Lecture 9 - Predicate Logic and Induction

6.042 - March 11, 2003

The previous lecture covered *propositional logic*. The main components were propositions (statements that are true or false) and five connectives ($\wedge$, $\vee$, $\neg$, $\rightarrow$, and $\leftrightarrow$). Unfortunately, many important mathematical ideas can not be expressed in propositional logic. We need something stronger called *predicate logic*. This will allow us, in particular, to express the idea of *mathematical induction*, one of the most widely used tools in this course and in mathematics generally.

1 Predicate Logic

Predicate logic is propositional logic with three additional components.

First, we add *predicates*. Informally, a predicate is a proposition with variables. For example, we could let $P(x, y, z)$ be the predicate "$x + y = z$". This predicate may be true or false, depending on the values assigned to the variables:

$$\begin{array}{ll} P(1,2,3) = \mathrm{T} & \quad \text{because } 1+2=3 \\ P(2,2,5) = \mathrm{F} & \quad \text{because } 2+2 \neq 5 \end{array}$$

A predicate does not have to be assigned a special name like P or Q. For example, we may refer to $x \geq 5$ as a predicate rather than defining $Q(x)$ to be the predicate "$x \geq 5$" and then referring to $Q(x)$.

Second, we must specify a *domain of discourse* or *universe*. This is a simply a set, which we'll always denote $\mathcal{U}$. The significance of this set is that all variables in our predicates take on values in $\mathcal{U}$. Thus, if we are proving facts about the integers, we might let $\mathcal{U} = \mathbb{Z}$ (the integers). If we are studying the roots of quadratic equations, we might let $\mathcal{U} = \mathbb{C}$ (the complex numbers). If we are proving facts about 6.042 students, we might let $\mathcal{U}$ consist of you and all your classmates.

Finally, we need two new symbols that are called *quantifiers*. The first is written $\forall$ and is read "for all". The second is written $\exists$ and is read "there exists". Each quantifier is always followed by a variable and then some predicate involving that variable. For example, we could write:

$$\forall x \; Q(x)$$

This is read, "For all x in the universe $\mathcal{U}$, the predicate $Q(x)$ is true." We could also write:

$$\exists x \; Q(x)$$

This is read, "There exists an x in the universe $\mathcal{U}$ such that the predicate $Q(x)$ is true." We can also string together quantifiers:

$$\forall x \forall z \exists y \; P(x, y, z)$$

This is read, "For all x and for all z, there exists a y such that the predicate $P(x, y, z)$ is true". (Here we're no longer bothering to state explicitly that variables take on values in the universe.)

If P is defined as before, is this last proposition true or false? The answer depends on the domain of discourse, $\mathcal{U}$. If $\mathcal{U} = \mathbb{Z}$, then the claim is true; for all integers x and z, there exists an integer y such that $x + y = z$. On the other hand, if $\mathcal{U} = \mathbb{N}$, then the claim is false; if $x = 5$ and $z = 3$, for example, then there is no natural number y such that $x + y = z$.

At this point, we can give a more formal definition of a predicate.

Definition 1 *A predicate $Q(x_1, x_2, \ldots, x_n)$ is a function mapping elements of U^n to the set $\{T, F\}$.*

So our example predicate, $P(x, y, z)$, is just a function that maps each triple of universe elements (x, y, z) to either true or false. In particular, it maps (x, y, z) to true if and only if $x + y = z$.

This is a lot to digest! But we've now covered all the components of predicate logic. The remainder of this section is devoted to understanding our new toys.

1.1 Valid Propositions

In the simpler world of propositional logic, we had the notion of a tautology, a proposition that is true under all truth assignments. For example, DeMorgan's laws are tautologies:

$$\begin{array}{rcl}
(X_1 \wedge X_2 \wedge \ldots \wedge X_n) & \leftrightarrow & \neg(\neg X_1 \vee \neg X_2 \vee \ldots \vee \neg X_n) \\
(X_1 \vee X_2 \vee \ldots \vee X_n) & \leftrightarrow & \neg(\neg X_1 \wedge \neg X_2 \wedge \ldots \vee \neg X_n)
\end{array}$$

In the woolier world of predicate logic, there is a notion analogous to tautology. We say that a proposition is *valid* if it is true for every domain of discourse and all definitions of the predicates. For example, the following statement is valid:

$$\forall x \forall y \; Q(x, y) \quad \rightarrow \quad \forall z \; Q(z, z)$$

This says that if the predicate $Q(x, y)$ is true for all x and y, then in particular it is true when $x = y$. This assertion holds for every domain of discourse and every definition of the predicate Q.

