The Essence of Proof

Mathematical proof is essentially persuasive prose.

- Like an essay, it is effective if it convinces the listener.
- Also like an essay, we can learn certain rhetorical tricks, e.g. “proof by induction” or “use of the contrapositive.”

Two Parts of a Proof

Some parts of a proof involve logical manipulation, regardless of what our statements mean.

Example: *Modus Ponens* is the rule that says “if you know \( p \) and you know \( p \rightarrow q \), then you may conclude \( q \).

- This rule does not depend on what \( p \) and \( q \) “mean.”

Other parts of a proof depend on the meaning of propositional variables or predicates.

Example:

\[
(\forall X)(\text{greenElephant}(X) \rightarrow \text{wearsBoxers}(X))
\]

is true (vacuously!) because we can argue that there are no green elephants.

- The general statement \( (\forall X)(p(X) \rightarrow q(X)) \) is not a theorem.

Succinct Notation

- **AND** replaced by concatenation (no operator, like multiplication).
- **OR** replaced by \(+\).
- **NOT** replaced by \(\neg\).
- **TRUE** and **FALSE** replaced by 0 and 1.
Truth Tables

The truth table for an expression has one row for each combination of truth-values for its variables, i.e., \(2^n\) rows if there are \(n\) variables.

- Assignment of TRUE or FALSE to each variable of the expression is a truth assignment.

The value in each row is the value of the expression for that truth assignment.

- Often, we evaluate an expression “bottom-up,” with a column for each subexpression.
  - Apply an operator to two columns by applying the operator row-wise.

Example: \((p \rightarrow q) \equiv (\neg q \rightarrow \neg p)\).

- The contrapositive law.

<table>
<thead>
<tr>
<th>(p)</th>
<th>(q)</th>
<th>(p \rightarrow q)</th>
<th>(\neg p)</th>
<th>(\neg q)</th>
<th>(\neg q \rightarrow \neg p)</th>
<th>whole</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Algebraic Laws (Tautologies)

1. Commutative laws: \((p + q) \equiv (q + p)\) and \(pq \equiv qp\).
2. Associative laws: \((p+q) + r \equiv p + (q + r)\) and \((pq)r \equiv p(qr)\).
3. Distributive laws: \(p(q+r) \equiv pq + pr\) and \(p + qr \equiv (p + q)(p + r)\).
   - That last one is a surprise; the other laws so far make AND and OR look just like times and plus.
4. Idempotence laws: \(pp \equiv p\) and \(p + p \equiv p\).
5. DeMorgan’s laws: \(\neg(pq) \equiv \neg p + \neg q\) and \(\neg(p + q) \equiv (\neg p)(\neg q)\).
Generalizes to any number of variables: the negation of any product is the sum of the negations, and the negation of any sum is the product of the negations.

Also generalizes to the “infinite case” involving quantifiers: $\neg((\forall X)e(X)) \equiv (\exists X)(\neg e(X))$ and $\neg((\exists X)e(X)) \equiv (\forall X)(\neg e(X))$.

Example: $\neg(pq + r) \equiv (\neg(pq))(\neg r) \equiv (\neg p + \neg q)(\neg r)$.

6. Double negation: $\neg(\neg p) \equiv p$.

Laws Useful in Designing Proofs

7. Contrapositive law: $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$.

To prove an implication, prove the reverse implication of the negations.

Example: Consider “if $X$ is not divisible by 4, then either $X$ is odd or $X = 2Y$ and $Y$ is odd.”

- Use propositions:
  - $p$: “$X$ is divisible by 4.”
  - $q$: “$X$ is odd.”
  - $r$: “$X$ is twice an odd number.”

- Statement is: $\neg p \rightarrow q + r$.

- Contrapositive: $(\neg q)(\neg r) \rightarrow p$.

- Argument:
  - $\neg q$ says “$X$ is even,” i.e., $X = 2A$ for some $A$.
  - $\neg r$ says $X$ is not twice any odd number. Since $X$ is twice $A$, $A$ is not odd. Thus, $A = 2B$ for some $B$.
  - Thus, $X = 4B$, which is statement $p$: “$X$ is divisible by 4.”

8. Proof by contradiction: $p \equiv (\neg p) \rightarrow 0$. 
Prove a statement by showing that its negation implies \texttt{FALSE}, i.e., a contradiction such as \( q(\neg q) \).

9. \textit{Modus ponens}: \((p(p \rightarrow q)) \rightarrow q\).

One way to prove a statement \( q \) is to prove some statement \( p \) and also show that \( p \) implies \( q \).

10. \textit{Transitivity of implication}: \(((p \rightarrow q)(q \rightarrow r)) \rightarrow (p \rightarrow r)\).

To prove \( p \) implies \( r \), find some intermediate \( q \); show \( p \rightarrow q \) and \( q \rightarrow r \).

Likewise \( \equiv \): \(((p \equiv q)(q \equiv r)) \rightarrow (p \equiv r)\)

11. \textit{Replacing implications}: \((p \rightarrow q) \equiv (\neg p + q)\).

Because we can often manipulate \texttt{AND} and \texttt{OR} by the familiar rules for times and plus, it is often easier to replace implications this way.

Similarly, \((p \equiv q) \equiv (pq + (\neg p)(\neg q))\).

12. \textit{Case analysis}: \(((p \rightarrow q)(\neg p \rightarrow q)) \rightarrow q\).

If \( q \) follows from both \( p \) and \( \neg p \), then \( q \) must be true.

More generally, if \( q \) follows from each of \( p_1, p_2, \ldots, p_n \), and at least one of the \( p_i \)'s must be true, then we may conclude \( q \).

\textbf{Example:} Consider

\begin{itemize}
  \item \( p \): “\( X \) is divisible by 4.”
  \item \( q \): “\( X \) is odd.”
  \item \( r \): “\( X \) is twice an odd number.”
\end{itemize}

We want to prove \( \neg p \rightarrow q + r \), or equivalently using (11): \( p + q + r \).

Consider 4 cases, depending on whether the remainder of \( X/4 \) is 0, 1, 2, or 3.

Surely at least one (in fact, exactly one) of these cases is true for any integer \( X \).
0: Then \( p \) is true. Since \( p \to p + q + r \) is a tautology, we may use modus ponens to conclude from that and \( p \) that \( p + q + r \).

1: Then \( q \) is true. Since \( q \to p + q + r \) is also a tautology, we can conclude \( p + q + r \) by modus ponens.

2: Then \( X/2 \) is odd, so \( r \) is true. \( r \to p + q + r \) is a tautology, so we conclude \( p + q + r \) by modus ponens.

3: Like case 1.

**Substitution Principle**

You may substitute for any or all propositional variables in a tautology.

- Even expressions involving predicate logic may be substituted.

**Example:** \( p + \neg p \) is a tautology. Substitute \( s(X, Y) + s(Y, X) \) for \( p \). It follows that

\[
s(X, Y) + s(Y, X) + \left( \neg(s(X, Y) + s(Y, X)) \right)
\]

is a tautology.

**Substitution of Equals for Equals**

Take any expression \( E \), find some subexpression \( F \), substitute for \( F \) an equivalent expression, and the resulting expression will be equivalent to \( E \).

**Example:** A substituted instance of De-Morgan’s law says \( \neg(s(X, Y) + s(Y, X)) \equiv \left( \neg s(X, Y) \right) \left( \neg s(Y, X) \right) \). Substitute the right side for the left in previous example to conclude \( s(X, Y) + s(Y, X) + (\neg s(X, Y))(\neg s(Y, X)) \) is a tautology.