Mathematics for Computer Science
Linear Algebra

Lecture 8: General (real) vector spaces

Andrei Krokhin

November 27, 2020

Contents for today's lecture

- General real vector spaces - abstract vectors
- Subspaces
- Linear combinations and spanning
- Fields - abstract scalars

Reminder: Euclidean vector spaces $\mathbb{R}^n$

- $\mathbb{R}^n = \{(a_1, \ldots, a_n) \mid \text{ all } a_i \in \mathbb{R}\}$, vectors are n-tuples of real numbers
- Operations on $\mathbb{R}^n$: addition and multiplication by a real scalar

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

$$k(a_1, \ldots, a_n) = (ka_1, \ldots, ka_n)$$

General (real) vector spaces

Definition

Let V be a set equipped with operations of "addition" and "multiplication by scalars", that is, for every $\mathbf{u}, \mathbf{v} \in V$ and every $k \in \mathbb{R}$,

- the "sum" $\mathbf{u} + \mathbf{v} \in V$ is defined, and
- the "product" $k\mathbf{u} \in V$ is defined.

V is called a (real) vector space, or linear space, if the following 8 axioms hold:

1. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$,
2. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$,
3. there is an element $\mathbf{0} \in V$ such that $\mathbf{u} + \mathbf{0} = \mathbf{0} + \mathbf{u} = \mathbf{u}$ for all $\mathbf{u}$,
4. for each $\mathbf{u} \in V$, there is $-\mathbf{u} \in V$ such that $\mathbf{u} + (-\mathbf{u}) = (-\mathbf{u}) + \mathbf{u} = \mathbf{0}$,
5. $k(\mathbf{u} + \mathbf{v}) = k\mathbf{u} + k\mathbf{v}$,
6. $(k + m)\mathbf{u} = k\mathbf{u} + m\mathbf{u}$,
7. $k(m\mathbf{u}) = (km)\mathbf{u}$,
8. $1\mathbf{u} = \mathbf{u}$.

The elements from V are called vectors.

Examples of vector spaces

- $\mathbb{R}^n = \{(a_1, \ldots, a_n) \mid \text{ all } a_i \in \mathbb{R}\}$ is a vector space.
- The set $\mathbb{R}^\infty$ of all infinite sequences $\mathbf{u} = (u_1, u_2, \ldots, u_n, \ldots)$ is a vector space with operations of point-wise addition and multiplication (just as in $\mathbb{R}^n$).

$$(u_1, u_2, \ldots, u_n, \ldots) + (v_1, v_2, \ldots, v_n, \ldots) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n, \ldots)$$

$$k(u_1, u_2, \ldots, u_n, \ldots) = (ku_1, ku_2, \ldots, ku_n, \ldots)$$

- All matrices of fixed size $m \times n$ form a vector space, denoted $\mathbb{M}_{mn}$, with the usual operations of matrix addition and multiplication by scalars.
- The set $F(-\infty, \infty)$ of real-valued functions with point-wise operations: if $\mathbf{f} = f(x)$ and $\mathbf{g} = g(x)$ then

$$(\mathbf{f} + \mathbf{g})(x) = f(x) + g(x)$$

$$(k\mathbf{f})(x) = k \cdot f(x)$$

is a vector space.

An unusual example and a non-example

An unusual vector space: Let V be the set of all real numbers, and, for any vectors $\mathbf{u} = u$ and $\mathbf{v} = v$ in it, define

- $\mathbf{u} + \mathbf{v} = u \cdot v$, i.e. define "addition" as the usual multiplication,
- $k\mathbf{u} = u^k$, i.e. define "multiplication by a scalar" as the usual exponentiation.

One can check that this is indeed a vector space, i.e. all 8 axioms hold.

