ANNOUNCEMENTS

- Homework 3 is out on Canvas:
  - Due date: May 25 (midnight) on Canvas
    - Should be submitted as a pdf file
- Quiz 7: This thursday, last 10 minutes of class.
  - Material: "Logic-Philosophical Wars" chapter from Logicomix and lectures on 5/14 and 5/19
- Exam 2: June 2. Canvas quiz during class time. Covering all month of May.

LAST CLASS: DIRECT PROOFS $P \rightarrow Q$ EQUIVALENTLY $P \vdash Q$

- *While* $p \rightarrow q$ *or* $p \vdash q$ are different in our formal proofs:
  - $p \rightarrow q$ *is a proposition*
  - $p \vdash q$. *says that q can be "proved" assuming p is a premise*
- In the proofs starting on Chapter 4 of ZyBooks the above are technically the same and in questions in and after chapter 4 we can use them interchangeably.

LAST CLASS: DIRECT PROOFS

$P \rightarrow Q \ OR \ P \vdash \ Q$

- Step 1:
  - Write down premises (hypothesis) i.e., p
- Step 2:
  - Use definitions to express premises/hypothesis P in mathematical terms
- Step 3:
  - Use definitions to express the conclusion Q in mathematical terms (what we want to prove)
- Step 4
  - Use algebra/previous results/etc. to arrive at the mathematical expression for Q.

INDIRECT PROOFS

- Proof by contraposition
- Proof by contradiction

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.

$\neg Q \rightarrow \neg P$ IS THE SAME AS $P \rightarrow Q$

- Two propositions are *equivalent* if they always have the same truth value.

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

CONTRAPOSITIVE PROOF OF $P \rightarrow Q$ I.E., DIRECT PROOF OF $\neg Q \rightarrow \neg P$

- Step 1:
  - Write down premises (hypothesis) i.e., $\neg Q$
- Step 2:
  - Use definitions to express premises/hypothesis $\neg Q$ in mathematical terms
- Step 3:
  - Use definitions to express the conclusion $\neg P$ in mathematical terms (what we want to prove)
- Step 4
  - Use algebra/previous results/etc. to arrive at the mathematical expression for $\neg P$.

PROOF BY CONTRAPOSITION: $P \to Q$ I.E. PROVING $\neg Q \to \neg P$

- *Proof by Contraposition*: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \to \neg p$ then we have a proof of $p \to q$.

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Thus

$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$

Therefore $3n + 2$ is even. Since we have shown $\neg q \to \neg p$, $p \to q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even).

◀

PROVING BY CONTRAPOSITION: $P \to Q$ I.E. PROVING $\neg Q \to \neg P$

Example: Prove that for an integer n, if n^2 is odd, then n is odd.

Solution: Use proof by contraposition. Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,

$$n^2 = 4k^2 = 2\,(2k^2)$$

and n^2 is even(i.e., not odd).

We have shown that if n is an even integer, then n^2 is even. Therefore by contraposition, for an integer n, if n^2 is odd, then n is odd.

◀

PROOFS BY CONTRAPOSITIVE WITH MULTIPLE PREMISES

- Suppose we want to prove:
  If H_1 and H_2 are both true then C is true.
- The contrapositive of this conditional statement is:
- If C is false, then it cannot be the case that H_1 and H_2 are both true.
- By De Morgan's law, the statement is equivalent to:
- If C is false, then H_1 is false or H_2 is false.
- which is in turn equivalent to:
- If C is false and H_1 is true, then H_2 is false.

WHY DOES THE PREVIOUS STEP WORK?

- This truth table shows that $\neg p \vee q$ is equivalent to $p \rightarrow q$.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

- *So*

$$
\begin{aligned}
p \wedge q \rightarrow r &\equiv \\
\neg r \rightarrow \neg p \vee \neg q &\equiv \\
\neg\neg r \vee \neg p \vee \neg q &\equiv \\
\neg(\neg r \wedge p) \vee \neg q &\equiv \\
\neg r \wedge p \rightarrow \neg q &
\end{aligned}
$$

ZyBook 4.5.7

INDIRECT PROOFS

- Proof by contraposition
- Proof by contradiction

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.

PROOF BY CONTRADICTION

Meta – Theorem Let Γ be a set of premises

$$\Gamma, \neg\alpha \vdash \beta, \neg\beta \implies \Gamma \vdash \alpha$$

Meta – Corollary

$$(a)\Gamma, \alpha \vdash \beta, \neg\beta \implies \Gamma \vdash \neg\alpha$$

$$(b)\Gamma, \neg\alpha \vdash \alpha \implies \Gamma \vdash \alpha$$

PROVING BY CONTRADICTION: $P \to Q$ (I.E. $P \vdash Q$)

- *Proof by Contradiction*: (AKA *reductio ad absurdum*).

To prove q, assume $\neg q$ and derive a contradiction such as $q \wedge \neg q$. (an indirect form of proof).

Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week. Because there are 7 days of the week, we could only have picked 21 days. This contradicts the assumption that we have picked 22 days.

