CMPSCI 250: Introduction to Computation

Lecture #4: Rules for Propositional Proofs
David Mix Barrington
11 September 2013

Rules for Propositional Proofs

- Equations in Algebra
- Equational Sequence Proofs
- Where Do the Rules Come From?
- Deductive Sequence Proofs
- When Can You Substitute?
- Some Equational Rules
- Some Implication Rules

Equations in Algebra

- Since your high school mathematics career you have been carrying out a sort of mathematical proof. In algebra, you often show two things (such as polynomials) to be equal by a series of steps, each justified by a rule:

$(x + 3)^2 =$	
$(x + 3)(x + 3) =$	Definition of squaring
$x(x + 3) + 3(x + 3) =$	Distributive law
$(x^2 + 3x) + (3x + 9) =$	Distributive law
$x^2 + (3x + 3x) + 9 =$	Associative law
$x^2 + 6x + 9$	

Algebraic Derivations

- If every step is justified, the expressions on every line are all equal, and thus the first one is equal to last one.
- If you make a mistake at any point in the process, of course, the derivation is invalid and you might well derive something that is false.
- You need to know the rules, and make good choices as to what rules to use.

Equational Sequence Proofs

- An **equational sequence proof** is exactly the same thing with compound propositions -- a sequence of expressions, each of which comes from the previous one by using a rule.
- We have to learn new rules, which we'll list at the end of this lecture (see also section 1.7 of the book). Next lecture we'll talk more about the strategies we might use to choose the right rules to use.

Equational Sequence Example

- Here's an example of an equational sequence proof, for the statement we proved by truth tables in the last lecture:

(x ∧ ¬y) ∧ (y ∧ ¬x) ↔	
x ∧ (¬y ∧ y) ∧ ¬x ↔	Associativity of ∧
x ∧ ¬(y ∨ ¬y) ∧ ¬x ↔	DeMorgan ∧ to ∨
x ∧ ¬1 ∧ ¬x ↔	Excluded Middle
0	Left and Right 0 rules for ∧

Where Do Rules Come From?

- Any tautology may be used as a rule. If we want to use a rule repeatedly, it is worth the time to verify it with a truth table and then remember it.
- In particular, if we have a tautology of the form $P \leftrightarrow Q$, where P and Q are compound

  propositions using some atomic variables, we can **substitute** other compound propositions for the variables, and still get a tautology. This is often how we use a rule.

Clicker Question #1

- In a step of an equational proof we can change P to Q if P and Q are equivalent, meaning that $P \leftrightarrow Q$ is a tautology. Which of these statements is equivalent to $x \wedge \neg y$?
- (a) $\neg x \vee y$
- (b) $\neg y \wedge x$
- (c) $x \rightarrow y$
- (d) $\neg x \wedge y$

Answer #1

- In a step of an equational proof we can change P to Q if P and Q are equivalent, meaning that P ↔ Q is a tautology. Which of these statements is equivalent to $x \wedge \neg y$?
- (a) $\neg x \vee y$
- (b) $\neg y \wedge x$
- (c) $x \rightarrow y$
- (d) $\neg x \wedge y$

Substitution Example

- For example, since $(x \wedge y) \leftrightarrow (y \wedge x)$ is a tautology, we can substitute $a \oplus b$ for x and $b \rightarrow (a \vee c)$ for y.
- In this way we get a new tautology, $((a \oplus b) \wedge (b \rightarrow (a \vee c)) \leftrightarrow ((b \rightarrow (a \vee c)) \wedge (a \oplus b))$.

  So in a step of a proof, we could substitute one side of this equivalence for the other.

Deductive Sequence Proofs

- We often want to verify tautologies of the form $P \rightarrow C$, where P is the premise and C is the conclusion.
- We can do this with a deductive sequence proof, which is a sequence of compound propositions where each one implies the next.
- If we have a rule $X \rightarrow Y$, then if we have X in one step of our proof we can take Y as the next one.

Deductive Sequence Proofs

- We can also use multiple previous statements to justify a new step. If we have A, B, and C as previous steps, for example, and $(A \wedge B \wedge C) \rightarrow D$ is a rule, we can take D as our next step.
- If the premise (our first step) is true, the definition of $\rightarrow$ tells us that each of the other steps must be true, and thus that the conclusion is true.
- Deductive sequence steps are not reversible in the way equivalences are.

Deductive Sequence Example

- In this derivation we begin with the premise $x \wedge (x \rightarrow y)$ and derive the conclusion y. As it happens, each rule we use except the last one is an equivalence rule.
- This is like an inequality proof in algebra, where we may use both = and $\leq$ steps to get a $\leq$ conclusion.
- We will have proved $(x \wedge (x \rightarrow y)) \rightarrow y$, the **Modus Ponens** rule.

Deductive Sequence Example

- This is equational until the last step:

$x \wedge (x \rightarrow y) \leftrightarrow$	
$x \wedge (\neg x \vee y) \leftrightarrow$	Definition of $\rightarrow$
$(x \wedge \neg x) \vee (x \wedge y) \leftrightarrow$	Distribute $\wedge$ over $\vee$
$\neg(\neg x \vee x) \vee (x \wedge y) \leftrightarrow$	DeMorgan $\wedge$ to $\vee$
$\neg 1 \vee (x \wedge y) \leftrightarrow$	Excluded Middle
$0 \vee (x \wedge y) \leftrightarrow$	$\neg 1 = 0$
$x \wedge y \rightarrow$	Left Identity for $\vee$
y	Right Separation

Clicker Question #2

- We haven't learned the rules yet, but we can go from P to Q if Q *must* be true when P is. Which of these statements follows from x?
- (a) $(y \wedge z) \vee x$
- (b) $(y \wedge z) \oplus x$
- (c) $(y \wedge z) \wedge x$
- (d) $(y \wedge z) \leftrightarrow x$

Answer #2

- We haven't learned the rules yet, but we can go from P to Q if Q *must* be true when P is. Which of these statements follows from x?
- (a) $(y \wedge z) \vee x$
- (b) $(y \wedge z) \oplus x$
- (c) $(y \wedge z) \wedge x$
- (d) $(y \wedge z) \leftrightarrow x$

When Can You Substitute?

