(c)2020 Karen Smith UM Math Dept

By-NC-SA 4.0 International License.

Math 217 Proof Techniques

This document lists some of the proof techniques we learn in Math 217.

1 General Techniques

GENERAL TECHNIQUE TO GET STARTED: Restate clearly your hypotheses (givens) using symbolic mathematical language.

Example: *Show that if the kernel of a linear transformation T is trivial, then T is injective.*
First Line: Assume $\ker T = 0$.

TECHNIQUE TO DISPROVE SOMETHING: Just give an explicit counterexample. It is fine (even desirable) to take the simplest possible example.

Example: *Prove or disprove that matrix multiplication is commutative.*

Proof: False! (State clearly what you will do.)

Let $A = \begin{bmatrix} 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. (State clearly your counterexample.)

Then $AB = [0]$ but $BA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. (Verify.)

TECHNIQUE TO PROVE SOMETHING EXISTS: Just give an explicit example. It is fine (even desirable) to take the simplest possible example.

Example: *Show that there exists a non-zero matrix such that $A^2 = 0$.*

Proof: Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Note A^2 is the zero matrix.

PROOF TECHNIQUE: INDUCTION. *This often works for statements $P(n)$ that are indexed by whole numbers n. First prove the* **base case** *(usually case $n = 1$). Then show $P(k) \implies P(k+1)$.*

Example: *Prove that* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^N = \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}$.

Proof: We induce on N.

Base Case: $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Inductive Assumption: Assume $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$.

Multiply both sides by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ to get

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}.$$

The proof is complete by induction.

TECHNIQUE TO SHOW SOMETHING IS "UNIQUE": assume there are two, do some math to show they are the same.

Example: *Show that the inverse of an invertible matrix is unique.*

Proof: Let A be an invertible matrix. (Name relevant objects.)
Suppose that B and C are both inverses to A. (Assume two.)
So $AB = BA = I_n$ and $AC = CA = I_n$. (Write out what things mean.)
So $AB = AC$ (by substitution). (Do some math.)
Multiply both sides by B on the left to get $B(AB) = B(AC)$. (Do some more math.)
So $(BA)B = (BA)C$ (associative property). (Do some math.)
So $I_nB = I_nC$, as $BA = I_n$. Finally, we conclude that $B = C$. (State conclusion nicely.)

PROOF BY CONTRAPOSITIVE : To "P implies Q," it is logically equivalent to prove "Not Q implies not P." Sometimes this is easier.

Example: *Let $V \xrightarrow{T} W$ be a linear transformation and let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_d$ be vectors in V. Prove that if $T(\vec{v}_1), \ldots T(\vec{v}_d)$ are linearly independent, then so are $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_d$.*

Proof:

We prove the contrapositive statement: (State the contrapositive:)
If $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_d$ are linearly dependent, then $T(\vec{v}_1), \ldots T(\vec{v}_d)$ are linearly dependent.
We have a relation $a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_d\vec{v}_d = 0$ with at least one $a_i \neq 0$. (Use the definition.)
Apply T. We get $T(a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_d\vec{v}_d) = T(0) = 0$. (Do some math).
So $a_1T(\vec{v}_1) + a_2T(\vec{v}_2) + \cdots + a_dT(\vec{v}_d) = 0$ because T is linear. (Use definitions.)
This is a non-trivial relation on $T(\vec{v}_1), \ldots T(\vec{v}_d)$ since some a_i is non-zero.
So $T(\vec{v}_1), \ldots T(\vec{v}_d)$ are linearly dependent. QED. (Restate conclusion clearly.)

2 General technique for inclusions, unions and intersections

TECHNIQUE TO SHOW TWO SETS X AND Y ARE THE SAME: First show $X \subset Y$. Next show $Y \subset X$.

Example: *Show that* $(X \cup Y)^c = X^c \cap Y^c$.

SCAFFOLD:
We first show that $(X \cup Y)^c \subset X^c \cap Y^c$.
MATH
We next show that $X^c \cap Y^c \subset (X \cup Y)^c$.

