CS375: Logic and Theory of Computing

Fuhua (Frank) Cheng

Department of Computer Science
University of Kentucky
Table of Contents:

- **Week 1: Preliminaries** (set algebra, relations, functions) (read Chapters 1-4)
- **Weeks 2&3: Propositional Logic** (Chapter 6)
- **Weeks 4&5: Predicate Logic** (Chapter 7)
- **Weeks 6&7: Computing with Logic** (Chapter 9)
- **Week 8: Algebraic Structures** (Chapter 10)
- **Weeks 9&10: Regular Languages, Finite Automata** (Chapter 11)
Table of Contents (conti):

- Weeks 11&12: Context-Free Languages, Pushdown Automata (Chapters 12)
- Weeks 13&14: Turing Machines (Chapter 13)
2. Propositional Logic — Formal reasoning

Using IP \( \rightarrow \) Indirect proof

To prove \( A \),
assume \( \neg A \) is true \( (\text{premise}) \)
If we can prove \( \neg A \rightarrow \text{False} \)
Then since \( A \equiv \neg A \rightarrow \text{False} \) so we have \( A \).
This is the IP rule.

Ex Prove \( \neg (A \land \neg A) \) is a tautology

1. \( \neg \neg (A \land \neg A) \) \( P \) [for \( \neg (A \land \neg A) \)]
2. \( A \land \neg A \) \( 1, \text{DN} \)
3. \( A \) \( 2, \text{Simp} \)
4. \( \neg A \) \( 2, \text{Simp} \)
5. \( \text{False} \) \( 3, 4, \text{Contr} \)
QED \( 1-5, \text{IP} \)

(Double Negation)
IP is most often used in a subproof setting when proving a conditional of the form \( V \rightarrow W \).

Start with \( V \) as a premise for a CP proof. Then start an IP subproof with premise \( \neg W \). When a contradiction is reached, we obtain \( W \) by IP. Then CP gives the result \( V \rightarrow W \).

As with CP subproofs, result of IP is written with no indentation.

**Example.** Prove the tautology \((A \rightarrow B) \land (A \lor B) \rightarrow B\).
Example. prove that the converse of \((A \lor B) \rightarrow (\neg B \rightarrow A)\).

Proof of \((\neg B \rightarrow A) \rightarrow (A \lor B)\):

1. \(\neg B \rightarrow A\) \hspace{1cm} P
2. \(\neg (A \lor B)\) \hspace{1cm} P \ [for A \lor B]
3. \(\neg B\) \hspace{1cm} P \ [for B]
4. \(A\) \hspace{1cm} 1, 3, MP
5. \(A \lor B\) \hspace{1cm} 4, Add
6. \(\text{False}\) \hspace{1cm} 2, 5, Contr
7. \(B\) \hspace{1cm} 3–6, IP
8. \(A \lor B\) \hspace{1cm} 7, Add
9. \(\text{False}\) \hspace{1cm} 2, 8, Contr
10. \(A \lor B\) \hspace{1cm} 2, 7–9, IP

\begin{align*}
\text{QED} & \quad 1, 4, CP.
\end{align*}
2. Propositional Logic — Formal reasoning

Derived Rules (they follow from the original rules)

- **Modus Tollens (MT)**
  \[ A \rightarrow B, \neg B \]
  \[ \neg A \]

- **Hypothetical Syllogism (HS)**
  \[ A \rightarrow B, B \rightarrow C \]
  \[ A \rightarrow C \]

- **Proof by Cases (Cases)**
  \[ A \lor B, A \rightarrow C, B \rightarrow C \]
  \[ C \]

- **Constructive Dilemma (CD)**
  \[ A \lor B, A \rightarrow C, B \rightarrow D \]
  \[ C \lor D \]

**Example.** prove the tautology \((A \rightarrow C) \land (B \rightarrow C) \rightarrow (A \lor B \rightarrow C)\).

1. \(A \rightarrow C\)
2. \(B \rightarrow C\)
3. \(A \lor B\)
4. \(C\)
5. \(A \lor B \rightarrow C\)

QED
2. Propositional Logic — Formal reasoning

Derived Rules (they follow from the original rules)

