MATH 22

Lecture K: 10/7/2003

MATHEMATICAL INDUCTION

The great tragedy of science: the slaying of a beautiful hypothesis by an ugly fact.

—T. H. Huxley,
"Biogenesis and Abiogenesis"

Administrivia

- http://denenberg.com/LectureK.pdf

- Test problem 3b revisited; answer is

  C(13,1)48 [4 of a kind]

  + C(13,2)C(4,2)^{2}44 [2 pair]

  + C(13,1)C(4,3)C(12,1)C(4,2) [full house]

  (a good lesson in the perils of multiple-counting)

- Unpicked-up homeworks, projects, exams, . . .

- Project 4 available today; due next week

Today: Mathematical induction [*VERY IMPORTANT*], binary relations

Well Ordering

Definition: Let S be any set of numbers. If every nonempty subset of S has a smallest member, then S is said to be *well-ordered*.

Examples:

$\underline{\mathbf{Z}}^+$, the positive integers, is well-ordered since any set of positive integers has a smallest member.

$\underline{\mathbf{Z}}$, the set of *all* integers, is *not* well-ordered. You can see this by taking the nonempty subset $\underline{\mathbf{Z}}$, which has no smallest member.

The set S of all rational numbers between 1 and 2 inclusive is *not* well-ordered. (Consider $S - \{ 1 \}$, the subset consisting of S with the number 1 removed.)

Obvious Theorem: If S is well-ordered, then so is any subset of S. Duh.

We don't actually care at all about well-ordering in this course except for the fact that $\underline{\mathbf{Z}}^+$ is well-ordered. (And even this we have to take this on faith, because we don't know enough about the integers to prove it rigorously!)

Mathematical Induction

Suppose we have a statement S about a number n, which we (now) write as $S(n)$. (S is an *open statement* with *free variable n,* just like p(x) or q(x,y).)

Suppose that we can prove two things:

- The statement is true for n=1, that is, $S(1)$ is true. (*Basis* step)
- Assuming the statement true for an unspecific n, we can prove it true for n+1, that is, $S(n) \rightarrow S(n+1)$. (*Inductive* step.)

We can conclude that $S(n)$ is true for all integers $n \geq 1$. This is the *Principle of Mathematical Induction*.

Proof: Suppose the two sentences above are true of S. Let T be the set of all positive integers k such that S(k) is *false*, that is, $T = \{ k \in \mathbb{Z}^+ \mid \neg S(k) \}$. We want to prove that T is empty.

By contradiction, suppose the contrary. Then T, being a nonempty subset of the positive integers, has a smallest element. Call that element m; so $S(m)$ is false. Now m can't be 1 (since $S(1)$ is true by the basis step), so $m > 1$, so $m-1 \geq 1$. Since $m-1 \notin T$ we know $S(m-1)$ is true (by definition of T). But then $S((m-1)+1)$ is true by the inductive step, which says that $S(m)$ is true. Contradiction.

How To Do It

To review: In order to prove a statement $S(n)$ by mathematical induction, you must do two things:

(a) Prove the *basis step* $S(1)$.

(b) Prove the *inductive step*, $S(n)$ implies $S(n+1)$. You do this by assuming that $S(n)$ is true and (using that assumption) proving that $S(n+1)$ is true.

[Does this seem like cheating, or like *begging the question*? It's not. You assume $S(n)$ for a single (general) n, and prove it true for a different n. It's not cheating. It is, however, magic.]

During the proof of the inductive step, the assumption that $S(n)$ is true is called the *inductive hypothesis*.

Example (reprise): $1 + 2 + 3 + \ldots + n = n(n+1)/2$

Basis step: Let $n=1$. Is $1 = 1(1+1)/2$? Yes; done.

Inductive step: Assume $1+2+\ldots+n = n(n+1)/2$.
To prove the theorem for $n+1$ we must prove that $1+2+\ldots+n+(n+1) = (n+1)((n+1)+1)/2$. Rewrite the LHS as $(1+2+\ldots+n) + (n+1)$, which using the inductive hypothesis is $n(n+1)/2 + (n+1)$. Use algebra to rearrange this into $(n+1)(n+2)/2$. QED

More Examples

For all $n \geq 1$, the number $n^3 + 2n$ is divisible by 3.

Proof by mathematical induction:

Basis step: $1^3 + 2(1) = 3$ is divisible by 3.

Inductive step: Assume $n^3 + 2n$ is divisible by 3. We must prove that $(n+1)^3 + 2(n+1)$ is divisible by 3. But this equals $n^3 + 3n^2 + 3n + 1 + 2n + 2$, which can be rearranged as $(n^3 + 2n) + 3(n^2 + n + 1)$. The first term here is divisible by 3 using the inductive hypothesis, and the second as well since it's 3 times something. The sum of things divisible by 3 is divisible by 3. QED

Let S be any set. If $|S| = n$, then $|P(S)| = 2^n$.

Proof by mathematical induction:

Basis step. If $|S| = 1$ then the only elements of P(S) are $\varnothing$ and S, so P(S) has cardinality $2 = 2^1$.

