Mathematics for Computer Science

MIT 6.042J/18.062J

Truth and Proof

Math vs. Reality

Propositional Logic

Proof by Cases

Evidence vs. Proof

Let $p(n) ::= n^2 + n + 41.$

Claim:

$\forall n \in \mathbb{N} \quad p(n)$ is a prime number

Only Prime Numbers?

Evidence:

$p(0) = 41$ prime

$p(1) = 43$ prime

$p(2) = 47$ prime

$p(3) = 53$ prime

$\vdots$

$p(20) = 461$ prime **looking good!**

$\vdots$

$p(39) = 1601$ prime **enough already!**

Only Prime Numbers?

$\forall n \in \mathbb{N} \quad p(n) ::= n^2 + n + 41$ is a prime number

This can't be a coincidence.
The hypothesis must be true.

BUT IT'S NOT:

$p(40) = 1681$ is NOT PRIME.

Only Prime Numbers?

Quickie:
Prove that 1601 is prime,
and 1681 is not prime.

Evidence vs. Proof: Deep Example

EULER'S CONJECTURE (1769)

$$a^4 + b^4 + c^4 = d^4$$

has no solution for a, b, c, d positive integers:

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \forall d \in \mathbb{Z}^+$$

$$a^4 + b^4 + c^4 \neq d^4$$

Evidence vs. Proof: Deep Example

Counterexample: 218 years later by Noam Elkies at Liberal Arts school up Mass Ave:

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

```
(= (+ (expt 95800  4)
      (expt 217519 4)
      (expt 414560 4))
   (expt 422481 4))
;Value: #t
```


Further Extreme Example

Hypothesis:

$$313 \cdot (x^3 + y^3) = z^3$$

has no positive integer solution.

False. But smallest counterexample has MORE THAN 1000 digits!

Evidence vs. Proof

Claim: All odd numbers greater than 1 are prime.

MATHEMATICIAN: 3 is prime, 5 is prime, 7 is prime, but $9 = 3 \times 3$ is not prime, so the proposition is false!

Evidence vs. Proof

Claim: All odd numbers greater than 1 are prime.

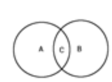
PHYSICIST: 3 is prime, 5 is prime, 7 is prime, 9 is ***not*** prime, but 11 is prime, 13 is prime. So 9 must be experimental error; the proposition is true!

Evidence vs. Proof

Claim: All odd numbers greater than 1 are prime.

LAWYER: Ladies and Gentleman of the jury, it is beyond all reasonable doubt that odd numbers are prime. The evidence is clear: 3 is prime, 5 is prime, 7 is prime, 9 is prime, 11 is prime, and so on.

Math



Sets

Numbers $\sqrt{7}, \pi, i+1$

T, F Booleans

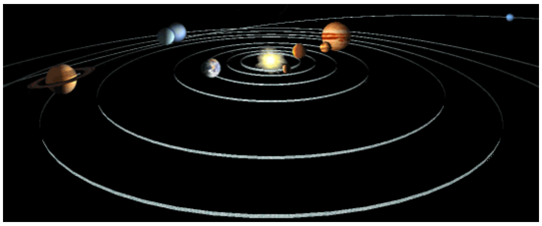
Strings $"a \wedge b"$

$f(x) = x^2 + 2$ Functions

Relations $a \leq b$

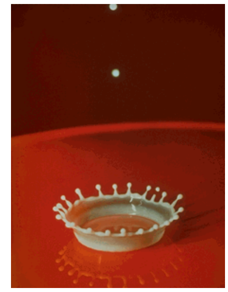
$\vec{F} = m \cdot \vec{a}$ Vectors

Not Math



Solar System

Not Math



Physical Motion

Not Math

Family

Not Math

Cats

Not Math: Cogito ergo sum

René Descartes'

MEDITATIONS

on First Philosophy in which the Existence of God and the Distinction Between Mind and Body are Demonstrated.

(Picture source: http://www.btinternet.com/~glynhughes/squashed/descartes.htm)

Propositional (Boolean) Logic

Proposition is either **True** or **False**

Examples: $2+2=4$ True

$1\times 1=4$ False

Non-examples: Wake up!

Where am I?

