Statements, Proofs, and Contradiction

Robert Y. Lewis

CS 0220 2022

January 28, 2022

Overview

What's a proposition?

Definition. A proposition is a statement that is either true or false.

- Proposition 1: $2 + 3 = 5$.
- Proposition 2: $1 + 1 = 3$.
- Proposition 3: The sum of any two odd numbers is even.
- Proposition 4: The product of any two odd numbers is even.

We'll stick with mathematical propositions in this class.

- Not-a-Proposition 1: Rob has a beautiful singing voice.
- Not-a-Proposition 2: Every action has an equal but opposite reaction.
- Not-a-proposition 3: How many students are in this class?

How can we tell if a proposition is true?

Definition: A *perfect square* is a number that can be written n^2 for some integer n.

- Proposition 5: There is a two-digit perfect square whose final digit is 4.
  True. An example is $8^2 = 64$.
- Proposition 6: There is a two-digit perfect square whose final digit is 8.
  False. I can't show you an example, because there is no such example.
  I could list *all* the two digit perfect squares, though: 16, 25, 36, 49, 64, 81. All other perfect squares are either shorter or longer. None end in 8.

Proposition about numbers

Definition: A *perfect square* is a number that can be written n^2 for some integer n.

- Proposition 7: There is perfect square whose final digit is 4.
  True. We showed it for two-digit perfect squares, so that's still true when we broaden the set of possibilities.
- Proposition 8: There is a perfect square whose final digit is 8.
  False. The approach of exhaustively listing the possibilities to show it is false doesn't work this time. We'll need another technique.

Final digits of perfect squares

Define $p(n) ::= n^2 \mod 10$, the remainder we get if we take n, square it, and divide by 10. It's the last digit of the square.

$p(0) = 0$
$p(1) = 1$
$p(2) = 4$
$p(3) = 9$
$p(4) = 6$
$p(5) = 5$
$p(6) = 6$
$p(7) = 9$
$p(8) = 4$
$p(9) = 1$
$p(10) = 0$
$p(11) = 1$
repeating? (Save for later.)

Is this proposition true?

Definition: A *prime* is an integer greater than one that is not divisible by any other integer greater than 1.

Example: 2, 3, 5, 7, 11, 13, 17, ...

- Proposition 9: For every nonnegative integer, n, the value of $n^2 + n + 41$ is prime.

  Define $p(n) ::= n^2 + n + 41$.
  $p(0) = 41$, which is prime.
  $p(1) = 43$, which is prime.
  $p(2) = 47$, which is prime.
  ...
  $p(10) = 151$, which is prime.
  Looking good!
  $p(40) = 1681 = 41^2$, not prime. So, no. Counterexample. Short proof (but hard to find).

Aside

The book says: There is no non-constant polynomial $p(n)$ with nonnegative integer coefficients that generates only primes.

Suppose there were such a polynomial p.
Let m be the constant coefficient of p (that's not multiplied by a power of n). Since $m = p(0)$ and $p(0)$ is prime, m must be prime. In particular it can't be 0 or 1.
Now, consider $p(m)$. All of the terms of $p(m)$ are divisible by m, so $p(m)$ is as well. Since the polynomial is not constant, and coefficients are nonnegative, $p(m) > m$. So $p(m)$ is divisible by a number other than 1 or itself, so it is not prime: a contradiction.

For our example $p(n) ::= n^2 + n + 41$, $p(41) = 1763 = 43 \times 41$.

Some useful notation

- $\mathbb{Z}$ is the integers $\{\ldots, -4, -3, -2, 1, 0, 1, 2, 3, 4, \ldots\}$.
- $\mathbb{Z}^+$ is the positive integers $\{1, 2, 3, 4, \ldots\}$.
- $\mathbb{N}$ is the non-negative integers $\{0, 1, 2, 3, 4, \ldots\}$.
- $\forall$ means "for all." It's an upside down A.
- $\exists$ means "exists." It's a backwards E. (Or is it?)
- Examples:
  $\exists n : \mathbb{N}, n^2 \bmod 10 = 6$.
  Can show exists is true with an example ($n = 6$).
  $\forall n : \mathbb{N}, n^2 + n + 41$ is prime.
  Can show forall is false with a counterexample ($n = 40$).

