Discussion #12

Deduction, Proofs and Proof Techniques
Topics

• Proofs = Sound Arguments, Derivations, Deduction

• Proof Techniques
  1. Exhaustive
  2. Equivalence to Truth
  3. If and only if (iff)
  4. Contrapositive Proof
  5. Contradiction (or Indirect)
  6. Conditional
  7. Case Analysis
  8. Induction
  9. Direct
1. Exhaustive Truth Proof

Show true for all cases.

– e.g. Prove \( x^2 + 5 < 20 \) for integers \( 0 \leq x \leq 3 \)

\[ \begin{align*}
0^2 + 5 &= 5 \quad < 20 \quad T \\
1^2 + 5 &= 6 \quad < 20 \quad T \\
2^2 + 5 &= 9 \quad < 20 \quad T \\
3^2 + 5 &= 14 \quad < 20 \quad T
\end{align*} \]

– Thus, all cases are exhausted and true.
– Same as using truth tables — when all combinations yield a tautology.
2. Equivalence to Truth

2a. Transform logical expression to T.

Prove: \( R \land S \Rightarrow \neg(\neg R \lor \neg S) \)

\[
R \land S \Rightarrow \neg(\neg R \lor \neg S) \\
\equiv R \land S \Rightarrow \neg \neg R \land \neg \neg S \quad \text{de Morgan’s law} \\
\equiv R \land S \Rightarrow R \land S \quad \text{double negation} \\
\equiv \neg (R \land S) \lor (R \land S) \quad \text{implication (P\Rightarrow Q \equiv \neg P \lor Q)} \\
\equiv T \quad \text{law of excl. middle (P \lor \neg P) \equiv T}
\]
2b. Or, transform lhs to rhs or vice versa.

Prove: \( P \land Q \lor \neg P \land Q \equiv Q \)

\[
P \land Q \lor \neg P \land Q \\
\equiv (P \lor \neg P) \land Q \quad \text{distributive law (factoring)}
\]
\[
\equiv T \land Q \quad \text{law of excluded middle}
\]
\[
\equiv Q \quad \text{identity}
\]
3. If and only if Proof

• Also called necessary and sufficient
• If we have $P \iff Q$, then we can create two standard deductive proofs, namely, $(P \implies Q)$ and $(Q \implies P)$.
• i.e. $P \iff Q \equiv (P \implies Q) \land (Q \implies P)$
• Transforms proof to a standard deductive proof — actually two of them
3. If and only if Proof: Example

Prove: $2x - 4 > 0$ iff $x > 2$.

Thus, we can do two proofs:
(1) If $2x - 4 > 0$ then $x > 2$.
(2) If $x > 2$ then $2x - 4 > 0$.

Proof:
(1) Suppose $2x - 4 > 0$. Then $2x > 4$ and thus $x > 2$.
(2) Suppose $x > 2$. Then $2x > 4$ and thus $2x - 4 > 0$.

Note that we could have also simply converted the lhs to the rhs.
Proof: $2x - 4 > 0 \equiv 2x > 4 \equiv x > 2$. 
4. Contrapositive Proof

Remember:

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>(P \implies Q)</th>
<th>\iff</th>
<th>(\neg Q \implies \neg P)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td></td>
<td>T F T F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td></td>
<td>T T F F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td></td>
<td>T F T T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td></td>
<td>T T T T</td>
</tr>
</tbody>
</table>
4. Contrapositive Proof (continued…)

Prove: if $s$ is not a multiple of 3, then $s$ is not a solution of $x^2 + 3x - 18 = 0$.

$P = s$ is a multiple of 3
$Q = s$ is a solution of $x^2 + 3x - 18 = 0$.

Instead of proving $\neg P \Rightarrow \neg Q$, we can prove $Q \Rightarrow P$ (because of the contrapositive equivalence)

Thus, we prove: if $s$ is a solution of $x^2 + 3x - 18 = 0$, then $s$ is a multiple of 3.
4. Contrapositive Proof: Example

Prove: if $s$ is a solution of $x^2 + 3x - 18 = 0$, then $s$ is a multiple of 3.

Proof: The solutions of $x^2 + 3x - 18 = 0$ are 3 and $-6$. Both 3 and $-6$ are multiples of 3. Thus, every solution $s$ is a multiple of 3.

Note: Using a contrapositive proof helps get rid of the not’s and makes the problem easier to understand — indeed, the contrapositive turns this into a simple proof we can do exhaustively.

