Proofs of non-existence – methods and examples

Demian von Below, Felix Morooka, David Mörtberg
Rosendalsgymnasiet, Uppsala

May 2021

Contents

1 Introduction

In this document, we wish to clarify this subject by giving you formal theories while giving you examples and going through some of the common misconceptions in proofs of non-existence as well as in other logical proofs, as these are very easy to miss and to be improperly stated as "trivial". We will also further develop some applications of proofs of non-existence in problem solving. Here is a quick explanation of what a proof of non-existence is. The word "Exist" refers to being a part of a set and on the other hand non-existence refers to an empty set.

Proofs on non-existence are necessary when answering questions such as "Find all…", "does there exist…" or "prove that this does not exist". The key is to find some restrictive property held by all elements in the given set, so that only a handful if any objects or values are possible solutions and, therefore, testing them is easy. If the solution consists of a large or infinite group of objects, it is necessary to prove that they are valid, since testing is impossible. It is of course not enough to fail proving that they are not valid. Remember that even if you have not managed to prove that some values are not possible does not mean that they are.

1.1 Logical notations

A good way to be clear about what a problem is about is to write it down with formal logic notation. Logical notations are also useful when you want to write down a statement quickly. Here is a table on the logical notations used in this essay.

Notation	Meaning
∃	"There exists"
¬	"NOT"
∀	"For all" / "For each" / "For every"
P(x)	TRUE: If x fulfills the property P. FALSE: If x does not fulfil the property P. ex: Say $P(x)$ is the equation $x^2 + x = 0$. If $x =- 1$, then $(-1)^2 + (-1) = 0$ and therefore $P(x)$ will hold the value TRUE.

2 Reversing statements

2.1 Non-existence

Here is how you can turn a non-existence problem into a different problem, and some examples of how it could be useful.

> If there exists an x at all, $\neg\exists x(P(x)) \Leftrightarrow \forall x(\neg P(x))$
> “There doesn’t exist an x such that a property holds”⇔”For all x, the property doesn’t hold”

Problem: Prove there does not exist an x such that $x$is even and $3x$ is odd
Proof: Restate the problem to the following: Prove that for all x, if x is even, then $3x$ is even. This is trivial, since $3 * 2n$ also is divisible by 2.

Problem: Show that, for all positive integers, $a^2 + 1$ is not divisible by 3.
Proof: We can restate the problem to “Show that there does not exist a positive integer a such that $a^2 + 1$ is divisible by 3”. Division by 3 can give us three different remainders (0, 1 and 2). Thus, we can divide all positive integers into 3 categories: numbers written in the form $3n$, $3n + 1$, $3n + 2$. In $mod\ 3$, these numbers are 0, 1 and 2. $0^2 + 1 \equiv 1, 1^2 + 1 \equiv 2, 2^2 + 1 = 5 \equiv 2\ mod\ 3$. None of these became $0\ mod\ 3$, which shows us that no positive integer will be divisible by 3.

2.2 Denying the consequent / Modus tollens

Problems which include proving that if one statement is true, another statement must also be true, can be reversed to proving that if the second statement is false, then the first must also be false. To show that a problem can be reversed like this, consider this example:

$$(It's\ raining \Rightarrow The\ cat\ is\ inside) \Leftrightarrow (The\ cat\ is\ not\ inside \Rightarrow It's\ not\ raining)$$

This reasoning is called Modus tollens or denying the consequent and it is quite often useful in non-existence proofs. The cat is inside if it is raining. The cat is not inside. therefore it is not raining,

It can also go the other way around. If the cat is not inside means that it is not raining, then the fact that it is raining implies that the cat must be inside.

Modus tollens:
If P then Q
Not Q
Therefore, not P

Problem: Show that if $2^n - 1$ is prime, then n is prime.

Proof: We use modus tollens, $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ to restate the problem to the following: Show that if n is not prime, then $2^n - 1$is not prime. Then if n is not prime, we can assume that $n = ab$ where $a$and b are two integers bigger than 1 and not equal to n.
Then we have:

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$$

We will use the well known formula of: $t^m - 1 = (t - 1)(1 + t + t^2 + ... + t^{m-1})$.
Apply $t^m - 1 = (t - 1)(1 + t + t^2 + ... + t^{m-1})$ to get
$(2^a)^b - 1 = (2^a - 1)(1 + 2^a + (2^a)^2 + ... + (2^a)^{b-1})$. Both factors in the equation are greater than 1 so $2^n - 1$ is not prime.