TECHNIQUE TO SHOW $X \subset Y$: Take an arbitrary element x of X and then do some math to see that also x is in Y.

Example: *Show that if* $T^2 = 0$, *then im* $T \subset \ker T$.
First Line: Take arbitrary $\vec{x} \in \text{im}\, T$. (The standard technique to show inclusion.)
Next line: We need to show $\vec{x} \in \ker T$.

TECHNIQUE TO SHOW $W \subset X \cap Y$: Show separately that $W \subset X$ and that $W \subset Y$.

Example: *Prove that* $(X \cup Y)^c \subset X^c \cap Y^c$.

Proof: Take arbitrary $x \in (X \cup Y)^c$. (The standard technique to show inclusion.)
This means $x \notin (X \cup Y)$. (Write out what things mean.)
So $x \notin X$, which means $x \in X^c$. (Showing each set separately.)
Also, $x \notin Y$, which means $x \in Y^c$. (Showing each set separately.)
Thus $x \in X^c \cap Y^c$. QED.

TECHNIQUE TO SHOW A MATRIX IS WHAT YOU CLAIM IT IS: check each column is what you claim by multiplication by $\vec{e}_i$ using the Unreasonably Useful Lemma.

Example: *Let $\mathbb{R}^n \xrightarrow{T_A} \mathbb{R}^m$ be the map given by left multiplication by A. Show that if T_A is the zero map, then A is the zero matrix.*

First line: Assume $T_A = 0$. (Restate givens.)

Second line: This means $T_A(\vec{x}) = 0$ for all $\vec{x}$. (Restate in precise, concise math.)

In particular $T_A(\vec{e_i}) = A\vec{e_i} = 0$ so the i-th column is zero. (The unreasonably useful lemma.)

Since this holds for all i, all columns are zero, and so the matrix is zero.

3 Techniques to show injectivity, surjectivity, invertibility.

TECHNIQUE TO SHOW A MAP $f : X \to Y$ IS INJECTIVE: Take two arbitrary $x_1, x_2 \in X$. Assume that $f(x_1) = f(x_2)$. Then do some math to show that actually $x_1 = x_2$.

Example: *Show that if the kernel of a linear transformation $V \xrightarrow{T} W$ is trivial, then T is injective.*

Proof: Assume $\ker T = 0$. (Restate givens).

Suppose that $T(\vec{x}) = T(\vec{y})$ for some $\vec{x}, \vec{y} \in V$. (The standard technique to show injectivity.)

Then $0 = T(\vec{x}) - T(\vec{y}) = T(\vec{x} - \vec{y})$ because T is linear. (Do some math...)

So $\vec{x} - \vec{y} \in \ker T$. (When stuck...how can I use my hypotheses?)

Since $\ker T = 0$, we deduce $\vec{x} - \vec{y} = 0$, so $\vec{x} = \vec{y}$. Thus T is injective.

Another technique is to make use of the following **important and very useful Theorem:** A LINEAR TRANSFORMATION IS INJECTIVE IF AND ONLY IF ITS KERNEL IS ZERO. This leads to...

ANOTHER TECHNIQUE TO SHOW A LINEAR TRANSFORMATION IS INJECTIVE: Just show the kernel is trivial. Do this by taking an arbitrary element in the kernel, then showing it must be zero.

Example: *Let $T : \mathbb{R}[x] \to \mathbb{R}[x]$ be the linear transformation sending $f \mapsto xf$. Prove that T is injective.*

[Here, the notation $\mathbb{R}[x]$ denotes the vector space of all polynomial functions, also called $\mathcal{P}$ in the worksheets.]

Proof:

It suffices to show $\ker T = 0$. (Standard technique: Just show the kernel is ZERO.)

Let $f = a_0 + a_1x + \cdots + a_nx^n$ be an arbitrary element in $\ker T$. (Write out arbitrary element)

This means $T(f) = xf = a_0x + a_1x^2 + \cdots + a_nx^{n+1} = 0$. (Write out what stuff means.)

So $a_0 = a_1 = \cdots = a_n = 0$.

So $f = 0$.

