Review: proofs

• Start with hypotheses and facts
• Use rules of inference to extend set of facts
• Result is proved when it is included in the set

Review: Modus Ponens

• If $p$ and $p \rightarrow q$ are both true then $q$ must be true

• Write this rule as $\begin{array}{c} p \\
\hline
\therefore q \end{array}$

• Given:
  – If it is Wednesday then you have a 311 class today.
  – It is Wednesday.

• Therefore, by modus ponens:
  – You have a 311 class today.

Review: Inference Rules

• Each inference rule is written as: $\begin{array}{c}
A, B \\
\hline
\therefore C, D
\end{array}$

...which means that if both $A$ and $B$ are true then you can infer $C$ and you can infer $D$.

– For rule to be correct $(A \land B) \rightarrow C$ and $(A \land B) \rightarrow D$ must be a tautologies

• Sometimes rules don’t need anything to start with. These rules are called axioms:
  – e.g. Excluded Middle Axiom $\begin{array}{c}
\hline
\therefore p \lor \lnot p
\end{array}$
Review: Propositional Inference Rules

Excluded middle plus two inference rules per binary connective, one to eliminate it and one to introduce it

\[
\begin{align*}
p \land q & \quad p, q \\
\therefore p, q & \quad \therefore p \land q \\
p \lor q, \neg p & \quad p \\
\therefore q & \quad \therefore p \lor q, q \lor p \\
p, p \rightarrow q & \quad p \Rightarrow q, q \rightarrow p \\
\therefore q & \quad \therefore p \rightarrow q
\end{align*}
\]

Review: Direct Proof of an Implication

\[p \implies q\] denotes a proof of \(q\) given \(p\) as an assumption

\[p \implies q\]

The direct proof rule:

If you have such a proof then you can conclude that \(p \implies q\) is true

**Example:**

1. \(p\) assumption
2. \(p \lor q\) intro for \(\lor\) from 1
3. \(p \rightarrow (p \lor q)\) direct proof rule

Review: Proofs using the Direct Proof Rule

Show that \(p \rightarrow r\) follows from \(q\) and \((p \land q) \rightarrow r\)

1. \(q\) given
2. \((p \land q) \rightarrow r\) given
   3. \(p\) assumption
   4. \(p \land q\) from 1 and 3 via Intro \(\land\) rule
   5. \(r\) modus ponens from 2 and 4
3. \(p \rightarrow r\) direct proof rule

Inference rules for quantifiers

\[
\begin{align*}
P(c) \text{ for some } c & \quad \forall x P(x) \\
\therefore \exists x P(x) & \quad \therefore P(a) \text{ for any } a \\
\therefore \forall x P(x) & \quad \therefore \exists x P(x) \\
\therefore \forall x P(x) & \quad \therefore P(c) \text{ for some } \text{special}** c
\end{align*}
\]

**“Let \(a\) be anything***” … \(P(a)\)

**By special, we mean that \(c\) is a name for a value where \(P(c)\) is true. We can’t use anything else about that value, so \(c\) has to be a NEW variable!**

*** By special, we mean that \(c\) is a name for a value where \(P(c)\) is true, and we can’t use anything else about that value, so \(c\) has to be a NEW variable!
Proofs using Quantifiers

“There exists an even prime number”

First, we translate into predicate logic:

\[ \exists x \text{ Even}(x) \land \text{Prime}(x) \]

1. Even(2) Fact (math)
2. Prime(2) Fact (math)
3. Even(2) \land Prime(2) Intro \wedge: 1, 2
4. \exists x (Even(x) \land Prime(x)) Intro \exists: 3

Those first two lines are sort of cheating; we should prove those “facts”.

1. \text{2} = \text{2} \times 1 \quad \text{Definition of Multiplication}
2. Even(2) Intro \exists: 1
3. There are no integers between 1 and 2 \quad \text{Definition of Integers}
4. 2 is an integer \quad \text{Definition of 2}
5. Prime(2) Intro \wedge: 3, 4
6. Even(2) \land Prime(2) Intro \wedge: 2, 4
7. \exists x (Even(x) \land Prime(x)) Intro \exists: 7

Even and Odd

Even(x) \equiv \exists y \ (x=2y)
Odd(x) \equiv \exists y \ (x=2y+1)

Domain: Integers

Prove: “The square of every even number is even.”

