1 Induction, continued

Last week we discussed induction, and did some relatively simple induction proofs. Today we do another induction proof that is a little bit different.

Using induction to prove a property about a function of two variables. Let $f : NxN \to N$ be defined by

- $f(n, m) = n + m$ if $n = 1$ or $m = 1$,
- $f(n, m) = f(n - 1, m) + f(n, m - 1)$, otherwise

Theorem: $f(n, m) \geq n + m$ for all integers $n \geq 1$ and $m \geq 1$.
Proof: Note that when $n = 1$ or $m = 1$, the statement is true. Our inductive hypothesis has to depend on a single parameter, but our function is defined by two parameters. How do we get one parameter out of these two? Hint: try adding the two parameter values.

Here's an attempt:

> $\exists K \geq 2$ such that $f(n, m) \geq n + m$ for all positive integers n, m with $n + m \leq K$

The base case is $K = 2$; hence $n = m = 1$ and the statement holds. Now assume that for some arbitrary K, the statement holds. We wish to show it holds also for $K + 1$. Let n, m be integers such that $n + m = K + 1$. We have to do a case analysis;

Case 1: $n = 1$ or $m = 1$. If $n = 1$ or $m = 1$, then $f(n, m) = n + m$, and the statement holds.

Case 2: Both n and m are at least 2. Then, by definition $f(n, m) = f(n - 1, m) + f(n, m - 1)$.

Since $n + m - 1 = K$, we can apply the inductive hypothesis; hence:

$$f(n - 1, m) \geq (n - 1) + m = n + m - 1$$

and

$$f(n, m - 1) \geq n + (m - 1)$$

Hence,

$$f(n, m) \geq 2(n + m - 1) = 2n + 2m - 2 > n + m - 1$$

Since K was arbitrary, the statement holds for all K. Q.E.D.

Using induction to "solve" the two-person game. Remember the original two person game?

Who wins?

Prove your assertion true by induction on the total number of rocks in the game.

What we learned about induction.

- The base case is sometimes more than one value.
- The inductive hypothesis is sometimes not on an obvious parameter, but on something built using obvious parameters (like the sum)
- Induction can be used to prove upper or lower bounds on recursively defined functions.
- Induction proofs are not difficult!

2 Sets

2.1 Overview of the material

Sets are collections of objects, where each object appears at most once. These objects can be numbers, strings, graphs, functions, or even sets. Thus, sets are quite general.

Sets can be described (and defined) in several ways, including *set builder notation*.

The empty set contains nothing! It is written as $\emptyset$. Furthermore, the empty set is always a subset of every set.

Sets can be defined recursively; therefore, you can prove theorems about sets using induction.

You can take unions of sets, intersections of sets, and compute the differences between sets. Venn Diagrams help you visualize these comparisons.

There are finite sets and also infinite sets. There are countable sets and uncountable sets. Understanding these issues involves understanding functions - and in particular, understanding what bijections are.

2.2 Notation

Consider the set $\{3, 4, 5, 6, 7, 8, 9, 10\}$. The following are equally good ways of defining this set - and there are many more!

- $\{10, 3, 5, 6, 9, 4, 7, 8\}$
- $\{x \in Z : 10 \geq x \geq 3\}$
- $\{x \in Z : 2 < x < 11\}$
- $\{x \in Z | 2 < x < 11\}$
- $\{x : x \in Z \wedge 3 \leq x \leq 10\}$

The last four ways of defining the set are using "set builder notation". Notice that in set-builder notation, you have two parts to the description: what comes before the divider (given either as ":" or as "—"), and what comes after. What comes before is just telling you the name of the elements that will be in the set (and sometimes the universe it can come from), and what comes after is some property that the elements must satisfy in order to be in the set.

Questions:

- what is $\{x \in Z^+ : 2 + 3 = 5\}$?
- what is $\{x \in Z^+ : 2 + 3 \neq 5\}$?

Sets don't have to only be of numbers. They can also be of any kind of object (graphs, functions, sets, alphanumeric strings, etc.).

