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:

\[ \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \text{For all } n \geq 1. \]

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 \( k \geq 1 \).

**Inductive step:**
We will show that \( \sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} \)

\[
\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) \\
= \frac{k(k+1)}{2} + (k+1) \quad \text{by the inductive hypothesis} \\
= \frac{k(k+1) + 2(k+1)}{2} \\
= \frac{(k+1)(k+2)}{2}
\]

It follows that \( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \) for all \( n \geq 1 \). ∙
Theorem:

\[ \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \text{For all } n \geq 1. \]

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 $k \geq 1$ such that that $\sum_{i=1}^{m} i = \frac{m(m+1)}{2}$ for all $m$, where $1 \leq m \leq k$.

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

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

\[
= \frac{k(k+1)}{2} + (k+1) \quad \text{by the inductive hypothesis}
\]

\[
= \frac{k(k+1) + 2(k+1)}{2}
\]

\[
= \frac{(k+1)(k+2)}{2}
\]

It follows that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all $n \geq 1$. •
• 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 $|V| \geq 1$. 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 $T_1=(V_1,E_1)$ and $T_2=(V_2,E_2)$ be strict binary trees with roots $r_1$ and $r_2$, respectively, where $V_1$ and $V_2$ do not intersect. In addition, let $r$ be a new vertex that is not in $V_1$ or $V_2$. Finally, let:

$$V_3 = V_1 \cup V_2 \cup \{r\}$$

$$E_3 = E_1 \cup E_2 \cup \{(r, r_1), (r, r_2)\}$$

Then $T_3=(V_3,E_3)$ 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.

\[ A \text{ iff } B: \]
\begin{align*}
1) & \quad A \text{ if } B \quad B \Rightarrow A \\
2) & \quad A \text{ only if } B \quad A \Rightarrow B
\end{align*}

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 follows the recursive structure of some set of objects, it is also called \textit{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., $|E| = 0$.

Let's evaluate $2*L(T) - 2$ and see if we can show it is equal to $|E|$.

$$2*L(T) - 2 = 2*1 - 2$$
$$= 0$$
$$= |E|$$
Since $L(T) = 1$

Since the observation tell us that $|E| = 0$
**Inductive hypothesis:**

Suppose there exists a \( k \geq 1 \) such that for every strict binary tree where \( 1 \leq L(T) \leq k \) that \( 2 \times L(T) - 2 = |E| \).

**Inductive step:**

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

Notes about \( T \):

1. Since \( k \geq 1 \) and \( L(T) = k + 1 \), it follows that \( L(T) > 1 \). Therefore \( T \) consists of a root \( r \) and two strict binary trees \( T_1 = (V_1, E_1) \) and \( T_2 = (V_2, E_2) \), where \( 1 \leq L(T_1) \leq k \) and \( 1 \leq L(T_2) \leq k \).

2. \( L(T) = L(T_1) + L(T_2) \) by definition of \( T \)

3. \( |E| = |E_1| + |E_2| + 2 \) also by definition of \( T \)

Lets start with \( 2 \times L(T) - 2 \) and, using 1-3, see if we can show that it is equal to \( |E| \).
\[2 \cdot L(T) - 2 = 2 \cdot (L(T_1) + L(T_2)) - 2 \quad \text{by (2)}\]
\[= 2 \cdot L(T_1) + 2 \cdot L(T_2) - 2\]
\[= (2 \cdot L(T_1) - 2) + (2 \cdot L(T_2) - 2) + 2\]

Since \(1 \leq L(T_1) \leq k\) and \(1 \leq L(T_2) \leq k\) from (1), it follows from the inductive hypothesis that:

\[2 \cdot L(T_1) - 2 = |E_1|\]
\[2 \cdot L(T_2) - 2 = |E_2|\]

Substituting these in the preceding equation gives:

\[= |E_1| + |E_2| + 2\]
\[= |E| \quad \text{by (3)}\]

Hence, for all strict binary trees, \(2 \cdot L(T) - 2 = |E|\). •

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) \mid a \in A \text{ and } b \in B\}

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

$$\{(a, a), (a, c), (a, d), (b, a), (b, c), (b, d), (c, a), (c, c), (c, d)\}$$

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

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

$$R = \{(a, a), (a, d), (b, c)\}$$

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 **partial function** from $A$ to $B$ if for every element $a \in A$, there is *at most* one element $b \in B$ such that $(a, b) \in R$. In such a case we use the notation $f(a) = b$.

