CS30 (Discrete Math in CS), Summer 2021 : Lecture 5

Topic: Proofs via Contradiction

Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

- Proofs by contradiction is one of the most commonly used styles of proof. When faced with a proposition p (either in propositional logic, or predicate logic – often the latter) which we wish to prove true, we *suppose for the sake of contradiction* that p were false. Then we logically deduce something *absurd* (like $0 = 1$ or 3 is even), that is, something which we know to be false. This implies that our supposition (which is, p is false) must be wrong. Therefore, the proposition p must be true. This method of proving is also called *reductio ad absurdum* — reduction to absurdity.

- Formally, in the jargon of logic, what the above argument captures is the fact that the following formula
$$(\neg p \Rightarrow \mathsf{false}) \Rightarrow p$$
is a *tautology*. Can you deduce this from the equivalences?

- A final word before we move on to concrete examples. Many times the false is obtained by showing that some other proposition q holds as well as its negation. That is, we end up showing $(\neg p \Rightarrow (q \wedge \neg q))$. Interestingly, sometimes this proposition is p itself.

  Just for this lecture, we write down our argument's steps in an itemized list so as to make sure all ideas are clear.

- **A Simple Warm-up.**

  Lemma 1. For all numbers n, if n^2 is even, then n is even.

  Proof.

  1. Suppose, for the sake of contradiction, the proposition is *not true*.
  2. That is, there exists a number n such that (a) n^2 is even **and** (b) n is not even. That is, n is odd. *Figuring out what the negation means is the first step.*
  3. Since n is odd, $n = 2k + 1$ for some integer k.
  4. This implies $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
  5. That is, n^2 is odd. This is a contradiction to (a) n^2 is even.
  6. Therefore, our supposition must be wrong, that is, the proposition is true. □

  Exercise: *Mimic the above proof to prove: For any number n, if n^2 is divisible by 3, then n is divisible by 3.*

Exercise: *Prove by contradiction: the product of a* non-zero *rational number and an irrational number is irrational.*

- **A Pythogorean[1] Theorem.**

Theorem 1. $\sqrt{2}$ is irrational.

Proof.

1. Suppose, for the sake of contradiction, that $\sqrt{2}$ is indeed rational.
2. Since $\sqrt{2}$ is rational, there exists two integers a, b such that $\sqrt{2} = a/b$.
3. By dividing out common factors, we may assume $\gcd(a, b) = 1$.
4. Since $a/b = \sqrt{2}$, we get $a = \sqrt{2} \cdot b$. Squaring both sides, we get $a^2 = 2b^2$.
5. Therefore a^2 is even.
6. Lemma 1 implies that a is even. And therefore $a = 2\ell$ for some ℓ.
7. Therefore, $a^2 = 4\ell$.
8. Since $a^2 = 2b^2$, we get $4\ell = 2b^2$, which in turn implies $b^2 = 2k$. That is, b^2 is even.
9. Lemma 1 implies that b is even.
10. Thus, we have deduced both a and b are even. This **contradicts** $\gcd(a, b) = 1$.
11. Therefore, our supposition that $\sqrt{2}$ is rational must be wrong. That is, $\sqrt{2}$ is irrational. □

Exercise: *Mimic the above proof to prove that* $\sqrt{3}$ *is irrational.*

- **A Euclidean Theorem.** Here is another classic example of Proof by Contradiction.

Theorem 2. There are infinitely many primes.

Proof.

1. Suppose, for the sake of contradiction, there were only finitely many primes.
2. Let q be the largest of these primes.
   Do you see how "finiteness" makes this statement well-defined? This is the only place the "finiteness" will be used.
3. Therefore, for any number $n > q$, n is *not* a prime.
4. Consider the number $n = q! + 1$. Recall, $q! = 1 \times 2 \times \cdots \times q$.
5. Since $n > q$, this n is not a prime.
6. Therefore, there exists some prime p such that $p \mid n$. (This is notation for saying "p divides n")

[1]This is of course not the famous Pythogorean theorem on right angled triangles, but nonetheless a Pythogorean may be the first to have proved it. See https://en.wikipedia.org/wiki/Irrational_number, for instance.

7. Since q is the largest prime, $p \leq q$.
8. But this means $p \mid q!$, which means $p \nmid q! + 1$. That is, $p \nmid n$.
9. We have deduced both $p \mid n$ and $p \nmid n$. Contradiction. Thus our supposition is wrong. There are infinitely many primes. □

- **The AM-GM inequality**

> **Theorem 3.** If a and b are two positive real numbers, then $a + b \geq 2\sqrt{ab}$.