Operators

$\wedge$ ::= AND

$\vee$ ::= OR

$\neg$ ::= NOT

$\rightarrow$ ::= IMPLIES

$\leftrightarrow$ ::= IFF (if and only if)

Proof by calculation: Truth Tables

DeMorgan's law

$\neg(p \vee q)$ is *equivalent* to $\overline{p} \wedge \overline{q}$

p	q	$\neg$	$(p \vee q)$
T	T	F	T
T	F	F	T
F	T	F	T
F	F	T	F

$\overline{p}$	$\overline{q}$	$\overline{p} \wedge \overline{q}$
F	F	F
F	T	F
T	F	F
T	T	T

Proof by Deductions

A student is trying to prove that propositions *P*, *Q*, and *R* are all true. She proceeds as follows.
First, she proves three facts:

- *P* implies *Q*
- Q implies *R*
- *R* implies *P*.

Then she concludes,
``Thus *P*, *Q*, and *R* are obviously all true."

Deductions

From: *P* implies *Q*, *Q* implies *R*, *R* implies *P*
Conclude: *P*, *Q*, and *R* are true.

Antecedents

$$\frac{(P \rightarrow Q),\ (Q \rightarrow R),\ (R \rightarrow P)}{P \wedge Q \wedge R}$$

Conclusion

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$r \rightarrow p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	
T	T	F	T	F	T	F	
T	F	T	F	T	T	F	
T	F	F	F	T	T	F	
F	T	T	T	T	F	F	
F	T	F	T	F	T	F	
F	F	T	T	T	F	F	
F	F	F	T	T	T	F	

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$r \rightarrow p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	
T	T	F	T	F	T	F	
T	F	T	F	T	T	F	
T	F	F	F	T	T	F	
F	T	T	T	T	F	F	
F	T	F	T	F	T	F	
F	F	T	T	T	F	F	
F	F	F	T	T	T	F	

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \to q$	$q \to r$	$r \to p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	
T	T	F	T	F	T	F	OK
T	F	T	F	T	T	F	OK
T	F	F	F	T	T	F	OK
F	T	T	T	T	F	F	OK
F	T	F	T	F	T	F	OK
F	F	T	T	T	F	F	OK
F	F	F	T	T	T	F	

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \to q$	$q \to r$	$r \to p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	OK
T	T	F	T	F	T	F	OK
T	F	T	F	T	T	F	OK
T	F	F	F	T	T	F	OK
F	T	T	T	T	F	F	OK
F	T	F	T	F	T	F	OK
F	F	T	T	T	F	F	OK
F	F	F	T	T	T	F	

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \to q$	$q \to r$	$r \to p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	OK
T	T	F	T	F	T	F	OK
T	F	T	F	T	T	F	OK
T	F	F	F	T	T	F	OK
F	T	T	T	T	F	F	OK
F	T	F	T	F	T	F	OK
F	F	T	T	T	F	F	OK
F	F	F	T	T	T	F	

Good (*Sound*) Rule

The conclusion is true whenever all the antecedents are true. Could check with Truth Table:

p	q	r	$p \to q$	$q \to r$	$r \to p$	$p \wedge q \wedge r$	sound?
T	T	T	T	T	T	T	OK
T	T	F	T	F	T	F	OK
T	F	T	F	T	T	F	OK
T	F	F	F	T	T	F	OK
F	T	T	T	T	F	F	OK
F	T	F	T	F	T	F	OK
F	F	T	T	T	F	F	OK
F	F	F	T	T	T	F	NOT OK!

Problems

Class Problem 1

Goldbach Conjecture

Every even integer greater than 2 is the sum of two primes.

Evidence:

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 5 + 3$$
$$\vdots$$
$$20 = ? \quad 13 + 7$$

Goldbach Conjecture

True for all even numbers with up to 13 digits! (Rosen, p.182)

It remains an OPEN problem: no counterexample, no proof.

UNTIL NOW!…

Goldbach Conjecture

The answer is on my desk!

(Proof by Cases)

Quicker by Cases

$$\frac{P \to Q,\ Q \to R,\ R \to P}{P \wedge Q \wedge R}$$

Case 1: P is true. Now, if antecedents are true, then Q must be true (because P implies Q). Then R must be true (because Q implies R). So the conclusion $P \wedge Q \wedge R$ is true.

This case is OK.

Quicker by Cases

$$\frac{P \to Q,\ Q \to R,\ R \to P}{P \wedge Q \wedge R}$$

Case 2: P is false. To make antecedents true, R must be false (because R implies P), so Q must be false (because Q implies R). This assignment does make the antecedents true, but the conclusion $P \wedge Q \wedge R$ is (very) False.

This case is not OK.

Problems

Class Problem 2