Example:

$$R = \{(a, a), (a, d), (b, c)\}$$ is not a partial function from $A$ to $B$

$$R' = \{(a, a), (b, c)\}$$ is a partial function from $A$ to $B$

If $f$ is a partial function from $A$ to $B$ then the **domain** of $f$ is:

$$\{a \mid a \in A \text{ and } \exists b \in B \text{ where } f(a) = b\}$$

In addition, the **range** of $f$ is:

$$\{b \mid b \in B \text{ and } \exists a \in A \text{ where } f(a) = b\}$$
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 $(a, b) \in R$.

Example:

$$R' = \{(a, a), (b, c)\}$$ is not a total function from $A$ to $B$

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

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

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

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

A function $f$ from $A$ to $B$ 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:

– Every total function is a partial function.
– The domain of a (total) function from $A$ to $B$ is the entire set $A$.
– A partial function $f$ from $A$ to $B$ is a total function iff (if and only if) the domain of $f$ is equal to $A$.
– A function $f$ from $A$ to $B$ is onto iff the range of $f$ equals $B$.
– 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.
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).

Given the above definitions, how would one prove that an arbitrary set is or is not countable infinite or, more generally, countable?
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 $\geq 2$, and let $B$ be the set of all positive integers (i.e., $\geq 1$). 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.*
Diagonalization

• **Definition:**

P(N) is the set of all subsets of N.

\[ P(N) = \{ \{\}, \{0\}, \{0, 1\}, \{1, 2, 3\}, \{2, 5, 9, 13\}, \{0, 2, 4, 6\ldots\} \ldots \} \]

• **Theorem:** P(N) is uncountable.

• **Proof:** (by contradiction) Suppose that P(N) is countable. Then by definition it is either finite or countably infinite. Clearly, it is not finite, therefore it must be countably infinite. By definition, since it is countably infinite it has the same cardinality as N (the natural numbers) and, by definition, there is a bijection \( f \) from N to P(N).
$f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$

$0 \rightarrow \mathbb{N}_0,$ $1 \rightarrow \mathbb{N}_1,$ $2 \rightarrow \mathbb{N}_2,$ \ldots \quad \text{*}\text{f is “onto” so every set in } \mathcal{P}(\mathbb{N}) \text{ is in this list.}

Consider the following table:

\[
\begin{array}{cccccc}
0 & 1 & 2 & 3 & \ldots \\
\hline
\mathbb{N}_0 & d^0_0 & d^0_1 & d^0_2 & d^0_3 \\
\mathbb{N}_1 & d^1_0 & d^1_1 & d^1_2 & d^1_3 \\
\mathbb{N}_2 & d^2_0 & d^2_1 & d^2_2 & d^2_3 \\
: & : & : & : & :
\end{array}
\]

$d^i_j = \begin{cases} 
0 & j \not\in \mathbb{N}_i \\
1 & j \in \mathbb{N}_i 
\end{cases} \quad \text{*The table is a 2 dimensional bit vector.}$
Consider/define the set $D$ such that for each $j \geq 0$:

$$j \in D \text{ if and only if } j \not\in N_j \quad (*)$$

Note that $D$ is represented by the complement of the diagonal.

Observations:

- $D$ is a (well-defined) subset of $\mathbb{N}$

- Since $N_0, N_1, N_2, \ldots$ is (supposedly) a list of all the subsets of $\mathbb{N}$, it then follows that $D = N_i (**)$, for some $i \geq 0$.

Question: Is $i \in D$ ?

