Massachusetts Institute of Technology
6.042J/18.062J: Mathematics for Computer Science
Professors Nancy Lynch and Srini Devadas

Handout 13
September 18, 1998

Notes for Recitation 2 (9/18/98)

We'll look at several more examples of proof by induction. Aside from the induction method, these examples demonstrate some Math that comes up a lot in Computer Science: sets, Boolean variables, and modular arithmetic. After that, we'll look at some variations on induction and wrap up with some team problems.

1 Examples of Proof by Induction

Induction Proof Method

While the plan for writing an induction proof is clear, there is no rigid plan for finding such a proof. There are, however, a few good tricks to know. There are usually two difficulties in completing a proof by induction: choosing the right induction hypothesis $P(n)$ and completing the inductive step. (Sometimes proving the base case is also hard.) The most obvious candidate for an induction hypothesis is the theorem statement itself.

Method 1 *When searching for a proof by induction, first try to lift an induction hypothesis directly from the theorem statement.*

To complete the inductive step, we must prove that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$. Typically $P(n)$ and $P(n+1)$ are very similar statements, but with some small difference or gap. The challenge is to clearly identify this gap and then to bridge it with some extra facts. Working "backward" is often helpful.

Method 2 *To prove $P(n) \Rightarrow P(n+1)$, write down $P(n+1)$ and then use $P(n)$ to reduce this statement to a simpler assertion; this assertion is the extra fact needed to bridge the gap from $P(n)$ to $P(n+1)$ and complete the proof.*

Examples

Theorem 1.1 *(Distributive Law) Let $A, B_1, B_2, \ldots, B_n$ be sets where $n \geq 1$. Then*

$$A \cap (B_1 \cup B_2 \cup \ldots \cup B_n) = (A \cap B_1) \cup \ldots \cup (A \cap B_n).$$

We saw a special case of this theorem last week in tutorial. In particular, we looked at the case of $n = 2$, i.e. $A \cap (B_1 \cup B_2) = (A \cap B_1) \cup (A \cap B_2)$. This was proven by showing that each set contains the other. We will actually use this result in the proof below of the more general theorem.

Here is the game plan for the proof. We'll take the induction hypothesis directly from the theorem statement. This means that in the inductive step, we will have to show that $A \cap (B_1 \cup B_2 \cup \ldots \cup B_n \cup B_{n+1})$ is equal to $(A \cap B_1) \cup \ldots \cup (A \cap B_n) \cup (A \cap B_{n+1})$. We can almost do this; by induction, we can transform the almost-as-big expression $A \cap (B_1 \cup B_2 \cup \ldots \cup B_n)$ into something good. All that remains is to handle that extra term, B_{n+1}. We'll do this by using the $n = 2$ result from last week.

This basic strategy, proving something for $n = 2$ and then generalizing with induction, is very common. In fact, we'll use exactly the same approach in the next example as well.

Proof. The proof is by induction on n.

Induction hypothesis: Let $P(n)$ be the predicate

$$A \cap (B_1 \cup B_2 \cup \ldots \cup B_n) = (A \cap B_1) \cup \ldots \cup (A \cap B_n).$$

Base case: $P(0)$ is true because both sides of the equation are equal to A.

Inductive step: For all $n \geq 0$, assume

$$A \cap (B_1 \cup B_2 \cup \ldots \cup B_n) = (A \cap B_1) \cup \ldots \cup (A \cap B_n)$$

in order to prove

$$A \cap (B_1 \cup B_2 \cup \ldots \cup B_n \cup B_{n+1}) = (A \cap B_1) \cup \ldots \cup (A \cap B_n) \cup (A \cap B_{n+1}).$$

Let $C = B_1 \cup B_2 \cup \ldots \cup B_n$. Then we can rewrite the left side of $P(n+1)$ as follows:

$$\begin{aligned}
A \cap (B_1 \cup B_2 \cup \ldots \cup B_n \cup B_{n+1}) &= A \cap (C \cup B_{n+1}) \\
&= (A \cap C) \cup (A \cap B_{n+1}) \\
&= (A \cap (B_1 \cup B_2 \cup \ldots \cup B_n)) \cup (A \cap B_{n+1}) \\
&= (A \cap B_1) \cup \ldots \cup (A \cap B_n) \cup (A \cap B_{n+1})
\end{aligned}$$

