Statements, Proofs, and Contradiction

Michael L. Littman

CS 22 2020

January 24, 2020

Overview

Propositions (1.1)

Predicates (1.2)

Proof by Contradiction (1.8)

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: This class is better than CS 33.
- Not-a-Proposition 2: Every action has an equal but opposite reaction.

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.
  Yes.
  An example is $8^2 = 64$.
- Proposition 6: There is a two-digit perfect square whose final digit is 8.
  No.
  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.
  Yes.
  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.
  No.
  The approach of exhaustively listing the possibilities to show "no" doesn't work this time. We'll need another technique.

Final digits of perfect squares

Define $p(n) ::= n^2 \bmod 10$, 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?

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 polynomial $p(n)$ with integer coefficients that generates only primes.

Let m be coefficient that's not multiplied by a power of n. We know m is prime because otherwise $p(0)$ wouldn't be. Now, consider $p(m)$. All of the terms of $p(m)$ are divisible by m, so $p(m)$ is as well. Therefore, $p(m)$ is not prime.

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 an upside down E. Don't let anyone tell you otherwise.
- Examples:
  $\exists n \in \mathbb{N}, n^2 \bmod 10 = 6$.
  Can show "yes" with an example ($n = 6$).
  $\forall n \in \mathbb{N}, n^2 + n + 41$ is prime.
  Can show "no" with a counterexample ($n = 40$).

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.
  $\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \forall d \in \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4$.
  $\forall a, b, c, d \in \mathbb{Z}^+, a^4 + b^4 + c^4 \neq d^4$.
  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.

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 consecutive numbers a and b is prime.
  True for $a = 3$ and $b = 4$. False for $a = 4$ and $b = 5$.
- 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

Also called an "indirect" proof. Some mathematicians find them distasteful. Some people don't like to even split infinitives. It's a matter of style.

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 our earlier argument, 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. 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?

The basic idea is that if *any time* A happens then B must happen *and* we know B didn't happen, well, then A couldn't have happened either. After all, if A *had* happened, it would have made B happen. But, B didn't happen, so A couldn't have happened.

If you give a mouse a cookie, he's going to ask for a glass of milk. You will give him the milk, and he's going to ask you for a straw. When he's finished, he'll ask you for a napkin. Then, he'll want to look in a mirror to make sure he doesn't have a milk mustache.

I note that the mouse didn't look in the mirror. Therefore, you must not have given him a cookie.