

# Mathematics for Computer Science

José Proença & Alexandre Madeira  
(slides from Luis Soares Barbosa)



Universidade do Minho

**Propositional Calculus**  
September-October, 2017

# Calculus

Boolean expressions can be defined by

- how they are evaluated (models)
- how they can be manipulated (proofs)

A calculus is a method or process of reasoning by calculation with symbols.

## Equational reasoning

**Axioms** i.e. boolean expressions that define basic manipulative properties of boolean operators

**Inference rules**

$$\frac{P = Q, Q = R}{P = R} \text{ (transitivity)}$$

$$\frac{P = Q}{E[z := P] = E[z := Q]} \text{ (Leibniz)}$$

$$\frac{P}{P[z := Q]} \text{ (substitution)}$$

where  $P, Q, \dots$  are arbitrary Boolean expressions, and  $p, q, r, z, \dots$  are Boolean variables.

# Equational reasoning

## Equivalence

$(\equiv \text{ associativity})$	$((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$
$(\equiv \text{ commutativity})$	$p \equiv q \equiv q \equiv p$
$(\equiv \text{ identity})$	$\text{TRUE} \equiv q \equiv q$

# Equational reasoning

## Negation

(FALSE definition)	$\text{FALSE} \equiv \neg \text{TRUE}$
( $\neg$ distributivity over $\equiv$ )	$\neg(p \equiv q) \equiv \neg p \equiv q$
( $\neq$ definition)	$(p \neq q) \equiv \neg(p \equiv q)$

## De Morgan laws – from the duality meta-theorem

( $\wedge$ -negation)	$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$
( $\vee$ -negation)	$\neg(p \vee q) \equiv (\neg p \wedge \neg q)$

# Equational reasoning

## Disjunction

$$(\vee \text{ commutativity}) \quad p \vee q \equiv q \vee p$$

$$(\vee \text{ associativity}) \quad (p \vee q) \vee r \equiv p \vee (q \vee r)$$

$$(\vee \text{ idempotency}) \quad p \vee p \equiv p$$

$$(\vee \text{ distributivity over } \equiv) \quad p \vee (q \equiv r) \equiv (p \vee q) \equiv (p \vee r)$$

$$(\text{excluded middle}) \quad p \vee \neg p \equiv \text{TRUE}$$

# Equational reasoning

## Conjunction

(golden rule)  $p \wedge q \equiv p \equiv q \equiv p \vee q$

# Equational reasoning

## Implication

( $\Rightarrow$  definition)

$$p \Rightarrow q \equiv p \vee q \equiv q$$

(consequence)

$$p \Leftarrow q \equiv q \Rightarrow p$$



## Example

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

$$\begin{aligned} & \neg p \equiv q \equiv p \equiv \neg q \\ = & \quad \{ \equiv \text{associativity, commutativity} \} \\ & (\neg p \equiv p) \equiv (q \equiv \neg q) \\ = & \quad \{ \neg \text{distributivity over } \equiv \} \\ & \neg(p \equiv p) \equiv \neg(q \equiv q) \\ = & \quad \{ \equiv \text{identity, FALSE definition} \} \\ & \text{FALSE} \equiv \text{FALSE} \\ = & \quad \{ \equiv \text{identity} \} \\ & \text{TRUE} \end{aligned}$$

# Example

Theorem:  $p \vee \text{TRUE} \equiv \text{TRUE}$

$$\begin{aligned} & p \vee \text{TRUE} \\ = & \quad \{ \equiv \text{identity} \} \\ & p \vee (p \equiv p) \\ = & \quad \{ \vee \text{ distributivity over } \equiv \} \\ & p \vee p \equiv p \vee p \\ = & \quad \{ \equiv \text{identity} \} \\ & \text{TRUE} \end{aligned}$$