- Axiom 1 $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ translates to $u \cdot v = v \cdot u$, which holds.
- For Axiom 3, what is an element $\mathbf{0} \in V$ with $\mathbf{u} + \mathbf{0} = \mathbf{0} + \mathbf{u} = \mathbf{u}$ for all $\mathbf{u}$?
- Axiom 5 $k(\mathbf{u} + \mathbf{v}) = k\mathbf{u} + k\mathbf{v}$ translates to $(u \cdot v)^k = u^k \cdot v^k$, which holds.
- **Exercise:** Check that all remaining axioms also hold.

A non-example. Modify $\mathbb{R}^2$ as follows: re-define $k(u_1, u_2)$ to be $(ku_1, 0)$. One can check that the first 7 axioms are satisfied, but $1\mathbf{u} \neq \mathbf{u}$ for any $\mathbf{u} = (u_1, u_2)$ with $u_2 \neq 0$. Hence this modified object is not a vector space.

Subspaces

Definition

A subset W of a vector space V is called a subspace of V if W is itself a vector space, with the operations inherited from V.

- To verify that W is a subspace of V, we don't need to check all 8 axioms.
- We only need to check that W is closed under the operations of V, that is, if $\mathbf{u}, \mathbf{v} \in W$ and $k \in \mathbb{R}$ then $\mathbf{u} + \mathbf{v} \in W$ and $k\mathbf{u} \in W$.

Examples of subspaces:

- $\{\mathbf{0}\}$ is a subspace (the zero subspace) of any vector space.
- For any fixed vector $\mathbf{a} \in V$, the set $\{k\mathbf{a} \mid k \in \mathbb{R}\}$ is a subspace of V. Indeed, if $\mathbf{u} = k_1\mathbf{a}$ and $\mathbf{v} = k_2\mathbf{a}$ then $\mathbf{u} + \mathbf{v} = (k_1 + k_2)\mathbf{a}$ and $k\mathbf{u} = k(k_1\mathbf{a}) = (kk_1)\mathbf{a}$.
- The solution set of any homogeneous linear system $A\mathbf{x} = \mathbf{0}$ with n variables is a subspace of $\mathbb{R}^n$. Indeed, if $\mathbf{u}$ and $\mathbf{v}$ are solutions, i.e. $A\mathbf{u} = \mathbf{0}$ and $A\mathbf{v} = \mathbf{0}$, and $k \in \mathbb{R}$ is any scalar then

$$A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} = \mathbf{0} + \mathbf{0} = \mathbf{0} \quad \text{and} \quad A(k\mathbf{u}) = k(A\mathbf{u}) = k\mathbf{0} = \mathbf{0}.$$

Examples of subspaces of $F(-\infty, \infty)$

Recall the vector space $F(-\infty, \infty)$ of real-valued functions with point-wise operations: if $\mathbf{f} = f(x)$ and $\mathbf{g} = g(x)$ then

$$(\mathbf{f} + \mathbf{g})(x) = f(x) + g(x)$$

$$(k\mathbf{f})(x) = k \cdot f(x)$$

It is easy to see that the following sets are subspaces of $F(-\infty, \infty)$.

- $C(-\infty, \infty)$ is the set of all continuous functions in $F(-\infty, \infty)$.
- $D(-\infty, \infty)$ is the set of all differentiable functions in $F(-\infty, \infty)$.
- P_∞ is the set of all polynomials, i.e. functions $p(x) = a_0 + a_1x + \ldots + a_kx^k$
- P_n is the set of all polynomials of degree $\leq n$
  (the degree of a polynomial is the largest k such that $a_k \neq 0$.)

In fact, each of them is a subspace of all the spaces above it in the list.

Linear combinations

Definition

A vector $\mathbf{w} \in V$ is a linear combination of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ if $\mathbf{w} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \ldots + k_r\mathbf{v}_r$ for some scalars $k_1, \ldots, k_r$.

How do we determine whether a given $\mathbf{w} \in \mathbb{R}^n$ is a linear combination of given $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{R}^n$?