1.2 Duality of Quantifiers

Two particularly useful valid propositions relate the quantifiers $\exists$ and $\forall$:

$$\forall x\ P(x) \quad \leftrightarrow \quad \neg\exists x\ (\neg P(x)) \tag{1}$$

$$\exists x\ P(x) \quad \leftrightarrow \quad \neg\forall x\ (\neg P(x)) \tag{2}$$

Let's try to understand why these two propositions are valid at an intuitive level. First, let's check that they hold in a special case. Suppose that the domain of discourse $\mathcal{U}$ is the set of 6.042 tutors, and let the predicate $P(x)$ be true if x is an MIT student. Then the first proposition above says:

"All 6.042 tutors are MIT students."
$\leftrightarrow$ "There is no 6.042 tutor who is not an MIT student."

These two phrases certainly seem to be equivalent! Proposition 2 says:

"Some 6.042 tutor is an MIT student."
$\leftrightarrow$ "Not every 6.042 tutor is not an MIT student."

Again, the two phrases seem to be equivalent.

More generally, these two propositions can be regarded as extensions of DeMorgan's laws from propositional logic. If we stick with our earlier definition of the domain of discourse $\mathcal{U}$ and predicate P, then proposition 1 is equivalent to the assertion:

$$\begin{aligned} &P(\text{Blaise}) \wedge P(\text{Min}) \wedge P(\text{Sam}) \wedge \ldots \wedge P(\text{Jon}) \\ &\qquad \leftrightarrow \quad \neg(\neg P(\text{Blaise}) \vee \neg P(\text{Min}) \vee \neg P(\text{Sam}) \vee \ldots \vee \neg P(\text{Jon})) \end{aligned}$$

This statement is a tautology by DeMorgan's laws. Of course, propositions 1 and 2 hold even when the domain of discourse is an infinite set, such as $\mathbb{N}$ or $\mathbb{R}$. In that case, we could not write an analogous statement in propositional logic.

1.3 Order of Quantifiers

The order of quantifiers matters! For example, the following two propositions are not equivalent when the domain of discourse is $\mathbb{N}$.

$$\forall x \exists y\ (x < y)$$
$$\exists y \forall x\ (x < y)$$

The first proposition says, "for every number, there exists a larger number", which is true. The second proposition says, "there exists a number that is larger than every number", which is false.

On the other hand, two quantifiers of the same type can be swapped freely. For example, the following two propositions are equivalent.

$$\exists x \exists y\ (x^2 = y^3)$$
$$\exists y \exists x\ (x^2 = y^3)$$

1.4 Predicates as Sets

A single-variable predicate is naturally associated with a subset of the domain of discourse, namely, the subset over which that predicate is true. This observation has an important consequence. Let P and Q be single-variable predicates, and let A and B be the associated subsets of the domain of discourse:

$$\begin{aligned} A &= \{x \in \mathcal{U} \mid P(x)\} \\ B &= \{x \in \mathcal{U} \mid Q(x)\} \end{aligned}$$

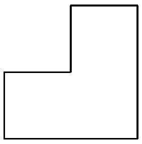
This establishes a correspondence between *set* operators and *logical* connectives. For example, we have:

$$\begin{aligned} A \cap B &= \{x \in \mathcal{U} \mid P(x) \wedge Q(x)\} \\ A \cup B &= \{x \in \mathcal{U} \mid P(x) \vee Q(x)\} \\ (A \subseteq B) &\leftrightarrow \forall x\ P(x) \rightarrow Q(x) \end{aligned}$$

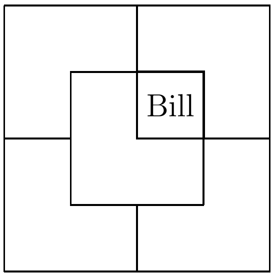
Thus, we can translate many statements about sets into logical assertions and vice versa. DeMorgan's laws, for example, can be regarded as set identities or logical tautologies.

