the presence of a subspace, then we pointed out that, we defined what it means to be a linear code. We showed that all the three example codes that we had to work with, where in fact, examples of linear codes.

And then after that, I talked about what it means for a set of vectors to be linear independent. We looked at examples in different settings in three-dimensional space with respect to the rows of a (( )) matrix, in the vector space of polynomials. Then we started talking about spanning.

(Refer Slide Time: 04:33)



Defn A set $\{ \underline{\alpha}_1, \underline{\alpha}_2 - \underline{\alpha}_n, .. \}$

is said to span a vector space V

if every vector $\underline{z} \in V$ can be

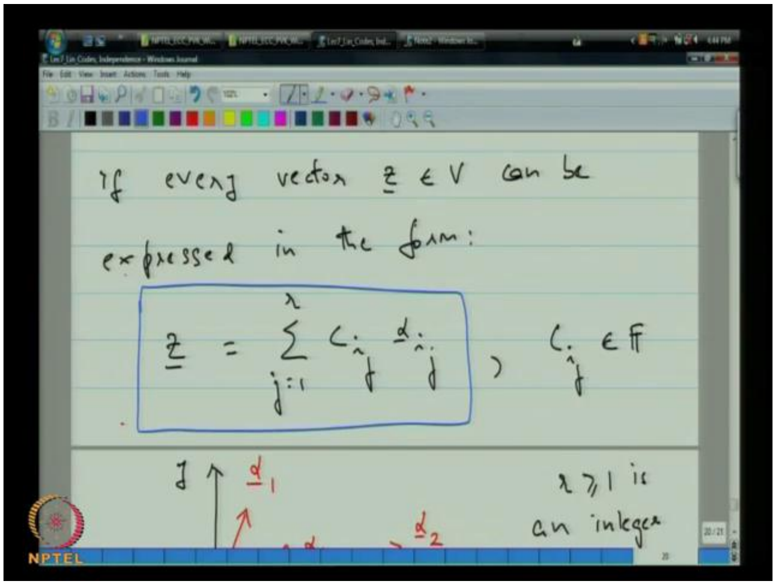
expressed in the form:

$\underline{z} = \sum^{\lambda} c_i \underline{\alpha}_i \qquad c_i \in \mathbb{F}$

So maybe I will just slow down a little bit here, so that because we need to pick up the discussion from where we left off here. So here, on the topic of spanning, a set of vectors is said to span a vector space, if every vector can be expressed as a linear combination of these vectors.

And whenever I defined these set, I have allowed this set to potentially contain an infinite number of elements. Although in all our applications, the set will be finite. So, in the case, when it is infinite what you really want is that in any particular instance, if you want to make sure that it is able to generate a certain vector z. Then all that you will do is you will call upon certain subset of r vectors.

(Refer Slide Time: 05:05)



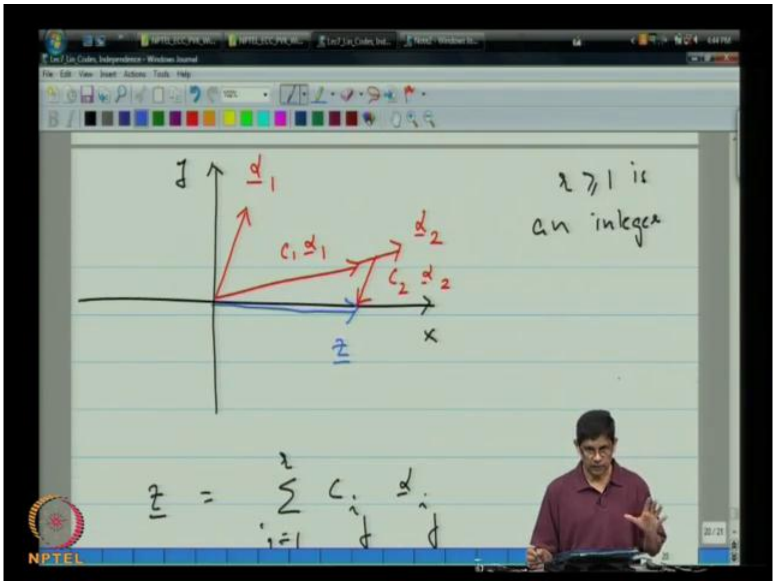
If every vector $\underline{z} \in V$ can be expressed in the form:

$$\boxed{\underline{z} = \sum_{j=1}^{r} c_j \underline{\alpha}_j} \quad , \quad c_j \in \mathbb{F}$$

$r \geq 1$ is an integer

So, whenever you take a linear combination, the linear combination will only involve a finite number of objects. However, the set from which that they are actually drawn can be infinite.

(Refer Slide Time: 05:25)

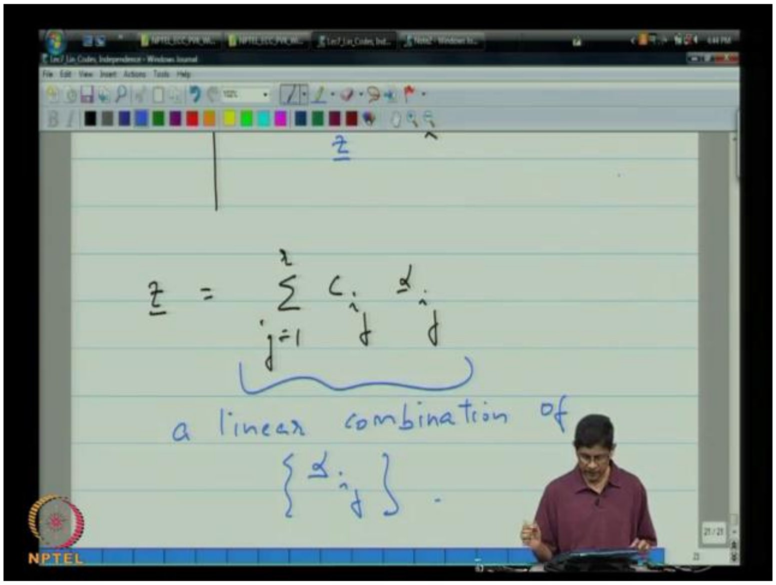


$l \geq 1$ is an integer

$$\underline{z} = \sum_{j=1}^{l} c_j \underline{\alpha}_j$$

So, that is subtle distinction. And here is a picture which tells you, what it means? What is the notion of spanning is all about.

(Refer Slide Time: 05:30)

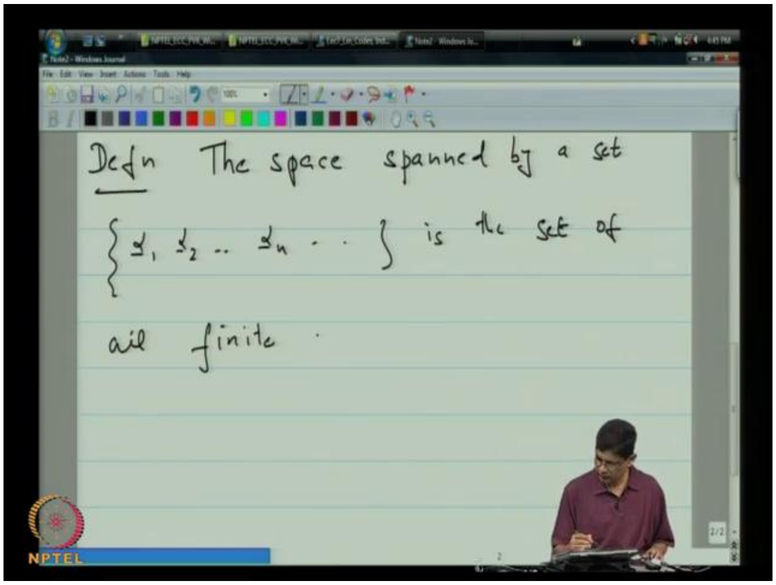


$$\underline{z} = \underbrace{\sum_{j=1}^{l} c_j \underline{\alpha}_j}$$

a linear combination of $\{\underline{\alpha}_j\}$.

And then this system analogy, this is explaining what we mean by linear combination. So we will pick up the discussion from here, and I will switch to my note book for this lecture.

(Refer Slide Time: 05:50)

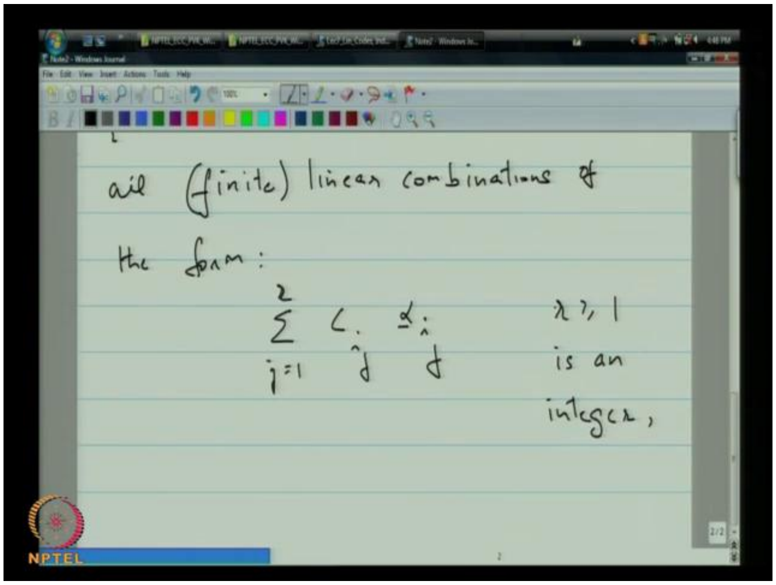


Defn The space spanned by a set $\{\alpha_1, \alpha_2 .. \alpha_n . . \}$ is the set of

all finite .

So there is another definition. The space spanned by a set alpha 1, alpha 2, alpha n is the set of all.

