A Logical Approach to Discrete Math

Propositional Calculus

Proposition: A declarative statement that is either true or false.

Axiom: A Boolean expression that defines the properties of boolean operators. Axioms are never proved. They are assumed to be valid.

Theorem: Either (1) an axiom, or (2) a theorem that is proved equal to an axiom or a previously proved theorem. All theorems are valid.

(3.1) **Axiom, Associativity of $\equiv$:** $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$

Allows us to write $p \equiv q \equiv r$

instead of $(p \equiv q) \equiv r$ or $p \equiv (q \equiv r)$

(3.2) **Axiom, Symmetry of $\equiv$:** $p \equiv q \equiv q \equiv p$

Can put ( ) anywhere

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

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

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

(3.2) **Axiom, Symmetry of $\equiv$:** $p \equiv q \equiv q \equiv p$

Prove $p \equiv p \equiv q \equiv q$

Proof

$$
\begin{array}{ll}
 & p \equiv p \equiv q \equiv q \\
= & \langle (3.2)\ (p \equiv q \equiv q) \equiv p \rangle \\
 & p \equiv p \\
= & \langle (3.2)\ (p \equiv q \equiv q) \equiv p \rangle \\
 & p \equiv q \equiv q \equiv p
\end{array}
$$

which is (3.2) //

(3.3) **Axiom, Identity of $\equiv$:** $true \equiv q \equiv q$

If $\star$ is a binary infix operator, the identity of $\star$ is the constant i such that $x \star i = x$.

1 is the identity of multiplication because $x \cdot 1 = x$.
0 is the identity of addition because $x + 0 = x$.
$true$ is the identity of $\equiv$ because $p \equiv true \equiv p$.

$$(3.4) \qquad true$$

Proof

$$\begin{array}{ll} & true \\ = & \langle (3.3) \text{ with } p := true, \quad true \equiv true \equiv true \rangle \\ & true \equiv true \\ = & \langle (3.3)\ true \equiv q \equiv q \rangle \\ & true \equiv q \equiv q \end{array}$$

which is (3.3) //

A Logical Approach to Discrete Math

Textual substitution

$$E[z := F]$$

↑ Must be a variable

$E[q := true]$ Legal, q is a variable.

$E[true := q]$ Illegal, $true$ is not a variable.

$E[q := q \wedge p]$ Legal, q is a variable.

$E[q \wedge p := q]$ Illegal, $q \wedge p$ is not a variable.

(3.6) **Proof method.** To prove that $P \equiv Q$ is a theorem, transform P to Q or Q to P using Leibniz.

A Logical Approach to Discrete Math

Now consider the following two proofs of (3.15), $\neg p \equiv p \equiv false$.

$$
\begin{array}{ll}
 & \neg p \equiv p \equiv false \\
= & \quad \langle (3.9),\ \neg(p \equiv q) \ \equiv\ \neg p \equiv q \text{, with } q := p \rangle \\
 & \neg(p \equiv p) \equiv false \\
= & \quad \langle \text{Identity of } \equiv \ (3.3) \text{, with } q := p \rangle \\
 & \neg true \equiv false \qquad \text{—theorem } (3.8)
\end{array}
$$

$$
\begin{array}{ll}
 & \neg p \equiv p \\
= & \quad \langle (3.9),\ \neg(p \equiv q) \ \equiv\ \neg p \equiv q \text{, with } q := p \rangle \\
 & \neg(p \equiv p) \\
= & \quad \langle \text{Identity of } \equiv \ (3.3) \text{, with } q := p \rangle \\
 & \neg true \\
= & \quad \langle (3.8) \rangle \\
 & false
\end{array}
$$

(3.22) **Principle:** Structure proofs to avoid repeating the same subexpression on many lines.

(3.23) **Heuristic of Definition Elimination:** To prove a theorem concerning an operator $\circ$ that is defined in terms of another, say $\bullet$, expand the definition of $\circ$ to arrive at a formula that contains $\bullet$; exploit properties of $\bullet$ to manipulate the formula; and then (possibly) reintroduce $\circ$ using its definition.

