Background Material

Reading: Sections 1.1 – 1.4

Some Things that will Matter

1. Words, terminology, vocabulary
   - lemma, theorem, proof, corollary, conjecture, antecedent (note: book calls this hypothesis), consequence
   - A *language* is regular, a DFA is not

2. Logical structure of statements and proofs
   - *if* A *then* B
   - A *if and only if* B
   - quantification, i.e., *there exists*, *for all*

3. Formal definitions

Mathematical Induction

- An inductive proof has three parts:
  - Basis case
  - Inductive hypothesis
  - Inductive step

- Related to recursive programming.

Theorem:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$ For all n>=1.

Proof #1: (by induction on *n*)

Basis:

n = 1

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

1 = 1

Inductive hypothesis:

Suppose that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ for some *k>=1*.

Inductive step:

We will show that $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1)$$ by the inductive hypothesis

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

It follows that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all *n>=1*. •

Theorem:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$ For all *n>=1*.

Proof #2: (by induction on *n*)

Basis:

n = 1

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

1 = 1

Inductive hypothesis:

Suppose there exists a *k>=1* such that that $\sum_{i=1}^{m} i = \frac{m(m+1)}{2}$ for all *m*, where *1 <= m <= k*.

Inductive step:

We will show that $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1)$$ by the inductive hypothesis

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

It follows that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all *n>=1*. •

- What is the difference between proof #1 and proof #2?
  - The inductive hypothesis for proof #2 assumes more than that for proof #1.
  - Proof #1 is sometimes called *weak* induction
  - Proof #2 is sometimes called *strong* induction

- Many times weak induction is sufficient, but other times strong induction is more convenient.

Strict Binary Trees

Definition #1:

Let *T=(V,E)* be a tree with |*V*|*>=1*. Then *T* is a *strict binary tree* if and only if each vertex in *T* is either a leaf or has exactly two children.

Definition #2: (recursive)

1. A single vertex is a strict binary tree.
2. Let *T1=(V1,E1)* and *T2=(V2,E2)* be strict binary trees with roots *r1* and *r2*, respectively, where *V1* and *V2* do not intersect. In addition, let *r* be a new vertex that is not in *V1* or *V2*. Finally, let:

$$V3 = V1 \cup V2 \cup \{r\}$$

$$E3 = E1 \cup E2 \cup \{(r,r1),(r,r2)\}$$

   Then *T3=(V3,E3)* is a strict binary tree.

3. Nothing else is a strict binary tree.

Note that the previous two definitions, although different, are equivalent.

In other words, tree T will satisfy definition #1 if and only if (iff) T satisfies definition #2.

A iff B:

1) A if B B => A
2) A only if B A => B

For our purposes here, definition #2 will be used.

Since definition #2 is a recursive definition, this will allow us to easily prove things about strict binary trees using induction.

An inductive proof that follows the recursive structure of some set of objects, it is also called ***structural induction***.

Theorem:

Let L(T) denote the number of leaves in a strict binary tree T=(V,E). Then

$$2*L(T) – 2 = |E|$$

Proof: (by induction on L(T))

Basis:

$L(T) = 1$

Observation: The only strict binary tree with $L(T) = 1$ has a single vertex and 0 edges, i.e., $|E| = 0$.

Lets evaluate 2*L(T)-2 and see if we can show it is equal to |E|.

$$\begin{aligned} 2*L(T) – 2 &= 2 *1 – 2 && \text{Since } L(T) = 1 \\ &= 0 \\ &= |E| && \text{Since the observation tell us that } |E| = 0 \end{aligned}$$

Inductive hypothesis:

Suppose there exists a k>=1 such that for every strict binary tree where 1<=L(T)<=k that 2*L(T) – 2 = |E|.

Inductive step:

Let T=(V,E) be a strict binary tree where L(T)=k+1. We must show that 2*L(T) – 2 = |E|.

Notes about T:

1. Since k>=1 and L(T)=k+1, it follows that L(T)>1. Therefore T consists of a root r and two strict binary trees T1=(V1,E1) and T2=(V2,E2), where 1<=L(T1)<=k and 1<=L(T2)<=k.

2. L(T) = L(T1) + L(T2)   by definition of T

3. |E| = |E1| + |E2| + 2   also by definition of T

Lets start with 2*L(T) - 2 and, using 1-3, see if we can show that it is equal to |E|.

