Introduction Propositional Calculus

- We know the correspondence in between a boolean variable and a proposition.
- Now we want to develop proof techniques by manipulating boolean expressions.

Propositional Calculus & Equational Logic

Definitions:
Propositions can be combined and manipulated on various ways. These manipulations are the subject of propositional calculus (also called equational logic $\equiv$).

In logic, a theory is given by a set of premises $^1$, together with all conclusions that can be derived from the premises. The premises of a theory are often called axioms. The conclusions that can be derived from the axioms are called theorems.

Axioms for $\equiv$

- **Associativity of $\equiv$**: $(p \equiv q) \equiv r \equiv (p \equiv (q \equiv r))$
  
  This axiom allows us to forget about the parentheses and simply write $p \equiv q \equiv r$.

- **Symmetry of $\equiv$**: $p \equiv q \equiv q \equiv p$
  
  The symmetry is seen by imagining parentheses $(p \equiv q) \equiv (q \equiv p)$.

- **Identity of $\equiv$**: $T \equiv q \equiv q$

Theorems

**Theorem:** $p \equiv p \equiv q \equiv q$

**Theorem:** $p \equiv q \equiv q$

Proof:
Using the axioms on the symmetry of $\equiv$, we write $(p \equiv q \equiv q) \equiv p$. Now we use the standard proof format:

- $p \equiv p \equiv q \equiv q$
- $(\text{Introduce parentheses})$
- $p \equiv (p \equiv q \equiv q)$
- $(\text{Use Axiom symmetry of } \equiv \text{ to replace } p \equiv q \equiv q \text{ by } p)$
- $p \equiv q \equiv p$
- $(\text{Use Axiom symmetry of } \equiv \text{ to replace the first } p \text{ by } p \equiv q \equiv q)$
- $(p \equiv q \equiv q) \equiv p$
- $(\text{Removing parentheses})$
- $p \equiv q \equiv q \equiv p$

Starting from the theorem (expression to prove), using the Axiom symmetry of $\equiv$, we show the equality with this same axiom. Therefore, by definition of a theorem, the first expression has just been proved to be a theorem.

Exercises

1. Prove the following theorem:
   **Theorem Reflexivity of $\equiv$**: $p \equiv p$

   Solution:
   $p \equiv p$
   - $(\text{Use Axiom symmetry of } \equiv \text{ to replace the first } p \text{ by } p \equiv q \equiv q)$
   $|p \equiv q \equiv q| \equiv p$
   - $(\text{Removing parentheses})$
   $p \equiv q \equiv q \equiv p$

   Starting from the theorem to demonstrate, we infer in several steps the Axiom of symmetry.

$^1$ or hypotheses.
### Axioms for Negation $\neg$, Inequivalence $\not\equiv$ and False $\bot$

**Definition of false:** $\bot \equiv \neg \top$

**Definition of $\neg$ over $\equiv$:**

$\neg (p \equiv q) \equiv \neg p \equiv q$

**Definition of $\not\equiv$:**

$(p \not\equiv q) \equiv \neg (p \equiv q)$

### Theorems for Negation $\neg$, Inequivalence $\not\equiv$ and False $\bot$

**Theorem:** $\neg p \equiv q \equiv p \equiv \neg q$

This is better understood using parentheses: $(\neg p \equiv q) \equiv (p \equiv \neg q)$.

**Theorem double negation:** $\neg \neg p \equiv p$

**Theorem Negation of $\bot$:** $\neg \bot \equiv \top$

**Theorem:** $(p \not\equiv q) \equiv \neg p \equiv q$

or $(p \not\equiv q) \equiv (\neg p \equiv q)$

**Theorem Symmetry of $\not\equiv$:**

$(p \not\equiv q) \equiv (q \not\equiv p)$

**Theorem Associativity of $\not\equiv$:**

$$((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$$

**Theorem Mutual associativity:**

$$((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$$

**Theorem Mutual interchangeability:**

$p \not\equiv q \equiv r \equiv p \equiv q \not\equiv r$

### Proofs

- Using Axioms, we just shew how to demonstrate theorems.
- Also, truth tables can be used to prove a theorem.
- Next, we formalise two methods to present a proof.