Note: In the proof we make true statements. Recall: we can always make any true statement we wish in a proof.
5. Proof by Contradiction

• Note:

<table>
<thead>
<tr>
<th>P</th>
<th>P $\iff$ $\neg$P $\Rightarrow$ F</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T F T</td>
</tr>
<tr>
<td>F</td>
<td>T T F</td>
</tr>
</tbody>
</table>

• Thus, $\neg$P $\Rightarrow$ F $\equiv$ P.

• By substituting R $\Rightarrow$ S for P, we can prove R $\Rightarrow$ S by proving $\neg$($R \Rightarrow S$) $\Rightarrow$ F.

\[
\neg(R \Rightarrow S) \Rightarrow F \equiv \neg(\neg R \lor S) \Rightarrow F \quad \text{implication}
\]
\[
\equiv \neg \neg R \land \neg S \Rightarrow F \quad \text{de Morgan’s law}
\]
\[
\equiv R \land \neg S \Rightarrow F \quad \text{double negation}
\]
5. Proof by Contradiction (continued…)

• Thus, since \( R \land \neg S \Rightarrow F \equiv R \Rightarrow S \), from \( R \Rightarrow S \), we negate the conclusion, add it as a premise, and derive a contradiction, i.e. derive \( F \).

• Any contradiction (e.g. \( P \land \neg P \)) is equivalent to \( F \), so deriving any contradiction is enough.

• BTW, in our project we will implement the semantics of Datalog by programming the computer to do a proof by contradiction.
5. Proof by Contradiction: Example

• Prove: the empty set is unique.

Since P ≡ (¬P ⇒ F), we can prove ¬P ⇒ F instead.

i.e. We can prove: if the empty set is not unique, then there is a contradiction, or, in other words, assuming the empty set is not unique leads (deductively) to a contradiction.

• Proof:

– Assume the empty set is not unique.
– Then there are at least two empty sets ∅₁ and ∅₂ such that ∅₁ ≠ ∅₂.
– Since an empty set is a set and an empty set is a subset of every set, ∅₁ ⊆ ∅₂ and ∅₂ ⊆ ∅₁ and thus ∅₁ = ∅₂.
– But now we now have ∅₁ ≠ ∅₂ and ∅₁ = ∅₂— a contradiction.
Informal Proofs in English vs. Formal Proofs

• Compare

Assume the empty set is not unique. Then there are at least two empty sets $\emptyset_1$ and $\emptyset_2$ such that $\emptyset_1 \neq \emptyset_2$. Since an empty set is set and an empty set is a subset of every set, $\emptyset_1 \subseteq \emptyset_2$ and $\emptyset_2 \subseteq \emptyset_1$ and thus $\emptyset_1 = \emptyset_2$. But now we now have $\emptyset_1 \neq \emptyset_2$ and $\emptyset_1 = \emptyset_2$ — a contradiction.

• vs.

1. Empty set not unique                              assumed premise
2. Empty set not unique $\Rightarrow$
   $\emptyset_1$ and $\emptyset_2$ exist $\land$ $\emptyset_1 \neq \emptyset_2$   uniqueness definition
3. $\emptyset_1$ and $\emptyset_2$ exist $\land$ $\emptyset_1 \neq \emptyset_2$   1&2, modus ponens
4. $\emptyset_1 \neq \emptyset_2$                               3 simplification
5. $\emptyset_1 \subseteq \emptyset_2$ and $\emptyset_2 \subseteq \emptyset_1$ property of empty sets
6. $\emptyset_1 \subseteq \emptyset_2$ and $\emptyset_2 \subseteq \emptyset_1 \Rightarrow \emptyset_1 = \emptyset_2$ set equality definition
7. $\emptyset_1 = \emptyset_2$                               5&6, modus ponens
8. $\emptyset_1 \neq \emptyset_2 \land \emptyset_1 = \emptyset_2$   4&7 combination

Discussion #F2 8 contradiction law ($P \land \neg P \equiv F$) 14/22
6. Conditional Proof

\[ P \Rightarrow (Q \Rightarrow R) \equiv (P \land Q) \Rightarrow R \]

- Much simpler form
  - Simple implication
  - extra premise
- Easy to remember: make lhs of conclusion a premise.