Since the kernel is trivial, the linear transformation T is injective.

TECHNIQUE TO SHOW A MAP $f : X \to Y$ IS SURJECTIVE: Take arbitrary $y \in Y$, then do some math to cook up some $x \in X$ so that $f(x) = y$.

Example: *Show that if A is an $d \times n$ matrix of rank d, then the linear transformation $T_A : \mathbb{R}^n \to \mathbb{R}^d$ given by multiplication by A is surjective.*

First line: Let A be a $d \times n$ matrix of rank d. (Restate givens.)
Next line: Take arbitrary $\vec{y} \in \mathbb{R}^d$. (Technique for surjectivity: Take arbitary $\vec{y}$ in the target.)
Next line: We need to find $\vec{x} \in \mathbb{R}^n$ such that $A\vec{x} = \vec{y}$. (Restate what needs to be done.)

ANOTHER TECHNIQUE TO SHOW SURJECTIVITY: Show that the image equals the target. For a linear transformation, it is also enough to show the dimension of the image equal to the dimension of the target (if this is finite dimensional).

Example: *Prove the map $T : \mathbb{R}^6 \to \mathbb{R}^3$ given by multiplication by the matrix* $\begin{bmatrix} 1 & 2 & 0 & 4 & 5 & 0 \\ 0 & \pi & 1 & 4 & 12 & 0 \\ 0 & \sqrt{17} & 0 & 4 & 5 & 1 \end{bmatrix}$ *is surjective.*

Proof:
The image of T is spanned by the columns. (Make use of Theorems.)
Note that the columns 1, 3, 6 are $\vec{e}_1, \vec{e}_2, \vec{e}_3$ span all of $\mathbb{R}^3$.
So the image is all of $\mathbb{R}^3$.
This means the map is surjective.

SOME TECHNIQUES TO SHOW A MAP $f : X \to Y$ IS BIJECTIVE (OR INVERTIBLE):

1. You can show BOTH f is injective AND f is surjective.
2. You can take arbitrary $y \in Y$ and show that there is a **unique** $x \in X$ such that $f(x) = y$.
3. You can **define** (or state what) the inverse map is; be sure to verify that it is really the inverse by checking the compositions in both orders.

Example for (3): *Prove that rotation counterclockwise by θ is a bijective map of $\mathbb{R}^2$.*

Proof: The inverse is clearly clockwise through an angle of θ.

4 Techniques for Dealing with Kernel and Image

TECHNIQUE TO WRITE ARBITRARY ELEMENT IN IMAGE: Given $X \xrightarrow{f} Y$, then an arbitrary y in the image of f can be written $y = f(x)$ for some $x \in X$.

Example: *Prove that im $T_A \subset W$ where T_A is left multiplication by A.*
First line: Take arbitrary $\vec{y} \in \text{im}\, T_A$. (The standard technique to show inclusion.)
Next Line: Write $y = T_A(\vec{x})$ for some $\vec{x}$. (The standard way to write elements in image.)
Next Line: So $y = A\vec{x}$. (Rewrite what stuff means.)

TECHNIQUE TO SHOW ELEMENTS ARE IN KERNEL: To show $\vec{x} \in \ker f$, just show $f(\vec{x}) = 0$.

Example: *Prove that if $A^2 = 0$, then im$T_A \subset$ ker T_A where T_A is left multiplication by A.*
First line: Assume $A^2 = 0$. (Restate givens concisely.)
Then: Take arbitrary $\vec{y} \in \text{im}T$. (Standard technique to show $X \subset Y$.)
Write $\vec{y} = T_A(\vec{x})$ for some $\vec{x}$. (Standard way to write elements of image.)
This means $\vec{y} = A\vec{x}$. (Restate what things mean.)
So $A\vec{y} = A(A\vec{x}) = A^2\vec{x} = 0\vec{x} = 0$. (Here we apply the transformation to check that we get 0.)