Formal proof of: \forall x (Even(x) \rightarrow Even(x^2))
**Even and Odd**

Prove: “The square of every even number is even.”

Formal proof of: \( \forall x (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)

1. \( \text{Even}(a) \) Assumption: \( a \) arbitrary integer
2. \( \exists y \ (a = 2y) \) Definition of Even
3. \( a = 2c \) By elim \( \exists \) : \( c \) special depends on \( a \)
4. \( a^2 = 4c^2 = 2(2c^2) \) Algebra
5. \( \exists y \ (a^2 = 2y) \) By intro \( \exists \) rule
6. \( \text{Even}(a^2) \) Definition of Even
7. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \) Direct proof rule
8. \( \forall x (\text{Even}(x) \rightarrow \text{Even}(x^2)) \) By intro \( \forall \) rule

**Counterexamples**

To disprove \( \forall x \ P(x) \) find a **counterexample:**

– some \( c \) such that \( \neg P(c) \)
– works because this implies \( \exists x \ \neg P(x) \) which is equivalent to \( \neg \forall x \ P(x) \)

**Proof by Contrapositive:** another strategy for implications

If we assume \( \neg q \) and derive \( \neg p \), then we have proven \( \neg q \rightarrow \neg p \), which is the same as \( p \rightarrow q \).

1. \( \neg q \) Assumption
   ...
3. \( \neg p \)
4. \( \neg q \rightarrow \neg p \) Direct Proof Rule
5. \( p \rightarrow q \) Contrapositive
Proof by Contradiction: one way to prove \( \neg p \)

If we assume \( p \) and derive \( F \) (a contradiction), then we have proven \( \neg p \).

1. \( p \)   assumption

...  

3. \( F \)
4. \( p \rightarrow F \)   direct Proof rule
5. \( \neg p \lor F \)   equivalence from 4
6. \( \neg p \)   equivalence from 5

Even and Odd

Domain: Integers

Prove: “No integer is both even and odd.”

English proof: \( \neg \exists x (\text{Even}(x) \land \text{Odd}(x)) \)

\[ \equiv \forall x \neg(\text{Even}(x) \land \text{Odd}(x)) \]

We go by contradiction. Let \( x \) be any integer and suppose that it is both even and odd. Then \( x = 2k \) for some integer \( k \) and \( x = 2m+1 \) for some integer \( m \). Therefore \( 2k = 2m+1 \) and hence \( k = m + \frac{1}{2} \).

But two integers cannot differ by \( \frac{1}{2} \) so this is a contradiction. So, no integer is both even an odd.

Rational Numbers

- A real number \( x \) is rational iff there exist integers \( p \) and \( q \) with \( q \neq 0 \) such that \( x = p/q \).

\[ \text{Rational}(x) \equiv \exists p \exists q ((x=p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land q \neq 0) \]

- Prove:
  - If \( x \) and \( y \) are rational then \( xy \) is rational
  - If \( x \) and \( y \) are rational then \( x+y \) is rational

Rational Numbers

Domain: Real numbers

- A real number \( x \) is rational iff there exist integers \( p \) and \( q \) with \( q \neq 0 \) such that \( x = p/q \).

\[ \text{Rational}(x) \equiv \exists p \exists q ((x=p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land q \neq 0) \]

- Prove: If \( x \) and \( y \) are rational then \( xy \) is rational

\[ \forall x \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \]
### Rational Numbers

- A real number $x$ is **rational** iff there exist integers $p$ and $q$ with $q \neq 0$ such that $x = p/q$.

$\text{Rational}(x) \equiv \exists p \exists q \ (x = p/q \land \text{Integer}(p) \land \text{Integer}(q) \land q \neq 0)$

- **Prove:**
  - If $x$ and $y$ are rational then $xy$ is rational
  - If $x$ and $y$ are rational then $x+y$ is rational
  - If $x$ and $y$ are rational then $x/y$ is rational

### Proofs

- Formal proofs follow simple well-defined rules and should be easy to check
  - In the same way that code should be easy to execute

- English proofs correspond to those rules but are designed to be easier for humans to read
  - Easily checkable in principle

- Simple proof strategies already do a lot
  - Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)