- By definition of $D$ given in *, $i \in D$ if and only if $i \not\in N_i$

- But $D = N_i$ by **, and substitution gives $i \in N_i$ if and only if $i \not\in N_i$

A contradiction. Hence, $P(\mathbb{N})$ is uncountable.
By the way…what is the significance of a set being uncountable?

Looking ahead:

• The set of computer programs is countable.
• The set of all functions is not countable.
• Therefore, some functions don’t have programs, i.e., some functions aren’t computable.

Also, if a set is uncountable, then it can’t be iterated over in an orderly way that guarantees any particular element in the set will be reached in a predictable amount of computational time.
Diagonalization

• **Theorem:** The real numbers are uncountable.

• **Proof:** (by contradiction) Let \( R \) denote the set of all real numbers, and suppose that \( R \) is countable. Then, by definition, it is either finite or countably infinite. Clearly, it is not finite, therefore it must be countably infinite. By definition, since it is countably infinite it has the same cardinality as \( N \) (the natural numbers) and, by definition, there is a bijection \( f \) from \( N \) to \( R \).
\[ f: \mathbb{N} \rightarrow \mathbb{R} \]

\[ 0 \mapsto r_0, \ 1 \mapsto r_1, \ 2 \mapsto r_2, \ldots \]  
* \( f \) is “onto” so every real number is in this list.

Consider the following table:

<table>
<thead>
<tr>
<th>( 0 )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( \ldots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r_0 )</td>
<td>( d^0_0 )</td>
<td>( d^0_1 )</td>
<td>( d^0_2 )</td>
<td>( d^0_3 )</td>
</tr>
<tr>
<td>( r_1 )</td>
<td>( d^1_0 )</td>
<td>( d^1_1 )</td>
<td>( d^1_2 )</td>
<td>( d^1_3 )</td>
</tr>
<tr>
<td>( r_2 )</td>
<td>( d^2_0 )</td>
<td>( d^2_1 )</td>
<td>( d^2_2 )</td>
<td>( d^2_3 )</td>
</tr>
<tr>
<td>\vdots</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

where \( r_i = x_i.d^i_0 d^i_1 d^i_2 \ldots d^i_m \ldots \) (padded with zeros to the right)

*The table is a 2 dimensional vector of digits.
Consider/define the real number:

\[ y = 0.y_0y_1y_2\ldots \text{(infinite)} \]

where:

\[ y_i = (d_i^i + 1) \mod 10 \quad \text{for all } i \geq 0 \quad (*) \]

Observations:

- \( y \) is a well-defined real number

- Since \( r_0, r_1, r_2, \ldots \) is supposedly a list of all real numbers, it follows that \( y \) must be in this list, i.e., \( y = r_j \), for some \( j \geq 0 \).

- This means that \( y = r_j = 0.d_j^0d_j^1d_j^2\ldots d_j^{i-1}d_j^i d_j^{i+1}\ldots \) (from the table)

- This also means that \( y_i = d_i^j \), for all \( i \geq 0 \), and, in particular, that:

\[ y_j = d_j^j \]

But by \( (*) \):

\[ y_j = (d_j^j + 1) \mod 10 \]

a contradiction. Therefore, no such one-to-one and onto function exists, and therefore the real numbers are uncountable.
Vacuously True Statements

Many statements are technically true, but apparently meaningless:

- FIT has never been defeated by an SEC football team.
- It is only two days after Christmas and I already have all the lights off the house.
- Some celebrities pay up to $900 or more for Botox injections.
- Nika took Kim Kardashian out on a date every time she visited Melbourne last year.
- Melissa has dated every Melbourne resident who appeared in GQ magazine.

Notes:
- Disproving the first and last two of the above requires a counter-example.
- Although one might argue they are somewhat misleading, vacuously true statements are not a matter of opinion; logically they are absolutely true.
- They are also not a government conspiracy.

Similar, yet less impressive statements will occur in the context of this course.
Vacuously True Statements

Some statements may appear contradictory, but are still both true:

– Every FIT basketball player in this class has a GPA over 3.5.
– Every FIT basketball player in this class has a GPA under 3.5.

Assuming there are no FIT basketball players in this classroom, both of the above statements are true.