3 Common Misconceptions

3.1 Affirming the consequent

A common mistake that follows from the use of Modus tollens is affirming the consequent, that is reasoning that if $Q \Rightarrow P$, then $P \Rightarrow Q$. For example, consider the following "proof" that $\sqrt{2} + \sqrt{6} < \sqrt{15}$:

$$\sqrt{2} + \sqrt{6} < \sqrt{15}$$
$$\Rightarrow (\sqrt{2} + \sqrt{6})^2 < 15$$
$$\Rightarrow 8 + 2\sqrt{12} < 15$$
$$\Rightarrow 2\sqrt{12} < 7$$
$$48 < 49$$

Here we did not prove that $48 < 49 \Rightarrow \sqrt{2} + \sqrt{6} < \sqrt{15}$, we only proved the other way around. An easy way to fix this would be to assume that $\sqrt{2} + \sqrt{6} \geq \sqrt{15}$, replace all "<" by "≥" in the proof and then contradict the assumption.

Here are two more examples:

$x = 5 \Rightarrow |x + 2| = 7$ but $|x + 2| = 7 \Rightarrow (x = 5 \; or \; x = -9)$

We know that all squares are rectangles, but all rectangles are not squares.

3.2 Know if your assumption exists

Some people might argue that "If I can calculate the solution to a problem, then surely I don't need to worry about whether a solution exists", but this is a misconception. Take this false proof as an example:

Example: Find the largest integer.

Proof: Let the largest integer be N, then $N \geq 1$. We also have $N \geq N^2$. So $N^2 - N \leq 0$ and in turn $N(N - 1) \leq 0$. Since N is positive, we can factor out N from the left side and get $(N - 1) \leq 0$ which leads to $N \leq 1$. Recall that $N \geq 1$ and therefore $N = 1$. The conclusion is that 1 is the largest integer.

We see that if there exist a largest integer, it has to be 1. But we know that $2 > 1$, so our assumption is false. Therefore, there does not exist a largest integer N. While it might be obvious in this example that the conclusion is false i.e. there is no largest integer, there are cases when the solution actually is true and in those circumstances this step is necessary for a complete proof of a theorem.

4 Proving that a set has no "boundary"

Assume that all elements in a set satisfies a property and that there exists an element in the set. We can prove that the set is infinite by proving that for any element in the set, there must exist another element with a value larger/smaller than the previous value.

Expressing that there exists no maximum/minimum: $\forall n \exists m (m > n)$ **or** $\forall n \exists m (m < n)$

Problem: Prove that there exist infinitely many positive integers n such that $4n^2 + 1$ is divisible both by 5 and 13.

Proof: Assume that $4n^2 + 1$ is divisible by 5 and 13 for some n. Let $m = n + k$, where k is a positive integer. Then we want to find a k such that $4m^2 + 1$ also is divisible by 5 and 13. $4m^2 + 1 = 4(n + k)^2 + 1 = 4n^2 + 8nk + 4k^2 + 1$ so we want to find a k such that $4n^2 + 8nk + 4k^2 + 1 \equiv 0 \, mod \, 5 \equiv 0 \, mod \, 13$. Recall that $4n^2 + 1$ is divisible by 5 and 13, so we want $8nk + 4k^2 = 4k(2n + k) \equiv 0 \, mod \, 5 \equiv 0 \, mod \, 13$. By dividing by 4 we get $k(2n + k) \equiv 0 \, mod \, 5 \equiv 0 \, mod \, 13$. Because 5 and 13 are relatively prime (Their greatest common divisor is 1), we can express $2n$ as $2n = 13a - 5b$ where a and b are integers and b is positive. Let $k = 5b$, then $2n + k = 13a$ which is divisible by 13 so $k(2n + k) \equiv 0 \, mod \, 5 \equiv 0 \, mod \, 13$. $m = n + k = n + 5b$ fulfills our desire. $n = 9$ gives $4n^2 + 1$ to be divisible by 5 and 13 so there exists an n with that property

Problem: Prove that there is no largest prime (*Euclid's theorem*)

