MATH/COMP61-03 Spring 2014 Notes: January 21st

Andrew Winslow

1 Counterexamples

A statement that hasn't been proved is a *conjecture*:

Conjecture. *If $n > 4$ is an integer, then $2^{2^n} + 1$ is composite.*

One goal of mathematics is to convert as many conjectures as possible into theorems. Surprisingly, many simple statements lack proofs and many conjectures have resisted significant efforts to find proofs for them. Sometimes a conjecture is so good at avoiding being proved for a sneaky reason: the conjecture is not true. These un-true conjectures will never become theorems, destined to roam the mathematics literature until they are put to rest by a proof that they cannot be true that we call a *counterexample*. For an if-then conjecture $A \Rightarrow B$, a counterexample is an instance with a true hypothesis A, and a false conclusion B. For instance:

Conjecture. *If v, w, x, y, z are integers greater than 0, then $v^5 + w^5 + x^5 + y^5 \neq z^5$.*

This conjecture was thought to be true from the 1700s until 1966 – people looked for a proof for 200 years! In 1966, someone found that $v = 27$, $w = 84$, $x = 110$, $y = 133$, and $z = 144$ (all integers greater than 0) have the property that $v^5 + w^5 + x^5 + y^5 = z^5$. That is, they proved the theorem:

Theorem. *There exists a set of integers v, w, x, y, z greater than 0 such that $v^5 + w^5 + x^5 + y^5 = z^5$.*

This theorem shows that the conjecture's hypothesis can be true while the conclusion is false. So the conjecture is false. We call such construction that satisfies the hypothesis but not the conclusion a *counterexample*. The search for counterexamples is an important part of proving theorems: if a counterexample exists, further attempts to prove the theorem are guaranteed to fail. Attempts to prove a theorem should be done with reasonable confidence that no counterexample can be found and, even better, with intuition for why no counterexample could exist. Consider the following conjecture:

Conjecture. *If n and a are integers with $a \mid n$, then $a \leq n$.*

Is it true? We have seen many examples of n and a with $a \mid n$ where $a \leq n$. For instance, $n = 12, a = 4$. But a proof needs more: $a \mid n$ must always imply that $a \leq n$.

Recall that $a \mid n$ only implies that $ab = x$ for some b, i.e. that n is a scaled by some integer amount. If $b > 0$ and $a > 0$, then $a = a \cdot 1 \leq a \cdot b = x$ and the conclusion holds.

But what if $b \leq 0$ or $a \leq 0$? For instance, $b = -1$, $a = 1$. Then $n = a \cdot b = -1$, $a = 1$, and $a \mid n$ (so the hypothesis is true), but $a \not\leq n$ (the conclusion is false), a counterexample!

2 Boolean Algebra

If we are being pedantic, "algebra" should probably be called "number algebra", since the equations like $7 = (3x + 1)/10$ have variables whose unknown values (like x) are numbers and operators (like $+$ and $/$) are applied to numbers to yield new numbers. In the previous lecture we learned about proofs and their various forms, including if-then statements, and-statements, and or-statements, that can be true or false.

Here we study an algebra of truth, called *boolean algebra*[1], where variables are truth values: *true* (T) or *false* (F), and the operators are things like *and* ($\wedge$), *or* ($\vee$), *not* ($\neg$), *implies* ($\rightarrow$), and *iff* ($\leftrightarrow$). That is, they are operators applied to truth values that yield new truth values.

We will see later how boolean algebra lets us reason about truth and proof, to better understand proofs we see and even make new kinds of proofs. For now, we consider boolean algebra on its own. Start with variables:

Definition. *A boolean* variable x *has one of two truth values:* true *or* false.

We can combine variables with *operators* to form *expressions*, just like number algebra. Because boolean variables only have two values, unlike integers that have infinitely many, we can define operators by what what happens for different values. Here are definitions of some of these operators:

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Notice how these match the more informal English versions of *and*, *or*, and *implies* in their truth values. Just like number algebra has *binary operators* that use two variables, like $+$, $-$, $\cdot$, $/$, and *unary operators*, like $-$ (negative), e.g. the number -4, which is 4 negated. The unary operator in boolean algebra is $\neg$, called *negation*:

x	$\neg y$
T	F
F	T

[1] It maybe should be called "truth algebra", but is named after George Boole, a guy who liked formal reasoning so much he thought it should have its own algebra.