- If $P \leftrightarrow Q$ is a tautology, then we can replace P by Q in any context. This is because P and Q are true in exactly the same lines of the truth table.
- If $P \rightarrow Q$ is a tautology, we know that Q is true in every line of the truth table where P is true, but it may also be true in additional lines where P is false.

When Can You Substitute?

- If we know $P \rightarrow Q$, it's true that $(P \wedge R) \rightarrow (Q \wedge R)$ and that $(P \vee R) \rightarrow (Q \vee R)$.
- That means that we can change a P to a Q in a step of a derivation if the entire statement is built from P or Q by $\wedge$ and $\vee$ operations.
- For example, from $P \rightarrow Q$ we could take the statement $(P \wedge R) \vee (S \wedge P)$ and derive $(Q \wedge R) \vee (S \wedge Q)$.

When Can You Substitute?

- But look at the statements $P \oplus R$ and $Q \oplus R$. Even if $P \rightarrow Q$ is true, we could have a situation where $P \oplus R$ is true (because P is false and R is true) but yet $Q \oplus R$ is false (because both Q and R are true). So $(P \oplus R) \rightarrow (Q \oplus R)$ fails.
- The safest thing is to apply deductive rules only on the statement as a whole.

Some Equational Rules

- The operators $\wedge$, $\vee$, and $\oplus$ are **commutative** ($a \wedge b \leftrightarrow b \wedge a$) and **associative** ($a \wedge (b \wedge c) \leftrightarrow (a \wedge b) \wedge c$). But they are not associative with each other -- for example $(a \wedge b) \vee c \leftrightarrow a \wedge (b \vee c)$ is not valid.
- We also have special rules for these operator's behavior with 0 and 1.

Equational Rules: Definitions

- We can translate $x \rightarrow y$, $x \leftrightarrow y$, and $x \oplus y$ as $(\neg x \vee y)$, $(x \wedge y) \vee (\neg x \wedge \neg y)$, and $(x \wedge \neg y) \vee (\neg x \wedge y)$ respectively.
- In addition, $x \leftrightarrow y$ translates to $(x \rightarrow y) \wedge (y \rightarrow x)$.
- These rules let us put things either mostly in terms of $\rightarrow$ or mostly in terms of $\wedge$, $\vee$, and $\neg$.

More Equational Rules

- Four equivalence rules deal with $\neg$: **Excluded Middle** says that $(x \vee \neg x) \leftrightarrow 1$, the **Double Negative** rule says that $\neg\neg x \leftrightarrow x$, and the two **DeMorgan** rules say that $\neg(x \wedge y) \leftrightarrow (\neg x \vee \neg y)$ and $\neg(x \vee y) \leftrightarrow (\neg x \wedge \neg y)$.
- The **Contrapositive Rule** lets us switch between $x \rightarrow y$ and $\neg y \rightarrow \neg x$. Note that neither $y \rightarrow x$ (**converse**) nor $\neg x \rightarrow \neg y$ (**inverse**) is equivalent to $x \rightarrow y$.

Clicker Question #3

- Let P be the statement $(x \vee y) \rightarrow (z \wedge y)$. Which of these statements is equivalent to P by the Contrapositive Rule?
- (a) $(\neg z \vee \neg y) \rightarrow (\neg x \wedge \neg y)$
- (b) $(z \wedge y) \rightarrow (x \vee y)$
- (c) $(\neg x \wedge \neg y) \rightarrow (\neg z \vee \neg y)$
- (d) $(\neg z \wedge \neg y) \rightarrow (\neg x \vee \neg y)$

Answer #3

- Let P be the statement $(x \vee y) \rightarrow (z \wedge y)$. Which of these statements is equivalent to P by the Contrapositive Rule?
- (a) *$(\neg z \vee \neg y) \rightarrow (\neg x \wedge \neg y)$*
- (b) $(z \wedge y) \rightarrow (x \vee y)$
- (c) $(\neg x \wedge \neg y) \rightarrow (\neg z \vee \neg y)$
- (d) $(\neg z \wedge \neg y) \rightarrow (\neg x \vee \neg y)$

Some Implication Rules

- The two **Joining Rules** give us $x \vee y$ and $y \vee x$ from x.
- The two **Separation Rules** give us either x or y from $x \wedge y$.
- We can derive $x \rightarrow y$ from either $\neg x$ (**Vacuous Proof**) or y (**Trivial Proof**).
- From $\neg x \rightarrow 0$ we can derive x by **Contradiction**.

More Implication Rules

- From $x \rightarrow y$ and $y \rightarrow z$ we can derive $x \rightarrow z$ by **Hypothetical Syllogism**.
- From $(x \wedge y) \rightarrow z$ and $(x \wedge \neg y) \rightarrow z$ we can derive $x \rightarrow z$ by **Proof By Cases**.
- Of course all these rules may be verified by truth tables.