Proof: Assume that the set of all prime numbers $[p_1, p_2, \dots, p_n]$ is finite. Consider the number $P = (p_1 p_2 \dots p_n)$ and let $q = P + 1$. Because all the prime numbers p_k in the set is bigger than 1, Pmust be bigger than p_k and furthermore, q is bigger than p_k. If q is a prime number, then because q doesn't exist in the set, it leads to a contradiction and thus the problem is solved. If not, then there exists a prime number p_k such that $p_k | q$. We also know that $p_k | P$, so $p_k | (q - P) = 1$, but since no number other than 1 divides 1, this is once again a contradiction. Therefore the assumption is false and the set of all prime numbers is infinite.

5. Uniqueness

Uniqueness problems, that is proving that a certain solution is the only possible solution, can sometimes be subtle and easy to miss. Many people would skip some steps by thinking it is obvious, so it is important to make it clear why exactly a solution is unique. This equation is expressing that if two values are solutions to a problem, then they have the same value.

Expressing that x is a unique solution: $\forall x \forall y (P(x) \land P(y) \Rightarrow x = y)$

Problem: Prove that for every x, there exists a unique y such that $(x + 1)^2 - x^2 = 2y - 1$.

Proof: Let $y = x + 1$, then $(x + 1)^2 - x^2 = x^2 + 2x + 1 - x^2 = 2(x + 1) - 1 = 2y - 1$. Although we have a description for how to find y, we've only proved the existence of a y. Now we have to prove the uniqueness of y. For every x, if y_0 and y_1 both satisfy the equation, then $2y_0 - 1 = (x + 1)^2 - x^2 = 2y_1 - 1$, so $2y_0 - 1 = 2y_1 - 1 \Rightarrow y_0 = y_1$.

Problem: If a and b are integers and b is positive, then there are integers q and r such that $a = bq + r$ and $0 \leq r < b$. Show that, for any given a and b, $a = bq + r$ has exactly one solution of the pair $(q, r)$for all a (We already know that there exists a solution).

Proof: Let $a = bq_1 + r_1 = bq_2 + r_2$, assume that $r_1 \leq r_2$, that leads to $0 \leq r_1 \leq r_2 < b$. Then because $r_2 < b$ and $r_1 \geq 0, 0 \leq r_2 - r_1 < b$. We have $bq_1 + r_1 = bq_2 + r_2 \Rightarrow r_2 - r_1 = bq_1 - bq_2$, so by substituting that into the previous equation and we get $0 \leq bq_1 - bq_2 < b$. Because b is positive, $0 \leq q_1 - q_2 < 1$. $q_1$and q_2 are integers and therefore $q_1 - q_2$must also be an integer . From the inequality we get $q_1 - q_2 = 0 \Rightarrow q_1 = q_2$. $r_2 - r_1 = b(q_1 - q_2) = 0$ gives $r_1 = r_2$.

6. Infinite descent

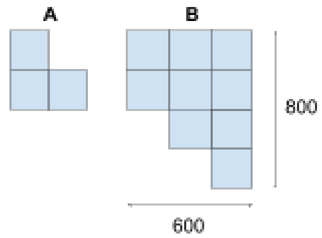
Infinite descent is a special type of proof by contradiction. The method is applied to something with a smallest value, for example the set of all natural numbers. For every natural number, if a specific natural number is a solution to a problem, then it can be proven that a smaller natural number also is a solution and yet an even smaller natural number is a solution. The iteration goes on until there does not exist a smaller natural number. Then there is a contradiction and therefore there does not exist a solution for natural numbers.

Infinite descent (special case): Let P be a property that integers may or may not possess. If the assumption that a positive integer $n_0$has property P leads to the existence of a smaller positive integer $n_1 < n_0$ that also satisfies P, then no positive integer has that property.

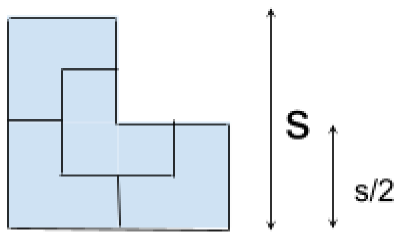
Problem: Show that any composite number is divisible by some prime number.

