MATH 22

Lecture G: 9/23/2003

QUANTIFIERS & PIGEONHOLES

But I am pigeon-livered, and lack gall
To make oppression [and Math 22] bitter . . .
—*Hamlet*, Act 2, sc. 2

Administrivia

- http://denenberg.com/LectureG.pdf
- Project 2, #4, and Homework 2, sect 1.4 #20 new grading standards
- Homework #3 due today, #4 on the web
- Exam #1
  - Monday, 9/29, 11:50–1:20, Robinson 253
  - Covers Chapters 1, 2, and Section 5.5
- Part of Thursday's class will be a review. Bring questions, or (better) *email questions to me in advance* (larry.denenberg@tufts.edu)

Today: More quantifier rules of equivalence and inference, proofs with quantifiers, the Pigeonhole Principle

Quantifiers: Review

- Free variables and open statements
- Bound variables and closed statements
- Existential and universal quantifiers
- Dummy variables, scope of quantifier
- Range of variables; universe of discourse
- Multiple quantifiers, order of quantifiers
- Equivalence rules for negation (similar to DeMorgan), leading to . . .
- Implicit relationship of $\exists$ to $\wedge$ and of $\forall$ to $\rightarrow$
- Equivalence rules for distributivity:
  $\exists$ over $\vee$
  $\forall$ over $\wedge$
- *Inference* (***not*** equivalence) rules for distributing $\exists$ over $\wedge$ and $\forall$ over $\vee$
- A few other quantifier rules

Yet More Q Rules

$(\forall x)p(x) \Rightarrow p(c)$ for any c in the universe

(The Rule of Universal Specification)

$p(c) \Rightarrow (\exists x)p(x)$

(The Rule of Existential Generalization)

Presumably these are reasonably obvious.

If c is arbitrary, $p(c) \Rightarrow (\forall x)p(x)$

(The Rule of Universal Generalization)

This one is tricky. It says that if you can prove that p is true about c, without any assumptions about special properties of c, then you could just as well have proved that p is true about any c whatsoever, that is, p must be true of all c in the universe.

In practice, c must have come from a use of Universal Specification. Like this: Suppose you know $(\forall x)p(x)$ and deduce $p(c)$. This c is arbitrary; it's nothing special; it stands for any c in the universe. If later you deduce $q(c)$, then you can use Universal Generalization to deduce $(\forall x)q(x)$, since the proof of $p(c)$ would have worked as well for any c.

Contra{positive,diction}

This is just a brief review of these two terms and how the principles behind them can be used in proofs. (Not just the formal proofs we've been doing; real-world proofs use both of these all the time.)

The *contrapositive* of a conditional $p \rightarrow q$ is the conditional $\neg q \rightarrow \neg p$. A conditional is equivalent to its contrapositive. So if you need to prove $p \rightarrow q$, you can just as well prove $\neg q \rightarrow \neg p$ and it's just as good.

A proof by *contradiction* works like this: You have a bunch of premises $p_1, p_2, \ldots, p_n$ and you're trying to prove a conclusion C. Instead, you can *assume $\neg C$ as a new premise*, and then prove any contradiction at all. For example, you can prove $r \wedge \neg r$ for any formula r, or you can prove $\neg p_i$ where p_i is one of your premises. (Because then you have $p_i \wedge \neg p_i$ by Conjunction.)

These two terms are somewhat related. If you're trying to prove that $p \Rightarrow q$, you can work by contradiction and assume $\neg q$ and then prove $\neg p$. But this just proves that $\neg q \rightarrow \neg p$, the contrapositive, is a tautology.

Definitional "if"

Definition: Let x be an integer. We say that x is *even* if there is an integer y such that $x=2y$.

Definition: Suppose some people are playing a game. We say that a player *wins* the game if that player has the most points at the end of the game.

Hey, shouldn't we be using "if and only if" here? Taken literally, nothing excludes the possibility that x is even in some cases where there's no such y! The English says

(a player has the most points) □ (that player wins)

but really the intent must be

(a player has the most points) ≡ (that player wins)

Grimaldi's answer: Definitions are traditionally phrased as implications but should be read as biconditionals.

Denenberg's answer: A definition is neither a conditional nor biconditional. It just records that we can use one term or phrase as shorthand for another phase. Some use "if" in idiomatic English to state a definition, but it's not the same "if" as "if-then" or "if-and-only-if".

Take your choice. Don't be confused. End of topic.

The Pigeonhole Principle

If m pigeons occupy n pigeonholes and $m > n$, then at least one pigeonhole contains two or more pigeons.

Proof: Suppose otherwise, namely that each hole contains at most one pigeon. Since there are n holes, there can be at most n pigeons. But there are m pigeons, and $m>n$. Contradiction.

[Why pigeons and holes? The Principle goes back to Dirichlet who stated it (in French) using chests of drawers. "Pigeonholes" are the little compartments in old-fashioned rolltop desks.]

More loosely stated: If sufficiently many objects are distributed over not too many classes, then at least one class contains many of these objects. (This is from the paper of Erdös in which the PP is first stated in English.)

Examples:

If there are 8 people in a room, there must be two who were born on the same day of the week. If there are 13, there must be two born in the same month. If there are 367, there must be two with the same birthday.

More Pigeons

Suppose S is a set of six integers, each between 1 and 12 inclusive. Then there must be two distinct nonempty subsets of S that have the same sum.

