Spanning sets, independent sets, bases, dimension

Let V be a vector space over a field F. We will often tacitly assume that V is not trivial, that is, it contains at least two elements.

Definition 1. *Let $S \subseteq V$. A* **linear combination** *of (some) vectors in S is a* finite *sum* $\sum c_i x_i$ *where all $x_i \in S$ and $c_i \in F$. We say that such a linear combination is* **non-trivial** *if all the vectors x_i are* distinct *and at least one of the coefficients c_i is non-zero. The set of all linear combinations of vectors in S is called the* **span** *of S and denoted by* $\operatorname{span}(S)$. *By convention,* $\operatorname{span}(\emptyset) = \{\mathbf{0}\}$.

Clearly, a linear combination of linear combinations of vectors in S is itself a linear combination of vectors in S. Hence, for any $S \subseteq V$, $\operatorname{span}(S)$ is a subspace of V. This is the smallest subspace of V containing S. If $W = \operatorname{span}(S)$, we say that "$S$ spans [or generates] the subspace W." Thus, $U \subseteq V$ is a subspace of V if and only if $span(U) = U$.

Definition 2. *A set $S \subseteq V$ is a* **spanning set** *if* $\operatorname{span}(S) = V$, *that is, if S generates the whole V (every vector in V is a linear combination of some vectors in S):*

$$(\forall v \in V)(\exists x_1, \dots, x_n \in S)(\exists c_1, \dots, c_n \in F)\, v = \sum c_i x_i.$$

Lemma 1 (Monotonicity). *Let $S \subseteq S' \subseteq V$. Then,* $\operatorname{span}(S) \subseteq \operatorname{span}(S')$.
In particular, if S is a spanning set and $S' \supseteq S$, then S' too is a spanning set.

Lemma 2. *Let S be a spanning set, and let the set S' be such that* $\operatorname{span}(S') \supseteq S$. *Then already S' is a spanning set.*

Informal proof: "Linear combinations of linear combinations are linear combinations."
Formal proof (using Lemma 1): $V = \operatorname{span}(S)$ and $S \subseteq \operatorname{span}(S')$ imply $V \subseteq \operatorname{span}(\operatorname{span}(S')) = \operatorname{span}(S')$. But, clearly, $\operatorname{span}(S') \subseteq V$, and hence they are equal.

Definition 3. *A vector space is* **finite-dimensional** *if it has a finite spanning set of vectors.*

Definition 4. *A set $S \subseteq V$ is* **linearly dependent** *[dependent, for short] if one of the vectors in S can be expressed with some other vectors in S as their linear combination:*

$$(\exists x \in S)\, x \in \operatorname{span}(S \setminus \{x\}).$$

If S is not linearly dependent, we say it is **linearly independent** *[independent, for short].*

It is easy to see that this is equivalent to the usual (less intuitive) definition:

A set $S \subseteq V$ is **linearly dependent** *if $\mathbf{0}$ is a non-trivial linear combination of some vectors in S, that is, if there are $n \in \mathbb{N}$, n* distinct *vectors $x_i \in S$, and n scalars $c_i \in F$ such that (i) not all c_i are 0, and (ii)* $\sum_{i=1}^{n} c_i x_i = \mathbf{0}$.

Definition 5. *A set $B \subseteq V$ is a* **basis** *(for V) if it is linearly independent and spans V. More generally, given a subspace W of V, we say that a subset $B \subseteq W$ is a basis for W if B is independent and* $\operatorname{span}(B) = W$.

Examples: The empty set $\emptyset$ is linearly independent, but $\{\mathbf{0}\}$ is dependent. The empty set $\emptyset$ spans (and hence it is a basis for) the subspace $\{\mathbf{0}\}$.

The following facts are easy to see.

- *If D is dependent and $D' \supset D$ (superset), then D' is also dependent.*
- *If I is independent and $I' \subset I$ (subset), then I' is also independent.*

The next lemma is a very useful tool. It states a property that distinguishes vector spaces from more general geometric spaces (called linear and near-linear spaces).

Lemma 3 (Dependence Lemma). *Let I be independent, and let $x \notin I$. Then $I \cup \{x\}$ is dependent* **iff** *$x \in \operatorname{span}(I)$.*

Here is a unified characterization of spanning sets, independent sets and bases.