### Proof method I

**Proof I:**

Theorem to prove

- $\langle$ Use axiom/inference rules $\rangle$
- $\ldots$
- $\langle$ Use axiom/inference rules $\rangle$
- $\ldots$
- $\langle$ An Axiom we know to be True $\rangle$

### Proof method II

**Proof II:** The proof takes the form

- $P$ (Use some Axiom or Theorem)
- $\ldots$
- $\langle$ Use some Axiom or Theorem $\rangle$
- $R$ (Use some Axiom or Theorem)
- $\ldots$
- $\langle$ Use some Axiom or Theorem $\rangle$
- $Q$
Proof method II

Example:
Proof of Negation of False \( \neg F \equiv T \) with method II

\[
\begin{align*}
\neg F & \quad < \text{Definition of } F > \\
\neg T & \quad < \text{Double Negation with } p = T > \\
T & 
\end{align*}
\]

Exercises

1. Prove theorem \( \neg p \equiv q \equiv p \equiv \neg q \) with the starting line \( \neg p \equiv q \) and ending with \( p \equiv \neg q \).

Solution question 1

Prove theorem \( \neg p \equiv q \equiv p \equiv \neg q \) with the starting line \( \neg p \equiv q \) and ending with \( p \equiv \neg q \).

\[
\begin{align*}
\neg p & \equiv q & < \text{definition of } \neg \text{ over } \equiv > \\
\neg (p \equiv q) & < \text{Symmetry of } \equiv > \\
\neg q & \equiv p & < \text{definition of } \neg \text{ over } \equiv > \\
\neg q & \equiv p & < \text{Symmetry of } \equiv > \\
p & \equiv \neg q \\
\end{align*}
\]

Solution question 2

Prove theorem \( \neg \neg p \equiv p \).

\[
\begin{align*}
\neg \neg p & \equiv p & < \text{definition of } \neg \text{ over } \equiv > \\
\neg \neg \neg p & < \text{Symmetry of } \equiv > \\
\neg \neg \neg p & < \text{definition of } \neg \text{ over } \equiv > \\
\neg \neg \neg p & < \text{definition of } \neg \text{ over } \equiv > \\
\neg \neg p & \equiv p & < \text{Identity of } \equiv \text{ with } q = \neg p > \\
T & 
\end{align*}
\]

Solution question 3

Prove theorem \( \neg p \equiv p \equiv F \). Proof:

\[
\begin{align*}
\neg p & \equiv p \equiv F & < \text{parentheses } > \\
\neg p & \equiv p \equiv F & < \text{definition of } \neg \text{ over } \equiv > \\
\neg (p \equiv p) & \equiv F & < \text{Identity of } \equiv > \\
\neg (T) & \equiv F & < \text{remove parentheses } > \\
\neg T & \equiv F & < \text{Symmetry of } \equiv > \\
F & \equiv \neg T & < \text{Definition of False } > 
\end{align*}
\]

Proof Heuristics & Principles

- **Heuristics**: Identify applicable theorems by matching the structure of expressions or subexpressions. The operators that appear in a boolean expression and the shape of its subexpressions can focus the choice of theorems to be used in manipulating it.

- **Principle**: Structure proofs to avoid repeating the same subexpression on many lines.

- **Heuristic of Definition Elimination**: To prove a theorem concerning an operator \( \circ \) that is defined in terms of another, say \( \bullet \):
  1. expand the definition of \( \circ \) to arrive at a formula that contains \( \bullet \),
  2. exploit the properties of \( \bullet \) to manipulate the formula,
  3. then (possibly) reintroduce \( \circ \) using its definition.
Example:

As an example, we will prove \((p \not\equiv q) \equiv (q \not\equiv p)\). Here, the operator \(\circ\) is \(\not\equiv\) and \(\bullet\) is \(\equiv\).

\[
\begin{align*}
p \not\equiv q \\
\neg (p \equiv q) \\
\neg (q \equiv p) \\
\neg \neg (q \equiv p) \\
q \not\equiv p
\end{align*}
\]