Mathematics for Computer Science

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

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY
INESCTEC

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

Equational reasoning

Equivalence

$$
\begin{array}{rrcl}
(\equiv \text{ associativity}) & ((p \equiv q) \equiv r) & \equiv & (p \equiv (q \equiv r)) \\
(\equiv \text{ commutativity}) & p \equiv q & \equiv & q \equiv p \\
(\equiv \text{ identity}) & \text{TRUE} & \equiv & q \equiv q
\end{array}
$$

Equational reasoning

Negation

$$
\begin{array}{rrcl}
(\textsc{False definition}) & \textsc{False} & \equiv & \neg\textsc{True} \\
(\neg \text{ distributivity over } \equiv) & \neg(p \equiv q) & \equiv & \neg p \equiv q \\
(\not\equiv \text{ definition}) & (p \not\equiv q) & \equiv & \neg(p \equiv q)
\end{array}
$$

De Morgan laws – from the duality meta-theorem

$$
\begin{array}{rl}
(\wedge \text{ negation}) & \neg(p \wedge q) \equiv (\neg p \vee \neg q) \\
(\vee \text{ negation}) & \neg(p \vee q) \equiv (\neg p \wedge \neg q)
\end{array}
$$

Equational reasoning

Disjunction

$$
\begin{aligned}
(\vee \text{ commutativity}) \quad & p \vee q \ \equiv \ q \vee p \\
(\vee \text{ associativity}) \quad & (p \vee q) \vee r \ \equiv \ p \vee (q \vee r) \\
(\vee \text{ idempotency}) \quad & p \vee p \ \equiv \ p \\
(\vee \text{ distributivity over } \equiv) \quad & p \vee (q \equiv r) \ \equiv \ (p \vee q) \equiv (p \vee r) \\
(\text{excluded middle}) \quad & p \vee \neg p \ \equiv \ \textsc{True}
\end{aligned}
$$

Equational reasoning

Conjunction

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

Equational reasoning

Implication

$$
\begin{array}{lrcl}
(\Rightarrow \text{definition}) & p \Rightarrow q & \equiv & p \vee q \equiv q \\
(\text{consequence}) & p \Leftarrow q & \equiv & q \Rightarrow p
\end{array}
$$

Example

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

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

$=$ $\{ \quad \equiv \text{ associativity, commutativity} \quad \}$

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

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

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

$=$ $\{ \quad \equiv \text{ identity, } \text{FALSE definition} \}$

$\text{FALSE} \equiv \text{FALSE}$

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

TRUE

Example

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

$p \vee \text{TRUE}$

$=$ $\{ \ \equiv$ identity $\}$

$p \vee (p \equiv p)$

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

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

$=$ $\{ \ \equiv$ identity $\}$

TRUE

Example

$$p \lor q \equiv p \lor \neg q \equiv p$$

$$p \lor q \equiv p \lor \neg q \equiv p$$

$= \qquad \{\ \lor \text{ distributivity over } \equiv\ \}$

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

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

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

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

$$p \equiv p$$

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

$$\text{TRUE}$$

Example

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

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

$=$ $\{$ golden rule $\}$

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

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

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

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

$p \equiv \neg p \vee q$

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

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

$=$ $\{$ golden rule $\}$

$p \wedge q$

Example

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

$(p \wedge q) \wedge r$

$=$ $\{$ golden rule $\}$

$(p \equiv q \equiv p \vee q) \wedge r$

$=$ $\{$ golden rule $\}$

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

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

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

$=$ $\{$ $\equiv$ associativity, commutativity $\}$

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

Example

(cont)

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

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

$$(q \wedge r) \equiv p \equiv p \vee q \equiv p \vee r \equiv p \vee q \vee r$$

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

$$(q \wedge r) \equiv p \equiv p \vee q \equiv p \vee (r \equiv q \vee r)$$

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

$$(q \wedge r) \equiv p \equiv p \vee (q \equiv r \equiv q \vee r)$$

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

$$(q \wedge r) \equiv p \equiv p \vee (q \wedge r)$$

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

$$p \wedge (q \wedge r)$$

Example

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

$p \Rightarrow q \equiv p \wedge q \equiv p$

$=$ $\{ \ \Rightarrow \text{definition} \ \}$

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

$=$ $\{ \ \equiv \text{associativity, commutativity} \}$

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

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

$p \wedge q \equiv p \wedge q$

Example (another proof technique)

$$\boxed{\text{Theorem: } (p \Rightarrow q) \Rightarrow p \vee r \Rightarrow q \vee r}$$