5 Span, linearly independence and bases

TECHNIQUE TO SHOW VECTORS SPAN: To show $\vec{v}_1, \ldots, \vec{v}_d$ span W,

1. Make sure each $\vec{v}_i \in W$ (usually given)
2. Next show an arbitrary element of W is a linear combination of $\vec{v}_1, \ldots, \vec{v}_d$.

Example: *Prove the plane defined by $x + y + z = 0$ is spanned by the vectors* $\begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$ *and* $\begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$.

Note that both $\begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$ satisfy $x + y + z = 0$. (Step 1.)

Take an arbitrary element $\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$ on the plane. (Starting Step 2.)

This means that $y_1 = -(x_1 + z_1)$. (Rewrite what stuff means.)

So $\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_1 - z_1 \\ z_1 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} + z_1 \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$. (Math.)

TECHNIQUE TO SHOW VECTORS ARE LINEARLY INDEPENDENT: To show $\vec{v}_1, \ldots, \vec{v}_d$ are linearly independent, write out a relation and show it must be trivial.

Example: *Prove that the columns of an invertible matrix are linearly independent.*

First Line: Let A be an invertible $n \times n$ matrix with columns $C_1, \ldots, C_n$.[1]

Next: Suppose $a_1C_1 + \cdots + a_nC_n = 0$ is a relation. (Write out a relation.)

This means that $\begin{bmatrix} C_1 & C_2 & \ldots & C_n \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \vec{0}$.

So $A \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = 0$.

Multiplying both sides by A^{-1}, we see $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = 0$. (Do some math to show the relation is trivial.)

Thus our relation must be trivial. This means $C_1, \ldots, C_n$ are linearly independent.

TECHNIQUE TO SHOW VECTORS ARE A BASIS: To show $\{\vec{v}_1, \ldots, \vec{v}_d\}$ are a basis for W, show that they BOTH span W AND are linearly independent.

Example: Prove that $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ form a basis for $\mathbb{R}^2$.

SCAFFOLD:

We first show $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ SPAN $\mathbb{R}^2$.

We next show that $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ are LINEARLY INDEPENDENT.

ALTERNATIVE TECHNIQUE TO SHOW VECTORS ARE A BASIS IF YOU KNOW THE DIMENSION: Let $\{\vec{v}_1, \ldots, \vec{v}_d\}$ be a set of d vectors in a vector space W of dimension d. To show they form a basis, you can prove **either** that they span W **or** that they are linear independent. You do not have to check both **if you know that you have the right number of vectors.**[2]

[2]The reason is THEOREM 3.3.4: A set of D vectors in a D-dimensional vector space V is linearly independent if and only if it spans V.

Example: *Prove that $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ form a basis for $\mathbb{R}^2$.*
First Line: Since we know that the dimension of $\mathbb{R}^2$ is 2, it suffices to show that $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ SPAN $\mathbb{R}^2$.
Alternate First Line: Since we know that the dimension of $\mathbb{R}^2$ is 2, it suffices to show that $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ are linearly independent.

6 Dealing with "and" and "or" Statements

TECHNIQUE TO PROVE "AND" STATEMENTS: To prove "P implies Q_1 and Q_2," you need to separately prove that "P implies Q_1" and also that "P implies Q_2".

TIP: If you first show that "P implies Q_1," you are allowed to assume Q_1 while showing that "P implies Q_2."

Example:. *Prove that if $T_A : \mathbb{R}^d \to \mathbb{R}^n$ is a linear transformation given by left multiplication by a rank n matrix A, then T_A is surjective and the kernel has dimension $d - n$.*

Proof: We first show that T_A is surjective. (Showing P implies Q_1.)
Recall that the dimension of $\operatorname{im} T_A$ equals the rank of A. (Making use of Theorems.)
So the image is a subspace of $\mathbb{R}^n$ of dimension n.
This means $\operatorname{im} T_A = \mathbb{R}^n$. (Using characterization of surjective.)
So T_A is surjective.

We next show that $\ker T_A$ has dimension $d - n$. (Showing P implies Q_2.)
Since $\dim \mathbb{R}^d$ (source) is d and $\dim \operatorname{im} T_A = n$, the Rank-Nullity theorem (Use Theorems!)
implies that $\dim \ker T_A = d - n$. QED.

TECHNIQUE TO PROVE "OR" STATEMENTS: To prove "P implies Q_1 or Q_2," you can assume "NOT Q_1 and then show that "P implies Q_2". Alternatively, of course, you can assume "NOT Q_2 and show that "P implies Q_1".

You should make sure you understand why this technique works. Note that if you need to show "P implies Q_1 OR Q_2," you would already be done if Q_1 holds. That is the reason you might as well assume Q_1 doesn't hold and just show "P and NOT Q_1 together imply Q_2."

Example:. *Let $\vec{v}_1, \ldots, \vec{v}_d$ be linearly independent elements in a vector space V. Then for every $\vec{w} \in V$, we have $\vec{w} \in$ Span $\{\vec{v}_1, \ldots, \vec{v}_d\}$ or $\{\vec{v}_1, \ldots, \vec{v}_d, \vec{w}\}$ is linearly independent.*

Proof: Assume $\vec{w} \notin \{\vec{v}_1, \ldots, \vec{v}_d\}$. (Technique for "or" statements.)
We need to show that $\{\vec{v}_1, \ldots, \vec{v}_d, \vec{w}\}$ is linearly independent.

Let $a_1\vec{v}_1 + \cdots + a_d\vec{v}_d + a_{d+1}\vec{w} = 0$ be a relation on $\{\vec{v}_1, \ldots, \vec{v}_d, \vec{w}\}$.
We need to show that the scalars $a_1, \ldots, a_{d+1}$ are all zero. (Technique for linear independence.)

Case 1: $a_{d+1} = 0$. General Technique: handle different cases separately.
In this case, $a_1\vec{v}_1 + \cdots + a_d\vec{v}_d = 0$ is a relation on $\{\vec{v}_1, \ldots, \vec{v}_d\}$,
and since $\{\vec{v}_1, \ldots, \vec{v}_d\}$ is independent, we have $a_i = 0$ for $i = 1, \ldots d+1$.

Case 2: $a_{d+1} \neq 0$. General Technique: handle different cases separately.
If $a_{d+1} \neq 0$, we can re-arrange the relation to get General Technique: check case-by-case.

$$\vec{w} = \frac{-a_1}{a_{d+1}}\vec{v}_1 + \cdots + \frac{-a_d}{a_{d+1}}\vec{v}_d.$$

This says that $\vec{w} \in$ Span $\{\vec{v}_1, \ldots, \vec{v}_d\}$.
The proof is complete.

7 When all else fails

PROOF TECHNIQUE: CONTRADICTION. *Assume the conclusion is false and try to deduce an obviously absurd statement.*

Example: *Let $T : V \to W$ be a linear transformation. Prove that if $\dim V > \dim W$, then T is not injective.*

Proof: Assume, on the contrary, that T is injective. Assume conclusion is false.
This means that $\ker T$ is trivial. Standard technique for handling injective linear transformation.
This means $\dim \ker T = 0$.
The Rank-Nullity Theorem says that $\dim V = \dim \text{im}T + \dim \ker T$, Make use of Theorems!
so in this case, $\dim V = \dim \text{im}T$.
Since $\text{im}T \subset W$, we also know that $\dim \text{im}T \leq \dim W$.
Combining the last two sentences, we have $\dim V \leq \dim W$.
This contradicts our hypothesis.
This contradiction completes the proof.

8 General Questions to Ask when you are stuck

1. What is the first line of the proof?
2. Can I scaffold the proof? For example, it is an "if and only if" statement, write out each direction to be proved separately.
3. Have I named the relevant objects?
4. What am I trying to prove again?
5. Have I written out what things mean?

6. How can I use the definition?
7. Have I used all the hypotheses?
8. What are some of the theorems related to the objects in the statement I am trying to prove?
9. Can I use rank-nullity? Theorem 3.3.4 is also very useful, can I use it?
10. What if restate the contrapositive? Can I get a start on the contrapositive statement?
11. Will induction work? Is there something I can induce on?
12. How would I start a proof by contradiction?