Discrete Mathematics lecture notes 2-1

September 14, 2013

4. Truth as a function: Boolean algebra

After proving a handful of theorems, we start to notice that certain logical structures begin to appear repeatedly. If we strip out the content of our arguments (*what* is being described, discussed, or proved) and concentrate only of the form of the arguments (*how* do we draw conclusions from our hypotheses), we will discover a new (meta)mathematical object, worthy of study in its own right. We will call this object *Boolean algebra*.

The first thing we need to do is figure out exactly how to ignore what we're talking about while still retaining our argumentation. We do this by replacing specific statements[1] by a placeholder symbols A, B, ... These *Boolean variables* play the same role as the variables we're used to in calculus, but now instead of allowing us to talk about all real numbers at once, we allow our variables to range over all[2] statements. And, just as with our real-valued variables, once we have Boolean variables to work with, what we really want to do is perform some calculus on them. Or at least algebra.

Definition 1. The *veracity function*[3] is an assignment to a statement exactly one of the symbols `T` or `F`.

We should think of this as saying that a given statement is either `T`rue or `F`alse. Thus, if A is a Boolean variable, and $v(A)$ denotes the veracity of A, we have $v(A) \in \{\mathtt{T}, \mathtt{F}\}$, and which one depends on *which statement A is standing in for in a given instant.*[4]

We have ways of making new statements from old, the overall truth of which is determined by *truth tables*, i.e., recording the veracity of all component Boolean variables in our new statement, along with the veracity of the statement as a whole:

Definition 2. Let A and B be Boolean statements.

- The *negation of A* is the Boolean statement is $\neg A$ (read "not A"), with truth table

A	$\neg A$
T	F
F	T

- The *conjunction of A with B* is the Boolean statement $A \wedge B$ (read "A and B").
- The *disjunction of A with B* is the Boolean statement $A \vee B$ (read "A or B).
- The Boolean statement $A \Rightarrow B$ is read "A implies B."
- The Boolean statement $A \Leftrightarrow B$ is read "A iff B."

The truth table for conjunction, disjunction, implication, and logical equivalence must allow for *four* rows, to account for all four possible veracities of A and B taken together. The table defining these terms is:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

We can continue to combine Boolean statements using these (and other!) logical operators. We don't even need to restrict ourselves to two Boolean variables.

[1] E.g., "a is an integer," or "the natural numbers are well ordered," or "$5 < 2$," or ....

[2] That is to say, almost all. We don't like self-referential statements, like "This statement is false."

[3] Not standard terminology.

[4] Intuitively: If $\mathscr{S}$ denotes the "set of Boolean statements"—circularly, those for which we can assign a value of true or fasle—v is a function $\mathscr{S} \to \{\mathtt{T}, \mathtt{F}\}$.

Example 3. Let A, B, C be Boolean variables, and let $E(A, B, C)$ be the Boolean statement defined by

$$v(E(A,B,C)) = \begin{cases} \mathtt{T} & \text{if } v(A) = v(B) = v(C) \\ \mathtt{F} & \text{else} \end{cases} .$$

Can you construct the truth table for $E(A, B, C)$ from this definition? What name should we give E?

Consider for the moment the expressions $x^2 - 1$ and $(x + 1)(x - 1)$, where x is now a standard variable from calculus (i.e., it's just playing the role of an unnamed real number). Our basic algebra knowledge tells us that these two expressions are the same[5]; similarly, there are may possible ways of writing the same Boolean statement in terms of our logical operations.[6]

Example 4. Consider the Boolean statement $(\neg A) \vee (A \wedge B)$. We can construct the truth table for this guy by looking first at the simpler sub-statements, which are determined by the definition of conjunction, disjunction, and negation above (i.e., read the columns of the table below from left to right to see how I computed each one). We have:

A	B	$\neg A$	$A \wedge B$	$(\neg A) \vee (A \wedge B)$
T	T	F	T	$(\mathtt{F} \vee \mathtt{T}) = \mathtt{T}$
T	F	F	F	$(\mathtt{F} \vee \mathtt{F}) = \mathtt{F}$
F	T	T	F	$(\mathtt{T} \vee \mathtt{F}) = \mathtt{T}$
F	F	T	F	$(\mathtt{T} \vee \mathtt{F}) = \mathtt{T}$

In fact, we've already seen the last column: This is the definition of the implication $A \Rightarrow B$. We conclude that the Boolean statements $A \Rightarrow B$ and $(\neg A) \vee (A \wedge B)$ are equal.[7]

Exercise. Let's test your understanding of this: Consider the trinary Boolean operation $E(A, B, C)$ defined above. Compare this to the statement $(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (C \Rightarrow A)$. There is an implicit claim in Lecture Notes 1-2 that is explained by this calculation: What is it?