2 The Triomino Puzzle

MIT is constructing an expensive new building called the Stata Center that will house many of MIT's computer science research groups. The architect has designed an atrium with a central plaza that is divided into $2^n \times 2^n$ squares. Most of this plaza will be covered by *triomino* tiles, each of which covers three plaza squares:



However, one square in the plaza will be occupied by a statue of Bill Gates, in the hope that he'll donate more money to cover the Stata Center's cost overruns. One possible configuration of the plaza is shown below. Here, $n = 2$ and Bill is near the center.



Can MIT offer to place the statue wherever Bill wants it to go? That is, can you prove that, regardless of where the statue is placed, the remainder of a $2^n \times 2^n$ plaza can be covered with triomino tiles?

2.1 Induction

The tiling problem can be solved using *mathematical induction*. Induction is by far the most commonly-used proof technique in discrete mathematics and computer science. Induction comes into play when you are trying to prove that some predicate $P(n)$ is true for all $n \in \mathbb{N}$. This is the case in the tiling problem, where we want to prove that the following predicate is true for all $n \in \mathbb{N}$:

$$P(n) \quad = \quad \text{“for all positions of the statue, a } 2^n \times 2^n \text{ plaza can be tiled with triominos”}$$

The principle of induction can be expressed concisely in logic notation, where the domain of discourse is $\mathbb{N}$:

$$\frac{\begin{array}{l} P(0) \\ \forall n \; P(n) \rightarrow P(n+1) \end{array}}{\forall n \; P(n)}$$

Let's use an analogy to clarify what this means. Suppose that we set up an infinite chain of dominoes numbered 0, 1, 2, 3, ... If we tip over the first domino and each domino knocks over the next one, then it makes sense that every domino falls over eventually. Induction makes sense for the same reason. If you prove proposition $P(0)$ (tip the first domino) and show that proposition $P(n)$ implies proposition $P(n+1)$ for all n (every domino knocks over the next one), then we can conclude that $P(n)$ is true for all n (every domino falls).

Here is a simple example of a theorem proved by induction.

Theorem 2 *For all $n \in \mathbb{N}$, the following equation holds:*

$$\sum_{i=1}^{n} 2i - 1 \quad = \quad n^2$$

Proof. The proof is by induction on n. Let $P(n)$ be the proposition that $\sum_{i=1}^{n} 2i - 1 = n^2$.

First, we must prove that $P(0)$ is true; that is, we must show that $\sum_{i=1}^{0} 2i - 1 = 0^2$. This equation holds, because both sides are equal to zero; in particular, the summation on the left contains no terms.

Next, we must prove that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. We do this by assuming that $P(n)$ is true and showing that this implies that $P(n+1)$ is true as well. (In terms of our analogy, we must show that the $(n+1)$-st domino falls, assuming that the n-th domino falls.) More specifically, we assume $\sum_{i=1}^{n} 2i - 1 = n^2$ in order to prove that $\sum_{i=1}^{n+1} 2i - 1 = (n+1)^2$. We can reason as follows:

$$\begin{aligned} \sum_{i=1}^{n+1} 2i - 1 \quad &= \quad \left(\sum_{i=1}^{n} 2i + 1 \right) + (2(n+1) - 1) \\ &= \quad n^2 + (2(n+1) - 1) \\ &= \quad (n+1)^2 \end{aligned}$$

In the first step, we split out the last term in the summation. In the second step, we use our assumption, $P(n)$. The final step is simplification. This shows that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. Therefore, by the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

This proof has five parts that should appear in every induction proof you write.

1. State that the proof is by induction. If there is chance of confusion, indicate what variable indexes the sequence of predicates that you are trying to prove.