To illustrate the use of this heuristic, we prove (3.16), $(p \not\equiv q) \equiv (q \not\equiv p)$. Here, $\circ$ is $\not\equiv$ and $\bullet$ is $\equiv$.

$$
\begin{array}{ll}
 & p \not\equiv q \\
= & \quad \langle \text{Def. of } \not\equiv \ (3.10) \rangle \\
 & \neg(p \equiv q) \\
= & \quad \langle \text{Symmetry of } \equiv \ (3.2) \rangle \\
 & \neg(q \equiv p) \\
= & \quad \langle \text{Def. of } \not\equiv \ (3.10), \text{ with } p, q := q, p \rangle \\
 & q \not\equiv p
\end{array}
$$

A Logical Approach to Discrete Math

(3.33) **Heuristic:** To prove $P \equiv Q$, transform the expression with the most structure (either P or Q) into the other.

Prove (3.29) $\quad p \vee true \equiv true$

Which side do you start with?

The side with the most structure, the left hand side.

Proof

$$
\begin{array}{ll}
 & p \vee true \\
= & \langle (3.3) \text{ with } q := p \rangle \\
 & p \vee (p \equiv p) \\
= & \langle (3.27) \text{ with } q, r := p, p \rangle \\
 & p \vee p \equiv p \vee p \\
= & \langle (3.3) \text{ with } q := p \vee p \rangle \\
 & true \text{ //}
\end{array}
$$

Prove (3.29) $p \vee true \equiv true$

It is more difficult to start with the right hand side.

Proof

$$
\begin{array}{ll}
 & true \\
= & \langle (3.3) \text{ with } q := p \vee p \rangle \\
 & p \vee p \equiv p \vee p \\
= & \langle (3.27) \text{ with } q, r := p, p \rangle \\
 & p \vee (p \equiv p) \\
= & \langle (3.3) \text{ with } q := p \rangle \\
 & p \vee true \; //
\end{array}
$$

Prove (3.29) $\quad p \vee true \equiv true$

It is more difficult to start with the right hand side.

Proof

$$
\begin{array}{ll}
 & true \\
= & \langle (3.3) \text{ with } q := p \vee p \rangle \\
 & p \vee p \equiv p \vee p \\
= & \langle (3.27) \text{ with } q, r := p, p \rangle \\
 & p \vee (p \equiv p) \\
= & \langle (3.3) \text{ with } q := p \rangle \\
 & p \vee true \ //
\end{array}
$$

(3.34) **Principle:** Structure proofs to minimize the number of rabbits pulled out of a hat —make each step seem obvious, based on the structure of the expression and the goal of the manipulation.

(3.35) **Axiom, Golden rule:** $p \wedge q \equiv p \equiv q \equiv p \vee q$

Defines conjunction in terms of disjunction.

(3.35) **Axiom, Golden rule:** $p \wedge q \ \equiv \ p \ \equiv \ q \ \equiv \ p \vee q$

Prove (3.39) Identity of $\wedge$: $p \wedge true \equiv p$

Proof

$p \wedge true \equiv p$

$=$ $\langle$(3.35) with $q := true$, $p \wedge true \equiv p \equiv true \equiv p \vee true\rangle$

$true \equiv p \vee true$

$=$ $\langle$(3.2) Symmetry of $\equiv\rangle$

$p \vee true \equiv true$

which is (3.29) Zero of $\vee$ //

(3.35) **Axiom, Golden rule:** $p \wedge q \equiv p \equiv q \equiv p \vee q$

Prove (3.42) $p \wedge \neg p \equiv false$

Proof

$$
\begin{array}{ll}
 & p \wedge \neg p \\
= & \langle (3.35) \text{ with } q := \neg p \rangle \\
 & p \equiv \neg p \equiv p \vee \neg p \\
= & \langle (3.2) \text{ Symmetry of } \equiv \rangle \\
 & \neg p \equiv p \equiv p \vee \neg p \\
= & \langle (3.15) \rangle \\
 & false \equiv p \vee \neg p \\
= & \langle (3.28) \text{ Excluded middle} \rangle \\
 & false \equiv true \\
= & \langle (3.3) \text{ with } q := false \rangle \\
 & false \ //
\end{array}
$$

(3.61) **Contrapositive:** $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

The converse of $p \Rightarrow q$ is $q \Rightarrow p$.

An implication is **not** equivalent to its converse.

The contrapositive of $p \Rightarrow q$ is $\neg q \Rightarrow \neg p$.