- **Modus Tollens (MT)**
  
  \[ \frac{A \rightarrow B, \neg B}{\neg A} \]

- **Hypothetical Syllogism (HS)**
  
  \[ \frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C} \]

**Proof by Cases (Cases)**

\[ \frac{A \lor B, A \rightarrow C, B \rightarrow C}{C} \]

**Constructive Dilemma (CD)**

\[ \frac{A \lor B, A \rightarrow C, B \rightarrow D}{C \lor D} \]

**Proof**

1. \( A \rightarrow B \) \( P \)
2. \( \neg B \) \( P \)
3. \( A \) \( P \) [for \( \neg A \)]
4. \( B \) \( 1, 3, \text{MP} \)
5. \( \text{False} \) \( 2, 4, \text{Contr} \)
6. \( \neg A \) \( 3, 5, \text{IP} \)

**QED** \( 1-6, \text{CP} \)
2. Propositional Logic — Formal reasoning

Derived Rules (they follow from the original rules)

- **Modus Tollens (MT)**
  \[
  \frac{A \rightarrow B, \neg B}{\neg A}
  \]

- **Hypothetical Syllogism (HS)**
  \[
  \frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}
  \]

- **Proof by Cases (Cases)**
  \[
  \frac{A \lor B, A \rightarrow C, B \rightarrow C}{C}
  \]

- **Constructive Dilemma (CD)**
  \[
  \frac{A \lor B, A \rightarrow C, B \rightarrow D}{C \lor D}
  \]

---

\[(A \rightarrow B) \land (B \rightarrow C) \rightarrow (A \rightarrow C)\]

**proof**

- **A → B** \( P \)
- **B → C** \( P \)
- **A** \( P \) [for **A → C** ]
- **B** \( MP \)
- **C** \( MP \)
- **A → C** \( CP \)
- **QED** \( CP \)
2. Propositional Logic — Formal reasoning

Derived Rules (they follow from the original rules)

Modus Tollens (MT)
\[
A \rightarrow B, \neg B \\
\neg A
\]

Hypothetical Syllogism (HS)
\[
A \rightarrow B, B \rightarrow C \\
A \rightarrow C
\]

Proof by Cases (Cases)
\[
A \lor B, A \rightarrow C, B \rightarrow C \\
C
\]

Constructive Dilemma (CD)
\[
A \lor B, A \rightarrow C, B \rightarrow D \\
C \lor D
\]

(A \lor B) \land (A \rightarrow C) \land (B \rightarrow C) \\
\rightarrow C

proof

<table>
<thead>
<tr>
<th>A \lor B</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>A \rightarrow C</td>
<td>P</td>
</tr>
<tr>
<td>B \rightarrow C</td>
<td>P</td>
</tr>
<tr>
<td>\neg C</td>
<td>P [for C ]</td>
</tr>
<tr>
<td>\neg A</td>
<td>MT</td>
</tr>
<tr>
<td>\neg B</td>
<td>MT</td>
</tr>
<tr>
<td>\neg A \land \neg B</td>
<td>Conj</td>
</tr>
<tr>
<td>\neg (A \lor B)</td>
<td>DM</td>
</tr>
<tr>
<td>False</td>
<td>Contra</td>
</tr>
<tr>
<td>C</td>
<td>IP</td>
</tr>
<tr>
<td>QED</td>
<td>CP</td>
</tr>
<tr>
<td>QED</td>
<td>CP</td>
</tr>
</tbody>
</table>

University of Kentucky
2. Propositional Logic — Formal reasoning

Derived Rules (they follow from the original rules)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modus Tollens (MT)</strong></td>
<td></td>
</tr>
<tr>
<td>[ A \rightarrow B, \neg B ]</td>
<td>\neg A</td>
</tr>
<tr>
<td><strong>Hypothetical Syllogism (HS)</strong></td>
<td></td>
</tr>
<tr>
<td>[ A \rightarrow B, B \rightarrow C ]</td>
<td>[ \neg (C \lor D) ]</td>
</tr>
<tr>
<td>[ A \rightarrow C ]</td>
<td></td>
</tr>
<tr>
<td>[ B \rightarrow D ]</td>
<td></td>
</tr>
<tr>
<td>[ \neg (C \lor D) \rightarrow \neg A \rightarrow \neg B \rightarrow \neg C \rightarrow \neg D \rightarrow \neg (A \lor B) \rightarrow False ]</td>
<td></td>
</tr>
</tbody>
</table>