5. Induction and Well-ordering

In addition to direct proof and proof by contradiction[8], there is another tool we will often make use of: Mathematical induction. The foundation for this *Axiom* is the following property of the natural numbers:

Axiom. Every natural number x has a *successor* $S(x) > x$.[9] Every natural number $y \neq 0$ other than zero is the successor of some other natural number $y = S(z)$. Finally, every natural number can be written as an iterated successor of 0, i.e., $\mathbb{N} = \{0, S(0), S(S(0)), S(S(S(0))), \ldots\}$.[10]

In practice, this becomes the following:

Axiom (Principle of Mathematical Induction)**.** Let $\{\mathcal{P}(n)\}_{n\in\mathbb{N}}$ be a collection of Boolean statements, indexed by the natural numbers. If

- $v(\mathcal{P}(0)) = \mathtt{T}$, and
- $v(\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)) = \mathtt{T}\ \forall\ n \in \mathbb{N}$,

[5] In the sense that whenever I plug in a particular real number to one and perform the stated operations, the result will be the same as if I plugged the same real number into the other.

[6] Looking ahead to the end of next week: Can you prove that there *must* be multiple expressions for the same statement just by counting?

[7] That is, their veracity functions are the same. Since we're interested in Boolean statements for their assigned truth value, there is no harm done if we identify two statements with identical veracity functions.

[8] In light of the previous section, explain the relevance of the Boolean statements $((A \Rightarrow B) \wedge A) \Rightarrow B$–*modus ponens*–and $((A \Rightarrow B) \wedge (\neg B)) \Rightarrow (\neg A)$–*modus tollens*–to these types of proof. Compute the truth tables for these statements. What is the meaning of this?

[9] One can define the order relation on $\mathbb{N}$ in terms of iterated succession; can you make this precise?

[10] I'm still not being precise, as you can tell from the ellipses. But we're getting closer!

then $v(\mathcal{P}(x)) = \mathtt{T}\ \forall\ x \in \mathbb{N}$.

We should understand this a follows: $\mathcal{P}(0)$ is some statement, which may be true or false. If it is true, $\mathcal{P}(1)$ is some other statement. We could try to prove that $\mathcal{P}(1)$ is true directly, or we could prove that the composite statement $\mathcal{P}(0) \Rightarrow \mathcal{P}(1)$ is true, because that, together with our earlier proof that $\mathcal{P}(0)$ is true, will imply that $\mathcal{P}(1)$ is true by *modus ponens*. We next consider $\mathcal{P}(2)$, and do not prove that it is true directly, but instead prove that $\mathcal{P}(1) \Rightarrow \mathcal{P}(2)$ is true; by the previous stage and *modus ponens*, this is enough. Etc. The point is that we know that this process eventually accounts for every natural number by our axiom that every natural number can be achieved as an iterated successor of 0.

A related notion is the following:

Definition 5. Let S be a set.

- A relation $<$ on S is an *ordering*[11] if it satisfies the following:
  1. (Trichotomy) Exactly one of the following is true $\forall\ x, y \in S$: (i) $x < y$, (ii) $y < x$, (iii) $x = y$.
  2. (Transitivity) If $x < y$ and $y < z$, then $x < z$.
- If S is a set with an ordering $<$, S is *well-ordered* if every nonempty subset $A \subseteq S$ has a smallest element x, i.e., $x < y\ \forall\ y \in A, y \neq x$.

Axiom. The standard ordering on $\mathbb{N}$ makes it into a well-ordered set.

In particular, suppose we want to prove a statement about all natural numbers at once.[12] If this statement does *not* hold for every natural number, there is a counterexample to the truth of our statement. Thus, the set of natural numbers for which the statement *fails* is nonempty. As $\mathbb{N}$ is well-ordered, there must be a least element, a *smallest counterexample*. This allows us a new way of approaching proof-by-contradiction: We can focus our attention on the smallest counterexample of a given statement and try to conclude something absurd from its existence (generally, that there is an even smaller counterexample); with such a contradiction in hand, we conclude that our smallest counterexample cannot exist. But because $\mathbb{N}$ is well-ordered, saying that there is no smallest counterexample is the same as saying that there is no counterexample whatsoever. If a statement has no counterexamples, it is true, and we have a new method of proof.

Bonus: The following is one of the stranger axioms that underlies the "standard" logic than (many) mathematicians use on a daily basis in their research.

Axiom (Well-Ordering Theorem)**.** Every set can be well-ordered.

If this doesn't seem strange, consider what it would mean for $\mathbb{R}$. The Well-Ordering Theorem is in fact equivalent to the *Axiom of Choice* (which is why I label it an *axiom*, despite its name), which we will hopefully get to talk about later in the course.

[11] Or *total ordering*.

[12] For instance, $v(\mathcal{P}(n)) = \mathtt{T}\ \forall\ n \in \mathbb{N}$, as is the goal of an inductive proof.