Discrete Mathematics lecture notes 2-2

September 14, 2013

6. Tautologies and Contradictions

Let's close the discussion of Boolean operators with a couple of examples referenced in the previous notes:

$$P(A,B) := ((A \Rightarrow B) \wedge A) \Rightarrow B \qquad\qquad T(A,B) := ((A \Rightarrow B) \wedge (\neg B)) \Rightarrow (\neg A)$$

These are both binary operators, in that each accepts 2 Boolean variables. What are their truth tables?

A	B	$A \Rightarrow B$	$(A \Rightarrow B) \wedge A$	$P(A,B)$	$\neg B$	$(A \Rightarrow B) \wedge (\neg B)$	$\neg A$	$T(A,B)$
T	T	T	T	T	F	F	F	T
T	F	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T	T
F	F	T	F	T	T	T	T	T

We see that, independent of the veracity of the inputs of P and T, the output is always the same: `T`. Such a Boolean operator is a *tautology*, a "universal truth."[1] In fact, these statements are simply formalizations logical jumps that we all intuitively use:

P is called *modus ponens*. It is the basis of our standard deductive reasoning: If we can show that A implies B and A is true, then B must be true as well. Note that the universal truth of P does *not* depend on the truth of A, B, or "A implies B," since any one of these might prove false while $P(A,B)$ will remain true. Thus saying that P is a tautology is really just saying that deductive reasoning is a valid form of inference.[2]

Similarly, T is *modus tollens*, and is the basis for proof by contraction: If we know that A implies B and B is false, then A must be false as well.

Here is another tautology: $A \vee (\neg A)$. This should be read as "any[3] statement is true or false." Here is the opposite extreme: $A \wedge (\neg A)$. No matter what truth value A takes,[4] this Boolean expression will always take on the value `F`. This should be read "no statement[5] is both true and false.

Aside: There is a subtle question that one could now pose: Suppose I have the statement of some theorem, and a proof of its truth. Does this mean that there is no proof of its falsehood? That is, is mathematics *consistent*, in which there are no true *and* false statements?[6] The answer: Yes, but. That answer ("you cannot prove a statement and its negation") itself is a logical claim, which you *cannot prove using the same logical system we are developing.* Instead, we have to develop a notion of *higher order logic*, which we can use to prove claims like the consistency of our first order logic. But is second order logic consistent? Yes, but to show this you need to go to a higher order still. And on it goes. . . .[7]

7. An induction nonexample

We've now seen several ways to use induction to prove statements about the natural numbers and we'll have many more examples coming in the days ahead. Equally important to understanding how induction works is to recognize how it can fail: If you look in the text you'll find several examples of how an inductive argument can go wrong. Generally Scheinerman's nonexamples focus on the situation where he's proved that, for some collection of statements $\mathcal{P}$ indexed by the natural numbers, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ but somehow has failed to prove $\mathcal{P}(0) = \texttt{T}$. You should explore these examples in detail, and make sure you see where the argument goes wrong. Here is a different way this could fail:

[1] This should be understood in the context of mathematical truth we have been developing and not as a metaphysical claim.

[2] At least in the logical system we're developing. . . .

[3] We haven't actually introduced the quantifier $\forall$ here, but we should. . . .

[4] That is, neither of the two possibilities `T` or `F`.

[5] Again, we probably should write this as $\neg\exists A$. . . .

[6] Note: Once we have *one* statement that is both true and false, then *all* statements are, thanks to the way we've defined $\Rightarrow$.

[7] I'm being almost criminally imprecise here, using technical terms in a very loose manner that would probably get me smacked by any logician that read them, but the goal is simply to impress on you some of the subtle problems that lurk behind our naïve understanding of logic and proof. For now, we could rephrase all the above a simply saying that in any logical system, there is a statement that is "true" but unprovable. For more, read about the work of Kurt Gödel.

Theorem 1. *All birds are the same color.*

Proof. Let $\mathcal{P}(n)$ be the statement "For any collection of n birds, all the birds in that collection are of the same color." If we show $\mathcal{P}(n)$ is true for all n, all birds must be of the same color, as there are only finitely many birds in the universe.[8] $\mathcal{P}(1)$ is true, because any bird is the same color as itself.[9] Suppose that $\mathcal{P}(n)$ is true, so *any* collection of n birds has them all of the same color. For any collection of $n+1$ birds, pictured below, we can find two subsets of n birds. By the inductive hypothesis, these subsets have the same color, and since they overlap, we conclude that the entire set consists of birds of the same color, so $\mathcal{P}(n+1)$ is true.

$$\overbrace{* + \rlap{$\underbrace{}_{n\text{ birds}}$}* + \ldots + *}^{n\text{ birds}} + * = (n+1)\text{ birds}$$

□

Exercise. Find the error in this argument.
Hint: I made a relevant comment in class as to why we defined $A \Rightarrow B$ to take the value `T` when A is `F`.