(Refer Slide Time: 06:43)



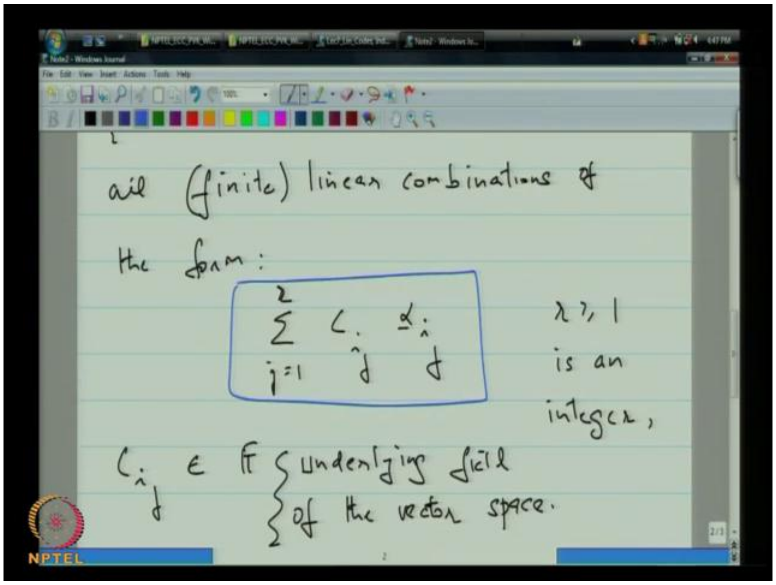
all (finite) linear combinations of

the form :

$$\sum_{j=1}^{r} c_{i_j} \alpha_{i_j} \qquad r \geq 1 \text{ is an integer,}$$

And in brackets I will write set of all finite linear combinations of the form sigma C i j alpha i j j is equal to 1to r, where r greater than or equal to 1 is an integer.

(Refer Slide Time: 07:26)



all (finite) linear combinations of the form:

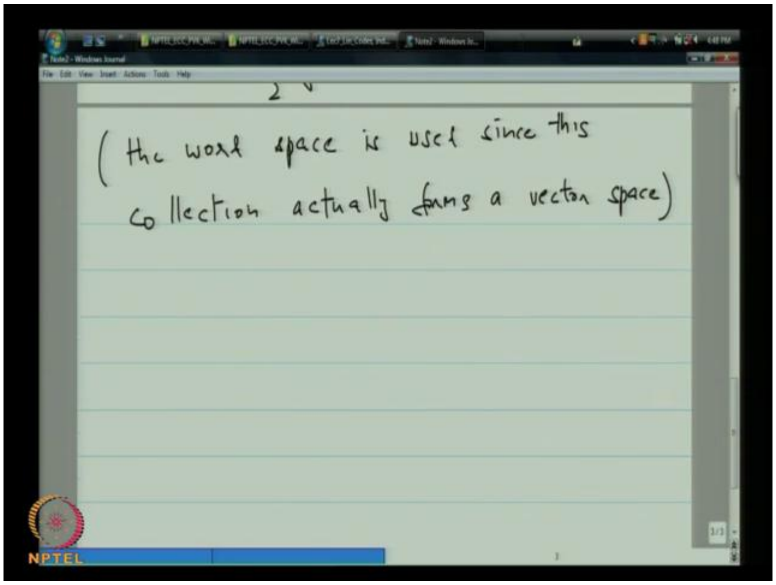
$$\boxed{\sum_{j=1}^{l} c_{i_j} \underline{\alpha}_{i_j}}$$

$l \geq 1$ is an integer,

$c_{i_j} \in \mathbb{F}$ } underlying field of the vector space.

And where, this C i j all belong to the f which is the underlying field. So, this is the underlying field of the vector space. Now, one comment here, I have used the word space, the space spanned. So, if where has basically, if you look at this. This is the set right it is a set possibly infinite.

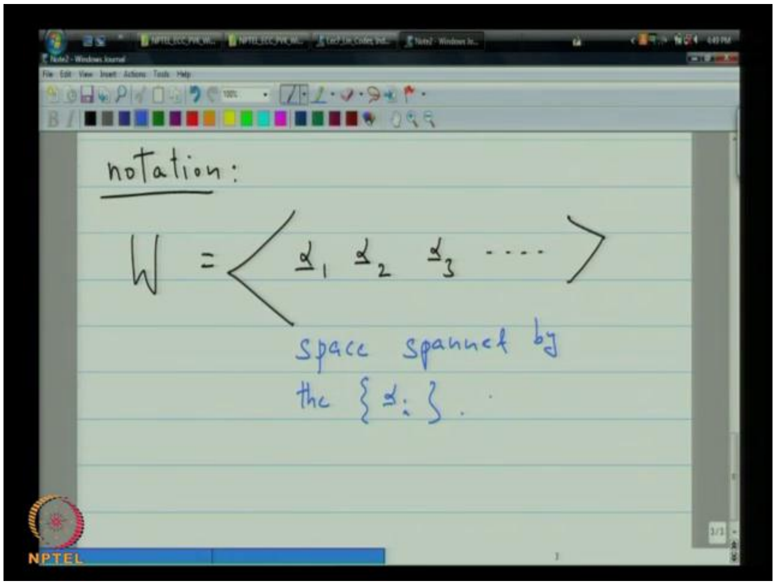
(Refer Slide Time: 08:30)



(the word space is used since this collection actually forms a vector space)

So, why do I call it a space instead of a set? The reason for that is you can actually show without much difficulty, that this space is actually a vector space. The word space is used, since this collection actually form a vector space. And you can verify that as an exercise.

(Refer Slide Time: 09:19)



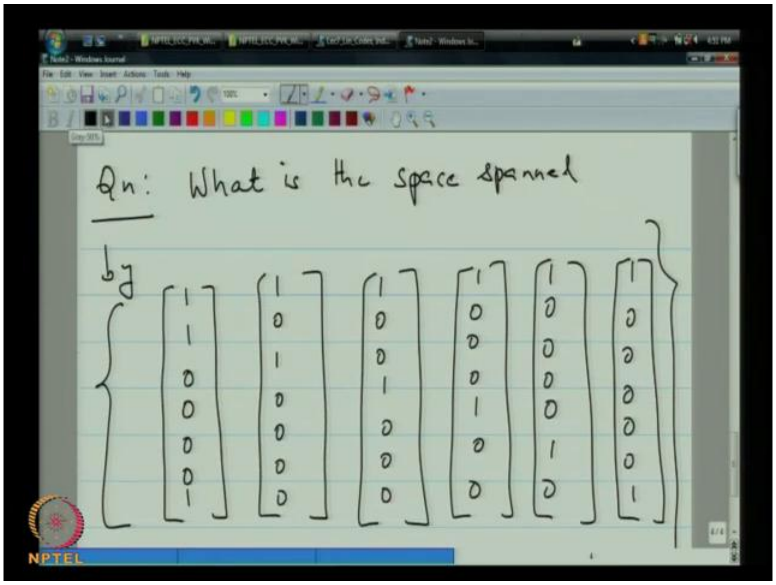
notation:

$$W = \langle \underline{\alpha}_1 \; \underline{\alpha}_2 \; \underline{\alpha}_3 \; \cdots \rangle$$

space spanned by the $\{\underline{\alpha}_i\}$.

Now, we will use the following notation, when we want to refer to this space. So, we will say that W is we will put angular brackets, and then will put alpha 1 alpha 2 alpha 3 dot dot dot. So this is terminology for the space spanned by. This is the space spanned by the alpha i.

(Refer Slide Time: 10:26)



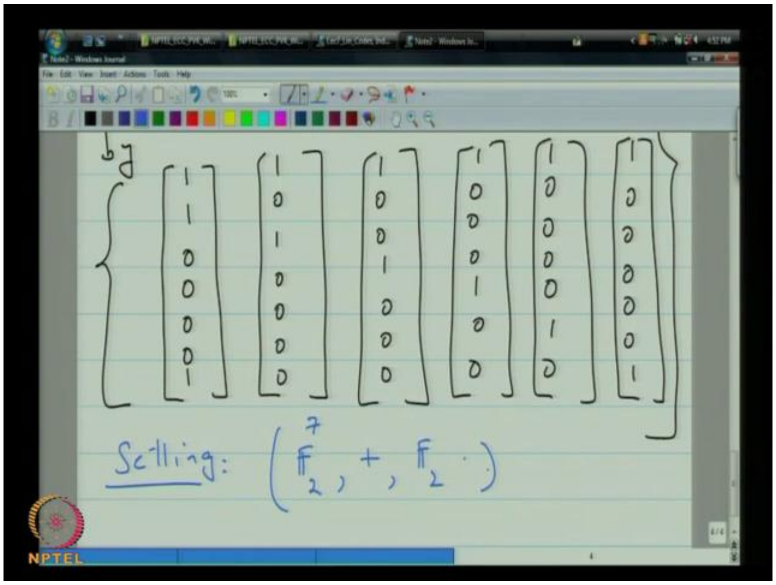
Qn: What is the space spanned by

$$\left\{ \begin{bmatrix}1\\1\\0\\0\\0\\0\\1\end{bmatrix} \begin{bmatrix}1\\0\\1\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\1\\0\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\1\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\0\\1\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\0\\0\\1\end{bmatrix} \right\}$$

Now, here is the question. So, if this, where in regular class room, I would pose this question to those in the audience. But you might want to think about it. So what is this space spanned by the following set? So I have put down 6 vectors here.

So, these commas here are little distracting. So perhaps I will just remove them. So we have 6 vectors here and the question is what is the space spanned by them? Now strictly speaking you cannot answer this question without knowing the setting.