We show this on an example in $\mathbb{R}^3$: Let $\mathbf{v}_1 = (1, 2, -1)$ and $\mathbf{v}_2 = (6, 4, 2)$. Which of vectors $\mathbf{w} = (9, 2, 7)$ and $\mathbf{w}' = (4, -1, 8)$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$?

Here's what we need to find out:

- Are there scalars k_1 and k_2 such that $\mathbf{w} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2$, or

$$(9, 2, 7) = (k_1 + 6k_2, 2k_1 + 4k_2, -k_1 + 2k_2) \ ?$$

- Are there scalars k_1' and k_2' such that $\mathbf{w}' = k_1'\mathbf{v}_1 + k_2'\mathbf{v}_2$, or

$$(4, -1, 8) = (k_1' + 6k_2', 2k_1' + 4k_2', -k_1' + 2k_2') \ ?$$

Example continued

- Does this have a solution: $(9,2,7) = (k_1 + 6k_2, 2k_1 + 4k_2, -k_1 + 2k_2)$?
- Does this have a solution: $(4,-1,8) = (k_1' + 6k_2', 2k_1' + 4k_2', -k_1' + 2k_2')$?

Algorithm: re-write the vector equation as a linear system (or directly as the augmented matrix of the system) and transform the matrix to row echelon form:

$$\begin{array}{rrl} k_1 & +6k_2 & = 9 \\ 2k_1 & +4k_2 & = 2 \\ -k_1 & +2k_2 & = 7 \end{array} \qquad \left(\begin{array}{rr|r} 1 & 6 & 9 \\ 2 & 4 & 2 \\ -1 & 2 & 7 \end{array}\right) \rightsquigarrow \left(\begin{array}{rr|r} 1 & 6 & 9 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array}\right)$$

$$\begin{array}{rrl} k_1' & +6k_2' & = 4 \\ 2k_1' & +4k_2' & = -1 \\ -k_1' & +2k_2' & = 8 \end{array} \qquad \left(\begin{array}{rr|r} 1 & 6 & 4 \\ 2 & 4 & -1 \\ -1 & 2 & 8 \end{array}\right) \rightsquigarrow \left(\begin{array}{rr|r} 1 & 6 & 4 \\ 0 & 1 & 9/8 \\ 0 & 0 & 1 \end{array}\right)$$

Recall: a solution exists $\Leftrightarrow$ row echelon form has <u>no</u> leading 1 in the last column.

Conclusion: $\mathbf{w}$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$, but $\mathbf{w}'$ is not.

If actual values for k_1 and k_2 are needed, finish solving the first system.

Linear combinations

How do we determine whether a given $\mathbf{w} \in \mathbb{R}^n$ is a linear combination of given $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{R}^n$?

General algorithm:

1. Form the matrix $A = [\mathbf{v}_1 | \ldots | \mathbf{v}_r | \mathbf{w}]$ whose columns are our vectors.
2. Transform A to row echelon form B.
3. If B has no leading 1 in the last column, answer yes. Otherwise, answer no.

Span

Recall that a vector $\mathbf{w} \in V$ is a linear combination of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ if $\mathbf{w} = k_1\mathbf{v}_1 + k_2\mathbf{v}_2 + \ldots + k_r\mathbf{v}_r$ for some scalars $k_1, \ldots, k_r$.

Definition

For a non-empty subset S of a vector space V, the span of S, denoted $span(S)$, is the set of all linear combinations of vectors in S.

Theorem

If S is a non-empty subset of a vector space V then $span(S)$ is a subspace of V. Moreover, it is the smallest (inclusion-wise) subspace of V that contains S.

Proof.

The proof is almost obvious. Clearly, if $\mathbf{u}$ and $\mathbf{v}$ are linear combinations of vectors from S then so is $\mathbf{u} + \mathbf{v}$, and, for any $k \in \mathbb{R}$, so is $k\mathbf{u}$. So, $span(S)$ is a subspace.