# Example

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

$$p \vee q \equiv p \vee \neg q \equiv p$$

$$= \quad \{ \vee \text{ distributivity over } \equiv \}$$

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

$$= \quad \{ \neg \text{ distributivity over } \equiv \}$$

$$p \vee \text{FALSE} \equiv p$$

$$= \quad \{ \text{theorem - exercise below} \}$$

$$p \equiv p$$

$$= \quad \{ \equiv \text{ identity} \}$$

$$\text{TRUE}$$

## Example

Theorem:  $p \wedge (\neg p \vee q) \equiv (p \wedge q)$

$$p \wedge (\neg p \vee q)$$

$$= \quad \{ \text{golden rule} \}$$

$$p \equiv \neg p \vee q \equiv p \vee \neg p \vee q$$

$$= \quad \{ \equiv \text{associativity, excluded middle} \}$$

$$p \equiv \neg p \vee q \equiv \text{TRUE} \vee q$$

$$= \quad \{ \text{theorem above: } p \vee \text{TRUE} \equiv \text{TRUE} \}$$

$$p \equiv \neg p \vee q$$

$$= \quad \{ \text{theorem above: } p \vee q \equiv p \vee \neg q \equiv p \}$$

$$p \equiv p \vee q \equiv q$$

$$= \quad \{ \text{golden rule} \}$$

$$p \wedge q$$

## Example

Theorem:  $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

$$\begin{aligned} & (p \wedge q) \wedge r \\ = & \quad \{ \text{golden rule} \} \\ & (p \equiv q \equiv p \vee q) \wedge r \\ = & \quad \{ \text{golden rule} \} \\ & (p \equiv q \equiv p \vee q) \equiv r \equiv ((p \equiv q \equiv p \vee q) \vee r) \\ = & \quad \{ \vee \text{ distributivity over } \equiv \} \\ & p \equiv q \equiv p \vee q \equiv r \equiv p \vee r \equiv q \vee r \equiv p \vee q \vee r \\ = & \quad \{ \equiv \text{ associativity, commutativity} \} \\ & p \equiv q \equiv r \equiv p \vee q \equiv p \vee r \equiv q \vee r \equiv p \vee q \vee r \end{aligned}$$

# Example

(cont)

$$\begin{aligned} & p \equiv q \equiv r \equiv p \vee q \equiv p \vee r \equiv q \vee r \equiv p \vee q \vee r \\ = & \quad \{ \text{golden rule} \} \\ & (q \wedge r) \equiv p \equiv p \vee q \equiv p \vee r \equiv p \vee q \vee r \\ = & \quad \{ \vee \text{ distributivity over } \equiv \} \\ & (q \wedge r) \equiv p \equiv p \vee q \equiv p \vee (r \equiv q \vee r) \\ = & \quad \{ \vee \text{ distributivity over } \equiv \} \\ & (q \wedge r) \equiv p \equiv p \vee (q \equiv r \equiv q \vee r) \\ = & \quad \{ \text{golden rule} \} \\ & (q \wedge r) \equiv p \equiv p \vee (q \wedge r) \\ = & \quad \{ \text{golden rule} \} \\ & p \wedge (q \wedge r) \end{aligned}$$

## Example

Theorem:  $p \Rightarrow q \equiv p \wedge q \equiv p$

$$\begin{aligned} & p \Rightarrow q \equiv p \wedge q \equiv p \\ = & \quad \{ \Rightarrow \text{definition} \} \\ & p \vee q \equiv q \equiv p \wedge q \equiv p \\ = & \quad \{ \equiv \text{associativity, commutativity} \} \\ & (p \equiv q \equiv p \vee q) \equiv p \wedge q \\ = & \quad \{ \text{golden rule} \} \\ & p \wedge q \equiv p \wedge q \end{aligned}$$

## Example (another proof technique)

Theorem:  $(p \Rightarrow q) \Rightarrow p \vee r \Rightarrow q \vee r$

$$\begin{aligned}
 & p \vee r \Rightarrow q \vee r \\
 = & \quad \{ \Rightarrow \text{definition} \} \\
 & p \vee r \vee q \vee r \equiv q \vee r \\
 = & \quad \{ \vee \text{ idempotency, } \equiv \text{ associativity, commutativity} \} \\
 & p \vee q \vee r \equiv q \vee r \\
 = & \quad \{ \vee \text{ distributivity over } \equiv \} \\
 & (p \vee q \equiv q) \vee r \\
 \Leftarrow & \quad \{ \text{weakning: } p \Rightarrow p \vee q \} \\
 & p \vee q \equiv q \\
 = & \quad \{ \Rightarrow \text{definition} \} \\
 & p \Rightarrow q
 \end{aligned}$$



# Exercises

- $p \vee \text{FALSE} \equiv p$
- $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv p \equiv q$
- $(p \Rightarrow q) \equiv \neg p \vee q$
- $(\neg p \wedge \neg q) \vee (q \wedge p) \equiv p \equiv q$

# Resolution

Theorem:  $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv p \equiv q$

$$\begin{aligned}
 & (p \Rightarrow q) \wedge (q \Rightarrow p) \\
 = & \quad \{ \Rightarrow \text{alternative definition} \} \\
 & (\neg p \vee q) \wedge (\neg q \vee p) \\
 = & \quad \{ \wedge, \vee \text{ distributivity} \} \\
 & ((\neg p \vee q) \wedge \neg q) \vee (\neg p \vee q) \wedge p) \\
 = & \quad \{ \wedge, \vee \text{ distributivity} \} \\
 & (\neg p \wedge \neg q) \vee (q \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge p) \\
 = & \quad \{ a \wedge \neg a \equiv \text{FALSE}, a \vee \text{FALSE} \equiv a \} \\
 & (\neg p \wedge \neg q) \vee (q \wedge p) \\
 = & \quad \{ \text{Theorem: } (\neg p \wedge \neg q) \vee (q \wedge p) \equiv p \equiv q \} \\
 & p \equiv q
 \end{aligned}$$