8. More well-ordering and the beginning of number theory

Let us use the Well Ordering Principle[10] to prove a fact we used last week: We can divide (with remainders) integers:

Theorem 2 (Division in $\mathbb{Z}$)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ with $0 \le r < b$ and*

$$a = qb + r.$$

Proof. This is a very common sort of Theorem, which secretly is two Theorems wrapped in one: We must show not only *existence* of the integers q and r, but their *uniqueness* as well. These are logically independent statements; it is conceivable that either (1) there exist many such pairs (q, r), or (2) there are no such pairs, but *if there were*, all of them would be equal.[11] To illustrate the point, we will prove uniqueness first, *before we know that any solutions exist at all.*

Uniqueness: Suppose that we have two pairs of solutions, say (q, r) and (q', r'). Because both of these satisfy the conclusions of the Theorem, we know $q, r, q', r' \in \mathbb{Z}$ and $0 \le r, r' < b$ and

$$a = qb + r \qquad \text{and} \qquad a = q'b + r'.$$

We can combine these equalities to conclude $qb+r = q'b+r'$, or after rearranging and using the distributivity of multiplication over addition, that $(q - q')b = r' - r$. Since all terms of this equality are integers, we see that this is exactly the definition of $b|(r' - r)$. But $r, r' \in \{0, 1, \ldots, b-1\}$, so[12] $0 \le |r - r'| \le b - 1$. As multiplication by a positive number (b) preserves $<$, we see that the only number $x \in \{0, 1, \ldots, b-1\}$ such that $b|x$ is $x = 0$. Thus $r - r' = 0$, or $r = r'$.

Now, our equality $(q - q')b = r' - r$ reduces to $(q - q')b = 0$. As $b > 0$, this forces[13] $q - q' = 0$, or $q = q'$. Thus any two solutions must in fact be the same, and there is a unique solution.[14] Note that this proof of uniqueness did not assume that q and r actually exist.

Existence: So let's prove they do exist. Set $S = \{a - cb \big| c \in \mathbb{Z}, a - cb \ge 0\}$. That is, S is the set of integers that can be written $a - cb$ for some $c \in \mathbb{Z}$, and such that $a - cb \ge 0$. Thus S is actually a subset of the natural numbers, so by the well ordering of $\mathbb{N}$, there is a smallest element $r \in S$.

[8] Let's take this as an axiom. . . .

[9] If we wanted to start with 0, $\mathcal{P}(0)$ is also true in a vacuous sense: If I have a collection of 0 birds, then every bird in that collection—that is, no birds—is the same color as every other bird.

[10] I.e., the Axiom that the standard ordering on $\mathbb{N}$ makes it into a well-ordered set.

[11] In other words, uniqueness could be vacuously true.

[12] One perhaps should prove this claim here with a separate induction.

[13] Why?

[14] What does the last claim have to do with the bird problem above?

By definition, as $r \in S$, there is some $q \in \mathbb{Z}$ such that $r = a - qb$. Rearranging this gives $a = qb + r$, which looks very similar to the conclusion of the Theorem. Of course, we're not actually done yet: There was also the condition that $0 \leq r < b$ that we have to verify. By construction, $r \in \mathbb{N}$, so $0 \leq r$, so all we have to do is show that $r < b$, and existence will be proved.

Suppose not. If $r \geq b$, there is some $r' > 0$ such that $r = b + r'$. Note that $0 \leq r' < r$. I claim that $r' \in S$, which will contradict our choice of r as the minimal element of S: We can write

$$r' = r - b = (a - qb) - b = a - (q + 1)b.$$

This, together with our assumption that $0 \leq r'$, is exactly the definition of $r' \in S$, so we have constructed an element smaller than our minimal element of S, a contradiction.

We only made one assumption that led to a contradiction: That $r \geq b$. By *modus tollens*, we must have that this is false, or $r < b$. Thus r satisfies all the conditions required, and the pair (q, r) is a solution to the Theorem. □

Definition 3. If $a, b \in \mathbb{Z}$ with $b > 0$, when we write $a = qb + r$ with $0 \leq r < b$, we will write $r = a \mod b$ or sometimes just $r = a \pmod{b}$ if there's no cause for confusion.