What’s on today’s menu?

- Wrap up of Proof Techniques
- Review of Chapter 1
- Introduction to Sets

Existence Proofs

- Goal: Prove $\exists x \, P(x)$
- Two ways:
  - 1st way: Constructive proof
  - 2nd way: Destructive proof
  - 2nd way: Non-constructive proof
Constructive Existence Proof

Goal: Prove $\exists x \ P(x)$

**Constructive proof method:** Construct an $a$ such that $P(a)$ is true.

Example: Prove that there exist nonzero integers $x, y, z$ such that $x^2 + y^2 = z^2$.

Proof: Let $x = 3, \ y = 4, \ z = 5$. (Actually, infinitely many solutions)

**Homework:** Prove this for $x^n + y^n = z^n$ for all integers $n > 2$.

Scratch that. This is Fermat’s last theorem: Took 358 years to prove! See > 100-pages proof by Wiles (1995).

Non-Constructive Existence Proof

Goal: Prove $\exists x \ P(x)$

**Non-constructive proof method:** Prove indirectly, e.g., via a contradiction.

Example: A real no. $r$ is rational iff $\exists$ integers $p,q$ s.t. $r = p/q$. A real no. is irrational iff it is not rational. Prove that $\exists$ irrational $x,y$ s.t. $x^y$ is rational.

Pf. We know $\sqrt{2}$ is irrational (see text). Consider $\sqrt[2]{\sqrt{2}}$.

Two possibilities: (a) $\sqrt[2]{\sqrt{2}}$ is rational. Then, choose $x = y = \sqrt{2}$.

(b) $\sqrt[2]{\sqrt{2}}$ is irrational. Choose $x = \sqrt[2]{\sqrt{2}}$ and $y = \sqrt{2}$. Then, $x^y = 2$ is rational. Either way, we have shown $\exists x,y$ s.t. $x^y$ is rational.

(Doesn’t say which is true!)
Review of Chapter 1

✦ Propositional Logic
  ➤ Propositions, logical operators →, ∧, ∨, ⊕, →, ↔, truth tables for operators, precedence of logical operators
  ➤ Compound propositions, truth tables for compound propositions
  ➤ Converse, contrapositive, and inverse of p → q
  ➤ Converting from/to English and propositional logic

✦ Propositional Equivalences
  ➤ Tautology versus contradiction
  ➤ Logical equivalence p ≡ q
  ➤ Tables of logical equivalences (tables 6, 7, 8 in text)
  ➤ De Morgan’s laws
  ➤ Showing two compound propositions are logically equivalent via (a) truth table method and (b) via equivalences in tables 6, 7, 8.

Predicate Logic

✦ Predicates and Quantifiers
  ➤ Predicates, variables, and domain of each variable
  ➤ Universal and existential quantifiers ∀ and ∃ (uniqueness ∃!)
  ➤ Truth value of a quantifier statement
  ➤ Restricting domain of a quantifier, precedence over other operators, and binding variable to a quantifier
  ➤ Logical equivalence of two quantified statements
  ➤ Negation and De Morgan’s laws for quantifiers
  ➤ Translating to/from English

✦ Nested Quantifiers
  ➤ Quantifiers as loops
  ➤ Order of quantifiers matters!
  ➤ Translating to/from English, negating nested quantifiers
Rules of Inference

- Argument, Premises, Conclusion, Argument form
  - Valid argument and valid argument form (show it is a tautology).

- Rule of inference = valid argument form. Table 1 (p. 66).
  - Modus ponens: \([p \land (p \rightarrow q)] \rightarrow q\)
  - Modus tollens: \([((p \rightarrow q) \land \neg q) \rightarrow \neg p]\)
  - Hypothetical Syllogism: \([((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)]\)
  - Disjunctive Syllogism: \([((p \lor q) \land \neg p) \rightarrow q]\)
  - Addition, Simplification, Conjunction
  - Resolution: \([((p \lor q) \land (\neg p \lor r)) \rightarrow (q \lor r)]\)

- Using rules of inference to prove statements from premises

- Rules of inference for quantified statements: instantiation and generalization

Proofs and Proof Methods

- Direct proof of \(p \rightarrow q\): Assume \(p\) is true; show \(q\) is true.
  - Example in class: If \(n\) is an even integer, then \(n^2\) is even.

- Proof of \(p \rightarrow q\) by contraposition: Assume \(\neg q\) and show \(\neg p\).
  - Example in class: If \(n^2\) is even for integer \(n\), then \(n\) is even.

- Vacuous and Trivial Proofs of \(p \rightarrow q\)

- Proof by contradiction of a statement \(p\): Assume \(p\) is not true and show this leads to a contradiction \((r \land \neg r)\).
  - Example in class: Pigeonhole principle

- Proofs of equivalence for \(p \leftrightarrow q\): Show \(p \rightarrow q\) and \(q \rightarrow p\)

- Proof by cases and Existence proofs
Enuff review, let’s move on to sets!!