Lecture 6

Proofs and Proof Systems

A proof is a formal demonstration that a statement is true. It must be mechanically checkable—meaning we could write a program to verify it. A proof is generally syntactic. The syntactic rules permit mechanical checking.

We notate “there is a proof with premises $\Sigma$ and conclusion $\phi$” by: $\Sigma \vdash \phi$

Generically, a proof consists of a sequence of formulas:

- The premises, if any, appear first.
- Each subsequent formula must be a valid inference from preceding formulas.
  That is, there is an inference rule (defined by the proof system) that justifies the formula, based on the previous formulas in the sequence.
- The final formula is the conclusion.

The key here is the set of inference rules which define a proof system.

In general, an inference rule is written as:

$$\frac{\alpha_1 \alpha_2 \ldots \alpha_i}{\beta}.$$

Meaning given formulas $\alpha_1, \alpha_2, \ldots, \alpha_i$ (they already have appeared in the proof), then one may infer the formula $\beta$ (write $\beta$ as the next formula of the proof).

We notate “there is a proof in system $s$ with premises $\Sigma$ and conclusion $\phi$” by: $\Sigma \vdash_s \phi$

Resolution

Resolution is a proof system that is widely used for computer-aided proofs. It is important to note two distinctive features:

- Resolution only applies to formulas in CNF.
- Resolution is used only to prove contradictions.

Rather than proving $\Sigma \vdash_{Res} \alpha$, we will prove $\Sigma \cup \{\neg\alpha\} \vdash_{Res} \bot$. We use the symbol $\bot$ as the "contradiction formula". Because of this, Resolution is sometimes called a "refutation" system.

Note: To refute a statement is to disprove the statement.

Resolution has only one rule:

$$\frac{(\alpha \lor p) \ (\neg p) \lor \beta}{\alpha \lor \beta}.$$
With two special cases:

Contradiction: \[
\frac{p}{\bot} \quad \frac{\neg p}{\bot}
\]

Unit resolution: \[
\frac{\alpha \lor p}{\alpha} \quad \frac{\neg p}{\bot}
\]

Steps to prove \(\phi\) from \(\Sigma\), via a Resolution refutation:

1. Negate \(\phi\) and move it to the set of premises.
   Remember, we can only prove contradictions, so we must prove \(\Sigma \cup \{\neg \phi\} \vdash Res \bot\)

2. Convert all formulas to CNF.

3. Split the CNF formulas at the \(\land\)s, yielding a set of clauses (premises in the proof).
   (i.e. The CNF formula \(p \land q\) becomes the clauses \(p, q\))

4. From the resulting set of clauses, keep applying the resolution inference rule until either:
   - \(\bot\) (the empty clause) results. In this case, \(\Sigma \vdash \phi\) is a theorem.
   - The rule can no longer be applied to give a new formula.
     In this case, \(\Sigma \vdash \phi\) is not a theorem.

There are two acceptable notations for Resolution proofs: one uses the clauses as formulas and the other as sets of literals. Both are shown in the example below—use only one in your proofs.

**Example:** Prove \(\{p, q\} \vdash Res (p \land q)\).

Step 1: Since we can only prove contradictions in Resolution, we must negate the conclusion and move it with the premises: \(\{p, q, (\neg(p \land q))\}\).
Now we can attempt to prove \(\vdash Res \bot\)

Step 2: Convert all of the formulas to CNF: \(\{p, q, ((\neg p) \lor (\neg q))\}\)

Step 3: Split the CNF formulas at the \(\land\)s to yield a set of clauses.
In this case, there are no \(\land\)s to split so we can just list the premises:

<table>
<thead>
<tr>
<th>Formula Notation</th>
<th>Set Notation</th>
<th>Justifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (p)</td>
<td>{p}</td>
<td>Premise</td>
</tr>
<tr>
<td>2. (q)</td>
<td>{q}</td>
<td>Premise</td>
</tr>
<tr>
<td>3. ((\neg p) \lor (\neg q))</td>
<td>{\neg p, \neg q}</td>
<td>Premise (from negated conclusion)</td>
</tr>
</tbody>
</table>

Step 4: Apply the resolution inference rule until we either result in \(\bot\) or cannot create a new formula. Continuing the proof above:

| 4. \(\neg q\)     | \{\neg q\}   | Unit Resolution on Lines 1,3 |
| 5. \(\bot\)       | \{\}         | Contradiction on Lines 2,4   |

Refutation complete!

Note: It is important to justify *each* line of the proof with the rule of inference and the formulas used for the invocation of the rule.
This proof can be visualized:

\[
\begin{array}{c}
q \\

\downarrow
\end{array}
\quad
\begin{array}{c}
p \\

\downarrow
\end{array}
\quad
\begin{array}{c}
(\neg p) \lor (\neg q) \\

\downarrow
\end{array}
\quad
\begin{array}{c}
(\neg q) \\

\downarrow
\end{array}
\quad
\begin{array}{c}
\bot
\end{array}
\]

Where each pair of lines arriving at a common formula indicates an invocation of the Resolution inference rule.

*For more examples, see the common overheads.*