Proofs by Contradiction

CS 234

0 Introduction

This document contains examples of good proofs written up from the lecture material. These are not the only ways to write good proofs.

These proofs may contain footnotes explaining different thought processes that occurred in their construction, to help show you how to think about writing proofs. Commentary may also be provided at the end about alternative approaches.

1 Proofs

Maximality

Theorem 1. *There is no largest natural, i.e.,* $\neg\exists m \in \mathbb{N}. \forall n \in \mathbb{N}. m \geq n$

Proof. Suppose for the sake of contradiction that there is such a largest natural number m that is at least as big as every other natural. Then consider $m + 1$. This number is a natural number, as naturals are closed under addition, and $m + 1 > m$. This contradicts m being the largest natural number since $m + 1$ is larger, and thus the initial assumption is false and there is no largest natural number.

□

Irrationality

Theorem 2. *The square root of 2 is irrational, i.e.,* $\sqrt{2} \notin \mathbb{Q}$.

Proof. Suppose for the sake of contradiction that actually $\sqrt{2} \in \mathbb{Q}$. Then there must exist some integers p, q where $q \neq 0$ such that $\sqrt{2} = p/q$. Morover, since $\sqrt{2} > 0$, we can let p and q both themselves be greater than 0, so p and q are natural numbers at least 1.[1]

Now if $\sqrt{2} = p/q$, then squaring both sides and multiplying both sides by q^2 tells us $2q^2 = p^2$. Since p and q are both naturals, each of the expressions in the equality are both naturals, and so they have prime factorizations by the fundamental theorem of arithmetic. We now examine each side in more detail.

The right-hand side is p^2, and it has a unique prime factorization with some number of primes. In particular, if the prime factorization of p has m primes, then the prime factorization of p^2 has $2m$ primes since $p^2 = p \cdot p$, and each p contributes m primes from its prime factorization. By definition $2m$ is even.

The left-hand side is $2q^2$, and it has a unique prime factorization with some number of primes. In particular, if the prime factorization of q has n primes, then the prime factorization of $2q^2$ has $2n + 1$ primes since $2q^2 = 2 \cdot q \cdot q$, each q contributes n primes from its prime factorization, and the coefficient of 2 contributes itself as one more prime. By definition, $2n + 1$ is odd.

Supposing that $2q^2 = p^2$, the fundamental theorem of arithmetic tells us that each side should have the same unique prime factorization. However, the prime factorizations of each side cannot be the same, as one has an odd number of primes and one has an even number of primes. This is a contradiction.[2]

Since assuming $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction, we can conclude $\sqrt{2} \notin \mathbb{Q}$, completing the proof.

□

[1] If we wanted to be more explicit:

- The square root function never yields negative numbers by definition, so $\sqrt{2} \geq 0$.
- If $\sqrt{2} = 0$, then $2 = \sqrt{2}^2 = 0^2 = 0$ which is a contradiction, so $\sqrt{2} > 0$.
- If $p = 0$, then $p/q = 0$, but we already know that $\sqrt{2} > 0$
- If exactly 1 of p or q is negative, then $p/q < 0$, but we already know $\sqrt{2} > 0$.
- If both of p and q are negative, then picking their negations gives us the positive p and q we want.

[2] If we wanted to be explicit: $2m + 1 = 2n \rightarrow m + \frac{1}{2} = n$ for naturals m and n, but $m + \frac{1}{2}$ is clearly not a natural number, so it cannot be equal to the natural n.

Infinitude

Theorem 3. *There are infinitely many primes.*

Proof. Suppose instead that there are only finitely many primes.[3] Call this number of primes n, Clearly $n \geq 1$ since 2 is a prime.

Now let p_i represent the i^{th} of the finitely-many primes and consider the following number:

$$1 + \prod_{i=1}^{n} p_i$$

This number is a natural number, as naturals are closed under addition and multiplication. This number is also at least 1. Thus the fundamental theorem of arithmetic applies and it must have some prime factorization that is unique. Moreover, the prime factorization of the number cannot be empty, as $n \geq 1$ forces the number to be strictly greater than 1. Thus the factorization contains at least one prime number q.

Since q is prime, it must be in the finite list of primes. Suppose that q is the j^{th} prime in the list so that $q = p_j$. Then consider factoring out q from the number as follows:

$$\begin{aligned} \frac{1 + \prod_{i=1}^{n} p_i}{p_j} &= \frac{1 + \prod_{i=1}^{n} p_i}{q} && [q = p_j] \\ &= \frac{1}{p_j} + \prod_{i=1}^{j-1} p_i \prod_{i=j+1}^{n} p_i && [math] \end{aligned}$$

As the q is a factor of the number, this division should yield an integer. However, the resulting right-hand side is clearly not an integer because it is $\frac{1}{p_j}$ more than the integer $\prod_{i=1}^{j-1} p_i \prod_{i=j+1}^{n} p_i$, and $0 < \frac{1}{p_j} < 1$. This is a contradiction, so the original assumption must be false, and thus there are infinitely many primes.

□

[3] I have chosen to phrase my assumption for the sake of contradiction differently here. It is still just as fine.