date: 2025-09-30

1 proof methods

previously we learned to prove theorems stated as implications. however, not all theorems can be in the form of $p \to q$. sometimes, we need to prove a theorem in the form of something like this:

$(p_1 \vee p_2 \vee p_3 \vee ... \vee p_n) \to q$

therefore, we might need to examine multiple cases; and we introduce several methods just to do that.

1.1 exhaustive proof

in an **exhaustive proof**, we prove a theorem by exhausting all the possibilities. this works best on theorems that only requires a small amount of examples to be proven.

1.1.1 example

theorem: there exists a number n where $n^2 + 1 \geq 2n$, and n is a positive integer with $1 \leq n \leq 4$.

proof:
- $n = 1$: $1^2 + 1 = 2$, $2 \cdot 1 = 2$, $2 > 2$ ✓
- $n = 2$: $2^2 + 1 = 5$, $2 \cdot 2 = 4$, $5 > 4$ ✓
- $n = 3$: $3^2 + 1 = 10$, $2 \cdot 3 = 6$, $10 > 6$ ✓
- $n = 4$: $4^2 + 1 = 17$, $2 \cdot 4 = 8$, $17 > 8$ ✓

since we have verified all four cases of n from 1 to 4, we have shown that $n^2 + 1 \geq 2n$ where $1 \leq n \leq 4$. ■

1.2 proof by cases

proof by cases is used when we need to examine multiple possibilities, but an exhaustive check is not feasible. instead of checking every *individual* value, we group possibilities into different categories, or *cases* that cover all potential scenarios.

1.2.1 example

theorem: if x and y are real numbers, then $|x| + |y| \geq |x + y|$.

note: if $|x| \geq 0$, $|x| = x$, otherwise $|x| = -x$

proof:
1. $x \geq 0$ and $y \geq 0$

- $|x| + |y| = x + y$, $|x + y| = x + y$
- $x + y \geq x + y$ ✓

2. $x < 0$ and $y < 0$
   - $|x| + |y| = -x - y$, $|x + y| = -x - y$
   - $-x - y \geq -x - y$ ✓
3. $x \geq 0$ and $y < 0$
   - if $x \geq |y|$, then $|x + y| = x - |y|$, $|x| + |u| = x + |y|$
     - $x + |y| \geq x - |y|$ ✓
   - if $x < |y|$, then $|x + y| = |y| - x$, $|x| + |y| = x + |y|$
     - $x + |y| \geq |y| - x$ ✓
4. symmetrical to case 3. ■

1.3 existence proof

an existence proof is a proof that demonstrates that an element with a certain property exists. there are two types of an existence proof: **constructive**, and **non-constructive**.

1.3.1 constructive existence proof

in a **constructive** existence proof, we prove the claim by finding and showing an actual example that satisfies the condition, similar to how existential generalization works.

1.3.1.1 example

theorem: there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$
the positive integer 1729 is the sum of both 10 and 9 cubed, as well as 12 and 1 cubed. ■

1.3.2 non-constructive existence proof

in an **non-constructive** existence proof, we prove that an element with the desired property is guaranteed to exist without actually finding a specific example; it often works by showing that one of several possibilities must be true, even if we don't know which one.

1.3.2.1 example

theorem: there exists two irrational numbers x and y such that x^y is rational.

proof: we know that $\sqrt{2}$ is irrational, so let $x, y = \sqrt{2}$.

cases:
1. if $\sqrt{2}^{\sqrt{2}}$ is rational, then we have completed the goal.
2. if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, which both are irrational. we now calculate $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2$, which is rational, completing the goal. ■

note: what makes this a non-constructive proof is that we don't necessarily know whether $\sqrt{2}^{\sqrt{2}}$ is irrational or rational. however, in either case, we can use it to construct a rational number.

1.4 uniqueness proofs

we use uniqueness proofs to show that not only the desired solution/element exists for the theorem, it is the only solution/element.

to prove the uniqueness of the solution:
1. provide an existence proof
2. show that any solution to the problem is equivalent to the solution generated in step 1.

1.4.1 example

theorem: let a and b be real numbers. there exists a unique real number r such that $a \cdot r + b = 0$.

proof:
- $r = -\frac{b}{a}$ is a solution to this equality since $-\frac{ab}{a} + b = -b + b = 0$. *(existence step)*
- assume that $as + b = 0$.
- then $a \cdot s = -b$, so $s = -\frac{b}{a}$, which means $s \equiv r$. *(uniqueness step)* ■