2. Define the predicate $P(n)$. This is usually called the *induction hypothesis*.

3. Prove that $P(0)$ is true. This is usually called the *base case.*

4. Prove that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. Do this by assuming that $P(n)$ is true while you are trying to prove that $P(n+1)$ is true. This is usually called the *inductive step.*

5. Conclude that $P(n)$ is true for all $n \in \mathbb{N}$ by the principle of induction.

2.2 Solving the Puzzle

Now let's use induction to prove that the plaza can be tiled, regardless of where Bill wants his statue.

Theorem 3 *A $2^n \times 2^n$ plaza with a statue in any position can be tiled with triominos.*

Proof. The proof is by induction on n. Let $P(n)$ be the proposition that for all positions of the statue, a $2^n \times 2^n$ plaza can be tiled with triominos.

First, note that $P(0)$ is true trivially. A statue can only be placed in one position in a $2^0 \times 2^0 = 1 \times 1$ plaza, and then there is nothing left to tile.

Now we must prove that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$. We do this by assuming $P(n)$ and then showing that this implies $P(n+1)$. More specifically, we assume that for all positions of the statue, a $2^n \times 2^n$ plaza can be tiled with triominos. Then we must show that for all positions of the statue, a $2^{n+1} \times 2^{n+1}$ plaza can be tiled with triominos.

The argument is as follows. Divide the $2^{n+1} \times 2^{n+1}$ plaza into four quadrants, each of size $2^n \times 2^n$. One quadrant must contain the statue. We can tile this quadrant by our assumption, $P(n)$. Now place a triomino in the center of the courtyard so that it covers one square in each remaining quadrant. All that remains is to tile each of these three quadrants, excluding the one square in each that is already covered. However, this can also be done by our assumption $P(n)$; if we suppose that a statue occupies the one already-covered square, then $P(n)$ says that the remainder of the quadrant can be tiled. This proves that $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$.

Therefore, the theorem is true by the principle of induction. □

3 The Unstacking Game

Here is another fun 6.042 game! You begin with a stack of n boxes. Then you make a sequence of moves. In each move, you divide one stack of boxes into two stacks. The game ends when you have n stacks, each containing a single box. You earn points for each move; in particular, if you divide one stack into two stacks with heights a and b, then you score

ab points for that move. Your overall score is the sum of the points that you earn for each move. What strategy should you use to maximize your total score in this game?

As an example, suppose that we begin with a stack of $n = 10$ boxes. Then the game might proceed as follows:

10										
5	5									25 pts
5	3	2								6 pts
4	3	2	1							4 pts
2	3	2	1	2						4 pts
2	2	2	1	2	1					2 pts
1	2	2	1	2	1	1				1 pts
1	1	2	1	2	1	1	1			1 pts
1	1	1	1	2	1	1	1	1		1 pts
1	1	1	1	1	1	1	1	1	1	1 pts
										45 pts

The heights of stacks are listed on the left and the score for each move is given on the right. This strategy gives 45 points. Can you do better?

3.1 Strong Induction

We'll analyze the unstacking game using a variant of induction called *strong induction*. Strong induction and ordinary induction are used for exactly the same thing: proving that a predicate $P(n)$ is true for all $n \in \mathbb{N}$. The principle of strong induction can be written in logic notation as follows:

$$\frac{\begin{array}{l} P(0) \\ \forall n \; P(0) \wedge P(1) \wedge \ldots \wedge P(n-1) \rightarrow P(n) \end{array}}{\forall n \; P(n)}$$

The only change from the ordinary induction principle is in the second line: strong induction allows you to assume more stuff in the inductive step of your proof! In an ordinary induction proof, you assume that $P(n)$ is true and try to prove that $P(n+1)$ is also true. In a strong induction argument, you may assume that $P(0)$, $P(1)$, ..., $P(n-1)$, and $P(n)$ are *all* true when you go to prove $P(n+1)$. These extra assumptions can only make your job easier!

There's no reason not to use strong induction all the time; you can't use it up! However, if you actually make use of $P(0)$, $P(1)$, ..., or $P(n-1)$ in the inductive step of your argument, you should warn the reader at the start of your proof by saying something like, "This proof uses strong induction" as opposed to something like "This proof uses induction."