Inductive step: Let $|S| = n+1$ and pick an $x \in S$. By the inductive hypothesis there are 2^n subsets of S$-\{x\}$; none of these subsets contains x. But adding x to any of these subsets creates a new subset of S that *does* contain x, producing 2^n more subsets of S. And this accounts for all the subsets of S. So the total number of subsets of S is $2^n + 2^n = 2(2^n) = 2^{n+1}$. QED

Horse of a Different Color

Theorem: All horses have the same color.

Proof: We this theorem by proving, via MI, the following statement: If S is any set consisting of n horses, then all horses in S have the same color.

Basis step: If n=1, the set S contains only one horse. Clearly all horses in S have the same color.

Induction step: Suppose that any set of n horses consists of horses all of the same color (inductive hypothesis).

Let S be any set of n+1 horses $H_1, H_2, H_3, \ldots, H_{n+1}$. If we remove H_{n+1} from S we get a set of n horses; by the inductive hypothesis these horses $H_1, H_2, \ldots, H_n$ all have the same color.

Now replace H_{n+1} and remove H_1; the resulting set $H_2, H_3, \ldots, H_{n+1}$ is also a set of n horses, and so by the inductive hypothesis they all have the same color.

But if H_1 is the same color as $H_2, H_3, \ldots, H_n$; and if H_{n+1} is also the same color as $H_2, H_3, \ldots, H_n$, then H_1 and H_{n+1} must be the same color, so $H_1, H_2, H_3, \ldots, H_{n+1}$ are all of the same color. QED

Is something wrong here?

Variation: $n_0 \neq 1$

We don't have to use $S(1)$ in the basis step; we can start by proving $S(0)$ or $S(-1)$ or $S(20)$. Then the resulting theorem, instead of being true for all $n \geq 1$ is true for all $n \geq$ whatever we used in the basis step.

Theorem: $n^{100} < 2^n$ for all $n \geq 1024$.

Proof by mathematical induction:

Basis step. Suppose $n = 1024 = 2^{10}$. Then

$$n^{100} = (2^{10})^{100} = 2^{1000} < 2^{1024} = 2^n$$

so the theorem is true for $n = 1024$.

Inductive step. Assume $n^{100} < 2^n$. Now

$$(n+1)^{100} = n^{100}(1 + 1/n)^{100}$$

The first of these factors is less than 2^n by the inductive hypothesis. And since n ≥ 1024 we have

$$(1+1/n)^{100} \leq (1+1/1024)^{100} \approx 1.1 < 2$$

so

$$n^{100}(1 + 1/n)^{100} < 2^n(2) = 2^{n+1}$$

proving that $(n+1)^{100} < 2^{n+1}$, which is what we were supposed to prove in the inductive step. QED

(The number 100 here is immaterial; it could actually be any integer no matter how large. For large enough n, an exponential function is larger than any polynomial!)

Variation: Strong Form

The following is a stronger way of stating the P. of M.I.:

Suppose $S(n)$ is an open statement with free variable n, and suppose that we can prove two things about $S(n)$:

- (Basis step) $S(1)$ is true.
- (Inductive step) Assuming that $S(1)$, $S(2)$, $S(3)$, . . . , $S(n)$ are all true, we can prove that $S(n+1)$ is true. That is, we can prove $S(1) \wedge S(2) \wedge \ldots \wedge S(n) \Rightarrow S(n+1)$.

Then $S(n)$ is true for all integers $n \geq 1$.

See the difference? In this form of MI we get a stronger inductive hypothesis: To prove $S(n+1)$ we can assume not just $S(n)$ but also all of $S(1)$, $S(2)$, . . ., $S(n-1)$.

(We can combine these variations and start at any n_0, not just 1, of course. Grimaldi gives an even more general version of the strong form, in which you must prove several basis steps.)

Example: Sequences

Define a sequence of numbers as follows:

$$b_0 = b_1 = 1$$

$$\text{for } n \geq 2, \qquad b_n = 2b_{n-1} + b_{n-2}$$

[This is an example of *recursive definition*, where a sequence of numbers (or a set) is defined by using previous elements of the sequence (or other elements of the set). More examples in Grimaldi 4.2.]

Theorem: $b_n < 6b_{n-2}$ for all $n \geq 4$.

Proof by Mathematical Induction (strong form):

Basis step: We must calculate a few more of the b_i:

$$b_2 = 2b_1 + b_0 = 2(1) + 1 = 3$$

$$b_3 = 2b_2 + b_1 = 2(3) + 1 = 7$$

$$b_4 = 2b_3 + b_2 = 2(7) + 3 = 17 < 18 = 6b_2$$

Inductive step: By the (strong) inductive hypothesis:

$$b_{n-1} < 6b_{n-3} \qquad \text{and} \qquad b_n < 6b_{n-2}$$

Therefore $b_{n+1} = 2b_n + b_{n-1} < 12b_{n-2} + 6b_{n-3}$

$$= 6\,(2b_{n-2} + b_{n-3}) = 6b_{n-1}$$ QED

(Notice that the inductive step doesn't go through if all we can use is the bound on b_n!)

Example: Networks

Suppose we start out with N computers that are isolated from each other. We connect them by building links. Each time we link two computers we make it possible for those two computers, and any they are linked to, to communicate. We want to make it possible for all N computers to communicate.

Theorem: We need a minimum of N–1 links to connect N computers.

(This is obvious if we choose one computer as a central server and connect all the others to it, but we want to prove the Theorem for arbitrary connection strategies!)

Proof: Basis step. If there is only 1 computer, we need 0 links to connect it.

Inductive step. Suppose we connect N+1 computers in any way whatever. When we make the final link, we join a set S_1 containing k linked computers (for some k) to a set S_2 containing $(N+1)–k$ linked computers. By the (strong) inductive hypothesis, it took at least k–1 links to connect S_1, and at least $N+1–k–1 = N–k$ links to connect S_2. Then we made one last link at the end Thus we've made a minimum of $(k–1) + (N–k) + 1 = N$ links. QED.

Binary Relations

A *binary relation* is (loosely) a way in which two things may or may not be connected. Our first goal is to get an intuitive understanding of what this means.

Example: "is less than" is a binary relation on numbers. For example, 9 and 12 have the "less than" relation. Of course we usually write the relation symbol between them: $9 < 12$. Note that order is important: 12 and 9 do *not* have the "less than" relation.

Example: "is a parent of" is a binary relation on people. Given two people x and y, "x is a parent of y" may or may not be true. We could use the symbol P for this relation, writing $x \, P \, y$ when x is a parent of y.

Example: "is within 100 miles of" is a binary relation on (say) cities. For example, Boston and Providence have this relation.

Example: "is the same color as" is a binary relation on (say) horses. There definitely exist two horses that *don't* have this relation, spurious proofs notwithstanding.

Formalization

Here's the mathematical definition of binary relations: Given a set S, a *binary relation on S* is a subset of $S \times S$. That is, a binary relation on a set S is a set of ordered pairs where each component is an element of S.

For example, take the binary relation $<$ on the integers:

$$< \;=\; \{\ (9,12),\ (8,50),\ (-3,12),\ (0,9),\ (9,11),\ \ldots\ \}$$
$$=\; \{\ (x,y) \in \mathbf{Z} \times \mathbf{Z} \mid y-x \in \mathbf{N}\ \}$$

To say that $x < y$ means that x and y stand in the relationship $<$ to each other, that is, $(x,y) \in <$.

The binary relation "is a parent of" is a set of ordered pairs of people:

{ (Adam,Cain), (Eve,Cain), (Henry IV, Henry V) . . . }

The binary relation "is within 100 miles of" is a set of ordered pairs of cities, etc.

If R is a binary relation and the ordered pair (a,b) is in R, we often write $a\mathrm{R}b$ (as in $a < b$).

Note that *any* subset of $S \times S$ is a binary relation on S, even if it doesn't make sense.

[Special Relations]

Here are three very important kinds of binary relations.

A binary relation R on a set S is *reflexive* if xRx for every $x \in S$. That is, R is reflexive if

$$\{ (x,x) \mid x \in S \} \subseteq \text{R}.$$

For example, "is within 100 miles of" is reflexive (any city is within 100 miles of itself) and so is "is the same color as". The relation $<$ is *not* reflexive, since it's not true that $x < x$, but the relation $\leq$ *is* reflexive.

A binary relation R on a set S is *symmetric* if whenever xRy it's also true that yRx. For example, "is within 100 miles of" is symmetric, but $<$ is not symmetric.

A binary relation R on a set S is *transitive* if whenever we have xRy and yRz we also have xRz. For example, $<$ is transitive ($a < b$ and $b < c$ implies $a < c$) but "is within 100 miles of" and "is a parent of" are not transitive.

[Exercise: For each example relation we've seen, tell whether it's reflexive, symmetric, or transitive. Do the same for: "is a sibling of", "is a sister of", the empty relation, "is equal to", "has shaken the hand of".]

Another Flavor

Up to now we've been speaking only of binary relations on S, that is, subsets of $S \times S$. Here's another kind of binary relation: If S and T are any sets, a *binary relation from S to T* is any subset of $S \times T$.

Example: "is a city in" is a binary relation *from* the set of cities *to* the set of states:

"is a city in" = { (Boston,MA), (Omaha,NE),
(Ogden,UT), (Medford,MA), . . . }

This relation is a set of ordered pairs whose first component is a city and whose second is a state. (Note that it's *not* a relation on the set of cities, nor on the set of states.)

If S and T are sets, how many binary relations are there from S to T? This is the same as asking how many subsets are there of $S \times T$, since any subset of $S \times T$ is a binary relation. We know that $S \times T$ has $(|S|)(|T|)$ elements (last lecture; Rule of Product) and the number of subsets of a set of size k is 2^k, so there are $2^{(|S|)(|T|)}$ binary relations from S to T. Of course this includes some silly ones, like the empty relation.

Tree Diagrams

These are a pictorial representation of cross products.
Be sure to read all about them on pages 248–250 of G.