In the first step, we replace a bunch of terms with the variable C. This simplifies the original expression enough so that we can use the result from last week, which gives the second equality. In the third step, we substitute that bunch of terms back for C so that in the last step, we can use the induction hypothesis. This proves that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$. ■

DeMorgan's Law for boolean variables is

$$\overline{x \vee y} = \overline{x} \wedge \overline{y}$$

where x and y are Boolean variables. We can prove this with the truth table method:

x	y	$\overline{x \vee y}$	$\overline{x} \wedge \overline{y}$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

By inspection of the truth table, $\overline{x \vee y} = \overline{x} \wedge \overline{y}$ in all cases.

The next theorem generalizes DeMorgan's Law to an arbitrary number of Boolean variables in much the same way that the previous theorem generalized the distributive law to an arbitrary number of sets.

Theorem 1.2 *(DeMorgan's Law) For Boolean variables $x_1, x_2, \ldots, x_n$ and $n \geq 1$,*

$$\overline{(x_1 \vee x_2 \vee \ldots \vee x_n)} = \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n}.$$

We will follow the same strategy as before. $P(n)$ and $P(n+1)$ are very similar except that $P(n+1)$ contains one more variable. We will bridge this gap between $P(n)$ and $P(n+1)$ with the two-variable special case of the theorem proven above.

Proof. The proof is by induction on n.

Induction hypothesis: Let $P(n)$ be the predicate:

$$\overline{(x_1 \vee x_2 \vee \ldots \vee x_n)} = \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n}$$

Base case: The predicate $P(1)$ true because both sides are equal to $\overline{x_1}$.

Inductive step: For all $n \geq 1$ assume

$$\overline{(x_1 \vee x_2 \vee \ldots \vee x_n)} = \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n}$$

in order to prove

$$\overline{(x_1 \vee x_2 \vee \ldots \vee x_n \vee x_{n+1})} = \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n} \wedge \overline{x_{n+1}}.$$

Let $y = (x_1 \vee x_2 \vee \ldots \vee x_n)$. Then we can rewrite the left side of $P(n+1)$ as follows:

$$\begin{aligned}
\overline{(x_1 \vee x_2 \vee \ldots \vee x_n \vee x_{n+1})} &= \overline{(y \vee x_{n+1})} \\
&= \overline{y} \wedge \overline{x_{n+1}} \\
&= \overline{x_1 \vee x_2 \vee \ldots \vee x_n} \wedge \overline{x_{n+1}} \\
&= \overline{x_1} \wedge \overline{x_2} \wedge \ldots \wedge \overline{x_n} \wedge \overline{x_{n+1}}
\end{aligned}$$

The rationale for each step exactly parallels the previous proof. In the first step, we replace a bunch of terms with the variable y. This simplifies the original expression so that we can use the two variable result. This gives the second equality. In the third step, we substitute the bunch of terms back for y. Finally, we use the induction hypothesis. This proves that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$. ■

A Review of Modular Arithmetic

Recall the $\equiv$ mod notation from Rosen 2.3: $x \equiv y \pmod{q}$ iff $q|(x-y)$ for integers x, y, q. In words, this says x is "congruent" to y "mod" q if and only if q evenly divides $x - y$; another way to formulate this is to say that x and y have the same remainder after division by q. For example, $15 \equiv 3 \pmod{6}$ since 6 evenly divides $15 - 3 = 12$; both 15 and 3 have remainder 3 after division by 6.

While $x \equiv y \pmod{q}$ is a statement, like an equation, the similar-looking notation $a \bmod b$ stands for an integer quantity, namely, $a \bmod b$ is the remainder when a is divided by b. More precisely, this is the number r such that $a = bq + r$ where q is an integer and $0 \leq r < b$. The number b is required to be at least 1. For example, $15 \bmod 6$ is equal to 3 because $15 = 6 \cdot 2 + 3$. Now we have:

$$x \equiv y \pmod{q} \quad \text{iff} \quad [x \bmod q = y \bmod q].$$

Theorem 1.3 *If n is an positive odd integer, then $n^2 \equiv 1 \pmod{8}$.*

This theorem is a little different in that we are not required to prove a result for all positive n, but just for positive *odd* n.