# Resolution

Theorem:  $(\neg p \wedge \neg q) \vee (q \wedge p) \equiv p \equiv q$

$$\begin{aligned} & (\neg p \wedge \neg q) \vee (q \wedge p) \\ = & \quad \{ \text{golden rule} \} \\ & (\neg p \equiv \neg q \equiv (\neg p \vee \neg q)) \vee (q \wedge p) \\ = & \quad \{ \vee \text{ distributivity} \} \\ & ((\neg p \equiv \neg q) \vee (p \wedge q)) \equiv ((\neg p \vee \neg q) \vee (p \wedge q)) \\ = & \quad \{ \text{de Morgan} \} \\ & ((\neg p \equiv \neg q) \vee (p \wedge q)) \equiv (\neg(p \wedge q) \vee (p \wedge q)) \\ = & \quad \{ \text{excluded middle, } \equiv \text{ identity} \} \\ & (\neg p \equiv \neg q) \vee (p \wedge q) \\ = & \quad \{ \vee \text{ distributivity} \} \\ & (\neg p \vee (p \wedge q)) \equiv (\neg q \vee (p \wedge q)) \end{aligned}$$

# Resolution

(cont)

$$\begin{aligned}
 & (\neg p \vee (p \wedge q)) \equiv (\neg q \vee (p \wedge q)) \\
 = & \quad \{ \wedge, \vee \text{ distributivity} \} \\
 & (\neg p \vee p) \wedge (\neg p \vee q) \equiv (\neg q \vee p) \wedge (\neg q \vee q) \\
 = & \quad \{ \text{excluded middle, } \text{TRUE} \wedge a \equiv a \} \\
 & (\neg p \vee q) \equiv (\neg q \vee p) \\
 = & \quad \{ \text{theorem: } a \vee b \equiv a \vee \neg b \equiv a \} \\
 & (\neg p \vee q) \equiv (q \vee p) \text{ dimpp} \\
 = & \quad \{ \wedge, \vee \text{ distributivity} \} \\
 & q \equiv (p \vee \neg p) \equiv p \\
 = & \quad \{ \text{excluded middle, } \equiv \text{ identity} \} \\
 & q \equiv p
 \end{aligned}$$

# Resolution

Theorem:  $\neg(p \wedge q) \equiv \neg q \vee \neg p$

$$\begin{aligned} & \neg(p \wedge q) \\ = & \quad \{ \text{golden rule} \} \\ & \neg(q \equiv p \equiv p \vee q) \\ = & \quad \{ \neg \text{ distributivity} \} \\ & \neg q \equiv p \equiv p \vee q \\ = & \quad \{ a \vee \text{FALSE} \equiv a \} \\ & \neg q \equiv p \vee \text{FALSE} \equiv p \vee q \\ = & \quad \{ \vee \text{ distributivity} \} \\ & \neg q \equiv (\text{FALSE} \equiv q) \vee p \\ = & \quad \{ \neg a \equiv (\text{FALSE} \equiv a) \} \\ & \neg q \equiv \neg q \vee p \end{aligned}$$

# Resolution

(cont)

$$\begin{aligned} & \neg q \equiv \neg q \vee p \\ = & \quad \{ \textcolor{blue}{a \vee \text{FALSE} \equiv a} \} \\ & \neg q \vee \text{FALSE} \equiv \neg q \vee p \\ = & \quad \{ \textcolor{blue}{\vee \text{ distributivity}} \} \\ & \neg q \vee (\text{FALSE} \equiv p) \\ = & \quad \{ \textcolor{blue}{\neg a \equiv (\text{FALSE} \equiv a)} \} \\ & \neg q \vee \neg p \end{aligned}$$

$$(\equiv \text{ associativity}) \quad ((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$$

$$(\equiv \text{ commutativity}) \quad p \equiv q \equiv q \equiv p$$

$$(\equiv \text{ identity}) \quad \text{TRUE} \equiv q \equiv q$$

$$(\text{FALSE definition}) \quad \text{FALSE} \equiv \neg \text{TRUE}$$

$$(\neg \text{ distributivity over } \equiv) \quad \neg(p \equiv q) \equiv \neg p \equiv q$$

$$(\neq \text{ definition}) \quad (p \neq q) \equiv \neg(p \equiv q)$$

$$(\wedge\text{-negation}) \quad \neg(p \wedge q) \equiv (\neg p \vee \neg q)$$

$$(\vee\text{-negation}) \quad \neg(p \vee q) \equiv (\neg p \wedge \neg q)$$

$$(\vee \text{ commutativity}) \quad p \vee q \equiv q \vee p$$

$$(\vee \text{ associativity}) \quad (p \vee q) \vee r \equiv p \vee (q \vee r)$$

$$(\vee \text{ idempotency}) \quad p \vee p \equiv p$$

$$(\vee \text{ distributivity over } \equiv) \quad p \vee (q \equiv r) \equiv (p \vee q) \equiv (p \vee r)$$

$$(\text{excluded middle}) \quad p \vee \neg p \equiv \text{TRUE}$$

$$(\text{golden rule}) \quad p \wedge q \equiv p \equiv q \equiv p \vee q$$

$$(\Rightarrow \text{ definition}) \quad p \Rightarrow q \equiv p \vee q \equiv q$$

$$(\text{consequence}) \quad p \Leftarrow q \equiv q \Rightarrow p$$