Subspaces in near-linear spaces

Let $S = (P, L)$ be a near-linear space. Recall that a set $Q \subseteq P$ is a **subspace** means that whenever a line has at least two points in Q, all points of the line must be in Q:

$$(\forall \ell \in L) \text{ if } |\ell \cap Q| \geq 2, \text{ then } \ell \subseteq Q$$

Note that, formally, a subspace is not a space but a subset of P, but it naturally defines a near-linear space $S' = (Q, L')$ where $L' = \{l \in L : l \subseteq Q\}$.

Examples: In *any* near-linear space, $\emptyset$ is a subspace, any one-point set (called a singleton) is a subspace (in fact, any set of pairwise non-collinear points is a subspace), any line is a subspace, and the whole P is a subspace. In the Fano plane, these are the only subspaces.

The following two properties are critical in dealing with subspaces:

(i) P itself is a subspace.

(ii) The intersection of any nonempty family of subspaces is a subspace.

For $A \subseteq P$, we define the **closure** of A (also called "the subspace generated by A") as the "smallest" subspace containing A as a subset, that is, the set C such that

(a) C is a subspace.

(b) $C \supseteq A$.

(c) If D is any subspace containing A, then $D \supseteq C$.

Properties (i) and (ii) guarantee that such a set C exists, is unique, and is equal to the intersection of *all* subspaces containing A. The closure of A is denoted by $\langle A \rangle$. In linear algebra, the standard name is "the span of A" and the notation is $\text{span}(A)$.

Some simple properties of closure

The following properties hold for all $A, B, C, D \subseteq P$:

(1) $A \subseteq \langle A \rangle$ and $\langle A \rangle$ is a subspace. [by def.]

(2) C is a subspace iff $\langle C \rangle = C$.
Also: C is a subspace iff there is an $A \subseteq P$ such that $C = \langle A \rangle$.

(3) If D is a subspace and $D \supseteq A$, then $D \supseteq \langle A \rangle$. [by def.]

(4) Idempotency of closure: $\langle\langle A \rangle\rangle = \langle A \rangle$. [follows from (2)]

(5) Monotonicity: $A \subset B$ implies $\langle A \rangle \subseteq \langle B \rangle$.

(6) Step-by-step closure: $\langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle$.

Definitions

T is a **spanning set** (or generating set) if $\langle T \rangle = P$. (We also say that "T is spanning P".)
T is a **minimal spanning set** if T is a spanning set, but no proper subset of T is. The latter is equivalent to saying that, for every $x \in T$, the set $T \setminus \{x\}$ is not spanning. (Why?)

I is an **independent set** if $(\forall x \in I) x \notin \langle I - x \rangle$. Otherwise I is dependent.
I is a **maximal independent set** if I is independent, but no set properly containing I is. The latter is equivalent to saying that, for every $y \notin I$, the set $I \cup \{y\}$ is not independent. (Why?)

> Remark: The $\emptyset$ is always independent. Also, by (5), subsets of independent sets are independent, and supersets of spanning sets are spanning.

B is a **basis** if it's both spanning and independent.

> Remark: Some books define bases as maximal independent sets (not the same!).

A space S is said to be **finite dimensional** if it contains a finite spanning set (otherwise it's infinite dimensional). By (III) below, every finite dimensional space has a finite basis. (Note that the definition of *finite dimensional* did not involve the notion of dimension!)

The following lemma easily follows from (3).

Lemma 1. *If T is spanning P, and $\langle A \rangle \supseteq T$, then already A is spanning P.*

Some basic facts (see the proofs on page 4):

(I) Every basis is a minimal spanning set. [Easy.]

(II) Every minimal spanning set is independent – hence a basis. [Follows from Lemma 1.]

(III) Bases are exactly the minimal spanning sets. [Combining (I) and (II).]

(IV) Every basis is a maximal independent set. [Easy.]

Caution! The converse to (IV) may be false: in some spaces, not all maximal independent sets are bases! Example: $\{1, 4, 7\}$ in Figure 1.4.1 on page 10 of Lynn Batten's book is a maximal independent set, but it is not a spanning set, hence not a basis. Notice that in this example the set $\{1, 4, 7\}$ is independent, the enlarged set $\{1, 4, 7, 3\}$ is dependent, yet $3 \notin \langle \{1, 4, 7\} \rangle$ — a situation impossible in linear algebra! This phenomenon is the reason for the anomaly of a maximal independent set not being a basis. It is also responsible for the fact that, in the same example, the sets $\{1, 2, 3\}$ and $\{5, 6, 7, 8\}$ are both bases – even though they are of different sizes! In spaces where this phenomenon does not occur, these anomalies disappear (see the Dependence Axiom on the next page).