There are two ways to handle this problem. One approach is to reformulate the theorem: if $k \geq 0$, then $(2k+1)^2 \equiv 1 \pmod{8}$. It is easy to see that this is equivalent to the original theorem, since the expression $2k+1$ will take on all positive odd values as k takes on all non-negative values. Now an ordinary proof by by induction on k will work.

A second approach is to use a variant of induction. Suppose that we prove proposition $P(1)$ and prove that for all positive odd integers n, $P(n) \Rightarrow P(n+2)$. Then we should believe that $P(1), P(3), P(5), \ldots$ are all true for the same reason that we believe ordinary induction works. In effect, we introduce a new axiom just as credible as the original induction axiom. We will use this second approach in the proof.

Introducing new induction-like axioms all the time might not seem like a good idea. But all of these little variants on induction can be proven from the simple, original axiom. So there is no great harm. The key point is that there must be a chain of implications extending from each predicate back to the base case (or cases).

Proof. The proof is by induction on n.

Induction hypothesis: Let $P(n)$ be the predicate $n^2 \equiv 1 \pmod 8$.

Base case: $P(1)$ is true because $1^2 \equiv 1 \pmod 8$.

Inductive step: For all $n \geq 1$ assume that $n^2 \equiv 1 \pmod 8$ and n is a positive odd integer to show that $(n+2)^2 \equiv 1 \pmod 8$. Since n is an odd integer, $4n + 4 \equiv 0 \pmod 8$. Adding this to the induction hypothesis implies $n^2+4n+4 \equiv 1+0 \pmod 8$. Rewriting the left side gives $(n+2)^2 \equiv 1 \pmod 8$. Therefore for all positive odd n, $P(n) \Rightarrow P(n+2)$. ■

This proof contains a little mystery. Where did the magic term $4n + 4$ come from? Here is the reasoning that one might follow to discover the inductive step in this proof. We want to prove that $(n+2)^2 \equiv 1 \pmod 8$, and we can assume that $n^2 \equiv 1 \pmod 8$. To go from the assumption to the desired result, we need to add a little bit to the left side, changing n^2 to $(n+2)^2$. The value of this little bit is $(n+2)^2 - n^2 = 4n+4$. We lucked out because, it is not hard to see that this is always a multiple of 8 when n is odd. Arranging these observations into a straight line of reasoning gives the proof.

2 Proving Statements with Two Variables

Sometimes the statement of a theorem involves two natural-valued variables. In such situations, panicking is not strictly necessary, but sometimes unavoidable. Here is an example:

Theorem 2.1 *For all n and k such that $n \geq k \geq 0$, $k!$ divides $n(n-1)(n-2)\ldots(n-k+1)$.*

First a notation clarification. If $k = 0$, then the expression $n(n-1)(n-2)\ldots(n-k+1)$ is a product with no terms, which we define to be 1. If $k = 1$, then the expression is n.

There are several ways to approach this problem. One way is to define a sort of two-dimensional array of predicates $Q(n, k)$. Then we could prove sufficient base cases and implications so that every predicate $Q(n,k)$ followed from some proven bases cases through a chain of proven implications. The theorem would then follow from a fancy variant of the induction axiom.

A second approach is to eliminate a variable and use ordinary induction. Eliminating a variable may not be easy. The next two theorems will demonstrate different ways that sometime work.

The first way is to introduce a quantifier into the induction hypothesis. In this example, we can use the hypothesis, "For all k such that $n \geq k \geq 0$, $k! \mid n(n-1)\ldots(n-k+1)$. If we prove this statement for all $n \geq 0$, then we have proven the theorem. Though the induction hypothesis contains two variables, we only need to induct on n; you never have to induct on a quantified variable. In effect, we will prove a whole row of $Q(n,k)$ predicates in each step of the proof.

Proof. The proof is by induction on n.

Induction hypothesis: Let $P(n)$ be the predicate that for all k such that $n \geq k \geq 0$, $k! \mid n(n-1)\ldots(n-k+1)$.

Base case: $P(0)$ is true because k is then restricted to be 0, and $0! = 1$ divides every integer.