Proof.

1. Suppose, for the sake of contradiction, that there exists positive reals a, b with $a + b < 2\sqrt{ab}$.
2. Since both sides of the above inequality are positive, we can square both sides. That is, $(a+b)^2 < \left(2\sqrt{ab}\right)^2$.
   Please note how crucial the fact that both sides were positive is. Otherwise, we cannot square and maintain the inequality. And indeed, the theorem is incorrect for negative numbers. Consider $a = -1$ and $b = -1$. The RHS is 2 but the LHS is -2.
3. That is, $a^2 + 2ab + b^2 < 4ab$.
4. That is, $a^2 - 2ab + b^2 < 0$.
5. That is, $(a - b)^2 < 0$.
6. But $(a - b)^2 \geq 0$, since it is a square. Thus, we have reached a contradiction. □

Answers to some exercises

- **Exercise:** *Mimic the above proof to prove: For any number n, if n^2 is divisible by 3, then n is divisible by 3.*

1. Suppose, for the sake of contradiction, the proposition is *not true*.
2. That is, there exists a number n such that (a) n^2 is divisible by three **and** (b) n is not divisible by 3.
3. Since n is not divisible by 3, $n = 3k + r$ for some integer k and integer $r \in 1, 2$. This r is the *remainder* when n is divided by 3.
4. This implies $n^2 = (3k + r)^2 = 9k^2 + 6kr + r^2 = 3(3k^2 + 2kr) + r^2$.
5. When $r = 1$, $r^2 = 1$. Thus, $n^2 = 3(3k^2 + 2kr) + 1$ implying if we divide n^2 by 3, we will get remainder 1. This contradicts the fact that n^2 is divisible by 3.
6. When $r = 1$, $r^2 = 4$. Thus, $n^2 = 3(3k^2 + 2kr) + 4 = n^2 = 3(3k^2 + 2kr + 1) + 1$ implying if we divide n^2 by 3, we will get remainder 1. This contradicts the fact that n^2 is divisible by 3.
7. In **either case**, we get a contradiction to (a) n^2 is divisible by 3.
8. Therefore, our supposition must be wrong, that is, the proposition is true.

- **Exercise:** *Prove by contradiction: the product of a* non-zero *rational number and an irrational number is irrational.*

1. Suppose, for the sake of contradiction, the proposition is *not true*.
2. That is, there exists a non-zero rational number r and an irrational number a such that the product $r \cdot a$ is a *rational number* b.
3. Since r is rational and non-zero, $r = p/q$ where p and q are two integers, neither of which are 0.
4. Since b is irrational, $b = m/n$ where m and n are two integers and n is non-zero.
5. Thus, we get
$$\frac{p}{q} \cdot a = \frac{m}{n} \quad \underbrace{\Rightarrow}_{\text{rearranging}} \quad a = \frac{qm}{pn}$$
6. Since product of integers are integers, we get that a is a ratio of two integers $A = qm$ and $B = pn$, and $B \neq 0$ since p and n are both non-zero. That is, a is rational.
7. But this contradicts the irrationality of a.
8. Therefore, our supposition must be wrong, that is, the proposition is true.

- **Exercise:** *Mimic the above proof to prove that $\sqrt{3}$ is irrational.*

1. Suppose, for the sake of contradiction, that $\sqrt{3}$ is indeed rational.
2. Since $\sqrt{3}$ is rational, there exists two integers a, b such that $\sqrt{3} = a/b$.
3. By dividing out common factors, we may assume $\gcd(a, b) = 1$.
4. Since $a/b = \sqrt{3}$, we get $a = \sqrt{3} \cdot b$. Squaring both sides, we get $a^2 = 3b^2$.
5. Therefore a^2 is divisible by 3.

6. The exercise after Lemma 1 implies that a is divisible by 3. And therefore $a = 3\ell$ for some ℓ.
7. Therefore, $a^2 = 9\ell$.
8. Since $a^2 = 3b^2$, we get $9\ell = 3b^2$, which in turn implies $b^2 = 3k$. That is, b^2 is divisible by 3.
9. Once again, the exercise after Lemma 1 implies that b is divisible by 3.
10. Thus, we have deduced both a and b are divisible by 3. This **contradicts** $\gcd(a, b) = 1$.
11. Therefore, our supposition that $\sqrt{3}$ is rational must be wrong. That is, $\sqrt{3}$ is irrational.

Remark: *How far can you generalize? Can you prove that* $\sqrt{n}$ *is irrational if* n *is not a* perfect square*, that is,* n *is not* a^2 *for some integer* a*?*