Sometimes we write these as $\exists n \in \mathbb{N}$ and $\forall n \in \mathbb{N}$.

Toughies

- Proposition 10 (Euler's conjecture): $a^4 + b^4 + c^4 = d^4$ has no solution when a, b, c, and d are positive integers.
  $\forall a : \mathbb{Z}^+, \forall b : \mathbb{Z}^+, \forall c : \mathbb{Z}^+, \forall d\ \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4$.
  $\forall a\ b\ c\ d : \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4$.
  No! $a = 95800$, $b = 217519$, $c = 414560$, $d = 422481$. (Took 200+ years to resolve.)
- Proposition 11: $313(x^3 + y^3) = z^3$ has no solution when $x, y, z \in \mathbb{Z}^+$.
  Also, no; but, shortest counterexample is 1000+ digits long.
- Proposition 12: Every map can be colored with 4 colors so that adjacent regions have different colors.
  Yes, and the proof is very very long.
- Proposition 13 (Goldbach's conjecture): Every even integer greater than 2 is the sum of two primes.
  Remains unresolved since 1742.

Who decides "truth"?

- We defined “prime number”
  - And “integer,” and “divisible,” and “1,” ...
- The goal of mathematics is “common knowledge”: give anyone the definitions, and a proof or counterexample, and they can check it. Even a computer could do it.
- This is why we’re focusing on *mathematical* propositions here. Truth in the real world is a little complicated.

What's a Predicate?

A *predicate* is a proposition whose truth depends on the value of one or more variables.

Examples:

- n is odd.
  True for $n = 25$, false for $n = 98$.
- The sum of two numbers a and b is prime.
  True for $a = 3$ and $b = 4$. False for $a = 4$ and $b = 6$.
- x is an integer and $2x$ is even.
  True for all integers x.

Predicates to propositions

Predicate notation:
$P(n) ::=$ "n is a perfect square".

$P(16)$ is true and $P(10)$ is false.

If $P(n)$ is a predicate, then:

- $P(22)$ is a proposition.
- $\forall n, P(n)$ is a proposition.
- $\exists n, P(n)$ is a proposition.
- $P(n+1)$ is a predicate.
- $P(n) + 1$ is a type error.

Idea

We'll talk more about proof next week. But if there's time today, something to mull over for the weekend...

Proof by contradiction is also called an "indirect" proof. Some mathematicians find them distasteful. It's a matter of style, and what rules of logic we accept.

Method: To prove a proposition P by contradiction:

1. Write, "We prove P by contradiction."
2. Write, "Suppose P is false."
3. Deduce some proposition Q known to be false (a logical contradiction).
4. Write, "Since Q is false, we've reached a contradiction. Therefore, P must be true."

Example proof by contradiction

Proposition: $\sqrt{2}$ is irrational.

We prove that $\sqrt{2}$ is irrational by contradiction. Suppose $\sqrt{2}$ is rational. By the definition of "rational", that means $\sqrt{2} = p/q$ where p and q are integers. Furthermore, we can choose p and q to be in lowest terms so they have no factors in common. Squaring both sides, we get $2 = p^2/q^2$ or $2q^2 = p^2$. Since q^2 is an integer, and p^2 is an integer times 2, p^2 is even. By a similar argument to the one for odd squares, that means p must be even. If p is even, p^2 must be divisible by 4. Since $2q^2$ is divisible by 4, q^2 must be divisible by 2 (the other factor of two must be there). That means both p and q are even. But, then p/q is not in lowest terms. Since we already asserted that p/q is in lowest terms when p and q were chosen, we've reached a contradiction. Therefore, $\sqrt{2}$ must be irrational.

Why does this argument make sense?

We live in a world where things make sense. (...)

In our sensible world, some statements are true and some are false. But none are true *and* false.

Our argument goes like this. “Pretend *A* happens in our world. For reasons we explain, *B* must happen too. But, for other reasons, we know that *B doesn’t* happen! Our pretend world doesn’t make sense. So *A* must not happen.”

It’s dry outside today. Proof: suppose it weren’t dry. Whenever it rains or snows, I wear my boots. But today I’m wearing my nice shoes. This fantasy world doesn’t make sense.