CMPSCI 250: Introduction to Computation

Lecture #5: Strategies for Propositional Proofs
David Mix Barrington
13 September 2013

Strategies for PropCalc Proofs

- The Forward-Backward Method
- Transforming the Proof Goal
- Contrapositives and Indirect Proof
- Proof By Contradiction
- Hypothetical Syllogism: Two Proofs in Series
- Proof By Cases: Two Proofs in Parallel
- An Example: Exercises 1.8.3 and 1.8.4

The Setting for PropCalc Proofs

- In an equational sequence or a deductive sequence proof, we begin with one compound proposition, our premise, and we want to get to another, our conclusion, by applying rules.
- We are in effect searching through a path in a particular space, where the points are compound propositions and the moves are those authorized by the rules.

The Forward-Backward Method

- The **forward-backward method** (first named, AFAIK, by Daniel Solow in his *How to Read and Do Proofs*) is a way of organizing this search.
- Given a search from P to C, we can look for a **forward move**, which is some compound proposition P' where we can move from P to P'.
- This reduces our search problem to finding a way from P' to C.

The Forward-Backward Method

- A **backward move** is some C’ such that we can move from C’ to C. This reduces our search to getting from P to C’.
- If a forward or backward move is well chosen, it gets us to an easier search. If it is not, it gets us to a harder search. How to tell? In general there is no firm guideline, but we’d like to make the ends of the new search *more similar* to one another.

Transforming the Proof Goal

- Some of the rules we listed last time help us transform a proof goal in other ways. Again suppose we are trying to get from P to C. Suppose we are able to prove C *without using the assumption P at all.*
- In this case $P \rightarrow C$ is true -- the tautology $C \rightarrow (P \rightarrow C)$ is called the rule of **trivial proof**. This does actually happen -- our breakdowns of proofs sometimes leaves very easy pieces.

More Transformations

- Similarly we may be able to prove $\neg P$, and since $\neg P \rightarrow (P \rightarrow C)$ is a tautology, called the rule of **vacuous proof**, this is good enough to prove $P \rightarrow C$. For example, we can prove "If this animal is a unicorn, it is green" in this way.
- An equivalence $P \leftrightarrow C$ is often proved by two deductive sequence proofs rather than a single equational sequence proof. The **equivalence and implication rule** says that $(P \leftrightarrow C) \leftrightarrow ((P \rightarrow C) \wedge (C \rightarrow P))$. This allows us to prove an "if and only if" by "proving both directions".

Indirect Proof

- Assuming P and using it to prove C is called a **direct proof** of $P \rightarrow C$. Sometimes we may find it easier to work with the terms of C than those of P. If we assume $\neg C$ and use it to prove $\neg P$, we have made a direct proof of the implication $\neg C \rightarrow \neg P$.
- But this implication, called the **contrapositive** of the original $P \rightarrow C$, is equivalent to the original. So proving $\neg P$ from $\neg C$ is sufficient to prove $P \rightarrow C$, and this is called an **indirect proof**.

Clicker Question #1

- How would you carry out an indirect proof of the implication “If you expected this, it isn’t the Spanish Inquisition.”
- (a) Assume you expected this, prove it isn’t SI.
- (b) Assume it isn’t SI, prove you expected it.
- (c) Assume you didn’t expect it, prove it is SI.
- (d) Assume it is SI, prove you didn’t expect it.

Answer #1

- How would you carry out an indirect proof of the implication “If you expected this, it isn’t the Spanish Inquisition.”
- (a) Assume you expected this, prove it isn’t SI.
- (b) Assume it isn’t SI, prove you expected it.
- (c) Assume you didn’t expect it, prove it is SI.
- (d) *Assume it is SI, prove you didn’t expect it.*

Bad Indirect Proofs

- Be careful to use the contrapositive rather than other, related implications that are not equivalent to $P \rightarrow C$.
- Simply reversing the arrow gets you $C \rightarrow P$, the **converse** of $P \rightarrow C$, which may well be true when $P \rightarrow C$ is false, or vice versa.
- Simply taking the negation of both sides gives you $\neg P \rightarrow \neg C$, the **inverse** of $P \rightarrow C$, which is not equivalent to $P \rightarrow C$ either. (In fact the converse is the contrapositive of the inverse and vice versa, so they are equivalent to each other.)

Proof By Contradiction

- In Discussion #1 we saw an example of **proof by contradiction**, when we assumed that some natural number was neither even nor odd.
- We wound up using this assumption to prove that there was a "neither number" that was smaller than the smallest "neither number", which is impossible.

Proof By Contradiction

- The negation of the implication $P \rightarrow C$ is $P \wedge \neg C$, because the only way the implication can be false is if the premise is true and the conclusion false.
- If we can assume $P \wedge \neg C$ and prove 0, the always false proposition, we have made a direct proof of the implication $(P \wedge \neg C) \rightarrow 0$, and one of our rules says that $(P \rightarrow C) \leftrightarrow ((P \wedge \neg C) \rightarrow 0)$ is a tautology.

Proof By Contradiction

- The reason we might want to do this is that the more assumptions we have, the more possible steps we have available. Trying proof by contradiction is often a good way to get started.
- But it's important to keep track of what the assumption was, so we know exactly what we are proving to be false. And of course any error in a proof can cause a contradiction.