$p \vee r \Rightarrow q \vee r$

$=$ $\{ \ \Rightarrow \text{ definition } \}$

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

$=$ $\{ \ \vee \text{ idempotency, } \equiv \text{ associativity, commutativity} \}$

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

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

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

$\Leftarrow$ $\{ \ \text{weakning: } p \Rightarrow p \vee q \ \}$

$p \vee q \equiv q$

$=$ $\{ \ \Rightarrow \text{ definition } \}$

$p \Rightarrow q$

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

$(p \Rightarrow q) \wedge (q \Rightarrow p)$

$=$ { $\Rightarrow$ alternative definition }

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

$=$ { $\wedge, \vee$ distributivity }

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

$=$ { $\wedge, \vee$ distributivity }

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

$=$ { $a \wedge \neg a \equiv \text{FALSE}, \ a \vee \text{FALSE} \equiv a$ }

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

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

$p \equiv q$

Resolution

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

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

$=$ { golden rule }

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

$=$ { $\vee$ distributivity }

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

$=$ { de Morgan }

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

$=$ { excluded middle, $\equiv$ identity }

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

$=$ { $\vee$ distributivity }

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

Resolution

(**cont**)

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

= $\quad\{ \ \wedge, \vee \text{ distributivity } \}$

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

= $\quad\{ \text{ excluded middle, } \text{TRUE} \wedge a \equiv a \ \}$

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

= $\quad\{ \text{ theorem: } a \vee b \equiv a \vee \neg b \equiv a \ \}$

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

= $\quad\{ \ \wedge, \vee \text{ distributivity } \}$

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

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

$$q \equiv p$$

Resolution

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

$\neg(p \wedge q)$

$=\qquad \{$ golden rule $\}$

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

$=\qquad \{$ $\neg$ distributivity $\}$

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

$=\qquad \{$ $a \vee \text{FALSE} \equiv a$ $\}$

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

$=\qquad \{$ $\vee$ distributivity $\}$

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

$=\qquad \{$ $\neg a \equiv (\text{FALSE} \equiv a)$ $\}$

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

Resolution

(**cont**)

$$\neg q \equiv \neg q \lor p$$

$$= \qquad \{ \quad a \lor \text{FALSE} \equiv a \ \}$$

$$\neg q \lor \text{FALSE} \equiv \neg q \lor p$$

$$= \qquad \{ \quad \lor \text{ distributivity } \}$$

$$\neg q \lor (\text{FALSE} \equiv p)$$

$$= \qquad \{ \ \neg a \equiv (\text{FALSE} \equiv a) \ \}$$

$$\neg q \lor \neg p$$

($\equiv$ associativity)	$((p \equiv q) \equiv r)$	$\equiv$	$(p \equiv (q \equiv r))$
($\equiv$ commutativity)	$p \equiv q$	$\equiv$	$q \equiv p$
($\equiv$ identity)	TRUE	$\equiv$	$q \equiv q$
(FALSE definition)	FALSE	$\equiv$	$\neg \text{TRUE}$
($\neg$ distributivity over $\equiv$)	$\neg(p \equiv q)$	$\equiv$	$\neg p \equiv q$
($\not\equiv$ definition)	$(p \not\equiv q)$	$\equiv$	$\neg(p \equiv q)$
($\wedge$ negation)	$\neg(p \wedge q)$	$\equiv$	$(\neg p \vee \neg q)$
($\vee$ negation)	$\neg(p \vee q)$	$\equiv$	$(\neg p \wedge \neg q)$
($\vee$ commutativity)	$p \vee q$	$\equiv$	$q \vee p$
($\vee$ associativity)	$(p \vee q) \vee r$	$\equiv$	$p \vee (q \vee r)$
($\vee$ idempotency)	$p \vee p$	$\equiv$	p
($\vee$ distributivity over $\equiv$)	$p \vee (q \equiv r)$	$\equiv$	$(p \vee q) \equiv (p \vee r)$
(excluded middle)	$p \vee \neg p$	$\equiv$	TRUE
(golden rule)	$p \wedge q$	$\equiv$	$p \equiv q \equiv p \vee q$
($\Rightarrow$ definition)	$p \Rightarrow q$	$\equiv$	$p \vee q \equiv q$
(consequence)	$p \Leftarrow q$	$\equiv$	$q \Rightarrow p$