(Refer Slide Time: 12:24)



by

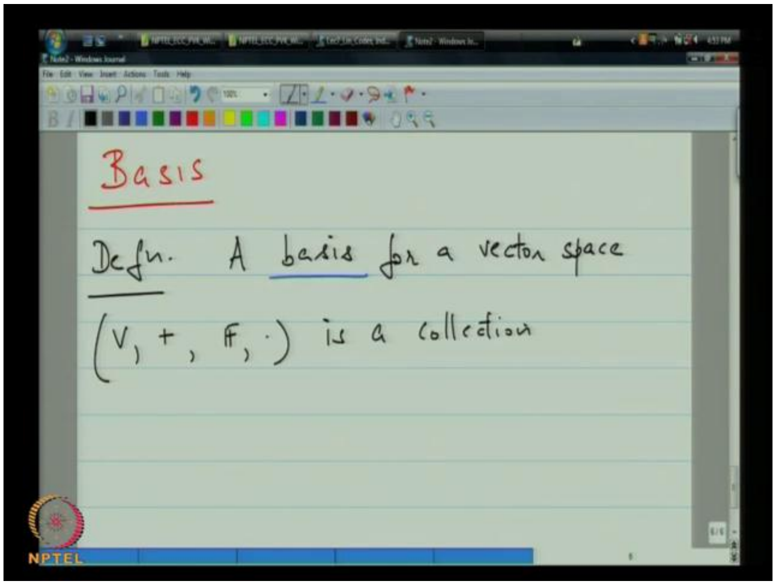
$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Setting: $\left(\mathbb{F}_2^7, +, \mathbb{F}_2 \cdot \right)$

So, this setting; so let me just say that the setting in which I am asking you this question is the setting in which, we are working inside the vector space F 2. So, we are inside this vector space. And the question is, we if you think about these vectors as vectors belonging to this vector space. Then what is the space spanned by these vectors?

So what I will do is I will continue with my lecture and I will come back and answer this. So, that you have a few minutes to think about it. So, I will leave a blank page so that I can answer that. And now, let us go on to the next linear algebraic notion, and this will be our last linear algebraic notion after this will get back to talking only about error correcting code, so some time to come.

(Refer Slide Time: 13:30)

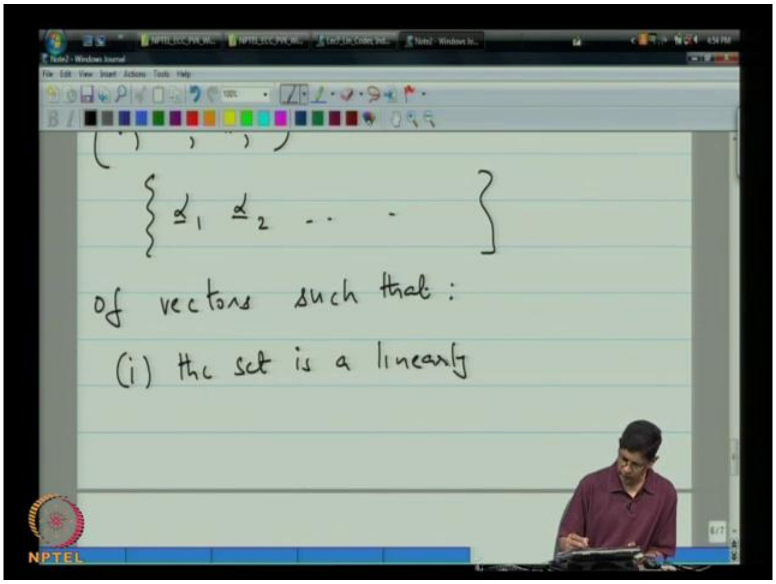


Basis

Defn. A basis for a vector space $(V, +, \mathbb{F}, \cdot)$ is a collection

So the notion is that of a basis, a basis for a vector space is a collection of vectors.

(Refer Slide Time: 14:37)



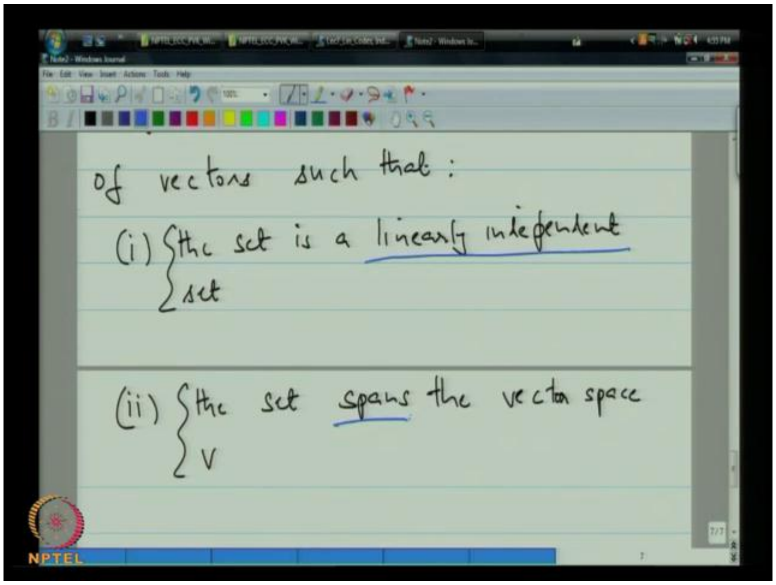
$\{ \alpha_1 \quad \alpha_2 \quad .. \quad . \quad \}$

of vectors such that:

(i) the set is a linearly

Such that, 1: the set spans the vector space V.

(Refer Slide Time: 15:31)



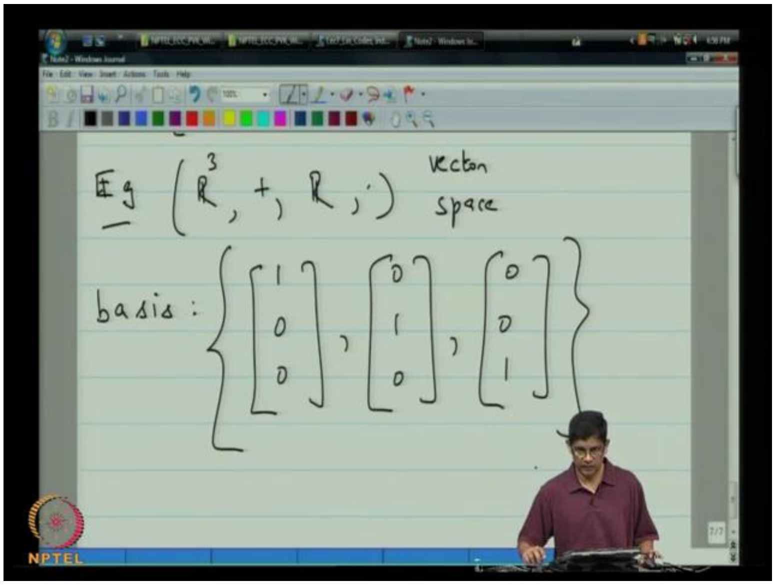
of vectors such that:

(i) {the set is a linearly independent set

(ii) {the set spans the vector space V

So, basis is something that combines the 2 notions that we had introduced earlier. One is that of linear independence and that is the other one of spanning. Now, one comment here is that when you look at this, and you see it for the first time. When you see this infinite collection of vectors, you might feel uncomfortable and I do not blame you for that.

(Refer time: 16:22)

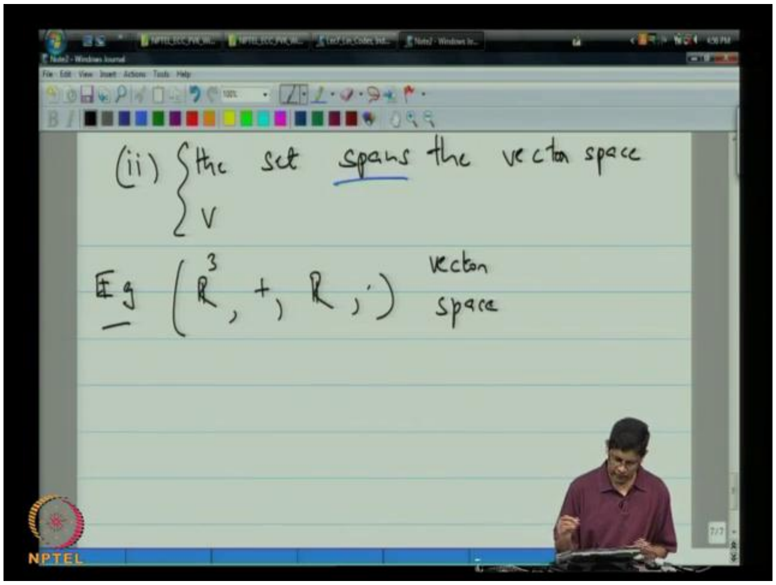


Eg $(\mathbb{R}^3, +, \mathbb{R}, \cdot)$ vector space

basis: $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$

So, if it is making uncomfortable you can pretend that it is finite, because as I mentioned earlier in all applications the set will actually be finite. So, let us pretend if you like, you can pretend that it is finite. So, this is the finite set and this set I mean it is said to be a basis for the vector space, if this set if is a linear independence set and then it spans a vector space.

(Refer Slide Time: 16:16)

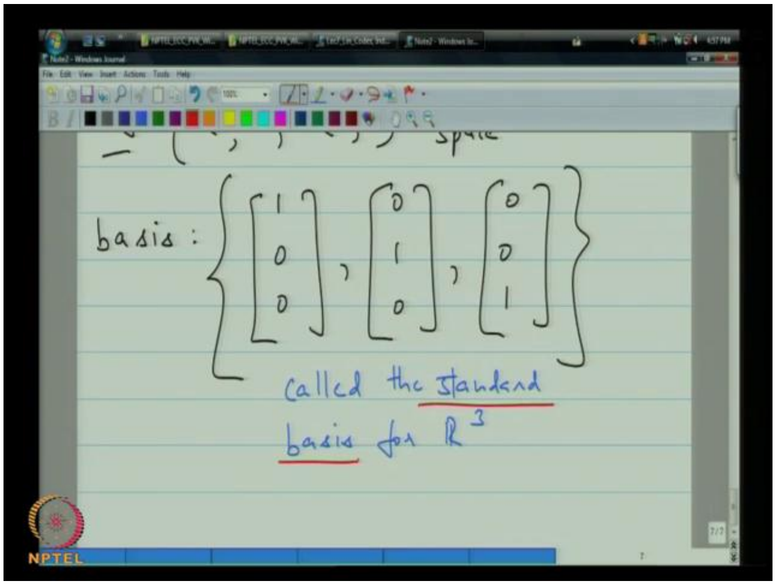


(ii) { the set spans the vector space V

Eg $(\mathbb{R}^3, +, \mathbb{R}, \cdot)$ vector space

So, let us look at some examples. Now, if your vector space is R 3 plus R.