Examples:

- The set $\{f : R \rightarrow R\}$ (i.e., the set of functions from the real numbers to the reals).
- The set $\{f : R \rightarrow R : \forall x \in Z, f(x) = x\}$ (the set of functions from the reals to the reals that act as the identity function on the integers)
- The set Σ^*, where Σ is an alphabet, is the set of all finite length strings (including the empty string, λ) over Σ
- The set Σ^+, where Σ is an alphabet, is the set of finite length strings - not including the empty string - over Σ
- $\mathcal{P}(X)$, the set of all subsets of X (called the power set of X). Note $\emptyset \in \mathcal{P}(X)$ for all X.

Elements and subsets. Let A be a set.

- We write "$X \in A$" if X is one of the elements of A.
- We say "X is a **subset** of A" (written $X \subseteq A$) if X is a *set* and every element of X is an element of A. Note, we can also write this as $A \supseteq X$, and say that "A is a **superset** of X".
- We say that "X is a **proper subset** of A" if X is a subset of A but $X \neq A$. This is denoted by $X \subset A$ (or as $A \supset X$). We express this also as "A is a proper superset of X."

Let $A = \{1, 5, 7, 10, 12\}$. Which of the following statements are true?

- $1 \in A$
- $\{1, 3\} \in A$
- $\{1, 5\} \in A$
- $\{1, 5\} \subset A$
- $A \subset \{1, 5\}$

- $\emptyset \in A$
- $\emptyset \subset A$

Let A and B be sets. Then

- $A \cup B = \{x : x \in A \vee x \in B\}$
- $A \cap B = \{x : x \in A \wedge x \in B\}$
- $A \setminus B = \{x \in A : x \notin B\}$. Sometimes this is written as $A - B$.
- $A \triangle B = (A \cup B) \setminus (A \cap B)$
- For the complement of a set to be defined, we need to know the **universe** (often denoted by U). Then $A^c = U \setminus A$.

2.3 De Morgan's laws.

Let U denote the universe, and A and B subsets of U. Then

- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

2.4 Venn Diagrams

Venn Diagrams are useful ways of visualizing sets and their intersections; see http://mathworld.wolfram.com/VennDiagram.html

2.5 Inclusion-Exclusion.

The Inclusion-Exclusion "principle" lets you calculate the size of a multi-way union of sets. It's easy if we start with only two sets.

- Question: What is $|A \cup B|$?
- Answer: $|A \cup B| = |A| + |B| - |A \cap B|$
- Proof: Venn Diagram

Now, what about three sets?

- Question: What is $|A \cup B \cup C|$?
- Answer: $|A \cup B \cup C| =$

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$$
$$+|A \cap B \cap C|$$

- Proof: Venn Diagram

Think about how this might generalize to four or more sets.

We can use Inclusion-Exclusion to solve problems. Here's a simple one: How many numbers are there between 1 and 1000 that are divisible by 3 or by 7?

Answer: Apply Inclusion-Exclusion.

Let $A = \{x \in Z^+ : 1 \leq x \leq 1000 \wedge 3|x\}$

Let $B = \{x \in Z^+ : 1 \leq x \leq 1000 \wedge 7|x\}$

Then we want to know $|A \cup B|$.

- By Inclusion-Exclusion, $|A \cup B| = |A| + |B| - |A \cap B|$
- $A = \{3, 6, 9, \ldots, 999\}$, so $|A| = 333$
- $B = \{7, 14, 21, \ldots, 987\}$, so $|B| = 141$
- $A \cap B = \{21, 42, \ldots, 987\}$, so $|A \cap B| = 47$

Hence, $|A \cup B| = 333 + 141 - 47 = 427$

2.6 Recursively defined sets

Let the sets $A_1, A_2, \ldots, A_n$ be defined by:

- $A_1 = \{3\}$
- $A_n = \{x : \exists y \in A_{n-1}, x = y + 1\}$, for $n > 1$

Questions:

- What is A_2?
- What is A_3?
- Find a closed form solution for A_n and prove your formula correct by induction on n.
- What is $\bigcup_i A_i$? Prove your statement true.

Other recursively defined sets

- $A_0 = \{\{0\}\}$.
- $A_n = A_{n-1} \cup \{B \cup \{n\} : B \in A_{n-1}\}$ for $n \geq 1$.