An implication **is** equivalent to its contrapositive.

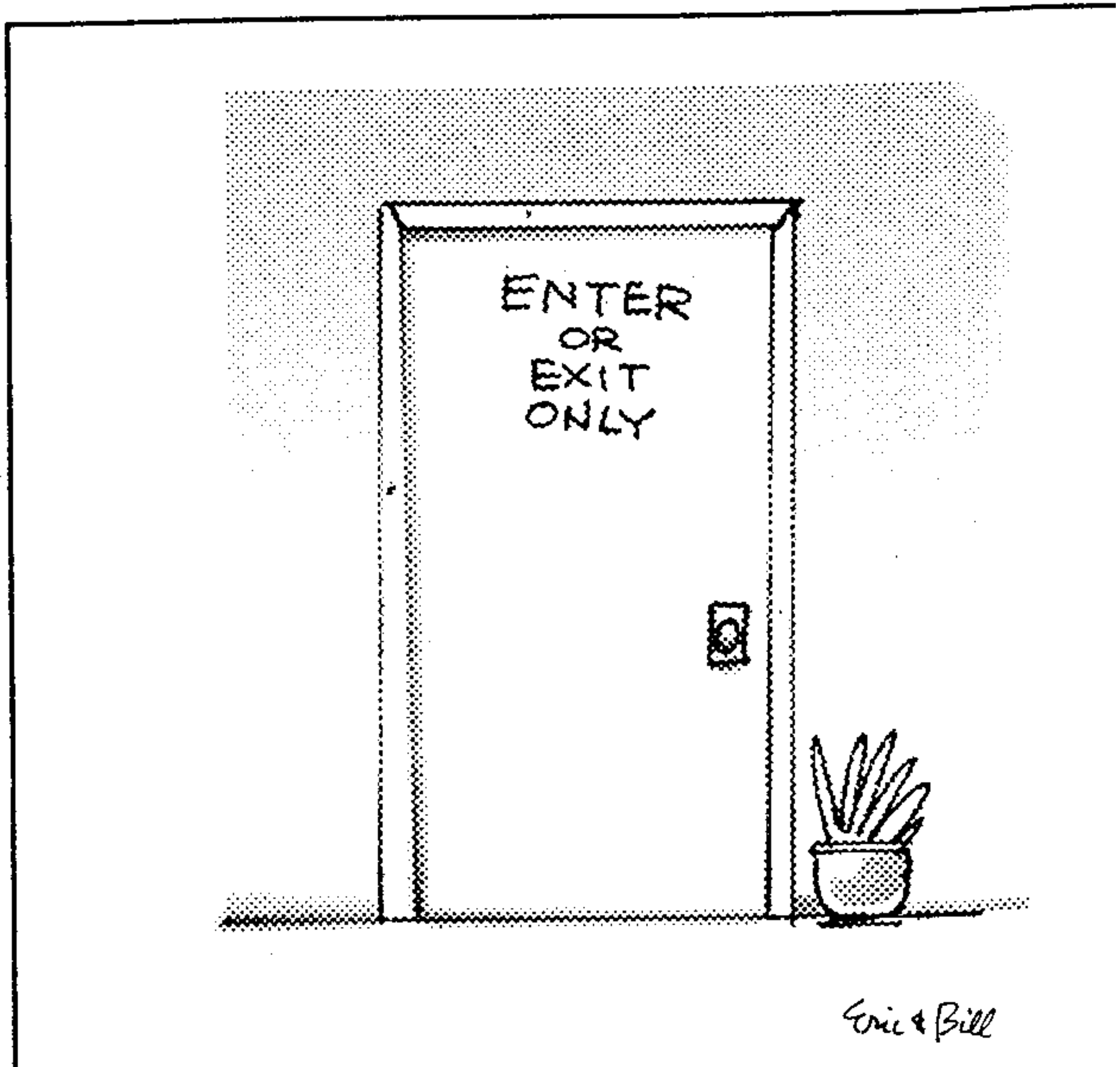
A Logical Approach to Discrete Math

Axiom

Excluded Middle

$$p \vee \neg p$$

BOTTOM LINERS By Eric and Bill Teitelbaum



©1993 Tribune Media Services, Inc.
All Rights Reserved

A Logical Approach to Discrete Math

WARPED By Mike Cavna

3.33 Proof of De Morgan's second law, (3.47b), beginning with the LHS.

$$
\begin{array}{ll}
 & \neg(p \lor q) \\
= & \quad \langle \text{Golden rule (3.35)} \rangle \\
 & \neg(p \equiv q \equiv p \land q) \\
= & \quad \langle \text{Distributivity of } \neg \text{ over } \equiv \text{ (3.9)} \rangle \\
 & \neg p \equiv q \equiv p \land q \\
= & \quad \langle \text{Golden rule (3.35)} \rangle \\
 & \neg p \equiv p \equiv p \lor q \\
= & \quad \langle (3.32),\ p \lor q \equiv p \lor \neg q \equiv p \rangle \\
 & \neg p \equiv p \lor \neg q \\
= & \quad \langle (3.32),\ p \lor q \equiv p \lor \neg q \equiv p \text{, with } p, q := \neg q, \neg p \rangle \\
 & \neg p \equiv \neg q \lor \neg p \equiv \neg q \\
= & \quad \langle \text{Golden rule (3.35)} \rangle \\
 & \neg p \land \neg q
\end{array}
$$

A Logical Approach to Discrete Math

Here is a second proof, which is one step, shorter.

$$\begin{array}{ll}
 & \neg(p \vee q) \\
= & \quad \langle \text{Golden rule (3.35)} \rangle \\
 & \neg(p \equiv q \equiv p \wedge q) \\
= & \quad \langle \text{Distributivity of } \neg \text{ over } \equiv \text{ (3.9)} \rangle \\
 & p \equiv q \equiv \neg(p \wedge q) \\
= & \quad \langle \text{De Morgan (3.47a)} \rangle \\
 & p \equiv q \equiv \neg p \vee \neg q \\
= & \quad \langle \text{(3.11)}, \ \neg p \equiv q \equiv p \equiv \neg q \ \rangle \\