**Proof by Cases (Cases)**

\[ \frac{A \lor B, A \rightarrow C, B \rightarrow C}{C} \]

**Constructive Dilemma (CD)**

\[ \frac{A \lor B, A \rightarrow C, B \rightarrow D}{C \lor D} \]

\[ (A \lor B) \land (A \rightarrow C) \land (B \rightarrow D) \rightarrow (C \lor D) \]
Derived Rules (they follow from the original rules)

- **Modus Tollens (MT)**
  \[
  \frac{A \rightarrow B, \neg B}{\neg A}
  \]

- **Hypothetical Syllogism (HS)**
  \[
  \frac{A \rightarrow B, B \rightarrow C}{A \rightarrow C}
  \]

- **Proof by Cases (Cases)**
  \[
  \frac{A \lor B, A \rightarrow C, B \rightarrow C}{C}
  \]

- **Constructive Dilemma (CD)**
  \[
  \frac{A \lor B, A \rightarrow C, B \rightarrow D}{C \lor D}
  \]

**Example.** Prove the tautology \((A \rightarrow C) \land (B \rightarrow C) \rightarrow (A \lor B \rightarrow C)\)

1. \(A \rightarrow C\)  
2. \(B \rightarrow C\)  
3. \(A \lor B\)  
4. \(C\)  
5. \(A \lor B \rightarrow C\)  

QED
2. Propositional Logic — Formal reasoning

Second proof of the tautology

\[(A \rightarrow C) \land (B \rightarrow C) \rightarrow (A \lor B \rightarrow C).\]

\[
\begin{align*}
1. & \quad A \rightarrow C \\
2. & \quad B \rightarrow C \\
3. & \quad A \lor B \\
4. & \quad \neg C \\
5. & \quad \neg A \\
6. & \quad B \\
7. & \quad \neg B \\
8. & \quad \text{False} \\
9. & \quad C \\
10. & \quad A \lor B \rightarrow C
\end{align*}
\]

QED
2. Propositional Logic — Formal reasoning

Example. Prove \((A \rightarrow C) \land \neg (A \rightarrow B) \rightarrow \neg (C \rightarrow B)\) with IP somewhere.

Example. Consider the following argument:
I eat spinach (S) or ice cream (I). If I study logic (L) then I will pass the exam (P). If I eat ice cream then I will study logic. If I eat spinach then I will play golf (G). I failed the exam. Therefore, I played golf.
Example. Consider the following argument:

I eat spinach (S) or ice cream (I). If I study logic (L) then I will pass the exam (P). If I eat ice cream then I will study logic. If I eat spinach then I will play golf (G). I failed the exam. Therefore, I played golf.

The argument has five premises

\{S \lor I, L \rightarrow P, I \rightarrow L, S \rightarrow G, \neg P\} and conclusion G.

Prove that the argument is valid.
Premises: \( S \lor I, L \rightarrow P, I \rightarrow L, S \rightarrow G, \neg P \)

Conclusion: \( G \)

Prove:

1. \( S \lor I \)
2. \( L \rightarrow P \)
3. \( I \rightarrow L \)
4. \( S \rightarrow G \)
5. \( \neg P \)
6. \( \neg L \)
7. \( \neg I \)
8. \( S \)
9. \( G \)

\[ 2, 5, \text{MT} \]
\[ 3, 6, \text{MT} \]
\[ 1, 7, \text{DS} \]
\[ 4, 8, \text{MP} \]

QED.
Alternative Proof:

6. \( I \rightarrow P \)  
7. \( \neg I \)  
8. \( S \)  
9. \( G \)  

QED.

Alternative Proof:

6. \( G \vee L \)  
7. \( \neg L \)  
8. \( G \)  

QED.

Alternative Proof:

6. \( I \rightarrow P \)  
7. \( G \vee L \)  
8. \( G \)  

QED.
2. Propositional Logic — Formal axiom systems

By a **formal axiom system** we mean a specific set of axioms (a fixed set of premises) and **proof rules**. The aims of a formal axiom system are **soundness and completeness**:

- **Soundness**: All proofs yield theorems that are tautologies.
- **Completeness**: All tautologies are provable as theorems.