(Refer Slide Time: 16:37)



space

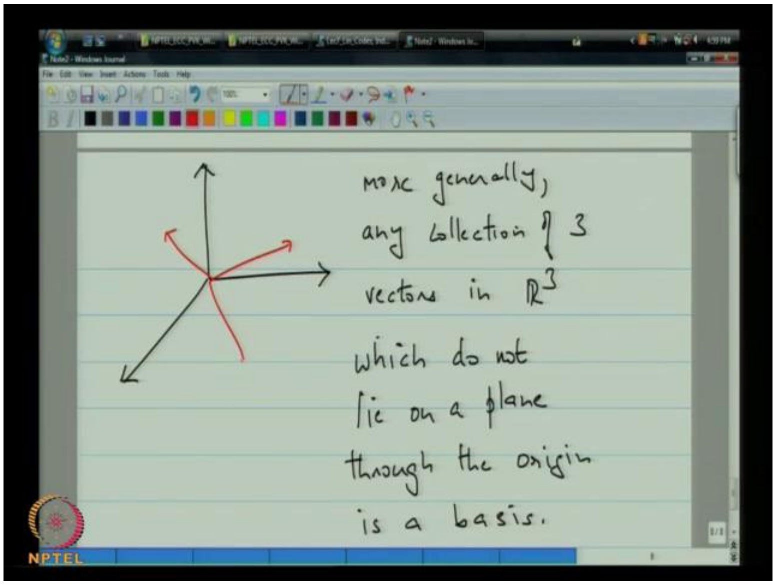
basis : $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$

called the standard basis for $\mathbb{R}^3$

Then If this is your vector space, then the following is the basis and it does not take much effort to actually, see that these collection of vectors is linearly independent and then further expanse the space; simply because you can express any vector in 3 dimensional space as a linear combination of these.

So, this clearly is the basis, just one remark that whenever you have in the spaces R n vectors like these are called; the basis of this type is called as standard basis. So, we will just make a quick remark here. This is called the standard basis for R 3. And of course, as you might imagine, there exist standard basis for other high dimensional spaces R n as well.

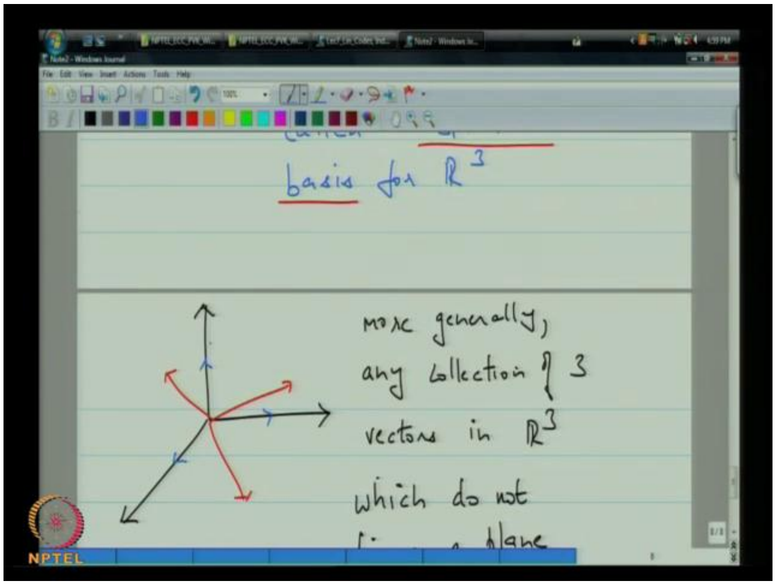
(Refer Slide Time: 18:18)



more generally,
any collection of 3
vectors in $\mathbb{R}^3$
which do not
lie on a plane
through the origin
is a basis.

Now, of course, this vector space is nothing but our familiar 3 dimensional Euclidean space. So, we can attach geometry to this. So if you were to ask the question. In general could you lay down a condition for bunch of vectors to be a basis, and answer is yes. So, more generally any collection of 3 vectors in R 3 with which do not lie on a plane through the origin is a basis. So, you can picture if these 3 vectors do not lie on a plane then they form a basis.

(Refer Slide Time: 19:59)



basis for $\mathbb{R}^3$

more generally, any collection of 3 vectors in $\mathbb{R}^3$ which do not

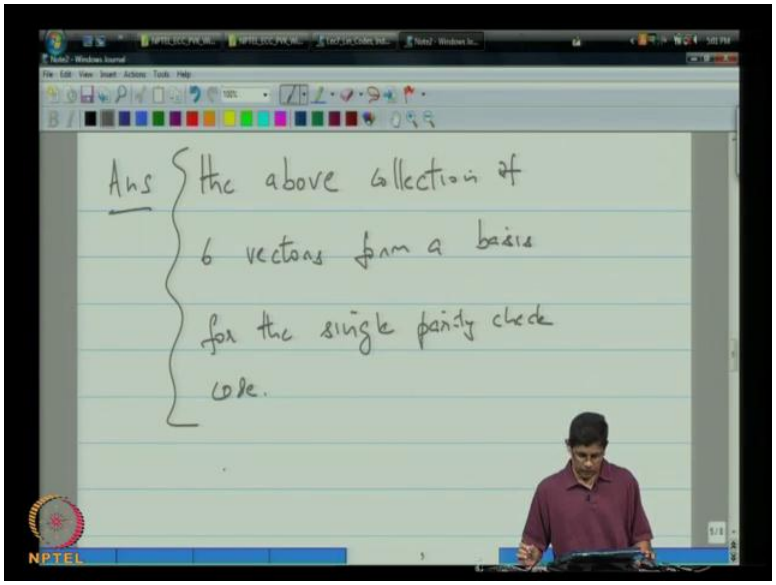
plane

And of course, this standard basis that we introduced earlier merely corresponds to vectors along the coordinate axis and it is clear that they do not lie on a plane through the origin.

Now, let me just quickly go back and answer this question that I raised earlier. So, the question was. How do you describe this space this spanned by all of these? And hopefully at least, some of you all have got this. It is not hard to see just by inspection that if you look at each of these vectors individually. There is a small typo here, I did not I hope this did not throw you off, is the typo here.

So, perhaps it was not a fair question. But in the intention was that each of these vectors has even parity. So, it belongs to the even parity code and you can actually, check that even parity code can be expressed as the linear combination of these. And why is that? Because you can see that, if you just ignore the first component and focus your attention on the last 6 components, you can generate by taking an appropriate linear combination, whatever you like in those 6 components, and of the seventh component of the first one is forced. From this it follows that this; in fact, the above 6 vectors form a basis for the even parity code.

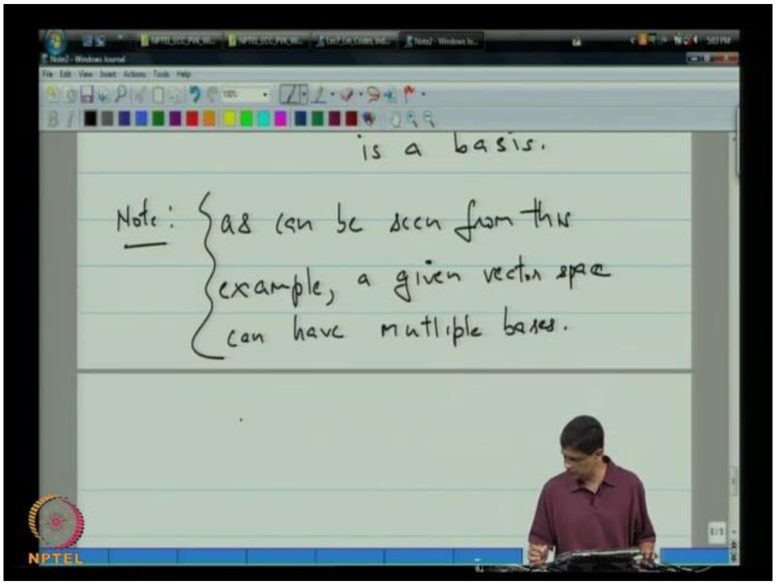
(Refer Slide Time: 21:24)



Ans: the above collection of 6 vectors form a basis for the single parity check code.

So, the answer is the above collection of 6 vectors form a basis for the single parity check code.

(Refer Slide Time: 22:42)



is a basis.

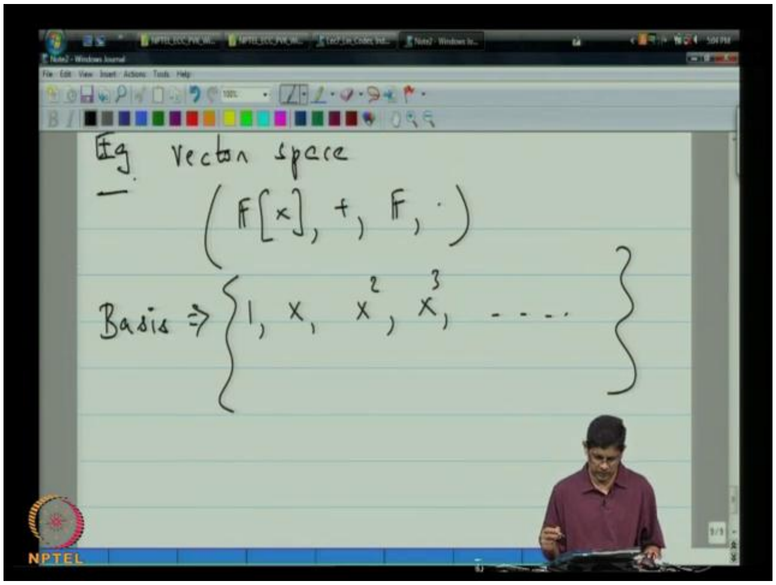
Note: as can be seen from this example, a given vector space can have multiple bases.