The Dependence Axiom. *If I is independent but $I + x$ is dependent, then $x \in \langle I \rangle$.*

(We write $I + x$ for the disjoint sum $I \cup \{x\}$.)

Remarks. The Dependence Axiom holds in vector spaces, as well as in projective spaces.

The Dependence Axiom easily implies that maximal independent sets are spanning sets – hence bases. Thus, *under the Dependence Axiom, bases, maximal independent sets, and minimal spanning sets are all the same.* As we saw above, without the Dependence Axiom, bases (as well as maximal independent sets) can have different sizes. [It may even be possible to construct a finite dimensional space with an infinite dimensional subspace.]

The Dependence Axiom also implies (see page 5) the following very important inequality.

Corollary (Fundamental Inequality). *Assume that the Dependence Axiom holds in a near-linear space $S = (P, L)$. If $I \subseteq P$ is an arbitrary independent set and $T \subseteq P$ is an arbitrary spanning set, then $|I| \leq |T|$. (We also consider $|I| \leq |T|$ valid when T is infinite.)*

Corollary. *Assume that the Dependence Axiom holds in a near-linear space $S = (P, L)$. If S has bases, then any two bases of S have the same number of elements.*

Recall that a space is finite-dimensional if it has a finite spanning set.

Theorem 2. *Let $S = (P, L)$ be finite dimensional. Then S has a basis. In fact – by (II)– , every spanning set (of P) contains a basis [can be shrunk to a basis].*

Furthermore, if S satisfies the Dependence Axiom, then (by the Fundamental Inequality) every independent set is also finite, and every independent set is contained in a basis [can be expanded to a basis]

Dimension

Definition. *In a near-linear space in which there are bases and in which all bases have the same size, this common cardinality minus one is called the* **dimension** *of the space.*

(The reason that in linear algebra's dimension definition we don't subtract one from the size of a basis is that there we insist that all subspaces contain one more point: the zero vector.)

In spaces which have bases of different sizes, various definitions of dimension are in use; we prefer leaving the notion of dimension undefined in those spaces.

Proofs

Proof of (5): If $A \subset B$, then $\langle A \rangle \subseteq \langle B \rangle$. Indeed, $\langle B \rangle$ is a subspace containing B, hence it is a subspace containing A. Since $\langle A \rangle$ is the *smallest subspace* containing A, it is contained in *any* other subspace that contains A, e.g., in $\langle B \rangle$. $\square$

Proof of (6): $\langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle$.
Since $A \cup B \subseteq \langle A \rangle \cup B$, so, by monotonicity: $\langle A \cup B \rangle \subseteq \langle \langle A \rangle \cup B \rangle$.

We still need to show the other direction: $\langle A \cup B \rangle \supseteq \langle \langle A \rangle \cup B \rangle$.
Let $C = \langle \langle A \rangle \cup B \rangle$ and $D = \langle A \cup B \rangle$. Thus, we need to show $C \subseteq D$.

Now, C is the *smallest subspace* containing both $\langle A \rangle$ and B, so if we could show that the subspace D also contains these two sets, then we would have $C \subseteq D$.
Indeed, D clearly contains B, and since D is a subspace and it contains A, by virtue of (3) D also contains $\langle A \rangle$. $\square$

Proof of (I). Let B be a basis. Since B is a spanning set by definition, it remains to show that B is minimal (with respect to spanning), that is, for every $x \in B$, the set $B \setminus \{x\}$ is *not* spanning P. (Why is this equivalent to minimality?)

Assume - indirectly - that *there exists* a point $x_0 \in B$ such that already the smaller set $B' := B \setminus \{x_0\}$ *were* spanning P, that is, $(\forall p \in P) p \in \langle B' \rangle$. Then, in particular, $x_0 \in \langle B' \rangle$, contradicting the independence of B. $\square$

Proof of (II). Let M be a minimal spanning set. We need to show that M is independent.
Let $x \in M$ be arbitrary, and let $M' := M \setminus \{x\}$. We need to show that $x \notin \langle M' \rangle$.

