Lecture 7
CS 1813 – Discrete Mathematics

Equational Reasoning

Back to the Future: High-School Algebra

Some Laws of Algebra

- $a + 0 = a$ {+ identity}
- $(-a) + a = 0$ {+ complement}
- $a \times 1 = a$ {× identity}
- $a \times 0 = 0$ {× null}
- $a + b = b + a$ {+ commutative}
- $a + (b+c) = (a+b) + c$ {+ associative}
- $a \times (b+c) = a \times b + a \times c$ {distributive law}

Equations go both ways

Theorem $(-1) \times (-1) = 1$

$$
\begin{aligned}
& (-1) \times (-1) \\
= \; & ((-1) \times (-1)) + 0 && \{+ \text{ id}\} \\
= \; & ((-1) \times (-1)) + ((-1) + 1) && \{+ \text{ comp}\} \\
= \; & (((-1)\times(-1)) + (-1)) + 1 && \{+ \text{ assoc}\} \\
= \; & (((-1)\times(-1)) + (-1)\times 1) + 1 && \{\times \text{ id}\} \\
= \; & ((-1)\times((-1) + 1)) + 1 && \{\text{dist law}\} \\
= \; & ((-1)\times 0) + 1 && \{+ \text{ comp}\} \\
= \; & 0 + 1 && \{\times \text{ null}\} \\
= \; & 1 + 0 && \{+ \text{ comm}\} \\
= \; & 1 && \{+ \text{ id}\}
\end{aligned}
$$

QED

proof by equational reasoning

Laws of Boolean Algebra

page 1

$a \wedge \text{False}$	$=$	False	{$\wedge$ null}
$a \vee \text{True}$	$=$	True	{$\vee$ null}
$a \wedge \text{True}$	$=$	a	{$\wedge$ identity}
$a \vee \text{False}$	$=$	a	{$\vee$ identity}
a	$\rightarrow$	$a \vee b$	{disjunctive implication}
$a \wedge b$	$\rightarrow$	a	{conjunctive implication}
$a \wedge a$	$=$	a	{$\wedge$ idempotent}
$a \vee a$	$=$	a	{$\vee$ idempotent}
$a \wedge b$	$=$	$b \wedge a$	{$\wedge$ commutative}
$a \vee b$	$=$	$b \vee a$	{$\vee$ commutative}
$(a \wedge b) \wedge c$	$=$	$a \wedge (b \wedge c)$	{$\wedge$ associative}
$(a \vee b) \vee c$	$=$	$a \vee (b \vee c)$	{$\vee$ associative}
$a \wedge (b \vee c)$	$=$	$(a \wedge b) \vee (a \wedge c)$	{$\wedge$ distributes over $\vee$}
$a \vee (b \wedge c)$	$=$	$(a \vee b) \wedge (a \vee c)$	{$\vee$ distributes over $\wedge$}
$\neg(a \wedge b)$	$=$	$\neg a \vee \neg b$	{DeMorgan's law}
$\neg(a \vee b)$	$=$	$\neg a \wedge \neg b$	{DeMorgan's law}

From Fig 2.1, Hall & O'Donnell, *Discrete Math with a Computer*, Springer, 2000

Laws of Boolean Algebra

page 2

$\neg$True	=	False	{negate True}
$\neg$False	=	True	{negate False}
$a \wedge \neg a$	=	False	{$\wedge$ complement}
$a \vee \neg a$	=	True	{$\vee$ complement}
$\neg(\neg a)$	=	a	{double negation}
$a \wedge (a \rightarrow b)$	$\rightarrow$	b	{*Modus Ponens*}
$(a \rightarrow b) \wedge \neg b$	$\rightarrow$	$\neg a$	{*Modus Tollens*}
$(a \vee b) \wedge \neg a$	$\rightarrow$	b	{disjunctive syllogism}
$(a \rightarrow b) \wedge (b \rightarrow c)$	$\rightarrow$	$a \rightarrow c$	{implication chain}
$(a \rightarrow b) \wedge (c \rightarrow d)$	$\rightarrow$	$(a \wedge c) \rightarrow (b \wedge d)$	{implication combination}
$(a \wedge b) \rightarrow c$	=	$a \rightarrow (b \rightarrow c)$	{Currying}
$a \rightarrow b$	=	$\neg a \vee b$	{implication}
$a \rightarrow b$	=	$\neg b \rightarrow \neg a$	{contrapositive}
$(a \rightarrow b) \wedge (a \rightarrow \neg b)$	=	$\neg a$	{absurdity}
$a \leftrightarrow b$	=	$(a \rightarrow b) \wedge (b \rightarrow a)$	{equivalence}