Now, getting back to basis. We look at some other examples, but just one quick note here, as you can see in this particular instance, even when you focus on three dimensionally (( ))

space. They can be more than 1 basis. So, certainly the choice of basis for a vector space is not unique.

So, as can be seen from this example. So, as can be seen from this example, a given vector space a given vector space can have multiple basis.

(Refer Slide Time: 23:44)



Eg. vector space

$(F[x], +, F, \cdot)$

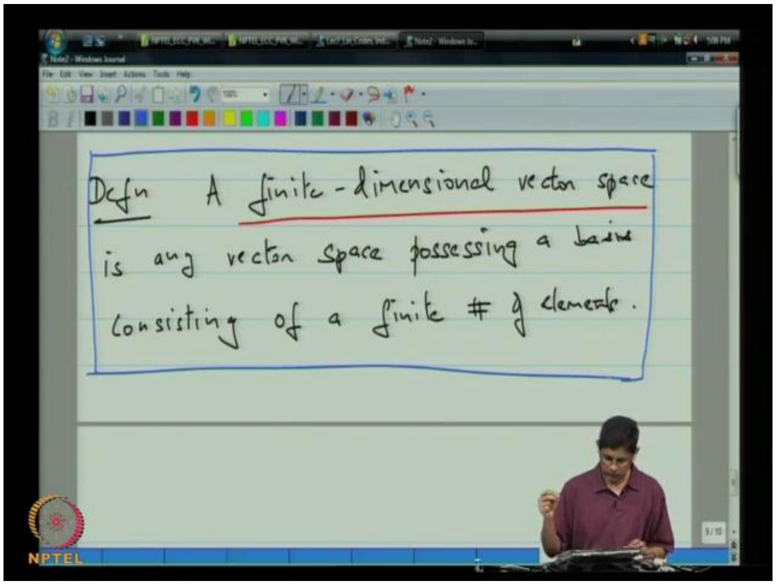
Basis ⇒ $\{1, x, x^2, x^3, \ldots\}$

Another example, supposing you are looking at the vector space of polynomials. Then you can verify that the following is the basis. The polynomials 1 x x square x cubed dot, dot, dot, this set is the basis, and you can verify that it satisfies the requirements.

Now, I just want to go back and talk about this issue of finite versus infinite. So, I told you that if you are uncomfortable with the idea that basis is an infinite set of vectors that you could think about is finite. Now, we will actually formally move on to consider to this restriction.

So in fact, you can actually divide vector spaces in; you can classify them, as being the finite dimensional or not, depending upon whether they have a basis that consists of a finite number of elements. And our interest is mostly in finite dimensional vector spaces, in which case the basis will always have a finite number of elements.

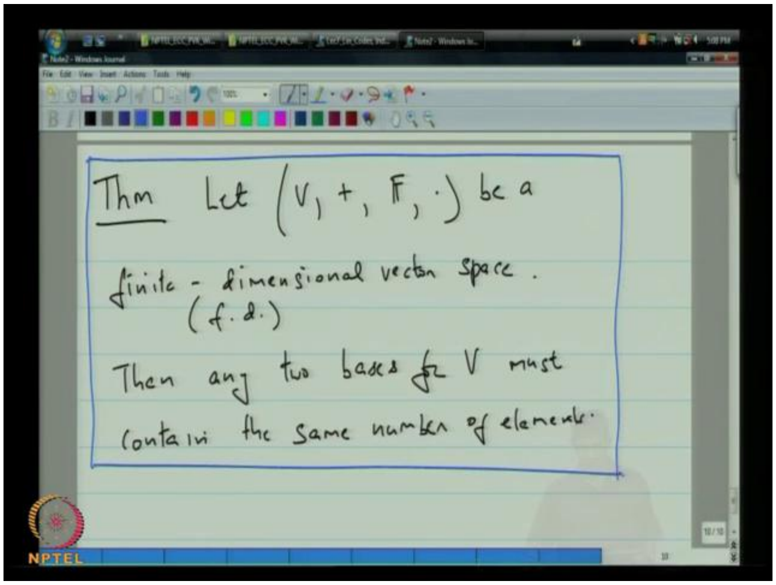
(Refer Slide Time: 25:29)



Defn A finite-dimensional vector space is any vector space possessing a basis consisting of a finite # of elements.

So let us make the definition. A finite dimensional vector space is any vector space possessing a basis that consists of a finite number of elements.

(Refer Slide Time: 26:53)

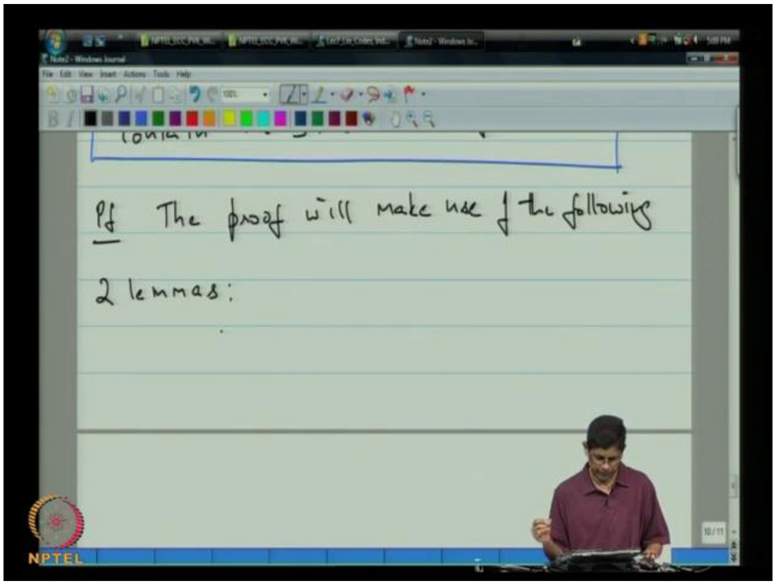


Thm Let $(V, +, \mathbb{F}, \cdot)$ be a finite-dimensional vector space.
(f.d.)

Then any two bases for V must contain the same number of elements.

And, now we are ready to lay down a theorem. Let V plus dot be a vector space, be a finite dimensional vector space. And will abbreviate finite dimensional by just f dot d dot. Then any 2 bases for V must contain the same number of elements. In particular it is not possible that if a vector space has one basis that consists of a finite number of elements. There it can have, at the same time another basis containing an infinite number of elements.

(Refer Slide Time: 28:43)



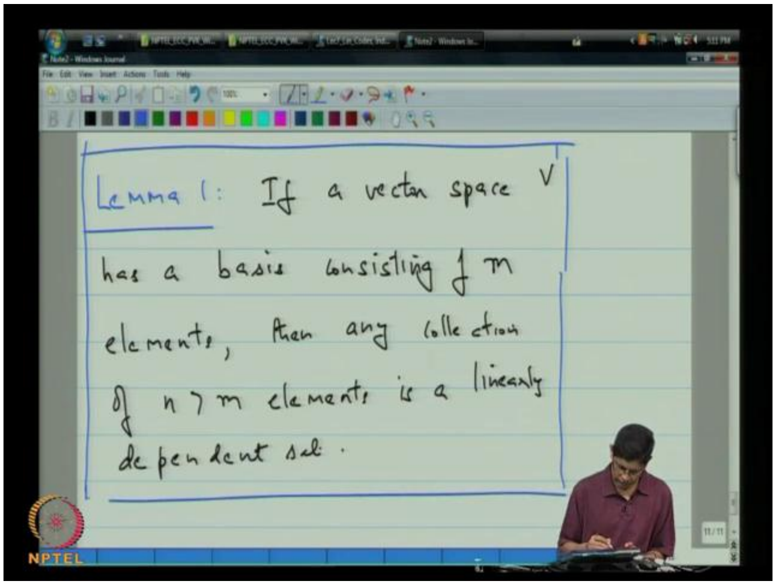
contain

Pf The proof will make use of the following

2 lemmas:

So in particular, finite dimensional vector spaces will always have finite basis. Moreover, the number of elements in the basis is fixed. How do we prove that the proof actually when we involve 2 lemmas, I will not prove the lemmas themselves because it will take us a little too far out. I will just state them, but we will use them to actually prove the theorem.

(Refer Slide Time: 29:30)

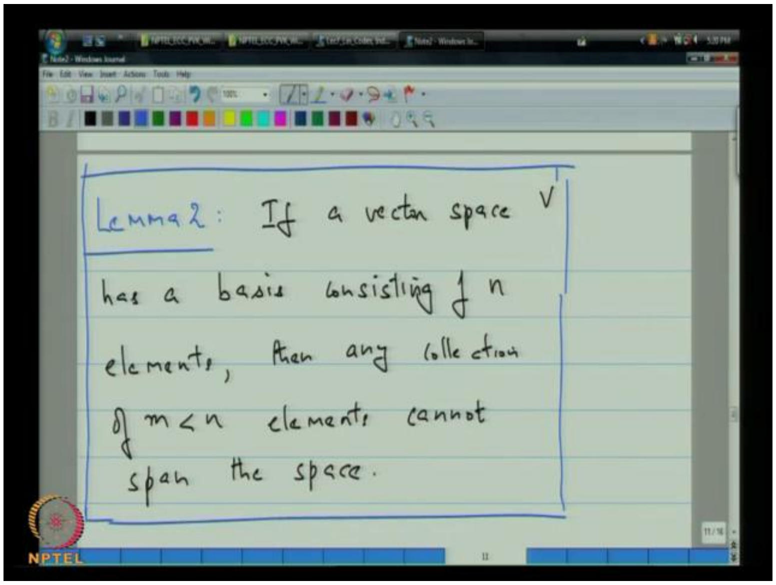


Lemma 1: If a vector space V has a basis consisting of m elements, then any collection of $n > m$ elements is a linearly dependent set.