 & \neg p \equiv \neg q \equiv \neg p \vee \neg q \\
= & \quad \langle \text{Golden rule (3.35)} \rangle \\
 & \neg p \wedge \neg q
\end{array}$$

A Logical Approach to Discrete Math

Finally, we present a third proof of second De Morgan's law, which is due to Andres A
student at Pepperdine (September 1993).

$$
\begin{array}{ll}
 & \neg(p \vee q) \\
= & \quad \langle \text{Double negation (3.12), twice} \rangle \\
 & \neg(\neg\neg p \vee \neg\neg q) \\
= & \quad \langle \text{De Morgan (3.47a)} \rangle \\
 & \neg\neg(\neg p \wedge \neg q) \\
= & \quad \langle \text{Double negation (3.12)} \rangle \\
 & \neg p \wedge \neg q
\end{array}
$$

Leibniz as an axiom.

This section uses the following notation: E^z_X means $E[z := X]$.

(3.83) **Axiom, Leibniz:** $e = f \Rightarrow E^z_e = E^z_f$

Inference Rule Leibniz: $$\frac{X = Y}{E[z := X] = E[z := Y]}$$

Inference Rule Leibniz: $$\frac{X = Y}{E^z_X = E^z_Y}$$

Leibniz as an axiom.

This section uses the following notation: E_X^z means $E[z := X]$.

(3.83) **Axiom, Leibniz:** $e = f \Rightarrow E_e^z = E_f^z$

Example

$E: \quad x \wedge z$

$e = f \Rightarrow (x \wedge e) = (x \wedge f)$

(3.83) **Axiom, Leibniz:** $e = f \Rightarrow E_e^z = E_f^z$

Prove (3.84a) $(e = f) \wedge E_e^z \equiv (e = f) \wedge E_f^z$

Proof

$$(e = f) \wedge E_e^z \equiv (e = f) \wedge E_f^z$$

$=$ $\langle$(3.62)$\rangle$

$$(e = f) \Rightarrow (E_e^z \equiv E_f^z)$$

$=$ $\langle$Replace $\equiv$ with **=** $\rangle$

$$(e = f) \Rightarrow (E_e^z = E_f^z)$$

$=$ $\langle$remove unnecessary parentheses$\rangle$

$$e = f \Rightarrow E_e^z = E_f^z$$

which is (3.83) //