A brief explanation of the Steinitz Exchange Lemma

Suppose we have a set of linearly independent vectors \( I = \{i_1, i_2, i_3\} \), and a set of spanning vectors \( S = \{s_1, s_2, s_3, s_4\} \). Then we may replace, one at a time, vectors in \( S \) with vectors in \( I \), until we get a spanning set \( T = \{i_1, i_2, i_3, s\} \), where \( s \) is one of the \( s_i \).

Since \( S \) spans, we know that \( i_1 \) may be written as a linear combination of elements of \( S \), say \( i_1 = \lambda_1 s_1 + \lambda_2 s_2 + \lambda_3 s_3 + \lambda_4 s_4 \). One of the \( \lambda_i \) must be non-zero, or else we have \( i_1 = 0 \), which contradicts \( I \) being linearly independent. So, by renaming the \( s_i \) if necessary, we may assume that \( \lambda_1 \neq 0 \).

We have \( s_1 = \frac{1}{\lambda_1} (i_1 - \lambda_2 s_2 - \lambda_3 s_3 - \lambda_4 s_4) \).

Then \( S' = \{i_1, s_2, s_3, s_4\} \) spans. Why? We know that \( S \) spans, so any vector is some combination of \( s_1, \ldots, s_4 \), and we can now replace the occurrence of \( s_1 \) by the above expression in \( i_1, s_2, s_3, s_4 \).

We now have the linearly independent set \( I' = \{i_2\} \) and the spanning set \( S' = \{i_1, s_2, s_3, s_4\} \).

Since \( S' \) spans, we know that \( i_2 \) may be written as a linear combination of elements of \( S' \), say \( i_2 = \mu_1 i_1 + \mu_2 s_2 + \mu_3 s_3 + \mu_4 s_4 \). This time, we know that one of \( \mu_2, \mu_3, \mu_4 \) must be non-zero, or else we have \( i_2 = \mu_1 i_1 \), which contradicts the original \( I \) being linearly independent. So, by renaming the \( s_i \) if necessary, we may assume that \( \mu_2 \neq 0 \).

We have \( s_2 = \frac{1}{\mu_2} (i_2 - \mu_1 i_1 - \mu_3 s_3 - \mu_4 s_4) \).

Then \( S'' = \{i_1, i_2, s_3, s_4\} \) spans. Why? Like before, we know that \( S' \) spans, so that any vector is some combination of \( i_1, s_2, s_3, s_4 \), and we can now replace the occurrence of \( s_2 \) with the above expression in \( i_1, i_2, s_3, s_4 \).

We now have the linearly independent set \( I'' = \{i_3\} \) and the spanning set \( S'' = \{i_1, i_2, s_3, s_4\} \).

Since \( S'' \) spans, we know that \( i_3 \) may be written as a linear combination of elements of \( S'' \), say \( i_3 = \nu_1 i_1 + \nu_2 i_2 + \nu_3 s_3 + \nu_4 s_4 \). This time, we know that one of \( \nu_3, \nu_4 \) must be non-zero, or else we have \( i_3 = \nu_1 i_1 + \nu_2 i_2 \), which contradicts the original \( I \) being linearly independent. So, by renaming the \( s_i \) if necessary, we may assume that \( \nu_3 \neq 0 \).

We have \( s_3 = \frac{1}{\nu_3} (i_3 - \nu_1 i_1 - \nu_2 i_2 - \nu_4 s_4) \).

Then \( S''' = \{i_1, i_2, i_3, s_4\} \) spans, for reasons just like before. And this is the set \( T \) we claimed existed at the start.

What would have happened if we’d started with the linearly independent set \( I = \{i_1, i_2, i_3, i_4\} \) and the spanning set \( S = \{s_1, s_2, s_3, s_4\} \)?

We would do one more step in the process above, and end up replacing all elements in \( S \) with those in \( I \), and we would conclude that \( I \) itself spans.
What if we’d started with the linearly independent set \( I = \{i_1, i_2, i_3, i_4, i_5\} \) and the spanning set \( S = \{s_1, s_2, s_3, s_4\} \) ?

Well, after four steps in the above process we would have reached the point where \( I^{\prime\prime\prime} = \{i_5\} \) and \( S^{\prime\prime\prime} = \{i_1, i_2, i_3, i_4\} \) were the sets under consideration. But this is impossible, for if this \( S^{\prime\prime\prime} \) spanned, then we could write \( i_5 \) as a linear combination of \( i_1, i_2, i_3, i_4 \), which would contradict \( I \) being linearly independent in the first place.

It is clear that if \( I \) is a finite linearly independent set and \( S \) is a finite spanning set, then the procedure above could be performed. In particular, we would find that \(|I| \leq |S|\).

An immediate corollary is that if a vector space has a finite basis, then any two bases for it have the same size. For if \( B_1 \) and \( B_2 \) are two bases for it, then taking \( I = B_1 \) and \( S = B_2 \), we see that \(|B_1| \leq |B_2|\), and taking \( I = B_2 \) and \( S = B_1 \), we see that \(|B_2| \leq |B_1|\).

This means that ‘dimension’ is well-defined.

We can also see that, in a finite-dimensional vector space, any linearly independent set may be extended to a basis: let \( I \) be the linearly independent set and let \( S \) be any basis you like, and at the end of the process we have reached a basis containing \( I \).

Note the use of the word ‘finite’ a few times above. The process described did assume that \( I \) and \( S \) were finite. We could have taken \( S \) to be infinite, and replaced \(|I|\) many elements of \( S \) with the elements of \( I \). That’s okay, because the process would still terminate after \(|I|\) many steps.

It’s not obvious what would happen if \( I \) were infinite. If the exchange process turns out to be invalid, then the corollaries might not follow. Is ‘dimension’ even well-defined for huge spaces, and does every vector space actually have a basis? The answers are yes – but you’ll have to go to Logic & Set Theory in the third year, and throw Zorn’s Lemma at the problem.

Please let me know of any corrections: glt1000@cam.ac.uk