Proof: Let n_0 be a composite number. Then a number $n_1 < n_0$ divides n_0. If n_1 is prime, then the problem is solved, so assume n_1 is composite. Repeat the process for n_2, n_3 and so on. Either the process ends with an n_k being a prime number, or the process is infinite. If the former option is true, then the problem is solved. If the latter option is true, then according to infinite descent it leads to a contradiction and therefore the problem is solved.

Problem: Peter has a puzzle frame B with integer height 800 and side length 600. He also has infinitely many puzzle pieces in all sizes with a shape similar to A. Peter's job is to fill the frame with as many of the pieces as possible so that he leaves no gaps and no pieces overlapping. Prove that all the pieces that Peter uses to fill the frame does not have integer side length.



Proof:



Notice that piece A can be constructed from 4 smaller pieces of itself. For every integer s, where s is the side length of piece A, assume that Peter thinks of using that piece to fill a part of the frame. But then 4 pieces of side length s/2 can instead be used to fill that same area, yet a piece with side length s/4 makes even better sense then he can fill that area with 16 pieces. If he continues to change his thoughts like this, the side length of the pieces that he chooses to use will not have an integer side length.

Problem: Prove the diophantine equation $9a^3 + 3b^3 + c^3 = 0$ only has the integer solution (0,0,0).

Proof: Assume that there exists another integer solution. Rewrite the equation as $9a^3 + 3b^3 =- c^3$. $3|9a^3 + 3b^3 \Rightarrow 3|c^3 \Rightarrow 3|c$ $(3\ is\ prime)$, $c = 3r$ where r is an integer. Substitute it in the equation and we get $9a^3 + 3b^3 + (3r)^3 = 3(9r^3 + 3a^3 + b^3) = 0 \Rightarrow 9r^3 + 3a^3 + b^3 = 0$. Observe that the new equation is written in the same form as the initial equation. Reiterate this process twice such that $9(a/3)^3 + 3(b/3)^3 + (c/3)^3 = 0$ where a, b, c are divisible by 3. This implies that if (a, b, c) is an integer solution, $(a/3,\ b/3,\ c/3)$is also an integer solution, and furthermore is $(a/9,\ b/9,\ c/9)$ an integer solution in the same way. At some point at least one of the integers will be not divisible by 3, and thus there will be a contradiction.

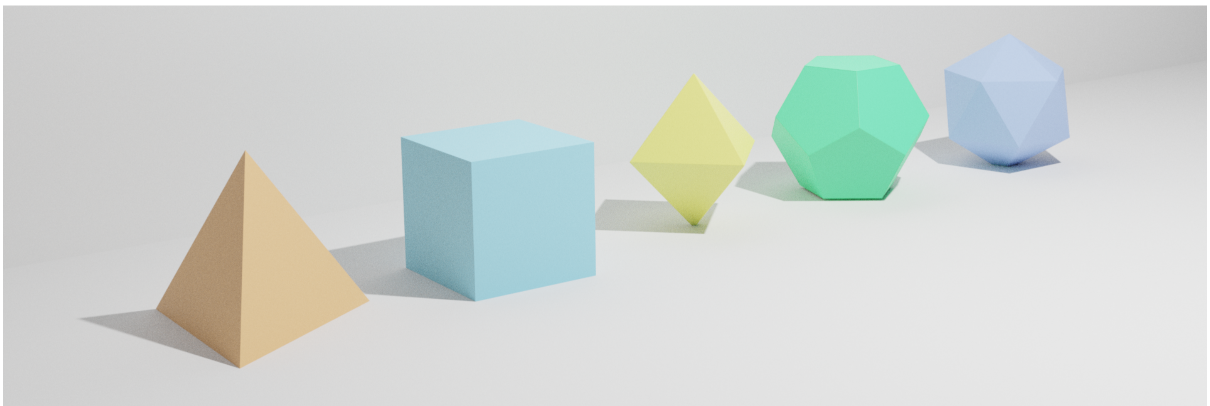
Problem: Prove that there doesn't exist a rational number such that it squared becomes 2.