From Fig 2.1, Hall & O'Donnell, *Discrete Math with a Computer*, Springer, 2000

Theorem $(a \wedge \text{False}) \vee (b \wedge \text{True}) = b$

equations	{*rule*} *substitution* [*formula in eqn / variable in rule*]
$(p \wedge \text{False}) \vee (q \wedge \text{True})$	names changed to clarify substitutions
$= \text{False} \vee (q \wedge \text{True})$	$\{\wedge$ null$\}$ [p /a]
$= (q \wedge \text{True}) \vee \text{False}$	$\{\vee$ comm$\}$ [False /a] [q$\wedge$True /b]
$= q \wedge \text{True}$	$\{\vee$ id$\}$ [q $\wedge$ True /a]
$= q$	$\{\wedge$ id$\}$ [q /a]

QED

Using Equational Proof Checker

Importing tools

```
import Stdm

th7 = (P `And` FALSE)  `Or`
                        ( Q  `And` TRUE)
        `thmEq`  Q

pr7 =
  startProof ((P `And` FALSE) `Or`
                        (Q `And` TRUE))
  <-> (FALSE `Or` (Q `And` TRUE),
                                andNull)
  <-> ((Q `And` TRUE) `Or` FALSE,
                                orComm)
  <-> (Q `And` TRUE,            orID)
  <-> (Q,                       andID)
```

Notepad window

Green indicates cmd from user

```
Prelude> :cd DMf00
Prelude> :cd Lectures
Prelude> :load lecture07.hs
Reading file "lecture07.hs":
Reading file "Stdm.lhs":
Reading file "lecture07.hs":

Hugs session for:
C:\HUGS98\lib\Prelude.hs
Stdm.lhs
lecture07.hs
Main> check_equation th7 pr7
The proof is correct
```

Hugs Session

Equations the Proof Checker Knows

andNull
orNull
andID
orID
andIdempotent
orIdempotent
andComm
orComm
andAssoc
orAssoc
andDistOverOr
orDistOverAnd

deMorgansLawAnd
deMorgansLawOr

negTrue
negFalse
andCompl
orCompl
dblNeg

currying
implication
contrapositive
absurdity

Theorem $(a \wedge b) \vee b = b$

$\vee$ ***absorption***

equations	{*rule*} *substitution* [*formula in eqn / variable in rule*]
$(p \wedge q) \vee q$	names changed to clarify substitutions
$= (p \wedge q) \vee (q \wedge \text{True})$	{$\wedge$ id} [q /a]
$= (q \wedge p) \vee (q \wedge \text{True})$	{$\wedge$ comm} [p /a] [q /b]
$= q \wedge (p \vee \text{True})$	{$\wedge$ dist over $\vee$} [q /a] [True /b] [p /c]
$= q \wedge \text{True}$	{$\vee$ null} [p /a]
$= q$	{$\wedge$ id} [q/a]

QED

Theorem $(a \vee b) \wedge b = b$

$\wedge$ **absorption**

equations {*rule*} *substitution* [*formula in eqn / variable in rule*]

$(p \vee q) \wedge q$ names changed to clarify substitutions

… exercise …

$= q$

Consistent, But Not Minimal

redundancy among laws of Boolean algebra

Deriving the contrapositive law

Theorem (contrapositive): $a \to b \;=\; \neg b \to \neg a$

A proof using laws other than the contrapositive law

equations	{*rule*}	*substitution* [*formula in eqn / variable in rule*]
$p \to q$		
$= (\neg p) \vee q$		{imp} [p /a] [q /b]
$= \neg(\neg((\neg p) \vee q))$		{dbl neg} [$(\neg p) \vee q$ /a]
$= \neg((\neg(\neg p)) \wedge (\neg q))$		{DeMorgan $\vee$} [$\neg p$ /a] [q /b]
$= \neg(p \wedge (\neg q))$		{dbl neg} [p /a]
$= (\neg p) \vee (\neg(\neg q))$		{DeMorgan $\wedge$} [p /a] [$\neg q$ /b]
$= (\neg(\neg q)) \vee (\neg p)$		{$\vee$ comm} [$\neg p$ /a] [$\neg(\neg(q))$ /b]
$= (\neg q) \to (\neg p)$		{imp} [$\neg q$ /a] [$\neg p$ /b]

This proof is sloppy!
Where's the shortcut?

QED

End of Lecture 7