The proof will make use of the following 2 lemmas. So, lemma 1 if a vector space V has a basis consisting of n elements. Then any collection of, let me just change this to m. I like to think of n is being greater than m.

Let us put m here and let us put n here. If a vector space has a basis consisting of m elements. Then any collection of n greater than m elements is the linearly dependent set. That is the first lemma.

(Refer Slide Time: 32:02)



Lemma 2: If a vector space V has a basis consisting of n elements, then any collection of $m < n$ elements cannot span the space.

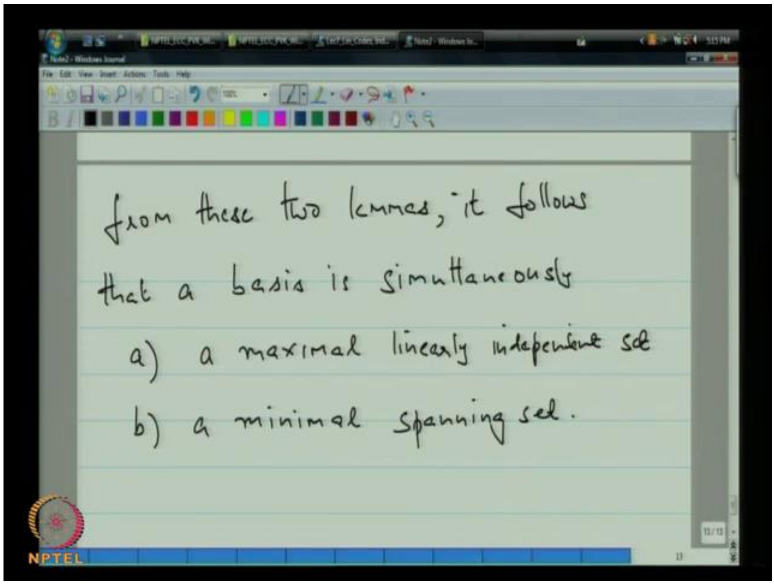
Now, I am going to use some electronic technology to actually make the next piece of writing a little bit easier. My next lemma is very similar to the first lemma. So, I am just going to make some changes.

So lemma 2, if a vector space V has a basis consisting of m elements, and I want to change this n to n; then any collection of m less than n elements cannot span the space. So, in the first case we actually said that supposing you have a basis that consists of m elements. So, there is going to be a pair of integers m and n. I am always going to think of n as being bigger than m in this particular case.

So, first lemma says that if you have a basis that consists of m elements, and someone gives me n elements from the vector space, where n is a larger number then m, then without even examining those vectors, you can just simply say well that must be a dependent set.

Say, that is the content of lemma 1. Lemma 2 says that if you have a basis that consist of n elements, and if someone comes with a smaller number of elements, then you can without again examining them you can say right away that this set cannot span the vector space. So, what these 2 lemmas, I am going to skip the proof in both cases and then I am just going to draw a conclusion from these 2 lemmas.

(Refer time: 34:08)



from these two lemmas, it follows that a basis is simultaneously

a) a maximal linearly independent set

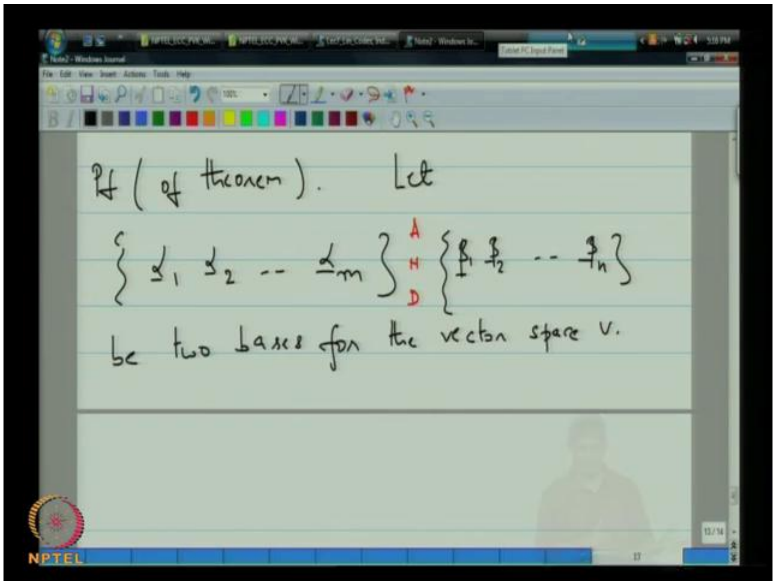
b) a minimal spanning set.

.

From these 2 lemmas, it follow that a basis is simultaneously a maximal linearly independent set and b: a minimal spanning set. So, it is maximal in terms of linearly independence for it is minimal in terms of spanning right.

So now let us just go back and see where we were, what we were trying to do was we were trying to prove the following theorem; the theorem which says that if I have a finite dimensional vector space, then any 2 basis for the vector space must contain the same number of elements.

(Refer Slide Time: 35:59)



Pf (of theorem). Let

$\{\alpha_1, \alpha_2 -- \alpha_m\}$ AND $\{\beta_1 \beta_2 -- \beta_n\}$

be two bases for the vector space V.

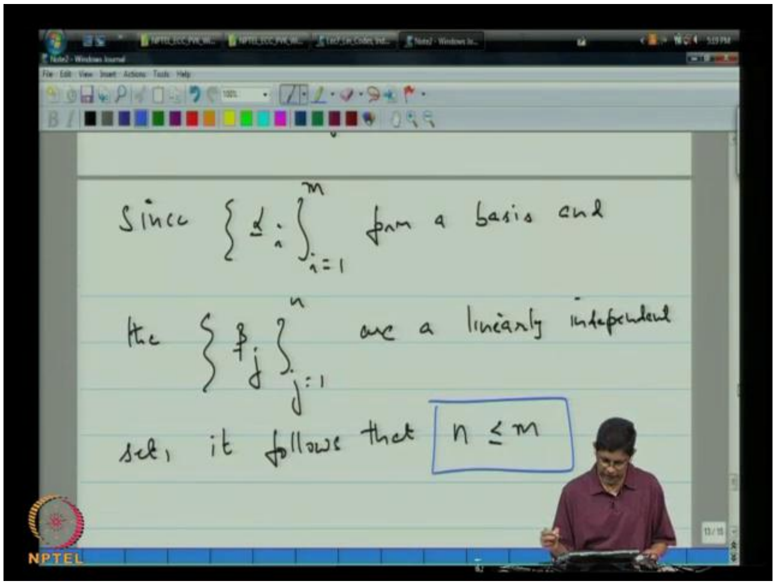
So now let us see how we can use these lemmas to prove it .So proof of theorem. Let alpha 1 alpha 2 alpha m and beta 1 beta 2 beta n be 2 basis for the vector space V. So, now you have 2 different basis, one seems to have m elements, this other since to have n elements.

Now, let us regard the basis consisting of the vectors alpha i as a kind of a reference. So, think of that as a reference, and then let us examine the vector set beta j in terms of this reference. So, then what it says is as that, look we have the alpha linearly or basis. So, if they cannot be a linearly independence set, whose size is larger than m, but the beta j form a basis, they must be linearly independents.

So, it must be that n must be less that are equal to m, because after all no linearly independent set can be of size larger than m. Again we are regarding alpha as reference. So, that is with respect to the notion of linear independence.

Now, let us switch few points to the notion of spanning. Now, the alpha i again r are our reference basis, and this reference basis contains m elements. So, if some other basis claims to span the vector space. It must contain at least m elements, from that point of view n must be at least equal to m. So, you have the two conditions n cannot be larger than m and n cannot be less than m. So, it has to be the same, so that is the proof.

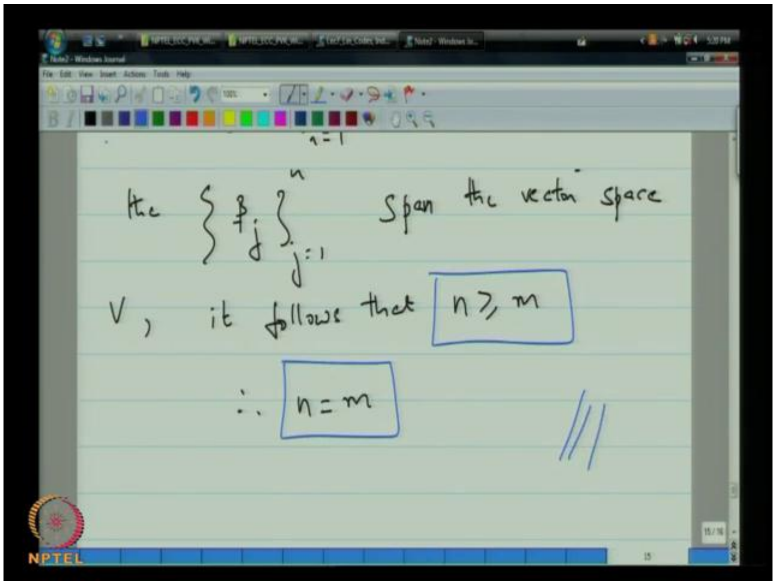
(Refer Slide Time: 38:19).



Since $\{\underline{\alpha}_i\}_{i=1}^{m}$ form a basis and the $\{\beta_j\}_{j=1}^{n}$ are a linearly independent set, it follows that $\boxed{n \leq m}$

Since the alpha i i is equal to 1 to m form a basis. And the set beta j j is equal to 1 to n are a linearly independent set. It follows that n must be less than or equal to m.