- *S is a spanning set* **iff** *every vector in V can be expressed* in at least one way *as a linear combination of some vectors in S.*
- *I is independent* **iff** *every vector in V can be expressed* in at most one way *as a linear combination of some vectors in I.*
- *B is a basis* **iff** *every vector in V can be* uniquely *expressed as a linear combination of some vectors in B.*

Here are two more characterizations of bases. Let $B \subseteq V$.

- *B is a basis* **iff** *it is a* **minimal** *spanning set (B spans V but no proper subset of B does).*
- *B is a basis* **iff** *it is a* **maximal** *independent set (it is linearly independent but is not a proper subset of another linearly independent set).*

(For two more characterizations of bases in finite-dimensional spaces, see the next page.)

The following property of bases can be used to replace matrix arguments in the discussion of linear independence and bases.

Theorem 1 (Exchange Property). *Let I be a linearly independent set of vectors and let S be a spanning set of vectors. Then, for every $x \in I$ there is a $y \in S$ such that $y \notin I \setminus \{x\}$ and the set $I' = (I \setminus \{x\}) \cup \{y\}$ is also linearly independent.*

Corollary 2 (Fundamental Inequality). *If I is an arbitrary independent set and S is an arbitrary spanning set, then $|I| \le |S|$. (We also consider $|I| \le |S|$ valid when S is infinite.) In particular,* **any two bases have the same number of elements.**

Theorem 3. *Let V be a finite dimensional vector space.*

(a) Then V has a basis.

(b) In fact, every independent set (in V) is contained in a basis [can be expanded to a basis],

(c) and every spanning set contains a basis [can be shrunk to a basis].

Remark. The Axiom of Choice implies that Theorem 3 holds in every vector space, finite-dimensional or not. In particular, **EVERY VECTOR SPACE HAS A BASIS.**

(But this may fail without AC, in particular, if AC is not assumed then $\mathbb{R}$ as a vector space over $\mathbb{Q}$ may not have a basis.)

Corollary 2 and Theorem 3 make the following definition meaningful.

Definition 6. *For a finite-dimensional V, the number of vectors in a basis of V is called the* **dimension** *of V and is denoted by* $\dim(V)$*. If V is not finite dimensional (called infinite-dimensional), we write* $\dim(V) = \infty$.

Corollary 4. *For every independent set $I \subseteq V$ and every spanning set $S \subseteq V$ we have*

$$|I| \leq \dim(V) \leq |S| \quad \textit{(some `quantities' here may be infinite).}$$

In fact,

$$\dim(V) = \sup\{|I| : I \subseteq V,\ I \textit{ is independent}\} = \inf\{|S| : S \subseteq V,\ S \textit{ is spanning } V\}.$$

Here are two characterizations of bases in finite dimensional spaces.

Corollary 5. *Let V be a vector space of finite dimension n, and let $B \subseteq V$.*

- *B is a basis if and only if B is spanning V* and $|B| = n$.
- *B is a basis if and only if B is independent* and $|B| = n$.

And finally, an important theorem about dimensions of subspaces:

Theorem 6 (Theorem 1.11 in the book).

Let U and W be two subspaces of a vector space V, and assume that

(a) W is finite dimensional, and

(b) $U \subseteq W$.

Then U is also finite dimensional, and $\dim(U) \leq \dim(W)$.

If [in addition to (a) and (b)] we also have $\dim(U) = \dim(W)$*, then $U = W$.*

Some proofs

Proof of the equivalence of bases and minimal spanning sets.

Part I. Let B be a basis. Then it is a spanning set. We need to prove minimality. It is enough to prove that for every $x \in B$, the set $B \setminus \{x\}$ cannot be spanning. (Why?)
Let $x \in B$. Since B is independent, $x \notin \mathrm{span}(B \setminus \{x\})$, so $B \setminus \{x\}$ is not spanning.

Part II. Let B be a minimal spanning set. We need to show that B is independent.
Indeed, assume that B were dependent: $(\exists x \in B)\, x \in \mathrm{span}(B \setminus \{x\})$. Then, by Lemma 2, already $B \setminus \{x\}$ would be spanning – contradicting the minimality of B. $\square$

Proof of the equivalence of bases and maximal independent sets.

Part I. Let B be a basis. Then it is independent. We need to prove maximality. It is enough to show that for every $y \notin B$, the set $B \cup \{y\}$ is dependent. (Why?)
Let $y \notin B$. Now, $y \in \mathrm{span}(B)$, since B is a basis. Hence the set $B \cup \{y\}$ is indeed dependent.