◀

PRACTICING VARIOUS METHODS

- Prove that if a is even and b is even, then a+b is even:
  - Direct proof
  - Proof by contrapositive
  - Proof by contradiction

- Document camera

ZyBooks 4.6

PROOF BY CONTRADICTION THEOREM 4.6.1 (ZYBOOKS)

Example: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors. Then

$$2 = \frac{a^2}{b^2} \qquad\qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (previously proven). Since a is even, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2 \qquad\qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational ◀

THERE ARE INFINITE PRIMES (EUCLID 300BC)

- **theorem**: There are infinitely many primes

  Solution: Assume by contradiction that there is a largest prime number. Call it p_n. Hence, we can list all the primes $2,3,..,p_n$. Form

$$r = p_1 \times p_2 \times \ldots \times p_n + 1$$

- r is larger than the largest prime and therefore it should not be a prime number (it should be composite)

Let q be a prime dividing r, q also divides $p_1 p_{2,} .. p_n$

It should also divide r- $p_1 p_{2,} .. p_n = 1$ but this is impossible

PROVING THEOREMS THAT ARE BICONDITIONAL STATEMENTS $P \leftrightarrow Q$

- **Example**: An integer x is even if and only if x^2 is even.

  Solution: The quantified assertion is

  $\forall x$ [x is even $\leftrightarrow x^2$ is even]

  We assume x is arbitrary.

  Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

  So, we have to prove the assertion both ways. These are considered in turn.

Continued on next slide →

THEOREMS THAT ARE BICONDITIONAL STATEMENTS $P \leftrightarrow Q$

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \to q$ and $q \to p$ are both true.

Example: Prove the theorem: "given n is an integer, n is even if and only if n^2 is even."

Sometimes *iff* is used as an abbreviation for "if an only if," as in

"n is even iif n^2 is even."

PROVE ONE DIRECTION $P \rightarrow Q$

→. We show that if x is even then x^2 *is* even using a direct proof (the *only if*).

If x is even then $x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 *on next slide* →

PROVE THE OTHER DIRECTION $Q \to P$

We show that if x^2 is even then x must be even (the *if* part). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2\text{k}) + 1$

which is odd and hence not even. This completes the proof of case 2.

Since x was arbitrary, the result follows by UG.

Therefore we have shown that x is even if and only if x^2 is even. ◀

PROOF BY CASES: SOMETIMES P CAN BE DIVIDED IN DIFFERENT PARTS

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

- Use the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- Each of the implications $p_i \rightarrow q$ is a *case*.

ZyBook 4.7

PROOF BY CASES

Example: Let a @ b = max{a, b} = a if $a \geq b$, otherwise a @ b = max{a, b} = b.

Show that for all real numbers a, b, c

(a @b) @ c = a @ (b @ c)

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

PROOF BY CASES

Case 1: $a \geq b \geq c$

(a @ b) = a, a @ c = a, b @ c = b

Hence (a @ b) @ c = a = a @ (b @ c)

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

WITHOUT LOSS OF GENERALITY

Example: Show that if x and y are integers and both $x{\cdot}y$ *and* $x{+}y$ are even, then both x and y are even.

Proof: Use a proof by contraposition. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m.

Case 1: y is even. Then $y = 2n$ for some integer n, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so $x \cdot y = (2m + 1)\,(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.

We only cover the case where x is odd because the case where y is odd is similar. The use phrase *without loss of generality* (WLOG) indicates this.

ZyBook Proof 4.7.3

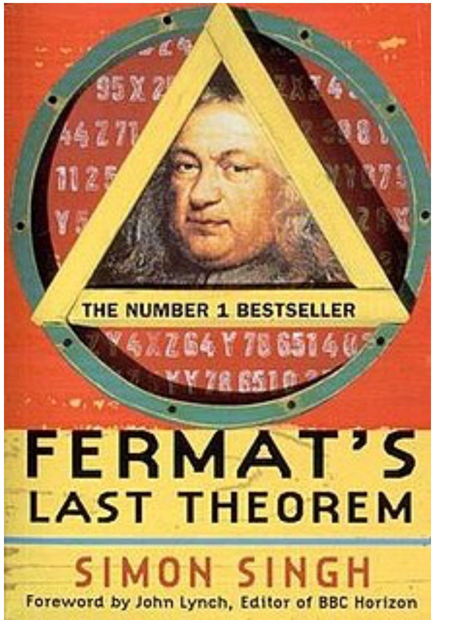
THE ROLE OF OPEN PROBLEMS

- Unsolved problems have motivated much work in mathematics. Fermat's Last Theorem was conjectured more than 300 years ago. It has only recently been finally solved.

  Fermat's Last Theorem: The equation $x^n + y^n = z^n$

  has no solutions in integers x, y, and z, with $xyz \neq 0$ whenever n is an integer with $n > 2$.

A proof was found by Andrew Wiles in the 1990s.



AN OPEN PROBLEM

- **The $3x + 1$ Conjecture**: Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$. For all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1.

For example, starting with $x = 13$:

$\mathbf{T}(13) = 3{\cdot}13 + 1 = 40$, $\mathbf{T}(40) = 40/2 = 20$, $\mathbf{T}(20) = 20/2 = 10$,

$\mathbf{T}(10) = 10/2 = 5$, $\mathbf{T}(5) = 3{\cdot}5 + 1 = 16$, $\mathbf{T}(16) = 16/2 = 8$,

$\mathbf{T}(8) = 8/2 = 4$, $\mathbf{T}(4) = 4/2 = 2$, $\mathbf{T}(2) = 2/2 = 1$

The conjecture has been verified using computers up to $5.6 \cdot 10^{13}$.

Other famous Examples, Hillbert Problems (as seen in Logicomix);
e.g. the Riemann hypothesis
https://en.wikipedia.org/wiki/Hilbert%27s_problems