Proof: The sum of all the elements of S is at most 7+8+9+10+11+12 = 57. So the sum of the elements of any nonempty subset of S is at least 1 and at most 57; there are 57 possibilities. But there are $2^6-1 = 63$ nonempty subsets of S. So there must be two with the same sum. (The book does a trickier analysis to show the same result where the numbers can go up to 14.)

Here's an obvious generalization of the PP: If m pigeons occupy n pigeonholes and $m > kn$, then at least one of the pigeonholes must contain at least $k+1$ pigeons. (The original version we stated is the case $k=1$.)

Example: If you have 37 people in a room, there must be three who were born in the same month. ($n=12$, $k=3$)

If you have 733, there must be three with the same birthday. ($n=366$, $k=2$).

(Digression: How many people do you need to have *a 50/50 chance* that there are two, or three, with the same birthday?)

Sequences & Subsequences

A *sequence* of numbers is, well, a sequence of numbers.

<8, 3, 9, 2, 11, 4, –2, 0, 16, 1, 23, 10, 15, 12, 6, 14, 19>

This is a sequence of *length* 17. Note that order matters (that's the difference between a sequence and a set). Sequences can have duplicates; this one happens not to.

A *subsequence* of a sequence is just what you'd think:

<8, 9, 11, 0, 16, 23, 15, 12>

(Digression: Given a sequence of length n, how many subsequences does it have?)

Theorem: Let n be an nonnegative integer and let S be a sequence of length n^2+1 containing distinct numbers,. Then S must contain *either* an increasing *or* a decreasing subsequence of length $n+1$.

So, for example, the sequence above must have either a decreasing or an increasing subsequence of length 5.

We prove this Theorem using the Pigeonhole Principle!

Proof

We prove the Theorem by contradiction, that is, we assume the negative of the conclusion and prove an absurdity. So suppose there is an $n > 0$, a sequence

$$S = \langle a_1, a_2, a_3, \ldots a_m \rangle$$

where $m = n^2 + 1$, all the a_i are distinct, and S has no ascending or descending sequence of length $n+1$.

For each position i in the sequence we calculate a pair of integers (x_i, y_i) defined like this:

> x_i is the length of the longest increasing subsequence of S that ends at a_i, and
>
> y_i is the length of the longest decreasing subsequence of S that ends at a_i.

Example: Let S be $\langle 8, 2, 4, 5, 1, 3 \rangle$ and look at $i=4$.

x_4 is 3 (because of <2,4,5>) and y_4 is 2 (because of <8,5>). Similarly, $x_6=2$; $y_5=3$; and $x_1=x_2=x_5=y_1=1$.

In each pair (x_i, y_i) both numbers are at least 1. (Why?) Furthermore, since we've assumed that there's no ascending or descending subsequence of length $n+1$ in S, both numbers must be $\leq n$. Summarizing: for each position i in S we have a pair of numbers (x_i, y_i) defined as above, where $1 \leq x_i, y_i \leq n$.

Proof, continued

Question: How many different pairs (x,y) can there be? This is an easy counting problem: If each number can independently be an integer from 1 to n, there are at most n^2 different pairs.

Now apply the pigeonhole principle: There are at most n^2 different pairs but there are at least n^2+1 places in S. By the Pigeonhole Principle, there must be two places in S (call them i and j) with the same pair:

$$<\ldots\ldots\ a_i,\ \ldots\ldots\ a_j,\ \ldots\ldots>$$

where $x_i=x_j$ and $y_i=y_j$.

But look: All the a_i are distinct, so either $a_i<a_j$ or $a_i>a_j$. Suppose $a_i<a_j$. By the definition of x_i there is an increasing subsequence of length x_i ending at a_i. But clearly if we tack a_j onto the end of such a subsequence we get an increasing subsequence of length x_i+1 ending at a_j. So the longest increasing subsequence ending at a_j has length *at least* x_i+1, that is, x_j is at least x_i+1, and so $x_i=x_j$ is impossible.

If $a_i>a_j$, a parallel argument shows that y_i and y_j can't be equal. In either case, it can't be that $x_i=x_j$ *and* $y_i=y_j$!

This contradiction proves that our assumption was false; it cannot be true that there is neither an ascending nor a descending subsequence of S with length $n+1$. QED

Ramsey's Theorem

Ramsey's Theorem is a profound generalization of the Pigeonhole Principle. We're not going to prove it.

Let $r \geq 1$ be an integer, and let $q_1, q_2, ..., q_n$ be integers all $\geq r$. Then there exists some integer m (which depends on $r, q_1, q_2, ..., q_n$) such that any set S with at least m elements has the following property:

For any way of partitioning the subsets of S that have exactly r elements into n groups $A_1, A_2, ..., A_n$, there is some j and some subset T of S such that (a) T has q_j elements, and (b) every subset of T that has exactly r elements is a member of A_j.

When r=1 and all the q_i are 2, then m=n+1, and the Theorem says that if you break up a set with n+1 or more elements into n subsets, at least one of those subsets has at least 2 elements. This is the Pigeonhole Principle.

An example with r=3, n=2, q_1=q_2=3 (for which m = 6): Given any 6 people, either there are 3 who have never met each other, or there are 3 all of whom have met each other.

[Pause for Erdös anecdote about n=2, r=q_1=q_2=5 or 6.]