Now, let W be any subspace of V such that $S \subseteq W$. Since W is closed under the operations of V, every linear combination of vectors in S must be in W. Hence, we have $span(S) \subseteq W$. □

Spanning $\mathbb{R}^n$

The standard unit vectors in $\mathbb{R}^n$ are $\mathbf{e}_1 = (1, 0, \dots, 0), \dots,\ \mathbf{e}_n = (0, \dots, 0, 1)$.

They span $\mathbb{R}^n$ because any vector $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ can be represented as

$$(a_1, a_2, \dots, a_n) = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \dots + a_n\mathbf{e}_n.$$

Theorem

For any $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{R}^n$, we have $span(\mathbf{v}_1, \dots, \mathbf{v}_n) = \mathbb{R}^n$ iff $det([\mathbf{v}_1| \dots |\mathbf{v}_n]) \neq 0$.

Proof.

- Observe: we have $span(\mathbf{v}_1, \dots, \mathbf{v}_n) = \mathbb{R}^n$ iff $\mathbf{e}_1, \dots, \mathbf{e}_n \in span(\mathbf{v}_1, \dots, \mathbf{v}_n)$, i.e. each vector $\mathbf{e}_j$ is a linear combination of the $\mathbf{v}_i$'s (Why?)
- Let $A = [\mathbf{v}_1| \dots |\mathbf{v}_n]$ and observe that $I = [\mathbf{e}_1| \dots |\mathbf{e}_n]$.
- Each vector $\mathbf{e}_j$ is a linear combination of the $\mathbf{v}_i$'s iff there is a matrix $B = (b_{ij})$ such that $AB = I$. Specifically, in this case $\mathbf{e}_j = b_{1j}\mathbf{v}_1 + \dots b_{nj}\mathbf{v}_n$ for all j.
- Such B exists iff A is invertible, i.e. iff $det(A) \neq 0$.

□

Fields

A vector space involves two types of objects: vectors and scalars

We have made vectors abstract, but used only real numbers as scalars.

In full generality, any field can be used as the set of scalars.

A field is an algebraic structure: any set with operations denoted by $+$, $-$, $\cdot$, $\div$ defined on it so that the operations satisfy the usual (for $\mathbb{R}$) properties such as:

- $a + b = b + a$, and $a \cdot b = b \cdot a$
- $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $a \cdot (b + c) = a \cdot b + a \cdot c$
- there is a "0" element for addition and a "1" element for multiplication
- each element a has a negative $-a$ and each non-0 element has an inverse a^{-1}. Then $a - b = a + (-b)$ and, if $b \neq 0$, $a/b = a \cdot b^{-1}$.

A non-example: The integers $\mathbb{Z}$ do not form a field - why?

Examples of fields

Examples of infinite fields (other than $\mathbb{R}$):

- The rational numbers $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ and } n \neq 0\}$.
- The complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$.

Examples of finite fields:

- The two-element field, denoted $\mathbb{Z}_2$ or $\mathrm{GF}(2)$: the set $\{0, 1\}$ with addition $\oplus$ (aka XOR) and multiplication (aka AND) modulo 2.
- More generally, $\mathbb{Z}_p$ or $\mathrm{GF}(p)$ for a prime number p: same as above, but with the set $\{0, 1, \ldots, p-1\}$ and operations working modulo p.
- Even more generally, arbitrary finite fields $\mathrm{GF}(p^k)$ with p^k elements where p is a prime and $k \geq 1$. The operations are more involved than just mod p^k.

Application in coding theory:

- Vector spaces formed by n-tuples of elements from $\mathrm{GF}(p^k)$ – i.e. like $\mathbb{R}^n$, but with $\mathrm{GF}(p^k)$ in place of $\mathbb{R}$ – are of central importance in coding theory. Subspaces of these spaces are called linear codes — this is a special type of error-correcting codes.

What we learnt today

General vector spaces

- Definition and examples
- Subspaces
- Linear combinations and span
- Fields - abstract scalars

Next time:

- Linear (in)dependence
- Bases and dimension of vector spaces