(Refer Slide Time: 40:10)



$i=1$

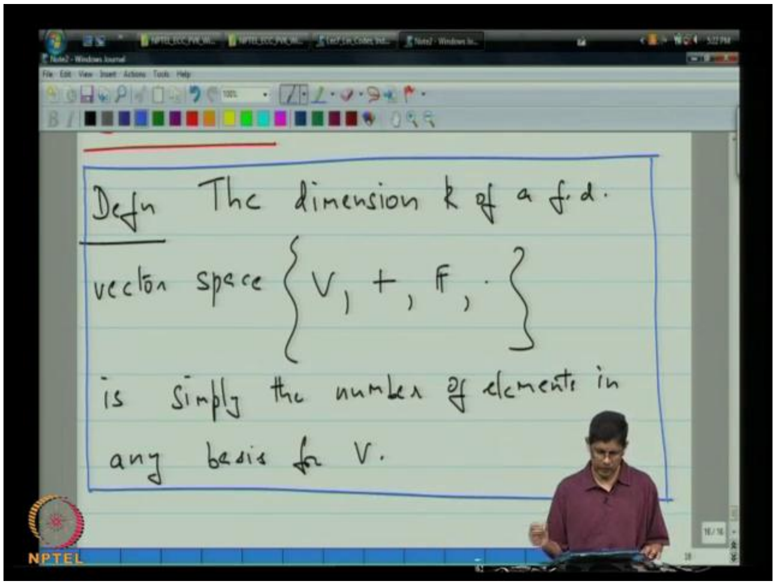
the $\{\beta_j\}_{j=1}^{n}$ span the vector space V, it follows that $\boxed{n \geq m}$

$\therefore \boxed{n = m}$ ///

Now I am again going to duplicate this page, again using similar reading. Since, the alpha i form a basis and the beta i span. And span the vector space V, it follows that n must be greater than or equal to m. Therefore n equals m and we are done.

So that proves the theorem, that any 2 basis must contain precisely the same number of elements. By the way just a comment, there were 2 lemmas that we used in this proof and I did not give you the proof. But the proof use is basically based on linear algebra. So, there is nothing very deep about it. It is just that it will take us too much time to actually go through the proof.

(Refer Slide Time: 41:22)



Defn The dimension k of a f.d. vector space $\{V, +, \mathbb{F}, \cdot\}$ is simply the number of elements in any basis for V.

Now, having established that we are now in a position to actually define what is meant by the dimension of a vector space. The dimension k of a finite dimensional vector space is simply the number of elements in any basis for V.

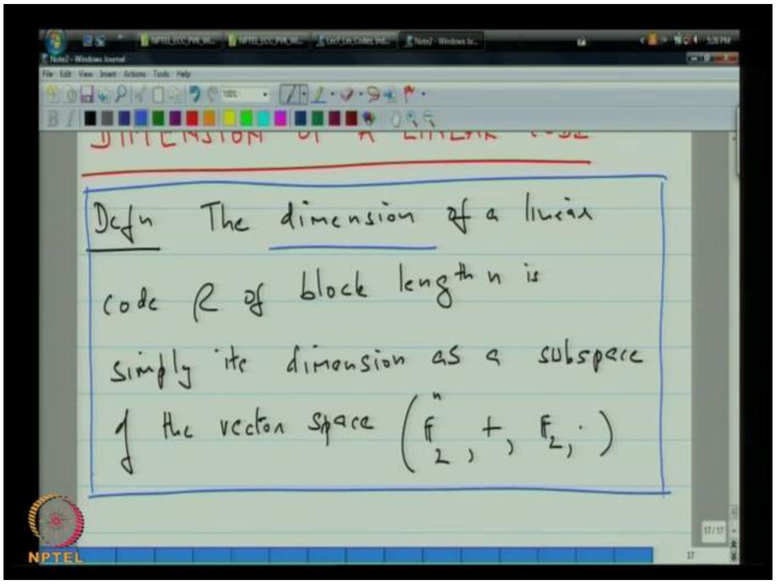
So, the dimension of a finite dimension vector space is simply the number of elements in a basis. And this definition makes sense, because we already established that if you come up with the basis and I come up with the basis for the same vector spaces. And even though our basis may not be the same, it is still it is true that the number of elements in each of the basis is the same.

So, we will come up with the same value for the dimension of this. Of course, this applies to the case of a finite dimensional vector space. We are not talking about those instances in which the number of elements in the basis can be infinite. Now, we have encountered examples of such spaces. Let us see if I can pull up a quick example.

For example, if you look at the space of all polynomials. Now, that is an infinite dimensional space, because it has in basis consisting of an infinite number of elements 1 x x square x cube it never stops. So, that is an example of infinite dimensional space.

But as I mentioned earlier, couple of times. In this course for as applications are concerned we will be restricted mostly to finite dimensional case, now getting back to coding theory. So, with that we are done with our detour into linear algebra and way back in on our topic of error correcting codes.

(Refer Slide Time: 44:36)

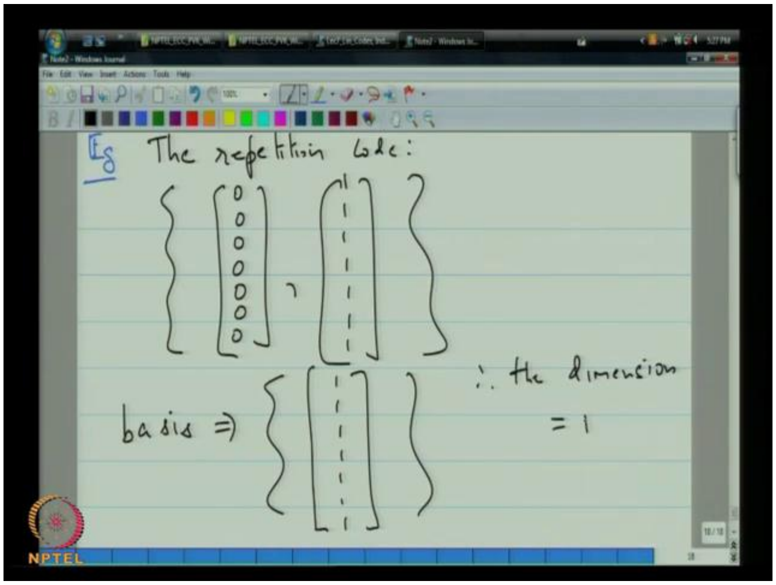


DIMENSION OF A LINEAR CODE

Defn The dimension of a linear code C of block length n is simply its dimension as a subspace of the vector space $(F_2^n, +, F_2, \cdot)$

So, dimension of a linear code. So the definition; the dimension of a linear code, C of block length n is simply its dimension as a subspace of the vector space F 2 to the n plus F 2 dot right. So, that is what we mean by the dimension. Let us look at some examples.

(Refer Slide Time: 46:28)



Eg The repetition code:

$$\left\{ \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\end{bmatrix} \right\}$$

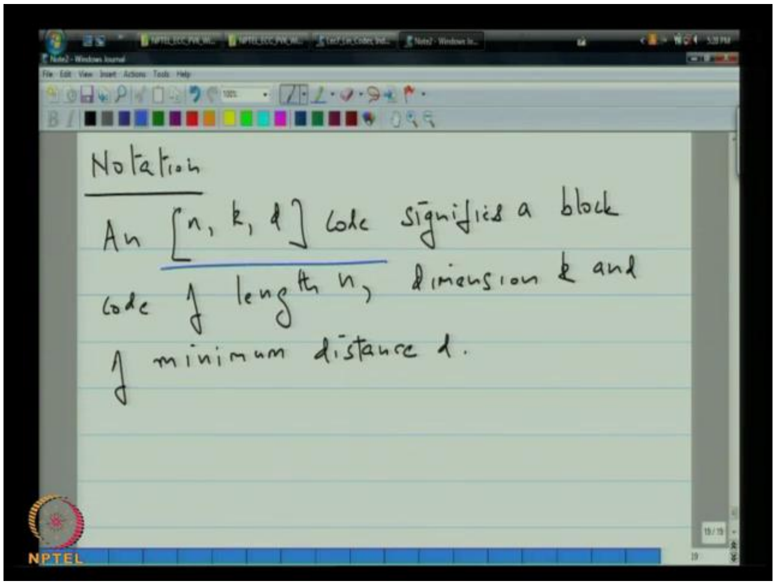
basis $\Rightarrow \left\{ \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\end{bmatrix} \right\}$

$\therefore$ the dimension $= 1$

If you look at the repetition code, which simply consisted of the all 0 vector, and the all one vector then a basis. Now, this is sub space of F 2 to the 7.

So, clearly a basis for this code is just the vector of all once. Therefore, the dimension is equals 1. Now just quick note here; so this is the instance, and the code has blocked length 7 and dimension 1 some notation.

(Refer Slide Time: 47: 50)

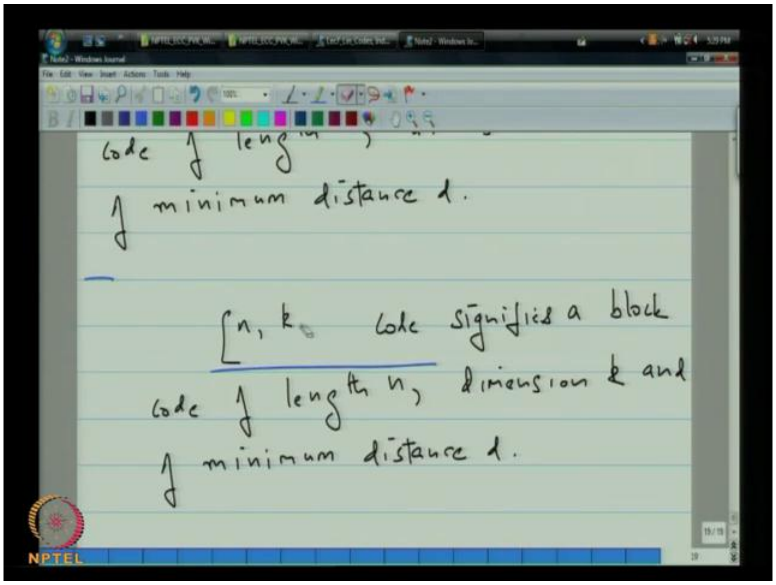


Notation

An $[n, k, d]$ code signifies a block code of length n, dimension k and of minimum distance d.