Boolean algebra also has the notion of equivalence (=), which is not an operator, but instead says two expressions always have the same value. This gives rise to a number of familiar algebraic rules:

1. $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ (Commutativity)
2. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$ (Associativity)
3. $x \wedge T = x$ and $x \vee F = x$ (Identity)
4. $\neg(\neg x) = x$ (Inverse)
5. $x \wedge x = x$ and $x \vee x = x$ (Self-Identity)
6. $x \wedge \neg x = F$ and $x \vee \neg x = T$ (Self-Negation)
7. $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ and $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ (Distributivity)
8. $\neg(x \vee y) = \neg x \wedge \neg y$ and $\neg(x \wedge y) = \neg x \vee \neg y$ (DeMorgan's Laws)

So now we have a real algebra up and running, with variables, operators, and some basic rules. What is it good for? The two boolean expressions $x \rightarrow y$ and $\neg x \vee y$ are equivalent, as seen by examining an enumeration of all possible values of the variables and resulting values of the expressions, called a *truth table*:

x	y	$x \rightarrow y$	$\neg x \vee y$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

The equivalence of these two expressions means that if a theorem matching the form of one expression is true, then so is the other theorem. For example, given an theorem:

Theorem. *If n is even, then n^2 is even.*

Proof. *Let n be even. Then $2 \mid n$ and so there exists an integer a such that $n = 2a$. Then $n^2 = (2a)^2 = 4a^2 = 2(2a^2)$. So $2 \mid n^2$. So n^2 is even.* □

Then the following theorem follows:

Theorem. *Let n be an integer. Then either n is odd, or n^2 is even.*

Proof. *Since the boolean equivalence $x \rightarrow y = \neg x \vee y$ is true, the theorem is equivalent to "Let n be an integer. Then either n is not even, or n^2 is even." Since every integer is either even or odd, "n is not even" is equivalent to "n is odd". So the theorem is equivalent to "Let n be an integer. Then either n is odd, or n^2 is even."* □

Showing that $x \to y = \neg x \vee y$ using a truth table is like showing $3(n+2) = 3n+6$ by showing $3(1+2) = 3(1)+6$, then $3(2+2) = 3(2)+6$, etc. for all possible integer values of n. It doesn't leverage the "power of algebra". Here's a proof of the equivalence ot two boolean expressions not using a truth table, but boolean algebra instead:

Theorem. $(x \to y) \wedge (y \to x) = (x \wedge y) \vee (\neg x \wedge \neg y)$

Proof. *Algebraically manipulate the left side of the equality:*

$$\begin{aligned}
(x \to y) \wedge (y \to x) &= (\neg x \vee y) \wedge (\neg y \vee x) && \text{(by previous truth table)}\\
&= (\neg x \wedge (\neg y \vee x)) \vee (y \wedge (\neg y \vee x)) && \text{(by distributivity)}\\
&= ((\neg x \wedge \neg y) \vee (\neg x \wedge x)) \vee ((y \wedge \neg y) \vee (y \wedge x)) && \text{(by distributivity)}\\
&= (\neg x \wedge \neg y) \vee (\neg x \wedge x) \vee (y \wedge \neg y) \vee (y \wedge x) && \text{(by associativity)}\\
&= (\neg x \wedge \neg y) \vee F \vee F \vee (y \wedge x) && (\mathrm{by\ self-negation})\\
&= (\neg x \wedge \neg y) \vee (y \wedge x) && (\mathrm{by\ self-identity})\\
&= (x \wedge y) \vee (\neg y \wedge \neg x) && \text{(by commutativity)}
\end{aligned}$$

□

Boolean algebra is used as "just another algebra" in many areas of mathematics and computer science, and in fact is equivalent in a way to specialized number algebras restricted to just 0 and 1. However, boolean algebra can also be used to say something about proofs and theorems as we already saw.

For instance, the last theorem, although it's just an algebraic equivalence, also says something about theorems: a theorem "A if and only if B" is equivalent to "Either both A and B are true, or both A and B are false." This application of boolean algebra is unique and different than number algebra, and is partly why George Boole invented it.[2] We will investigate this application more when we reach Chapter 4 of the book.

[2] Plus the fame and glory.