announcements

Reading assignment

– Logical inference
  1.6-1.7 7th Edition
  1.5-1.7 6th Edition

– Set theory
  2.1-2.3 (both editions)

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: an inference rule—Modus Ponens

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

• Write this rule as \( p, p \rightarrow q \quad \therefore q \)

• 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.
Each *inference rule* is written as: \[ \frac{A, B}{\therefore C, D} \]

...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 tautologies

Sometimes rules don’t need anything to start with. These rules are called *axioms*:

- e.g. *Excluded Middle Axiom*

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

- \[ p \land q \quad p, q \]
  \[ \therefore p, q \quad \therefore p \land q \]

- \[ p \lor q, \neg p \quad p \]
  \[ \therefore q \quad \therefore p \lor q, q \lor p \]

- \[ p, p \rightarrow q \]
  \[ \therefore q \quad \therefore p \rightarrow q \quad \text{Direct Proof Rule} \]

- \[ p \Rightarrow q \]
  \[ \therefore q \quad \therefore q \quad \text{Not like other rules} \]

p \Rightarrow q denotes a proof of q given p as an assumption

The direct proof rule:

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

**Example:**

1. p \hspace{1cm} \text{assumption}
2. \(p \lor q\) \hspace{1cm} \text{intro for} \lor \text{from 1}
3. \(p \rightarrow (p \lor q)\) \hspace{1cm} \text{direct proof rule}
4. q \hspace{1cm} \text{given}
5. (p \land q) \rightarrow r \hspace{1cm} \text{given}

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

1. q \hspace{1cm} \text{given}
2. (p \land q) \rightarrow r \hspace{1cm} \text{given}
3. p \hspace{1cm} \text{assumption}
4. p \land q \hspace{1cm} \text{from 1 and 3 via Intro} \land \text{rule}
5. r \hspace{1cm} \text{modus ponens from 2 and 4}
6. p \rightarrow r \hspace{1cm} \text{direct proof rule}
review: inference rules for quantifiers

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

“Let } a \text{ be anything}^* \text{”...} P(a) \\
\therefore \forall x P(x) \\
\quad \quad
\begin{array}{c}
\exists x P(x) \\
\therefore P(c) \text{ for some special } c \\
\end{array}

* in the domain of } P

review: proofs using quantifiers

“There exists an even prime number”

Prime(x): x is an integer > 1 and x is not a multiple of any integer strictly between 1 and x

even and odd

\[
\text{Even}(x) \equiv \exists y \ (x=2y) \quad \text{Odd}(x) \equiv \exists y \ (x=2y+1)
\]

Domain: Integers

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

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

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

even and odd

\[
\text{Even}(x) \equiv \exists y \ (x=2y) \quad \text{Odd}(x) \equiv \exists y \ (x=2y+1)
\]

Domain: Integers

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

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

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

English proof of: $\forall x \ (\text{Odd}(x) \rightarrow \text{Odd}(x^2))$

Let $x$ be an odd number. Then $x=2k+1$ for some integer $k$ (depending on $x$). Therefore $x^2=(2k+1)^2=4k^2+4k+1=2(2k^2+2k)+1$.

Since $2k^2+2k$ is an integer, $x^2$ is odd.

proof by contradiction: one way to prove $\neg p$

If we assume $p$ and derive False (a contradiction), then we have proved $\neg p$.

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

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

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

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

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

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

### 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 $\neg \forall x \ P(x)$

### 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)
set theory

- Formal treatment dates from late 19th century
- Direct ties between set theory and logic
- Important foundational language

A $\cap B$

definition: a set is an unordered collection of objects

- $x \in A$: “$x$ is an element of $A$”
- $x$ is a member of $A$
- “$x$ is in $A$”
- $x \notin A$: $\neg (x \in A)$

$A = \{1, 2, 7, \text{cat, dog, } \varnothing, \alpha\}$

- cat $\in A$
- fish $\notin A$

definitions

- A and B are equal if they have the same elements
  \[ A = B \equiv \forall x \,(x \in A \leftrightarrow x \in B) \]

- A is a subset of B if every element of A is also in B
  \[ A \subseteq B \equiv \forall x \,(x \in A \rightarrow x \in B) \]

empty set and power set

- Empty set $\emptyset$ does not contain any elements

- Power set of a set $A = \text{set of all subsets of } A$
  \[ \mathcal{P}(A) = \{ B : B \subseteq A \} \]
cartesian product

\[ A \times B = \{ (a, b) : a \in A, b \in B \} \]

set operations

\[ A \cup B = \{ x : (x \in A) \lor (x \in B) \} \]  
union

\[ A \cap B = \{ x : (x \in A) \land (x \in B) \} \]  
intersection

\[ A - B = \{ x : (x \in A) \land (x \notin B) \} \]  
set difference

\[ A \oplus B = \{ x : (x \in A) \lor (x \notin B) \} \]  
symmetric difference

\[ \overline{A} = \{ x : x \notin A \} \]  
(complement (with respect to universe U))

it's Boolean algebra again

- Definition for \( \cup \) based on \( \lor \)

- Definition for \( \cap \) based on \( \land \)

- Complement works like \( \neg \)

De Morgan's Laws

\[ \overline{A \cup B} = \overline{A} \cap \overline{B} \]

\[ \overline{A \cap B} = \overline{A} \cup \overline{B} \]

Proof technique:
To show \( C = D \) show
\[ x \in C \rightarrow x \in D \] and
\[ x \in D \rightarrow x \in C \]
distributive laws

\[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \]
\[ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \]