Math 371, Spring 2013, PSet 2

Aaron Michael Silberstein

January 28, 2013

This problem set will be due Friday, February 1, 2013 at 1 pm in Matti's mailbox.

1 The Craft (and Art) of Writing Proofs: Induction

This week, we will work on writing induction proofs. Unlike routine verification of axioms (last week's topic), induction proofs are somewhat less straightforward. However, they are one of the most powerful tools in the mathematician's toolbox.

A proof by induction uses the inductive principle of the natural numbers: let S be a subset of $\mathbb{N}$ such that $0 \in S$ and if $x \in S$ then $x^s \in S$ (remember: ^{s} means successor). Then $S = \mathbb{N}$. (Here, I am going against my upbringing and using the notation Prof. Pop used last semester: $0 \in \mathbb{N}$.) To prove statements using induction, we need to make a sequence of statements indexed over the integers, $\{\varphi_n\}_{n\in\mathbb{N}}$, and we want to prove that each φ_n is true. Let

$$S_\varphi = \{n \in \mathbb{N} \mid \varphi_n \text{ is true}\}.$$

1. If we show φ_0 is true, we have shown that $0 \in S_\varphi$ (this is called the **base case** of an induction proof).

2. If we show that, assuming φ_n we can prove φ_{n+1}, we have shown that $n \in S_\varphi \implies n^s \in S_\varphi$ so $S = \mathbb{N}$ (this is called the **inductive step**).

So these are our two goals. So in order to do an induction proof, we need to break our statement into an infinite number of statements ordered by the integers. We can do even better, though:

Problem 1. *Let $S \subseteq \mathbb{N}$ be such that $0 \in S$ and for all $n \in \mathbb{N}$, if $m < n \implies m \in S$ then $n \in S$. Prove, using induction, that $S = \mathbb{N}$.*

This problem shows us that, when proving φ_{n+1} we can assume all the statements φ_m for $m \leq n$; this means we have more true statements to use in our proof of the inductive step.

Problem 2. *Prove that the well-ordering principle and the inductive principle are equivalent.*

Here is a typical problem for which you would need induction. If k and n are positive integers, with $k \leq n$, let

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

(where $0! = 1$).

Theorem 1. $\forall\, n \geq 1, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Proof. The induction will be on n. That is, we have the statements

$$\varphi_n : (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

We first prove φ_1 is true. Indeed,

$$(x+y)^1 = x + y = \frac{1!}{0!1!}x + \frac{1!}{1!0!}y.$$

(Note: Usually, the base case of an inductive proof will be a straightforward verification.)

Now, we prove that $\varphi_n \implies \varphi_{n+1}$. So assuming φ_n, we have:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Now,

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y) \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Distributing (and this, itself, is an induction proof, whose steps we will skip over!) we have

$$(x+y)^{n+1} = y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{(k-1)} \right) x^k y^{n+1-k} + x^{n+1}.$$

So now our inductive step is equivalent to proving:

$$\binom{n}{k} + \binom{n}{(k-1)} = \binom{n+1}{k}.$$

So we write this out:

$$\binom{n}{k} + \binom{n}{(k-1)} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!((k-1)!(n-k+1)! + k!(n-k)!)}{k!(n-k)!(k-1)!(n-k+1)!}.$$

(Explanation, not to be included in a proof like what we write: We see that in the denominator, in order to get the correct denominator for $\binom{n+1}{k}$, we want to get rid of the $(n-k)!(k-1)!$. So factoring out the numerator, we have

$$\begin{aligned}\frac{n!((k-1)!(n-k+1)!+k!(n-k)!)}{k!(n-k)!(k-1)!(n-k+1)!} &= \frac{n!(k-1)!(n-k)!((n-k+1)+k)}{k!(n-k)!(k-1)!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n-k+1)!} \\ &= \binom{n+1}{k}.\end{aligned}$$

This proves the inductive step. □

In the next section, when in doubt, use induction!

2 Newton's Theorem on Symmetric Polynomials

At a key point in the quadratic formula, we needed to be able to write $\alpha - \beta$ in terms of coefficients of our quadratic polynomial. Newton's theorem tells us precisely what sorts of expressions in the roots of a polynomial can be written in terms of the coefficients of the polynomial.

We start with the polynomial

$$\prod_{i=1}^{n}(x-\alpha_i) = a_n(\alpha_1,\ldots,\alpha_n) + a_{n-1}(\alpha_1,\ldots,\alpha_n)x + \cdots + a_1(\alpha_1,\ldots,\alpha_n)x^{n-1} + x^n.$$

Our goal is to study these coefficients, the **elementary symmetric polynomials** of $\alpha_1,\ldots,\alpha_n$. Let

$$R_n = K[\alpha_1,\ldots,\alpha_n]$$

be the ring of polynomials in n variables over our field K. Then the symmetric group S_n acts on R_n by, for $\sigma \in S_n$ and $f \in R_n$,

$$f(x_1,\ldots,x_n)\sigma = f(x_{1\sigma},\ldots,x_{n\sigma}).$$

Remember that we always write our permutation actions on the right.

If a group G acts on a set X, we let

$$X^G = \{x \in X \mid \forall\, g \in G, gx = x\} \tag{1}$$

be the **set of G-invariants of X.**

Problem 3. *Prove that S_n acts by ring homomorphisms. In particular, $R_n^{S_n}$ is a subring.*

Problem 4. *Prove that $a_i(\alpha_1, \ldots, \alpha_n) \in R_n^{S_n}$.*

Problem 5. *Consider $\alpha_1^4 + \alpha_2^4 \in R_2$. Write down $\alpha_1^4 + \alpha_2^4$ as a polynomial in a_1 and a_2.*

Problem 6. *Let*

$$P_{n,d} = \{f(\alpha_1, \ldots, \alpha_n) \in K[\alpha_1, \ldots, \alpha_n] \mid f \text{ homogeneous of degree } d\};$$

*recall that a **homogeneous polynomial of degree** d is a sum of monomials, all of degree d. Prove that*

$$R_n = \bigoplus_{d=0}^{\infty} P_{n,d}$$

*is a **grading** of R_n; that is*

1. *If $a_d \in P_{n,d}$ and $a_{d'} \in P_{n,d'}$ then $a_d a_{d'} \in P_{n,d+d'}$.*
2. *Every element of R_n can be written uniquely as a finite sum of elements of $P_{n,d}$.*

Problem 7. *Prove that this grading is preserved under S_n. Thus*

$$R_n^{S_n} = \bigoplus_{d=0}^{\infty} P_{n,d}^{S_n}.$$

Problem 8. *Prove that $a_d(\alpha_1, \ldots, \alpha_n) \in P_{n,d}$. Deduce that*

$$a_1^{m_1} a_2^{m_2} \ldots a_n^{m_n} \in P_{n,\sum_{i=1}^n i m_i}.$$

Problem 9. *For every monomial*

$$\mu = \alpha_1^{m_1} \ldots \alpha_n^{m_n}$$

let

$$w(\mu) = (m_1, \ldots, m_n)$$

*be the ordered tuple of exponents; call this tuple the **weights**. Prove that for $\sigma \in S_n$,*

$$\mu\sigma = w(\mu)\sigma$$

*where S_n acts on n-tuples by permuting the coordinates. Thus, orbits of monomials correspond to unordered tuples $\{m_1, \ldots, m_n\}$. The unordered tuple associated to a monomial μ will be denoted by $\omega(\mu)$. We will think of $\omega(\mu)$ either as an unordered tuple, or we may put an order on it so it becomes non-decreasing (there is a unique way of doing this). In this way, we may use the dictionary order on nondecreasing finite sets to compare weights; we say that $\omega(\mu) \geq \omega(\mu')$ if this is so in the dictionary order, starting from the largest term. Given an unordered or ordered tuple of integers, we will call its **degree** the sum of its elements.*

Problem 10. *Let $a_1^{i_1} \dots a_n^{i_n}$ be a product of elementary symmetric polynomials. Prove that there is a term in $a_1^{i_1} \dots a_n^{i_n}$ of "highest weight".*

Problem 11. *Let $\Omega(\{\mu_1, \dots, \mu_n\})$ be the K-vector space generated by all monomials μ such that*

$$\omega(\mu) = \{m_1, \dots, m_n\}.$$

Prove that

$$P_{n,d} = \bigoplus_{\sum_i m_i = d} \Omega(\{m_1, \dots, m_n\})$$

and that this decomposition is stable under the action of S_n.

Problem 12. *Write down explicitly $\Omega(\{m_1, \dots, m_n\})^{S_n}$.*

Problem 13. *Prove that*

$$R_n^{S_n} = K[a_1, \dots, a_n]$$

so a polynomial is symmetric if and only if it can be written as a polynomial in the elementary symmetric polynomials; furthermore, there is a unique way to write it as such. This is Newton's theorem.