Indeed, if we had $x \in \langle M' \rangle$, then, since $M' \subseteq \langle M' \rangle$ too, we would have $M \subseteq \langle M' \rangle$. Thus, by Lemma 1, already M' would span P – contradicting the minimality of M. $\square$

Proof of (IV). Let B be a basis. Since B is an independent set by definition, it remains to show that B is maximal (with respect to independence), that is, for every $y \notin B$, the set $B \cup \{y\}$ *cannot be* independent. (Why is this equivalent to maximality?)

Indeed, let $y \notin B$ be arbitrary. Since B is a basis, it is spanning P, that is, $\langle B \rangle = P$, which means $(\forall x \in P) x \in \langle B \rangle$. In particular, $y \in \langle B \rangle$, hence $B \cup \{y\}$ is indeed *de*pendent. $\square$

Finally, we prove that **under the Dependence Axiom,** all maximal independent sets are bases.

Let I be a maximal independent set, and assume that the Dependence Axiom holds. We need to show that I is a basis. Since I is independent, we only need to show that I spans P, that is, $(\forall x \in P) x \in \langle I \rangle$.

Let $x \in P$ be arbitrary. If $x \in I$, then clearly $x \in \langle I \rangle$ (since $I \subseteq \langle I \rangle$).
If $x \notin I$, then, by the maximality of I, the set $I' := I \cup \{x\}$ is dependent. Hence, by the Dependence Axiom, $x \in \langle I \rangle$ as claimed. $\square$

Proof of the Fundamental Inequality

Replacement Lemma. *Let I be an independent set and let T be a spanning set. If the Dependence Axiom holds, then for every $x \in I$ there is a $y \in T$ such that $y \notin I \setminus \{x\}$ and the set $(I \setminus \{x\}) \cup \{y\}$ is independent.*

Proof (indirect). Assume that there is an $x \in I$ such that for every $y \in T$ 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 $y \in T$ be arbitrary.

Since I^- is independent but either $y \in I^-$ or $I^- \cup \{y\}$ is dependent, the Dependence Axiom implies that $y \in \operatorname{span}(I^-)$. Since $y \in T$ was chosen arbitrarily, we obtained $T \subseteq \operatorname{span}(I^-)$, and since T was a spanning set hence so is I^- (Lemma 1).

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

It is easy to see that the Fundamental Inequality $|I| \leq |T|$ follows from the Replacement Lemma. [Sketch: On replacing an element $x \in I \setminus T$ with some $y \in T \setminus I$, the obtained new set $I' = (I \setminus \{x\}) \cup \{y\}$ is independent, has the same size as I, and has one fewer element outside T than I did. Repeating this process yields an independent set $J \subseteq T$ with $|J| = |I|$.]

Exchange Properties

Let us write $\mathcal{C}$ for the family of all subspaces of S.

The Dependence Axiom follows from the following version of the **Exchange Property**:

$$(\forall A \subseteq P)(\forall x, y \notin \langle A \rangle)\ [x \in \langle A + y \rangle \text{ iff } y \in \langle A + x \rangle],$$

or equivalently,

$$(\forall C \in \mathcal{C})(\forall x, y \notin \mathcal{C})\ [x \in \langle \mathcal{C} + y \rangle \text{ iff } y \in \langle \mathcal{C} + x \rangle].$$

Remark: This Exchange Property holds in vector spaces, as well as in projective spaces (Lemmas 3.9.3-4). Does it hold in all affine spaces? Probably not.

Proof that the Exchange Property implies the Dependence Axiom:
Let I be independent and $I + x$ dependent. Let $y \in I + x$ be such that $y \in \langle I + x - y \rangle$. By the independence of I, we have $y \notin \langle I - y \rangle$. If $x \in \langle I - y \rangle$, we are done (by monotonicity), so assume it is not. Then we can apply the Exchange Property for $A = I - y$.

A more subtle question: If every subspace of S has a basis, then the Dependence Axiom and the Exchange Property are equivalent. A finite dimensional space certainly has a (finite) basis. But is it true that every subspace of a finite dimensional space is finite dimensional? Probably not. (It is true though under the Dependence Axiom.)

Literature: Chapter 1 of Lynn Margaret Batten, Combinatorics of finite geometries. Cambridge University Press 1986. QA 167.2 .B38 1986.