An n k d code signifies a block code of length n, dimension k and of minimum distance d. Now, it is important that when you write this down, we use rectangular basis. If you use curved races, then that is usually reserved for the case when the code is not necessarily linear. So, that is one, two sometimes it may be that we do not know the minimum distance of the code, in which case we will simply write an n k code.

(Refer Slide Time: 49:37)



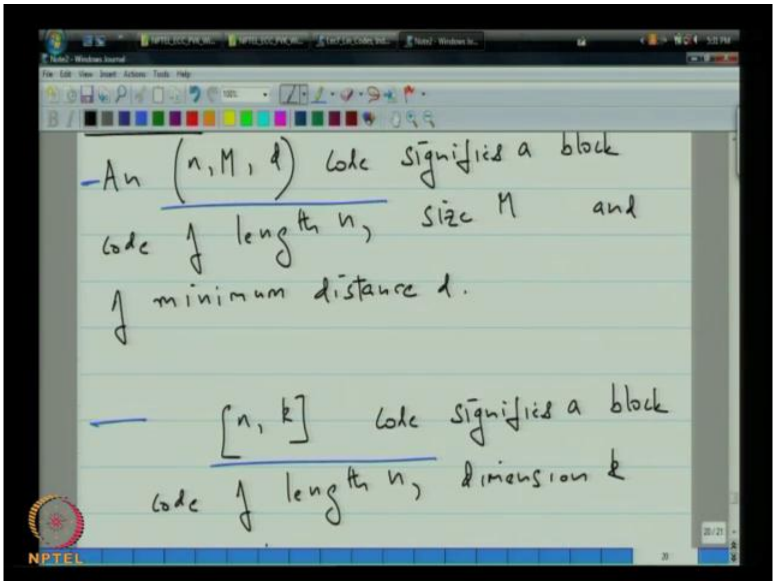
code of length

of minimum distance d.

[n, k code signifies a block code of length n, dimension k and of minimum distance d.

So let us actually make that (( )). So then in this case here an n k code signifies the code length, code of length and dimension k period. There is no mention of minimum distance, but again just note that we have used rectangular basis. Now, there is an analogous notion for the case when the code is not necessarily linear.

(Refer Slide Time: 50:58)



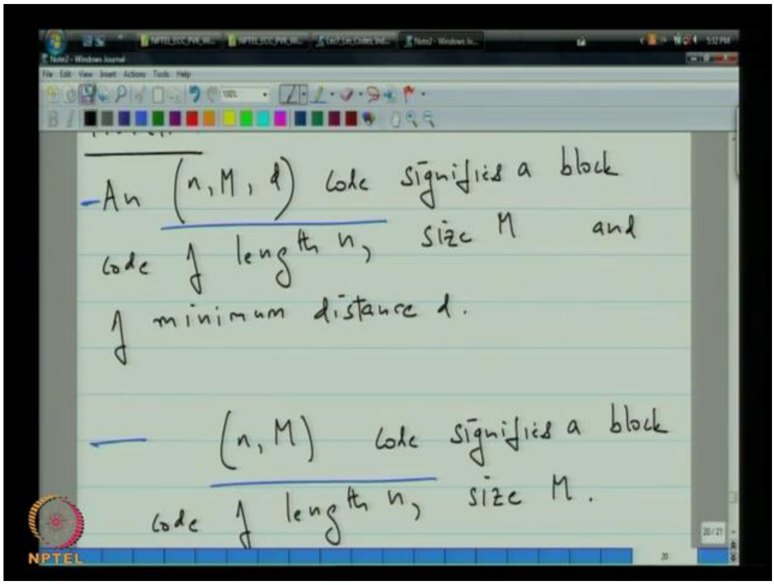
- An (n, M, d) code signifies a block code of length n, size M and of minimum distance d.

— $[n, k]$ code signifies a block code of length n, dimension k

So let me just again select the page I am going to give you the definition on the next page. So, what happens when the code is not necessarily linear. Then first of all, the basis change from rectangular to curved. And then you do not use k, what is typically used instead is the letter m, block code of length n.

Now, dimension does not necessarily make sense if the code is not necessarily linear. So, we will actually say instead of size M. So, there is a big difference between M and k because of the code is linear, then m is equal to 2 to the k in the case of a linear code.

(Refer Slide Time: 52:12)

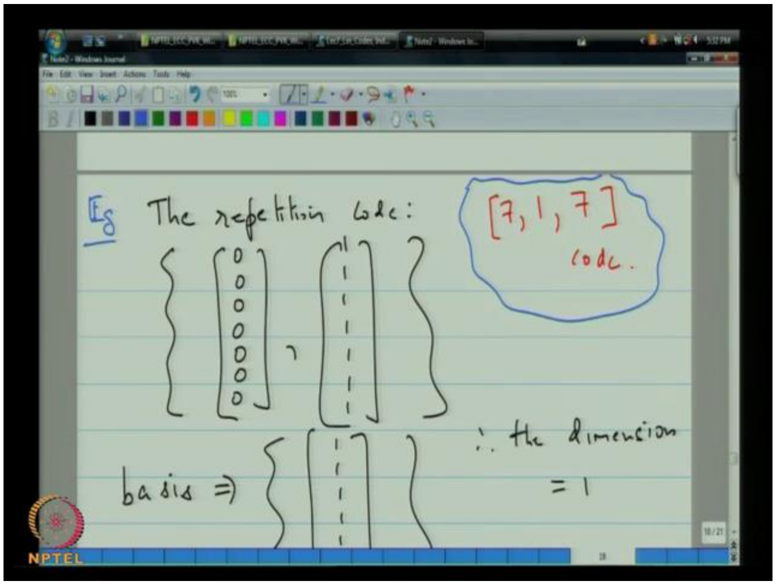


- An (n, M, d) code signifies a block code of length n, size M and of minimum distance d.

- (n, M) code signifies a block code of length n, size M.

And analogously when we do not know the minimum distance, we will just write n and will put down n M, code of length n and dimension and size M. So, that now we have got the notation straightened out. Let us go back and see for our example code here.

(Refer Slide Time: 52:41)



Eg The repetition code:

$$\left\{ \begin{bmatrix} 0\\0\\0\\0\\0\\0\\0 \end{bmatrix}, \begin{bmatrix} 1\\1\\1\\1\\1\\1\\1 \end{bmatrix} \right\}$$

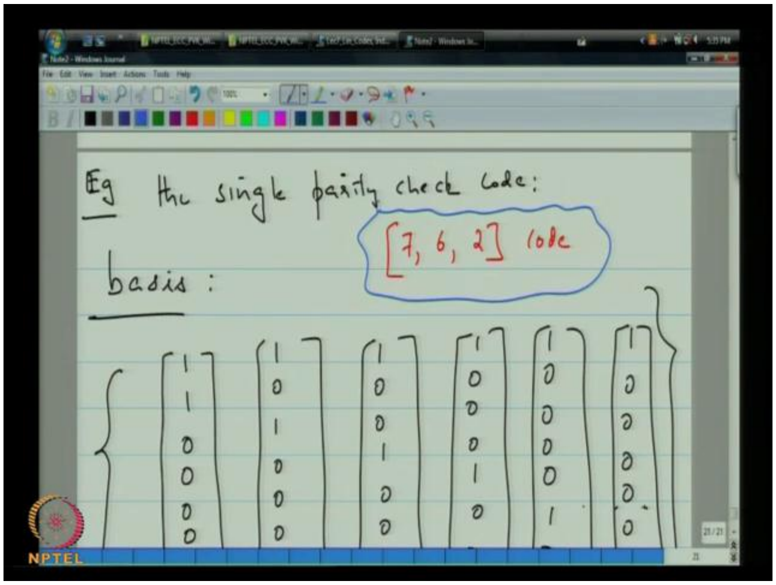
$[7, 1, 7]$ code.

basis $\Rightarrow \left\{ \begin{bmatrix} 1\\1\\1\\1\\1 \end{bmatrix} \right\}$

$\therefore$ the dimension $= 1$

So, this repetition code now. Let us take a look at what it is parameters are. So this code is now therefore, you can see that the block length is 7. Since, it has a basis consisting of a single element the dimension is 1, and the minimum distance we know from earlier is 7. So, this is the 7 1 7 code right.

(Refer Slide Time: 53:15)



Eg the single parity check code:

[7, 6, 2] code

basis :

$$\left\{ \begin{bmatrix}1\\1\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\1\\0\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\1\\0\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\1\\0\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\0\\1\end{bmatrix} \begin{bmatrix}1\\0\\0\\0\\0\\0\end{bmatrix} \right\}$$

So, that is what is next. Let us look at another example. Let us look at the example of the single parity check code. So, now for this I am going to again go back, because we did a computation which will help us determine the basis, once I find it.

So, I want to select this particular set that we looked at and come down here, and I will paste it. So here we have these 6 vectors. Now the singly parity check code, this is the basis for the code. Why is that well, what this example came up early and connection with spanning and I pointed out that this set spans the single parity check code, but they are obviously linear independent.

So, this is the basis. So as a result this code has parameters 7 6 and from earlier competitions it is 7 6 2 code. So, and I think with that we are coming to the end of our times. So we will stop here. So, what we have done in this lecture is, we have talked about the notion of spanning.

We have put linear independence and spanning together to talk about the basis, then we talked about dimension of a vector space, dimension of a code and looked at some examples.

So, we will continue from this point onwards the next time, when the topic will now we will introduce the notion of a dual code.