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>P \Rightarrow (Q \Rightarrow R)</th>
<th>\equiv</th>
<th>(P \land Q) \Rightarrow R</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Discussion #12
6. Conditional Proof: Example

Prove: If \( A \subseteq B \) and \( B \subseteq C \), then \( A \subseteq C \).

\[
\equiv \text{If } (x \in A) \Rightarrow (x \in B) \text{ and } (x \in B) \Rightarrow (x \in C) \text{ then } (x \in A) \Rightarrow (x \in C)
\]

\[
\equiv ((P \Rightarrow Q) \land (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)
\]

\[
\equiv (P \Rightarrow Q) \land (Q \Rightarrow R) \land P \Rightarrow R
\]

Proof:

1. \( P \) \hspace{2cm} \text{premise (assumed)}
2. \( P \Rightarrow Q \) \hspace{2cm} \text{premise}
3. \( Q \) \hspace{2cm} 1\&2, \text{modus ponens}
4. \( Q \Rightarrow R \) \hspace{2cm} \text{premise}
5. \( R \) \hspace{2cm} 3\&4, \text{modus ponens}
6. Conditional Proof: Example

Prove: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

\[ \equiv \text{If } (x \in A) \Rightarrow (x \in B) \text{ and } (x \in B) \Rightarrow (x \in C) \text{ then } (x \in A) \Rightarrow (x \in C) \]

\[ \equiv (((P \Rightarrow Q) \land (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)) \Rightarrow (P \Rightarrow R) \equiv (P \Rightarrow Q) \land (Q \Rightarrow R) \land P \Rightarrow R \]

Proof:

1. $x \in A$ premise (assumed)
2. $(x \in A) \Rightarrow (x \in B)$ premise
3. $x \in B$ 1&2, modus ponens
4. $(x \in B) \Rightarrow (x \in C)$ premise
5. $x \in C$ 3&4, modus ponens

Let $x \in A$. Then since $(x \in A) \Rightarrow (x \in B)$, $x \in B$. Thus, since $x \in B$ and $(x \in B) \Rightarrow (x \in C)$, $x \in C$. 
6. Conditional Proof: Example

Prove: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

$\equiv$ If $(x \in A) \Rightarrow (x \in B)$ and $(x \in B) \Rightarrow (x \in C)$ then $(x \in A) \Rightarrow (x \in C)$

$\equiv ((P \Rightarrow Q) \land (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$

$\equiv (P \Rightarrow Q) \land (Q \Rightarrow R) \land P \Rightarrow R$

Proof:

1. $x \in A$  premise (assumed)
2. $(x \in A) \Rightarrow (x \in B)$ premise
3. $x \in B$  1&2, modus ponens
4. $(x \in B) \Rightarrow (x \in C)$ premise
5. $x \in C$  3&4, modus ponens

Let $x \in A$. Then since $A \subseteq B$, $x \in B$.
Thus, since $x \in B$ and $B \subseteq C$, $x \in C$. 
7. Case Analysis

\[ P \equiv (Q \Rightarrow P) \land (\neg Q \Rightarrow P) \]

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \equiv (Q \Rightarrow P) \land (\neg Q \Rightarrow P)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T T T F T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T T T T T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T F F F T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T T F T F</td>
</tr>
</tbody>
</table>

- We can prove P by doing two proofs: (Q \Rightarrow P) and (\neg Q \Rightarrow P).
- And, we can choose any Q — presumably one that’s helpful.
7. Case Analysis: Example

Prove: There are no even primes except 2.

If n is a prime, then n=2 or n is odd.

\[ x \implies (y \lor z) \]

Now add cases:

\[ u \implies (x \implies y \lor z) \quad \text{where } u \text{ is } n=2 \]
\[ \neg u \implies (x \implies y \lor z) \quad \text{where } \neg u \text{ is } n \neq 2 \]

Now observe that we can use a conditional proof:

\[ u \land x \implies y \lor z \quad \text{if } n=2 \text{ and } n \text{ is prime, then } n=2 \text{ or } n \text{ is odd} \]
\[ \neg u \land x \implies y \lor z \quad \text{if } n \neq 2 \text{ and } n \text{ is prime, then } n=2 \text{ or } n \text{ is odd} \]
7. Case Analysis: Example

Prove: If \( n \) is a prime, then \( n=2 \) or \( n \) is odd.

Proof:

Case 1: \( n=2 \): Since \( n=2 \), \( n=2 \) or \( n \) is odd holds.

Case 2: \( n \neq 2 \): Since \( n \neq 2 \) and \( n \) is prime, \( n>2 \). Now \( n \) must be odd, for suppose that \( n \) is even, then \( n = 2k \) for some integer \( k>1 \). But then \( n \) is composite (not prime) — a contradiction. Thus, \( n \) is odd and hence \( n=2 \) or \( n \) is odd holds.
8. Proof by Induction

To be continued….