Equational Proofs

Last time, we saw a **direct way** to show that a propositional logic formula ϕ is valid, namely by constructing a truth table for the formula and checking that every truth assignment was a satisfying assignement (i.e., it made the formula true).

In this lecture, we study an **indirect way** to show that a propositional formula is valid, which will be useful in the future when we consider reasoning about programs written in ACL2, for which we will not have the luxury of being able to build truth tables.

The indirect way will be a form of *equational proof*. The idea is similar to how you derive proofs of equalities in, say, algebra, using equations. Suppose that you wanted to derive that $(a+b)^2 = a^2 + 2ab + b^2$. If you wante to be excrutiatingly pedantic, you would start with that equation and step by step rewrite it by replacing equals by equals until you ended up with an equality that was obviously true at the end. For instance:

$$\begin{aligned}
(a+b)^2 &= a^2 + 2ab + b^2 \\
(a+b)(a+b) &= a^2 + 2ab + b^2 \\
a^2 + ab + ba + b^2 &= a^2 + 2ab + b^2 \\
a^2 + ab + ab + b^2 &= a^2 + 2ab + b^2 \\
a^2 + 2ab + b^2 &= a^2 + 2ab + b^2
\end{aligned}$$

and the last line is obviously true because the left side is exactly the same as the right side.

So the idea is that we will use a similar approach to show the validity of formulas of the form $\phi \equiv \psi$. This may seem limiting, but the following result shows that we don't lose any generality considering only equivalences of formulas.

Fact 1 *Formula ϕ is valid if and only if $\phi \equiv true$ is valid.*

Therefore, if we have a technique for proving validity of equivalences, this fact can let us use the technique to establish the validity of an arbitrary formula.

The idea is as follows. We start with the equivalence $\phi \equiv \psi$ that we want to prove valid. We then repeatedly apply the Principle of Substitution to transform $\phi \equiv \psi$ into a series of equivalences that each are valid if and only if the original $\phi \equiv \psi$ is valid. If we eventually reach a formula of the form $\eta \equiv \eta$, which is clearly valid (by the Principle of Specialization applied to the valid formula $p \equiv p$), then we are done and we can infer that the original equivalence was valid.

This is all very abstract. Let's look at examples. Before doing that, though, we need a bank of simple equivalences to help us along. Indeed, the Principle of Substitution relies on us being able to use equivalences to perform substitutions. So we need to have some equivalences to start with. We saw a bunch of them last lecture, in Exercise 5. (Do that exercise, proving them valid using truth tables.) Those validities are some of the most basic ones. Here are further basic ones that will come in handy. Prove them directly, using truth tables.

Exercise 2 *Check that the following formulas are valid:*

(1) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

(2) $\neg(p \vee q) \equiv \neg p \wedge \neg q$

(3) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(4) $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$

(5) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(6) $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$

Note that the direction of the equivalence is of course not important:

Fact 3 *Formula $\phi \equiv \psi$ is valid if and only if $\psi \equiv \phi$ is valid.*

Let's try to come up with an equational proof for the equivalence $(a \wedge b) \Rightarrow c \equiv a \Rightarrow (b \Rightarrow c)$. (I am using a, b, c as propositional variables for variety.) I am going—and you will too when you write these kind of proofs up—to be very pedantic in terms of applying only one substitution per step. I'm also going to point out what equivalence I am using at each substitution. Those equivalences are going to be specializations of the equivalences we've seen already. In general, you can use any equivalence that we have proved in class or seen in exercises; any other equivalence that you want to use you have to prove.

Equational proof of: $(a \wedge b) \Rightarrow c \equiv a \Rightarrow (b \Rightarrow c)$

$$
\begin{array}{rcl}
(a \wedge b) \Rightarrow c & \equiv & a \Rightarrow (b \Rightarrow c) \\
 & & \textit{Substitution } (a \wedge b) \Rightarrow c \equiv \neg(a \wedge b) \vee c \\
\neg(a \wedge b) \vee c & \equiv & a \Rightarrow (b \Rightarrow c) \\
 & & \textit{Substitution } \neg(a \wedge b) \equiv \neg a \vee \neg b \\
(\neg a \vee \neg b) \vee c & \equiv & a \Rightarrow (b \Rightarrow c) \\
 & & \textit{Substitution } (\neg a \vee \neg b) \vee c \equiv \neg a \vee (\neg b \vee c)
\end{array}
$$

$$
\begin{array}{rcl}
\neg a \vee (\neg b \vee c) & \equiv & a \Rightarrow (b \Rightarrow c) \\
 & & \textit{Substitution } b \Rightarrow c \equiv \neg b \vee c \\
\neg a \vee (\neg b \vee c) & \equiv & a \Rightarrow (\neg b \vee c) \\
 & & \textit{Substitution } a \Rightarrow (\neg b \vee c) \equiv \neg a \vee (\neg b \vee c) \\
\neg a \vee (\neg b \vee c) & \equiv & \neg a \vee (\neg b \vee c)
\end{array}
$$

There, done. Note that sometimes I work on the left side of the equivalence, sometimes on the right side of the equivalence. There is no unique way of proving the above equationally—you can do things in different order. Try it. Make sure you understand all the substitutions that take place, and where the equivalences used in the substitutions come from. For instance, the first substitution uses the valid equivalence $(a \wedge b) \Rightarrow c \equiv \neg(a \wedge b) \vee c$, which is valid by the Principle of Specialization applied to the valid equivalence $p \Rightarrow q \equiv \neg p \Rightarrow q$ we saw last time, and replacing p by $a \wedge b$ and q by c. (Make sure you understand this!)

Here's another one.

Equational proof of: $(a \vee b) \Rightarrow c \equiv (a \Rightarrow c) \wedge (b \Rightarrow c)$

$$
\begin{array}{rcl}
(a \vee b) \Rightarrow c & \equiv & (a \Rightarrow c) \wedge (b \Rightarrow c) \\
 & & \textit{Substitution } (a \vee b) \Rightarrow c \equiv \neg(a \vee b) \vee c \\
\neg(a \vee b) \vee c & \equiv & (a \Rightarrow c) \wedge (b \Rightarrow c) \\
 & & \textit{Substitution } \neg(a \vee b) \equiv \neg a \wedge \neg b \\
(\neg a \wedge \neg b) \vee c & \equiv & (a \Rightarrow c) \wedge (b \Rightarrow c) \\
 & & \textit{Substitution } (\neg a \wedge \neg b) \vee c \equiv (\neg a \vee c) \wedge (\neg b \vee c) \\
(\neg a \vee c) \wedge (\neg b \vee c) & \equiv & (a \Rightarrow c) \wedge (b \Rightarrow c) \\
 & & \textit{Substitution } a \Rightarrow c \equiv \neg a \vee c \\
(\neg a \vee c) \wedge (\neg b \vee c) & \equiv & (\neg a \vee c) \wedge (b \Rightarrow c) \\
 & & \textit{Substitution } b \Rightarrow c \equiv \neg b \vee c \\
(\neg a \vee c) \wedge (\neg b \vee c) & \equiv & (\neg a \vee c) \wedge (\neg b \vee c)
\end{array}
$$

Again, done, because the last line is in fact a valid equivalence.

Exercise 4 *Give an equational proof that the formula* $a \Rightarrow (b \wedge c) \equiv (a \Rightarrow b) \wedge (a \Rightarrow c)$ *is valid.*