Proof: Assume that there exists a rational number with that property. Then $2 = (\frac{a}{b})^2$ where a and b are integers. We then have $a^2 = 2b^2$, so $2|a^2 \Rightarrow 2|a$ $(2\ is\ prime)$. We can therefore say that $a = 2r$ where r is an integer. Substitute $a = 2r$ into the equation $a^2 = 2b^2$ and we get $(2r)^2 = 2b^2 \Rightarrow 4r^2 = 2b^2 \Rightarrow 2r^2 = b^2$, so $2|b^2 \Rightarrow 2|b$. We can therefore say $b = 2s$ where s is an integer. Recall that $a = 2r$, so 2 can also be expressed as $2 = (\frac{a/2}{b/2})^2 = (\frac{r}{s})^2$ where r and s are integers smaller than a and b respectively. Infinite descent leads to a contradiction and therefore there doesn't exist a rational number such that it squared becomes 2. Notice that for this problem, the solution can actually be shortened by in the beginning assuming that a and b are relatively prime. We can do this because any fraction written in its reduced form has its numerator and its denominator being relatively prime. Then because $\frac{a}{b} = \frac{r}{s}$ where $r < a$ and $s < b$, r and s can't be integers.

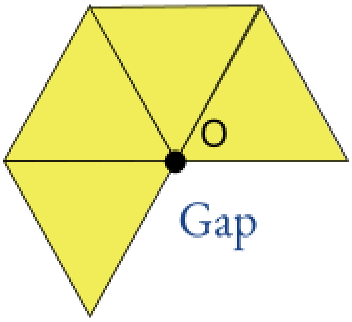
7. Platonic Solids

A platonic solid is constructed by congruent regular polygonal faces with the same number of faces meeting at each vertex. There are only 5 solids in three-dimensional space that fulfills this criteria. Here are the 5 platonic solids. From left to right their names are tetrahedron, hexahedron, octahedron, dodecahedron, icosahedron.

Problem: Why are there no more than 5 platonic solids?



Now we will prove that there exists only 5 platonic solids. Imagine that we take all the faces adjacent to one vertex O in a platonic solid and unravel it out onto a flat surface. Here is an example for the octahedron.



When doing this, notice that a gap will be created. The angle size of this gap is positive. For this example, there are 4 triangles and the angle of a triangle is 60°, so the size of the gap is $360^\circ - 4 \times 60^\circ = 120^\circ$. Similarly, the size of the gap for k regular n-gons is $360^\circ - k \times \frac{180^\circ(n-2)}{n}$ and we know that it must be bigger than 0. Now we try each case for n and k. Because the triangle is the polygon with the least amount of vertices, $n \geq 3$. Every vertex of a solid must be adjacent to at least 3 faces because otherwise, it is not a vertex. Therefore, the unraveled figure consists of at least 3 regular congruent polygons which means that $k \geq 3$.

$n = 3$ gives k =3, 4, or 5

$n = 4$ gives $k = 3$

$n = 5$ gives $k = 3$

$n > 5$ gives $\frac{180^\circ(n-2)}{n}$>108 so $k < 3$ which is a contradiction.

We then have 5 possibilities for the pair (n, k), which are $(3, 3)$, $(3, 4)$, $(3, 5)$, $(4, 3)$ and $(5, 3)$ and the problem is solved. See if you can match each pair with their corresponding platonic solid.

8. Euler's Polyhedron Formula

Euler's polyhedron formula: for all polyhedrons without holes, the formula $V - E + F = 2$ holds, where V stands for the number of vertices, E stands for the number of edges and F stands for the number of faces on the polyhedron.

Problem: Prove that there does not exist a polyhedron which consists of only hexagon sides.

If the number of faces is F, then the number of edges will be $\frac{6F}{2}$, since every face has six edges, but every edge is shared between two faces. This gives us the formula $V - \frac{6F}{2} + F = V - 2F = 2 \Rightarrow V = 2(F + 1)$.

The sum of all angles in a hexagon is 720 degrees, which means that the average angle is 120 degrees. All vertices of faces meeting in a vertex of the polyhedron have to have a total angle of less than or equal to 360 degrees. That means that a vertex with 4 faces will mean that another vertex has to have only two faces adjacent, which is not possible. Since all vertices are connected to three faces, we know that the amount of vertices can be expressed using the number of faces. For every face, we have six vertices, but every vertice share three faces, so $V = \frac{6F}{3}$. We now get that $\frac{6F}{3} = 2(F + 1) \Rightarrow F = F + 1$ which cannot be true. Therefore there cannot exist a polyhedron with only hexagon faces.