Part II. Let B be a maximal independent set. We need to show that B is a spanning set.
Let $x \in V$. We need $x \in \mathrm{span}(B)$. If $x \in B$, this is clearly so: $x = 1 \cdot x$. If $x \notin B$, then, by the maximality of B, the set $B \cup \{x\}$ is dependent, and thus, by the Dependence Lemma (Lemma 3), $x \in \mathrm{span}(B)$. $\square$

Hint for the **proof of Theorem 3.**

The claim that every independent set can be extended to a basis easily follows from the Fundamental Inequality and the fact that maximal independent sets are bases.

The claim that every *finite* spanning set contains a basis is even simpler; it follows from the fact alone that minimal spanning sets are bases.

But to show that even infinite spanning sets contain bases is more tricky; a natural way is to build up independent sets within a given spanning set:
Claim: If $I \subseteq S$, I is independent, S is spanning, and I is maximal *in* S, then I is a basis (maximal in V). **Proof.** It is easy to see that, $S \subseteq \mathrm{span}(I)$, and since $\mathrm{span}(S) = V$, so, by monotonicity, $\mathrm{span}(I) = V$.

Two proofs for the Exchange Property

Theorem (Exchange Property). *Let I be a linearly independent set of vectors and let S be a spanning set of vectors. Then, for every $x \in I$ there is a $y \in S$ such that $y \notin I \setminus \{x\}$ and the set $(I \setminus \{x\}) \cup \{y\}$ is linearly independent.*

Proof *(indirect): Assume that there is an $x \in I$ such that for every $y \in S$ either $y \in I \setminus \{x\}$ or the set $(I \setminus \{x\}) \cup \{y\}$ is dependent. Choose such an x, let $I^- = I \setminus \{x\}$, and let $y \in S$ be arbitrary.*

Since I^- is independent but $I^- \cup \{y\}$ is dependent, or $y \in I^-$, thus $y \in \operatorname{span}(I^-)$ by Lemma 3. Since $y \in S$ was chosen arbitrarily, we obtained $S \subseteq \operatorname{span}(I^-)$, and since S was a spanning set hence so is I^- (Lemma 2).

But then, in particular, $x \in \operatorname{span}(I^-)$ — contradicting the independence of I.

It is easy to see that the Fundamental Inequality $|I| \leq |S|$ follows from the Exchange Property. [Sketch: Assume $|S| < \infty$. On replacing an element $x \in I \setminus S$ with some $y \in S \setminus I$, the obtained new set $I' = (I \setminus \{x\}) \cup \{y\}$ is independent, has the same size as I, and has one fewer element outside S than I did. Repeating this process yields an independent set $J \subseteq S$ with $|J| = |I|$.] $\square$

Remark: *Instead of our Exchange Property, we could use the somewhat more complicated Replacement Theorem 1.10 on page 45 for proving the Fundamental Inequality.*

Here is an alternative "Math 250 proof" for the inequality $|I| \leq |S|$ using underdetermined systems of linear equations (Corollary to Theorem 3.8 on page 171).

Claim *(contrapositive form):* If S and I are finite sets, S is spanning, and $|I| > |S|$, then I must be dependent.

Proof. *Let $S = \{\alpha_1, \dots, \alpha_m\}$ and $I = \{\beta_1, \dots, \beta_n\}$ (hence $m < n$).*
Since S is spanning, there are scalars c_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n$, such that

$$\beta_j = \sum_{i=1}^{m} c_{ij}\alpha_i, \quad j = 1, 2, \dots, n.$$

To prove that the β-s are dependent, let's try to find a non-trivial linear combination of them giving $\mathbf{0}$: we need $x_1, \dots, x_n$ not all zero such that

$$\sum_{j=1}^{n} x_j\beta_j = \mathbf{0}.$$

Now

$$\sum_{1\leq j\leq n} x_j\beta_j = \sum_{1\leq j\leq n} x_j \sum_{1\leq i\leq m} c_{ij}\alpha_i = \sum_{1\leq i\leq m} \alpha_i \sum_{1\leq j\leq n} c_{ij}x_j$$

so we are done if we can find a non-trivial *solution to the system of equations:*

$$\sum_{j=1}^{n} c_{ij}x_j = 0, \quad i = 1, \dots, m.$$

But this is a homogeneous underdetermined system ($m < n$), and so it does have a non-trivial solution. $\square$