Inductive step: Assume that for all k such that $n \geq k \geq 0$, $k! \mid n(n-1)\ldots(n-k+1)$ in order to prove that for all k such that $(n+1) \geq k \geq 0$, $k! \mid (n+1)n(n-1)\ldots(n-k+2)$.

There are three cases to check. If $k = 0$, then the statement is true because $0! \mid 1$. If $k = n+1$, then the statement is true because $(n+1)! \mid (n+1)n(n-1)\ldots(1)$.

All that remains is to prove that $k! \mid (n+1)n(n-1)\ldots(n-k+2)$ for k in the range $n \geq k > 0$. By induction we know:

$$\begin{aligned}
&k! \mid n(n-1)\ldots(n-k+1) \\
&(k-1)! \mid n(n-1)\ldots(n-k+2)
\end{aligned}$$

(We need to use these two facts, and this is the reason why $k = 0$ and $k = n+1$ are treated as special cases. If $k = n+1$, then the first fact does not follow by induction. If $k = 0$, then the second fact does not follow.)

If we multiply both sides of the second fact by k, and then add both facts together, we obtain:

$$\begin{aligned}
& k! \mid n(n-1)\ldots(n-k+1) + kn(n-1)\ldots(n-k+2) \\
\Rightarrow\ & k! \mid ((n-k+1)+k)n(n-1)\ldots(n-k+2) \\
\Rightarrow\ & k! \mid (n+1)n(n-1)\ldots(n-k+2)
\end{aligned}$$

This shows that for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$ and completes the proof. ■

The algebra in this proof is sneaky and one probably wouldn't think of this proof right away. The key idea here is working with a quantifier in the induction hypothesis.

Sharing Chocolate

We are given a chocolate bar with $m \times n$ squares of chocolate and our task is to divide it into mn individual squares. We are only allowed to split one piece of chocolate at a time using a vertical or a horizontal break.

For example, suppose that the chocolate bar is 2×2. The first split makes two pieces, both 2×1. Each of these pieces requires one more split to form single squares. This gives a total of three splits. We would like to prove the following general result:

Theorem 2.2 *To divide up a chocolate bar with $m \times n$ squares, we need exactly $mn - 1$ splits.*

Once again, we have two variables. If one variable can be eliminated, then ordinary induction will suffice. We could try the previous technique of formulating an induction hypothesis with a quantifier.

But let's try a second approach. Intuitively, to break up a big chocolate bar, we need one split to make two pieces, and then we can break up the two pieces recursively. This suggests a proof using strong induction on the *size* of the chocolate bar. The size can be defined to be mn, the area measured in chocolate squares.

This gives a second trick for using ordinary induction to prove a theorem with two variables: apply induction on a *function* of the variables.

Proof. The proof is by strong induction on mn.

Inductive hypothesis: Let $P(k)$ be the predicate that a chocolate bar of size k requires $k - 1$ splits.

Base case: In the base case, $P(1)$ is true because there is only a single square of chocolate and so $1 - 1 = 0$ splits are required.

Inductive step: For all $k \geq 1$, assume that a chocolate bar of size s requires $s - 1$ splits where $k \geq s \geq 1$ in order to prove that a chocolate bar of size $k + 1$ requires k splits.

First, we will have to break the chocolate bar of size $k + 1$ into two smaller pieces of size p and q where $p + q = k + 1$. Then, by strong induction, breaking up the two pieces will require $p - 1$ and $q - 1$ splits. The total number of splits is therefore $1 + (p - 1) + (q - 1) = p + q - 1 = (k + 1) - 1 = k$. ■

3 Team Problems

1. *Handshakes.* I recently went to a party with my spouse; there were 11 other married couples there. A lot of handshaking happened (but of course no one shook hands with their spouse). At the end, it turned out that for every k from 0 to 22, someone other than me had shaken hands with exactly k people. How many people did I shake hands with? Prove your answer.

   Note that there are 24 people (12 couples) in this case.

   We will prove the following for a set of n couples:

   Theorem 3.1 *Suppose at a party for n couples (total) it turns out that someone other than me has shaken k hands for every k from 0 to $2n-2$. Then I must have shaken $n-1$ hands.*

   Proof. By induction on n.

   I.H. $P(n)$: At an n couple party, if someone other than me shakes k hands for every k from 0 to $2n-2$ then I must have shaken $n-1$ hands.