$2 * L(T) – 2 \quad = 2 * (L(T1) + L(T2)) – 2$ by (2)

$= 2 * L(T1) + 2 * L(T2) – 2$

$= (2 * L(T1) – 2) + (2 * L(T2) – 2) + 2$

Since 1<=L(T1)<=k and 1<=L(T2)<=k from (1), it follows from the inductive hypothesis that:

$2 * L(T1) – 2 = |E1|$ and

$2 * L(T2) – 2 = |E2|$

Substituting these in the preceding equation gives:

$= |E1| + |E2| + 2$

$= |E|$ by (3)

Hence, for all strict binary trees, 2 * L(T) – 2 = |E|. •

Finally, note the use of strong induction in the above proof.

Relations and Functions

Let *A* and *B* be two sets.

The cartesian product of *A* and *B*, denoted $A \times B$, is {(a,b) | a∈*A* and b∈*B*}

For example, if *A* = {a, b, c} and *B* = {d, e, f}, then $A \times B$ is:

{(a, d), (a, e), (a, f), (b, d), (b, e), (b, f), (c, d), (c, e), (c, f)}

A binary relation on *A* and *B* is a subset of $A \times B$.

Example (using *A* and *B)*:

R = {(a, d), (a, f), (b, e)}

Note that a binary relation is sometimes also referred to as a mapping.

A binary relation *R* on *A* and *B* is said to be a total function if for every element a$\in$ *A*, there is *exactly* one element b$\in$ *B* such that (a, b)$\in$ *R*. In such a case we use the notation *f(a) = b*.

Example:

R' = {(a, d), (b, e)} is not a total function from *A* to *B*

R'' = {(a, d), (a, f), (b, e)} is not a total function from *A* to *B*

R''' = {(a, d), (b, e), (c, e)} is a total function from *A* to *B*

For our purposes, a total function will be referred to simply as a function.

Let f be a function from A to B. Then f is said to be one-to-one if $f(a) \neq f(b)$, for all a, b$\in A$ where a$\neq$b.

Let f be a function from A to B. Then f is said to be onto if for each b$\in B$ there exists an a$\in A$ such that $f(a) = b$.

Let f be a function form A to B. Then f is said to be a bijection if it is one-to-one and onto.

If R is a binary relation on sets A and B then the inverse of R, denoted R^{-1}, is:

$$\{(b, a) \mid (a, b) \in R\}$$

Given the above definitions, the following observations can be made:

- A one-to-one function is not necessarily onto. Similarly, an onto function is not necessarily one-to-one.
- If a binary relation R is a function, then its inverse R^{-1} is not necessarily a function.
- If there is a bijection f from A to B then the inverse f^{-1} is a bijection from B to A (prove this as an exercise).

Now for Some "New" Definitions

Two sets A and B have the same cardinality iff there is a bijection (a one-to-one and onto function) from A to B (or, equivalently, from B to A).

Let $N = \{0, 1, 2,\ldots\}$ denote the natural numbers. Then a set is countably infinite iff it has the same cardinality as N.

A set is countable iff it is finite or countably infinite.

A set that is not countable is said to be uncountable.

Note:

- If A and B are finite sets and $A \subset B$ then A and B have different cardinality.
- If A and B are infinite sets and $A \subset B$ then A and B can still have the same cardinality!
- "Cardinality" is defined as a relation between two sets, and no definition for the "cardinality of a set" is given.

Given the above definitions, how would one prove that an arbitrary set is or is not countable infinite or, more generally, countable?

As another definition, a set is countably infinite iff it has the same cardinality as the set of integers (prove that this definition is equivalent to the one given above).

Countable and Countably Infinite Sets

Theorem: *N-{0}* and *N* have the same cardinality.

Proof:

Define a function *f* from *N-{0}* to *N* as *f(i) = i-1*.

- *f* is a function
- *f* is one-to-one
- *f* is onto

f is therefore a bijection and, by definition of cardinality, *N-{0}* and *N* have the same cardinality. •

Corollary: *N-{0}* is countably infinite.

Corollary: *N-{0}* is countable.

Tangent!
(vocabulary)

Lemma

Theorem

Proof

Corollary

Conjecture

Observation

Antecedent (hypothesis)

Conclusion

Theorem:

Let *A* be the set of all even integers >=2, and let *B* be the set of all positive integers (i.e., >=1). Then *A* and *B* have the same cardinality.

Proof:

Let *f(i) = i/2*. Then it can be easily verified that *f* is a bijection from *A* to *B*.•

Diagonalization

Fact: Many books exist.

Fact: Some books contain the titles of other books within them.

Fact: Some books contain their own titles within themselves, others do not.

Consider the following book with title *The Special Book*.

> *The Special Book is defined to be that book that contains the titles of all books that* ***do not*** *contain their own titles.*

Question: Does the special book exist? Could one write the special book?

A similar contradiction is known as *The Barber of Seville Paradox.*

More formally known as *Russell's Paradox*.