**Frege-Lukasiewicz (F-L) Axiom System**

- **Axiom 1**: $A \rightarrow (B \rightarrow A)$.
- **Axiom 2**: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.
- **Axiom 3**: $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$.
- **Proof Rule**: MP.
2. Propositional Logic — Formal axiom systems

By a formal axiom system we mean a specific set of axioms (a fixed set of premises) and proof rules. The aims of a formal axiom system are soundness and completeness:

- **Soundness**: All proofs yield theorems that are tautologies.
- **Completeness**: All tautologies are provable as theorems.

Frege-Lukasiewicz (F-L) Axiom System

- **Axiom 1**: $A \rightarrow (B \rightarrow A)$.
- **Axiom 2**: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.
- **Axiom 3**: $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$.
- **Proof Rule**: MP.

1. $A$  
2. $\neg(B \rightarrow A)$  
3. $B \land \neg A$  
4. $\neg A$  
5. False  
6. $B \rightarrow A$  
   QED
2. Propositional Logic — Formal axiom systems

Since the axioms of F-L are tautologies and MP maps tautologies to a tautology, the F-L system is sound. The F-L system is also complete, but that takes a bit of proof (see the text).

Example (Lemma). Use the F-L system to prove $A \to A$.

Proof:
1. $A \to ((A \to A) \to A)$  
   \hspace{1cm} Axiom 1
2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$  
   \hspace{1cm} Axiom 2
3. $(A \to (A \to A)) \to (A \to A)$  
   \hspace{1cm} 1, 2, MP
4. $A \to (A \to A)$  
   \hspace{1cm} Axiom 1
5. $A \to A$  
   \hspace{1cm} 3, 4, MP

QED.

We did not use $A$ as premise to prove $A \to A$
Deduction Theorem (The CP Rule)

If \( A \) is a premise in a proof of \( B \), then there is a proof of \( A \rightarrow B \) that does not use \( A \) as a premise.

Proof Idea: Assume the proof has the form
\[
A = B_0, \ldots, B_n = B.
\]
If \( n = 0 \), then \( A = B \). So we must find a proof of
\[
A \rightarrow B = A \rightarrow A
\]
that does not use \( A \) as a premise. A proof was given in the previous example (lemma). Let \( n > 0 \) and assume that for each \( k \) in the range \( 0 \leq k < n \) there is a proof of \( A \rightarrow B_k \) that does not use \( A \) as a premise.

This theorem justifies the conditional proof technique.
2. Propositional Logic — Formal axiom systems

Proof Idea (conti):
Show that there is a proof of $A \rightarrow B_n$ that does not use $A$ as a premise. If $B_n$ is a premise or an axiom, then we have the following proof that does not use $A$ as a premise:

1. $B_n$  
   Premise or Axiom
2. $B_n \rightarrow (A \rightarrow B_n)$  
   Axiom 1
3. $A \rightarrow B_n$  
   1, 2, MP
   QED.

If $B_n$ is neither a premise nor an axiom, then it is inferred by MP from $B_i$ and $B_j = B_i \rightarrow B_n$, where $i < n$ and $j < n$. So we obtain the following proof that does not use $A$ as a premise:
2. Propositional Logic — Formal axiom systems

Proof Idea (conti):

1. Proof of \( A \rightarrow B_i \) not using \( A \) as a premise
   Induction assumption
2. Proof of \( A \rightarrow (B_i \rightarrow B_n) \) not using \( A \) as a premise
   Induction assumption
3. \( (A \rightarrow (B_i \rightarrow B_n)) \rightarrow ((A \rightarrow B_i) \rightarrow (A \rightarrow B_n)) \)
   Axiom 2
4. \( (A \rightarrow B_i) \rightarrow (A \rightarrow B_n) \)
   2, 3, MP
5. \( A \rightarrow B_n \)
   1, 4, MP

QED.

Since \( B_n = B \), we have a proof of \( A \rightarrow B \) that does not use \( A \) as a premise. QED.
End of Propositional Logic II