Mathematics for Computer Science

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

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

$$
\begin{aligned}
(\equiv \text{ associativity}) \qquad & ((p \equiv q) \equiv r) \quad \equiv \quad (p \equiv (q \equiv r)) \\
(\equiv \text{ commutativity}) \qquad & p \equiv q \quad \equiv \quad q \equiv p \\
(\equiv \text{ identity}) \qquad & \textsc{True} \quad \equiv \quad q \equiv q
\end{aligned}
$$

Equational reasoning

Negation

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

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

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

Equational reasoning

Conjunction

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

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

$$\boxed{\text{Theorem: } \neg p \equiv q \equiv p \equiv \neg q}$$

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

Example

$\boxed{\text{Theorem: } p \vee \textsc{True} \equiv \textsc{True}}$

$$
\begin{array}{ll}
 & p \vee \textsc{True} \\
= & \quad \{ \equiv \text{identity} \} \\
 & p \vee (p \equiv p) \\
= & \quad \{ \vee \text{ distributivity over } \equiv \} \\
 & p \vee p \equiv p \vee p \\
= & \quad \{ \equiv \text{identity} \} \\
 & \textsc{True}
\end{array}
$$

Example

$$\boxed{\text{Theorem: } p \vee q \equiv p \vee \neg q \equiv p}$$

$$
\begin{array}{ll}
 & p \vee q \equiv p \vee \neg q \equiv p \\
= & \quad \{ \ \vee \text{ distributivity over } \equiv \ \} \\
 & p \vee (q \equiv \neg q) \equiv p \\
= & \quad \{ \ \neg \text{ distributivity over } \equiv \ \} \\
 & p \vee \textsc{False} \equiv p \\
= & \quad \{ \ \text{theorem - exercise below} \ \} \\
 & p \equiv p \\
= & \quad \{ \ \equiv \text{ identity} \ \} \\
 & \textsc{True}
\end{array}
$$

Example

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

$$\begin{array}{ll}
& p \wedge (\neg p \vee q) \\
= & \quad \{ \text{ golden rule } \} \\
& p \equiv \neg p \vee q \equiv p \vee \neg p \vee q \\
= & \quad \{ \equiv \text{ associativity, excluded middle } \} \\
& p \equiv \neg p \vee q \equiv \textsc{True} \vee q \\
= & \quad \{ \text{ theorem above: } p \vee \textsc{True} \equiv \textsc{True} \} \\
& p \equiv \neg p \vee q \\
= & \quad \{ \text{ theorem above: } p \vee q \equiv p \vee \neg q \equiv p \} \\
& p \equiv p \vee q \equiv q \\
= & \quad \{ \text{ golden rule } \} \\
& p \wedge q
\end{array}$$

Example

$$\boxed{\text{Theorem: } (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)}$$

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

Example

(cont)

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

Example

$$\boxed{\text{Theorem: } p \Rightarrow q \equiv p \wedge q \equiv p}$$

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

Example (another proof technique)

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

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

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

$$\boxed{\text{Theorem: } (p \Rightarrow q) \wedge (q \Rightarrow p) \equiv p \equiv q}$$

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

Resolution

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

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

Resolution

(cont)

$$
\begin{array}{ll}
 & (\neg p \vee (p \wedge q)) \equiv (\neg q \vee (p \wedge q)) \\
= & \quad \{\ \wedge, \vee \text{ distributivity } \} \\
 & (\neg p \vee p) \wedge (\neg p \vee q) \equiv (\neg q \vee p) \wedge (\neg q \vee q) \\
= & \quad \{ \text{ excluded middle, } \textsc{True} \wedge a \equiv a \ \} \\
 & (\neg p \vee q) \equiv (\neg q \vee p) \\
= & \quad \{ \text{ theorem: } a \vee b \equiv a \vee \neg b \equiv a \ \} \\
 & (\neg p \vee q) \equiv (q \vee p) \equiv p \\
= & \quad \{\ \wedge, \vee \text{ distributivity } \} \\
 & q \equiv (p \vee \neg p) \equiv p \\
= & \quad \{\ \text{excluded middle, } \equiv \text{ identity } \} \\
 & q \equiv p
\end{array}
$$

Resolution

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

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

Resolution

(cont)

$$
\begin{aligned}
& \neg q \equiv \neg q \vee p \\
= \quad & \{ \; a \vee \textsc{False} \equiv a \; \} \\
& \neg q \vee \textsc{False} \equiv \neg q \vee p \\
= \quad & \{ \; \vee \text{ distributivity } \} \\
& \neg q \vee (\textsc{False} \equiv p) \\
= \quad & \{ \; \neg a \equiv (\textsc{False} \equiv a) \; \} \\
& \neg q \vee \neg p
\end{aligned}
$$

$$
\begin{array}{rrcl}
(\equiv \text{ associativity}) & ((p \equiv q) \equiv r) & \equiv & (p \equiv (q \equiv r)) \\
(\equiv \text{ commutativity}) & p \equiv q & \equiv & q \equiv p \\
(\equiv \text{ identity}) & \textsc{True} & \equiv & q \equiv q \\
(\textsc{False} \text{ definition}) & \textsc{False} & \equiv & \neg\textsc{True} \\
(\neg \text{ distributivity over } \equiv) & \neg(p \equiv q) & \equiv & \neg p \equiv q \\
(\not\equiv \text{ definition}) & (p \not\equiv q) & \equiv & \neg(p \equiv q) \\
(\wedge \text{ negation}) & \neg(p \wedge q) & \equiv & (\neg p \vee \neg q) \\
(\vee \text{ negation}) & \neg(p \vee q) & \equiv & (\neg p \wedge \neg q) \\
(\vee \text{ commutativity}) & p \vee q & \equiv & q \vee p \\
(\vee \text{ associativity}) & (p \vee q) \vee r & \equiv & p \vee (q \vee r) \\
(\vee \text{ idempotency}) & p \vee p & \equiv & p \\
(\vee \text{ distributivity over } \equiv) & p \vee (q \equiv r) & \equiv & (p \vee q) \equiv (p \vee r) \\
(\text{excluded middle}) & p \vee \neg p & \equiv & \textsc{True} \\
(\text{golden rule}) & p \wedge q & \equiv & p \equiv q \equiv p \vee q \\
(\Rightarrow \text{ definition}) & p \Rightarrow q & \equiv & p \vee q \equiv q \\
(\text{consequence}) & p \Leftarrow q & \equiv & q \Rightarrow p
\end{array}
$$