   Base: $n = 1$. There are no other couples. My wife has shaken 0 hands (can't shake with me). I have shaken 0 hands ($= n-1$). (some party!)

   I.H. Assume $P(n-1)$ is true. To prove $P(n)$, consider a party with n couples.

   Someone has shaken $2n-2$ hands, i.e., with everyone in the room except themselves and their spouse. Therefore everyone else but this couple has shaken hands at least once. So the one who hasn't shaken hands at all must be this person's spouse. $2n-2$ is paired with 0. Consider the subparty of the remaining $n-1$ couples. I must be in this group since there cannot be two people who shook hands $2n-2$ times or 0 times. Consider the number of times this group of people has shaken hands among themselves, i.e., not counting handshakes with the $2n-2, 0$ couple. Then the number of handshakes I see is every number between 0 and $2n-4$. This is because this group of people has original handshake counts of $1, 2, 3, \ldots, 2n-3$. Since everyone shakes the $2n-2$ person's hand once, we are left with handshake counts of $0, 1, \ldots, 2n-4$. This is exactly the premise of $P(n-1)$. So by the I.H. I must have shaken $n-2$ hands within this group. Adding the one handshake with the $2n-2, 0$ couple, I must have shaken a total of $n-1$ hands. ■

   For $n = 12$, the answer is that I shook 11 hands.

2. *Geometric mean vs Arithmetic mean.* Show that for any real numbers $x_1, x_2, \ldots, x_n$,

$$(x_1 x_2 \ldots x_n)^{\frac{1}{n}} \leq \left(\frac{x_1 + x_2 + \ldots + x_n}{n} \right)$$

By strong induction on n.

Notation: $AM(x_1 \dots x_n) = \frac{x_1+..+x_n}{n}$

Ind. Hyp. $(x_1 x_2 \dots x_n) \leq (AM(x_1, .., x_n))^n$

Base case. $n = 1$: $x_1 \leq x_1$.

$n = 2$: $4x_1x_2 \leq (x_1 + x_2)^2$

or $0 \leq (x_1 - x_2)^2$ which is true.

Ind step. Assume $P(1) \wedge P(2) \wedge \dots \wedge P(n-1)$ is true to prove $P(n)$.We will prove $P(n)$ separately for odd values of n and even values of n.

1. n is even.

   Then,
   $$\begin{aligned}(x_1x_2 \dots x_n) &= (x_1x_2 \dots x_{n/2})(x_{n/2+1}x_{n/2+2} \dots x_n) \\ &\leq AM(x_1..x_{n/2})^{\frac{n}{2}} AM(x_{n/2+1}..x_n)^{\frac{n}{2}}\end{aligned}$$
   Using $P(\frac{n}{2})$,
   $$\begin{aligned}&\leq [AM(x_1..x_{n/2})AM(x_{n/2+1}..x_n)]^{\frac{n}{2}} \\ &\leq [(AM(x_1..x_{n/2}) + AM(x_{n/2+1}..x_n))/2]^n\end{aligned}$$
   (from $P(2)$)
   $$\leq [AM(x_1..x_n)]^n$$

2. n is odd. Then we show that
   $$P(\frac{n+1}{2}) \rightarrow P(n+1) \rightarrow P(n).$$
   Assume $n \geq 2$. Then $\frac{n+1}{2} < n$ and hence we can assume from the I.H. that $P(\frac{n+1}{2})$ is true. The proof of the first implication is then identical to earlier case.

   To show $P(n+1) \rightarrow P(n)$,

   Start with P(n+1). Let $x_{n+1} = \frac{x_1+x_2+...+x_n}{n}$. This implies $x_{n+1} = \frac{x_1+...+x_{n+1}}{n+1}$. Which means that $AM(x_1, \dots, x_n) = AM(x_1, \dots, x_{n+1})$ for this choice of x_{n+1}.

   Then $P(n+1)$ is
   $$x_1x_2 \dots x_nx_{n+1} \leq AM(x_1, \dots, x_{n+1})^{n+1}$$
   Dividing both sides by x_{n+1} we have:
   $$\begin{aligned}x_1x_2 \dots x_n &\leq AM(x_1, \dots x_{n+1})^n \\ &= AM(x_1, \dots x_n)^n\end{aligned}$$