3.2 Analyzing the Game

Now lets analyze the unstacking game using strong induction. We'll prove the remarkable fact that your score is determined entirely by the number of boxes; your strategy is irrelevant!

There is one trick in this proof that is used in many induction arguments. Ordinarily, we prove $P(0)$ and then show that $P(0) \wedge P(1) \wedge \ldots \wedge P(n) \rightarrow P(n+1)$ for all $n \geq 0$. In this case, however, we shift all our indices up by 1. That is, we prove $P(1)$ and then show $P(1) \wedge P(2) \wedge \ldots \wedge P(n) \rightarrow P(n+1)$ for all $n \geq 1$. This is purely a matter of convenience stemming from the fact that the unstacking game only makes sense when there is at least one box. Mathematically, it is no more significant than switching from variables named $z_0, \ldots, z_{k-1}$ to variables named $z_1, \ldots, z_k$.

Theorem 4 *Every way of unstacking n blocks gives a score of $n(n-1)/2$ points.*

Proof. The proof is by strong induction. Let $P(n)$ be the proposition that every way of unstacking n blocks gives a score of $n(n-1)/2$.

If $n = 1$, then there is only one block. No moves are possible, and so your score is $1(1-1)/2 = 0$. Therefore, $P(1)$ is true.

Next, for all $n \geq 1$, we must show that $P(n+1)$ follows, if we assume $P(1)$, $P(2)$, …, $P(n)$. So suppose that we have a stack of $n+1$ blocks. On your first move, you must split this into two nonempty substacks with sizes k and $n+1-k$ for some k. Now your total score is equal to the points you get for this first move plus the points you get for unstacking the first substack plus the points you get for unstacking the second substack; that is:

$$\begin{aligned}
&(\text{score for 1st move}) + (\text{score from 1st substack}) + (\text{score from 2nd substack}) \\
&\quad = k(n+1-k) + \frac{k(k-1)}{2} + \frac{(n-k+1)(n-k)}{2} \\
&\quad = \frac{2kn + 2k - 2k^2 + k^2 - k + n^2 - nk + n - nk + k^2 - k}{2} \\
&\quad = \frac{(n+1)((n+1)-1)}{2}
\end{aligned}$$

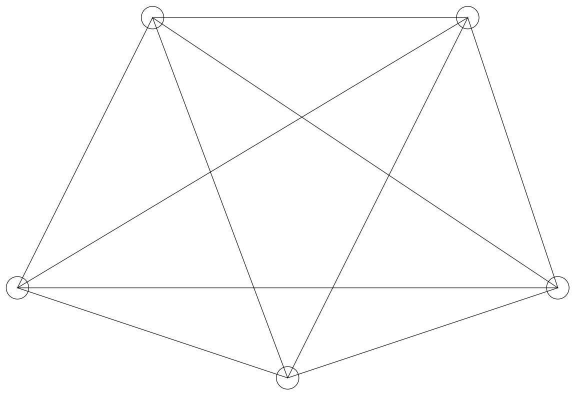
The first step uses the assumptions $P(k)$ and $P(n+1-k)$. We then expand in the second step and simplify in the third. This shows that $P(1)$, $P(2)$, …, $P(n)$ imply $P(n+1)$.

Therefore, the claim is true by strong induction. $\square$

3.3 An Alternative "Proof"

Suppose that we track your progress in unstacking n boxes on a diagram consisting of n dots, where each pair of dots is joined by a line. (Later, we'll learn that this is a picture of

K_n, the complete graph on n nodes.) This diagram has $n(n-1)/2$ lines, since each of the n dots touches $n-1$ lines, but this counts each line twice. For example, for $n = 5$, we would have the diagram:



Associate each box with a dot in this diagram. When you divide a stack of boxes into two substacks, mark every line that joins a box in the first substack to a box in the second substack. Notice that your score for a move is equal to the number of lines that you mark for that move. Furthermore, over the course of the game, you mark each line exactly once. Therefore, your total score for the unstacking game is exactly $n(n-1)/2$!