Clicker Question #2

- Consider the following argument: "If there is any number that is both even and odd, then there is a least such number x. Because 0 is not odd, $x \neq 0$. So x has a predecessor y that is not both even and odd. But y is odd because x is even, and y is even because x is odd." What do we *conclude* from this argument?
- (a) x is neither even nor odd
- (b) y cannot be both even and odd
- (c) No number is both even and odd.
- (d) Every number is either even or odd.

Answer #2

- Consider the following argument: "If there is any number that is both even and odd, then there is a least such number x. Because 0 is not odd, $x \neq 0$. So x has a predecessor y that is not both even and odd. But y is odd because x is even, and y is even because x is odd." What do we *conclude* from this argument?
- (a) x is neither even nor odd
- (b) y cannot be both even and odd
- (c) *No number is both even and odd.*
- (d) Every number is either even or odd.

Hypothetical Syllogism

- Our use of an arrow for implication certainly suggests that implication is **transitive**. This means that if we can get from P to Q and we can get from Q to C, then we can get from P to C.
- And in fact $((P \to Q) \land (Q \to C)) \to (P \to C)$ is a tautology, called the rule of **Hypothetical Syllogism**.

Hypothetical Syllogism

- This means that we can pick an intermediate goal for our proof -- if we pick a useful Q, it may be easier to figure out how to get from P to Q and how to get from Q to C than to figure out how to get from P to C all at once.
- But a *bad* choice of intermediate goal could make things worse -- the two subgoals might be harder to find or even impossible. The rule of hypothetical syllogism is an implication, *not* an equivalence. It is possible for $P \rightarrow C$ to be true and for one or both of $P \rightarrow Q$ or $Q \rightarrow C$ to be false.

Proof By Cases

- Another way to break up a proof problem into smaller problems is **case analysis**. If R is any proposition at all, and $P \rightarrow C$ is true, then the two implications $(P \wedge R) \rightarrow C$ and $(P \wedge \neg R) \rightarrow C$ are both true.
- Furthermore, if we can prove both of these propositions, the **Proof by Cases** rule tells us that $(((P \wedge R) \rightarrow C) \wedge ((P \wedge \neg R) \rightarrow C)) \rightarrow (P \rightarrow C)$ is a tautology.

Proof By Cases

- The way this works in practice is that you just say "assume R" in the middle of your proof, and carry on to get C. But now you have assumed P $\wedge$ R rather than just P, so you have proved only $(P \wedge R) \rightarrow C$. You need to start over and this time "assume $\neg R$", completing a separate proof of $(P \wedge \neg R) \rightarrow C$.

- You can break cases into subcases, and subsubcases, and so on. Of course the ultimate case breakdown is into 2k subcases, one for each setting of the k atomic variables. This is just a truth table proof!

Clicker Question #3

- I'm trying to prove $P \rightarrow C$. I assume Q, and prove $(P \wedge Q) \rightarrow C$. Then I start over and assume R, proving $(P \wedge R) \rightarrow C$. What do I still need to prove to reach my goal of $P \rightarrow C$?
- (a) $(P \wedge \neg Q \wedge \neg R) \rightarrow C$
- (b) $(\neg Q \wedge \neg R) \rightarrow C$
- (c) $(P \wedge Q \wedge R) \rightarrow C$
- (d) There is nothing left to prove, I am done.

Answer #3

- I'm trying to prove $P \to C$. I assume Q, and prove $(P \wedge Q) \to C$. Then I start over and assume R, proving $(P \wedge R) \to C$. What do I still need to prove to reach my goal of $P \to C$?
- (a) *$(P \wedge \neg Q \wedge \neg R) \to C$*
- (b) $(\neg Q \wedge \neg R) \to C$
- (c) $(P \wedge Q \wedge R) \to C$
- (d) There is nothing left to prove, I am done.

An Example: Exercises 1.8.3-4

- Let P be the compound proposition $p \wedge q$ and let C be $p \vee q$. Of course we could verify $(p \wedge q) \rightarrow (p \vee q)$ by truth tables, but let's look at how to approach the problem using our various strategies.
- Neither trivial nor vacuous proof will work. Let's try Hypothetical Syllogism. If we pick p as our intermediate goal, we can get from $p \wedge q$ to p by Left Separation, and from p to $p \vee q$ by Right Joining.

Example: Proof By Cases

- Let's try Proof by Cases, with p as the intermediate proposition. If we assume that p is true, we can prove $p \vee q$ by Right Joining, and this gives us a trivial proof of the original implication.
- On the other hand, if we assume that p is false, then its easy to show that $p \wedge q$ is false, giving us a vacuous proof of the original.

Example: Proof by Contradiction

- Using Proof by Contradiction, we assume both $p \wedge q$ and $\neg(p \vee q)$. The second assumption turns to $\neg p \wedge \neg q$ by DeMorgan.
- Once we have "$p \wedge q \wedge \neg p \wedge \neg q$", it's pretty straightforward to get 0. We use associativity and commutativity to get $(p \wedge \neg p) \wedge q \wedge \neg q$. We have $p \wedge \neg p \leftrightarrow 0$ by Excluded Middle, and our 0 rules say that $0 \wedge x \leftrightarrow 0$ for any x.