Math 23b Proof writing notes 4 Fall, 2007

Homeworks 4 and 5 are both about induction. (HW4 is simple induction. HW5 is more complicated forms of induction.)

Simple induction

Here is an outline of how simple induction proofs are written.

1 Write down the statement $P(n)$ and say that you will prove it "by induction on n."

2 Do the base case. This is usually $n = 1$ but it could be $n = 0$ or some other number. "First we will verify the base case when $n = 1$."

3 The induction step is logically: $P(n) \Rightarrow P(n+1)$. You need to say that your are assuming $P(n)$. For example: "We will assume by induction that the statement holds for n and we will show that it holds for $n + 1$."

3' The book changes the letter to k. This makes the logic a little clearer: "We will assume that the statement $P(n)$ holds for $n = k$. Then we will show that it holds for $n = k + 1$." I suggest you do that if it is not clear exactly what happens when you replace n with $n + 1$. (Substituting $n = k + 1$ is clearer. Then you know, e.g., that $k = n - 1$.)

Example 1

Prove that a finite set has 2^n elements where n is the number of elements of the set.

Answer 1. (standard method)

1) Suppose that S is a set containing n elements. Then we will show by induction on n that S has 2^n elements.

2) The base case is $n = 0$. In this case S is empty. The empty set has exactly one subset, namely itself. Here is a proof. Suppose that T is a subset of the empty set S. Then any element of T is an element of S which is a contradiction. Therefore, T has no elements. Therefore, T is the empty set.

3) Suppose by induction that any set with n elements has 2^n elements. Then we will show that any set with $n + 1$ elements has 2^{n+1} elements.

4) Let T be a set with $n+1$ elements. Call them $x_1, x_2, \cdots, x_n, x_{n+1}$. Let S be the subset $S = \{x_1, \cdots, x_n\}$. Then, we know by induction that S has $k = 2^n$ subsets. Let $A_1, A_2, \cdots, A_k$ be the subsets of S.

5) The subsets of T are $A_1, A_2, \cdots, A_k$ and $B_1, B_2, \cdots, B_k$ where $B_i = A_i \cup \{x_{n+1}\}$. To prove this, let C be any subset of T. Then either C contains x_{n+1} or it doesn't. If C does not contain x_{n+1} then C is contained in S. So, $C = A_i$ for some i. If C contains x_{n+1} then, when we delete x_{n+1} from C we get one of the sets A_i. So, $C = A_i \cup \{x_{n+1}\} = B_i$ in that case.

6) Since we have enumerated all of the subsets of T we see that it has $2 \times 2^n = 2^{n+1}$ subsets. Since T was an arbitrary set with $n + 1$ elements, this completes the induction and proves the statement for all $n \geq 0$.

Answer 2. (skipping obvious steps and adding unclear steps) We will show by induction on n that a set S with n elements has 2^n subsets. In the first case S is empty $S = \emptyset$ and it has only one subset, namely $\emptyset$. If $n = 1$ then $S = \{x\}$ has two subsets: $\emptyset$ and S since any subset $C \subseteq S$ either contains x or it doesn't. If C contains x then $C = S$ and if C doesn't contain x then $C = \emptyset$. Since $2^0 = 1$ and $2^1 = 2$, the statement holds for $n = 0$ and $n = 1$.

Now suppose by induction that any set with $n \geq 1$ elements has 2^n subsets. Let T be a set with $n + 1$ elements. Take any element $x \in T$. Then $S = T - \{x\}$ has n elements. So, S has 2^n subsets. Each subset A of S gives two subsets of T, namely A and $A \cup \{x\}$. To see that these are all of the subsets of T, take any subset $C \subseteq T$. If $x \notin C$ then C is one of the subsets of S. If $x \in C$ then $C = A \cup \{x\}$ where $A \subseteq S$. Therefore, T has exactly $2 \times 2^n = 2^{n+1}$ subsets and the statement holds for $n + 1$. Therefore, the statement hold for all finite $n \geq 0$.

Example 2

Show by induction on n that

$$\sum_{i=1}^{n} i(i-1)(i-2) = \frac{(n+1)n(n-1)(n-2)}{4} \qquad (*)$$

Answer We will prove this by induction on n. The case $n = 0$ is trivial since both sides are zero. So, suppose the equation holds for n. Then for $n+1$ we add one more term $(n+1)n(n-1)$ to the sum on the left and the same thing on the right to get

$$\sum_{i=1}^{n+1} i(i-1)(i-2) = \frac{(n+1)n(n-1)(n-2)}{4} + (n+1)n(n-1)$$

This simplifies to:

$$(n+1)n(n-1)\left[\frac{n-2}{4} + \frac{4}{4}\right] = (n+1)n(n-1)\left[\frac{n+2}{4}\right]$$

which is the right hand side of (*) for $n+1$. So, (*) holds for all $n \geq 0$.

Comments This proof does not have the "We want to show the following" statement. Since the proof begins with the statement "We will prove this by induction on n" and explicitly assumes the statement for n it is understood that we need to prove $P(n+1)$.

Strong induction

In strong induction you prove statement $P(n)$ assuming the statement holds for all numbers less than n. This is actually a proof by contradiction where n is the first case where the theorem fails.

A proof by strong induction can be phrased in many ways. Here are two basic wordings.

1 You can say "We may assume by induction that the statement holds for all numbers less than n." This assumes the reader is familiar with strong induction.

2 A wording which is closer to the truth is "Suppose the theorem is not true and let n be the smallest counterexample." This makes sense even if the reader has never heard of strong induction.

Note that there is *no base case* since $n = 1$ is included as a possible smallest counterexample. When you prove the statement for n, you actually get a contradiction since n is the first case where the statement fails.

Example 3

Show by induction that every integer $n \geq 2$ is either prime of a product of prime numbers.

Answer Let n be the smallest integer ≥ 2 which is neither prime nor a product of prime numbers. Since n is not prime, $n = ab$ where $a, b \geq 2$. Then $2 \leq a, b < n$. Therefore, by induction, a, b are products of one or more primes. Therefore their product $n = ab$ is a product of one or more primes. So, the theorem holds.

Example 4

Show that $\sqrt{2}$ is irrational.

Answer Suppose this is false. Then there exist positive integers n, m so that $\sqrt{2} = n/m$, i.e. $2 = (n/m)^2$. Let the denominator m be the smallest positive integer so that $n^2/m^2 = 2$ for some other positive integer n (the numerator). Then $n^2 = 2m^2$. So, n must be even. I.e., $n = 2k$ for some positive integer k. Then

$$n^2 = 4k^2 = 2m^2$$

which implies that $m^2 = 2k^2$ or $\sqrt{2} = m/k$. But this fraction has a denominator $k < m$ which contradicts the minimality of m. Therefore, $\sqrt{2}$ is not a rational number.