Note that for all i, $A_i \subset \mathcal{P}(Z)$.

- What is $|A_0|$?
- Is $A_0 \subseteq A_1$?
- Show one element of A_1.
- Show another element of A_1.

- What is $|A_1|$?
- Is $A_1 \subseteq A_2$?
- Give one element of $A_2 \setminus A_1$.
- Is $A_n \subseteq \mathcal{P}(\{0, 1, \dots, n\})$?
- Is $A_n = \mathcal{P}(\{0, 1, \dots, n\})$?
- What is $\bigcup_{i=0} A_i$? (infinite union)

2.7 Comparing two sets

Often you will want to compare two sets and see whether one is a subset of the other.

Proving a set X is a proper subset of Y A simple example is trying to prove that a set $X \subset Y$ (i.e., X is a proper subset of Y).

To do this, you need to:

- Prove $X \subseteq Y$
- Prove $X \neq Y$ (by proving that $\exists y \in Y \setminus X$)

Here's an example.

- $A = \{x \in Z : \exists y \in Z \text{ s.t. } x = 2y\}$
- $B = \{x \in Z : \exists y \in Z \text{ s.t. } x = 6y\}$

Which of the following are true?

- $A = B$
- $A \subseteq B$
- $B \subseteq A$

Note $2 \in A \setminus B$, so $A \neq B$. And so A cannot be a subset of B.
However, we will prove $B \subseteq A$.
Proof: We will show that every element of B is an element of A.

- Pick arbitrary $b \in B$.
- By definition, $\exists x \in Z$ such that $b = 6x$.
- Let $y = 3x$. Then $y \in Z$, and also $2y \in Z$.
- Note that $b = 2y$.
- Hence, by definition $b \in A$.
- Since b was arbitrary, this proves that $B \subseteq A$.

Since $B \neq A$ and $B \subseteq A$, it follows that B is a proper subset of A, i.e.,

$$B \subset A$$

Proving two sets are equal To prove two sets A and B are equal, you need to:

- Prove $A \subseteq B$
- Prove $B \subseteq A$

2.8 Finite sets and cardinality

A **finite set** is a set where you can write all the elements down explicitly.

For example, $A = \{1, 3, 4, 9\}$ is finite.

Given a finite set A, we write $|A|$ to denote the number of elements of A.

Thus, $|A| = 4$ for the set above.

What is $|\emptyset|$?

Bijections. A **bijection** from a set A to a set B is a function $f : A \to B$ such that

- f is 1-1 (so that $f(a) = f(b) \Rightarrow a = b$)
- f is *onto* (so that $\forall b \in B, \exists a \in A$ such that $f(a) = b$)

Note that every set has a bijection from itself to itself (the identity function).

Question: does there exist a set X and a proper subset Y of X such that there is a bijection from X to Y?

Infinite sets. An infinite set is a set where this isn't possible. A better definition is that a set A is *infinite* if there is a *proper subset* $B \subset A$ and there is a **bijection** (function that is 1-1 and onto) between A and B.

Example:

- Z^+ is infinite because there is a bijection from Z^+ to $A = \{2, 3, 4, \ldots\}$! Just let $f(n) = n + 1$; then $f : Z^+ \to A$, and f is $1 - 1$ and onto.
- $A = \{1, 3, 4, 9\}$ is not infinite; there is no proper subset B of A for which A and B have a bijection.

Can you show that the even integers are infinite?

2.9 Countable and uncountable sets

An infinite set can be countably infinite (also just called "countable") or uncountable. X is a countably infinite set *iff* $\exists f : Z^+ \to X$ s.t. f is a bijection.

Otherwise, X is said to be *uncountable*.

Questions:

- Is the set of rational numbers countable?

- Is the set of negative integers countable?
- Is the set of integers countable?
- Is the set of real numbers countable?
- Is the set $\{f : Z \to \{0, 1\}\}$ countable?
- Is the set $\{f : \{0, 1\} \to Z\}$ countable?
- Is the set $\{f : Z \to \{0\}\}$ countable?