SC/MATH 1090

5- Equational Proof

Ref: G. Tourlakis, *Mathematical Logic*, John Wiley & Sons, 2008.

York University

Department of Computer Science and Engineering

Overview

- Equational Proof
- Some examples
- Using assumptions in equational proofs

Equational Proof

- An equational-style proof is a proof of the form:

  (1) $A_1 \equiv A_2$ <annotation>

  (2) $A_2 \equiv A_3$ <annotation>

  …

  (n-1) $A_{n-1} \equiv A_n$ <annotation>

  (n) $A_n \equiv A_{n+1}$ <annotation>

- **Metatheorem**. $A_1 \equiv A_2 , A_2 \equiv A_3 , \ldots, A_n \equiv A_{n+1} \vdash A_1 \equiv A_{n+1}$

- **Corollary**. In an equational proof from assumptions Γ, we have $\Gamma \vdash A_1 \equiv A_{n+1}$.

- **Corollary**. In an equational proof from assumptions Γ, we have $\Gamma \vdash A_1$ **iff** $\Gamma \vdash A_{n+1}$.

Equational Proof Layout

- An equational-style proof is a proof of the form:

Instead of

(1)	A_1	$\equiv$	A_2	<annotation>
(2)	A_2	$\equiv$	A_3	<annotation>
…				
(n-1)	A_{n-1}	$\equiv$	A_n	<annotation>
(n)	A_n	$\equiv$	A_{n+1}	<annotation>

We write:

A_1

$\Leftrightarrow$ **<annotation>**

A_2

$\Leftrightarrow$ **<annotation>**

…

A_n

$\Leftrightarrow$ **<annotation>**

A_{n+1}

Equational Proof- framework

- To Prove $\vdash A \equiv B$:

Template 1

We write:

A

$\Leftrightarrow$ <annotation>

…

$\Leftrightarrow$ <annotation>

B

Template 2

Or, we write:

an axiom or a proven theorem

$\Leftrightarrow$ <annotation>

…

$\Leftrightarrow$ <annotation>

$A \equiv B$

Template 3

Or, we write:

$A \equiv B$

$\Leftrightarrow$ <annotation>

…

$\Leftrightarrow$ <annotation>

axiom or proven theorem

Equational Proof- framework

- To Prove $\vdash A$:

Template 2

Or, we write:

an axiom or a proven theorem

$\Leftrightarrow$ <annotation>

...

$\Leftrightarrow$ <annotation>

A

Template 3

Or, we write:

A

$\Leftrightarrow$ <annotation>

...

$\Leftrightarrow$ <annotation>

axiom or proven theorem

Equational Proof- framework

- To Prove $\Gamma \vdash A$:

Template 2

Or, we write:

an axiom or a <u>hypothesis</u> or proven theorem

$\Leftrightarrow$ <annotation>

...

$\Leftrightarrow$ <annotation>

A

Template 3

Or, we write:

A

$\Leftrightarrow$ <annotation>

...

$\Leftrightarrow$ <annotation>

axiom or a <u>hypothesis</u> or proven theorem

Useful tools: $\neg$, $\top$, and $\bot$

- Some properties of $\neg$

  $\vdash \neg(A \equiv B) \equiv \neg A \equiv B$

  $\vdash \neg(A \equiv B) \equiv A \equiv \neg B$

  $\vdash \neg\neg A \equiv A$ **Double Negation**

- Some properties of $\top$ and $\bot$

  $\vdash \top \equiv \neg \bot$

  $\vdash \bot \equiv \neg \top$

  $\vdash A \vee \top$

  $\vdash A \vee \bot \equiv A$

Useful tools: $\vee$

- Some properties of $\vee$
  - $\vdash A \vee B \equiv B \vee A$ **Axiom 6: Symmetry of $\vee$**
  - $\vdash (A \vee B) \vee C \equiv A \vee (B \vee C)$ **Axiom 5 : Associativity of $\vee$**
  - $\vdash A \vee (B \vee C) \equiv (A \vee B) \vee C$

    By above theorem, together with axiom 5 and 6, we can prove that in a chain of two '$\vee$'s, we can put the brackets around any subchain and we can move items around (similar to '$\equiv$'s). The general case of any number of '$\vee$'s also holds.

  - $\vdash (A \equiv B) \vee (C \equiv D) \equiv A \vee C \equiv B \vee C \equiv A \vee D \equiv B \vee D$

Useful tools: $\rightarrow$ and not $\equiv$

- Some properties of $\rightarrow$

  $\vdash A \rightarrow B \equiv \neg A \vee B$

  Corollary: $\vdash \neg A \vee B \equiv A \vee B \equiv B$

  $\vdash A \rightarrow (B \equiv C) \equiv A \rightarrow B \equiv A \rightarrow C$

- Definition:

$$A \not\equiv B \stackrel{\text{def}}{=} \neg(A \equiv B)$$

- Property of $\not\equiv$

$$\vdash \Big((A \not\equiv B) \not\equiv C\Big) \equiv \Big(A \not\equiv (B \not\equiv C)\Big)$$

De Morgan theorems

- De Morgan 1

  $\vdash A \land B \equiv \neg(\neg A \lor \neg B)$

  or

  $\vdash \neg(A \land B) \equiv \neg A \lor \neg B$

- De Morgan 2

  $\vdash A \lor B \equiv \neg(\neg A \land \neg B)$

  or

  $\vdash \neg(A \lor B) \equiv \neg A \land \neg B$

Useful tools: $\wedge$

- $\vdash A \wedge A \equiv A$
- $\vdash A \wedge \top \equiv A$
- $\vdash A \wedge \bot \equiv \bot$
- Distributivity of $\vee$ over $\wedge$

  $\vdash A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- Distributivity of $\wedge$ over $\vee$

  $\vdash A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

Some more theorems!

- $\vdash (A \vee B) \rightarrow C \equiv (A \rightarrow C) \wedge (B \rightarrow C)$
- $\vdash A \rightarrow (B \wedge C) \equiv (A \rightarrow B) \wedge (A \rightarrow C)$

Ping-Pong Theorem:

$$\vdash A \equiv B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$

Using Hypotheses (special axioms) in Equational Proofs

- $A \vdash A \equiv \top$
- Therefore using Leibniz, one can replace occurrences of hypothesis A by $\top$
- Conversely, any occurrence of $\top$ can be replaced by A.

Examples- important!

- $A, B \vdash A \wedge B$
- $A \vee A \vdash A$
- $A \vdash A \vee B$
- $A \wedge B \vdash A$

- **Metatheorem (Splitting/ Merging Hypotheses)**
  For any formulae A, B, C and set Γ, we have $\Gamma \cup \{A,B\} \vdash C$ iff $\Gamma \bigcup \{A \wedge B\} \vdash C$.

Very important tools!

- $A, A \rightarrow B \vdash B$ **Modus Ponens**
- $A \vee B,\ \neg A \vee C \vdash B \vee C$ **Cut Rule**
  - $A \vee B,\ \neg A \vee B \vdash B$
  - $A \vee B,\ \neg A \vdash B$
  - $A, \neg A \vdash \bot$
- $A \rightarrow B,\ B \rightarrow C \vdash A \rightarrow C$ **Transitivity of $\rightarrow$**
- $A \rightarrow C,\ B \rightarrow D \vdash A \vee B \rightarrow C \vee D$
  - $A \rightarrow C,\ B \rightarrow C \vdash A \vee B \rightarrow C$ **Proof by Cases**
  - $A \rightarrow C,\ \neg A \rightarrow C \vdash C$