CISS358: Algorithm Analysis
Assignment 2

Objectives

- Prove a statement using mathematical induction.

Proving $P(n)$ for all $n \geq n_0$ where n_0 is a fixed integer

Recall that if you want to prove $P(n)$ is true for all $n \geq 42$, you have to do two things:

- Prove $P(42)$ is true
- Let $n \geq 42$. Assume $P(n)$ holds and prove $P(n+1)$ holds as well.

If you can achieve the above two points, then you can claim

- $P(n)$ is true for all $n \geq 42$

This is one form of mathematical induction called **weak mathematical induction**. The **strong mathematical induction** says that if you can do two things:

- Prove $P(42)$
- Let $n \geq 42$. Assume $P(42), P(42+1), ..., P(n)$ holds and prove $P(n+1)$ holds as well.

If you achieve the above two points, then you can claim

- $P(n)$ is true for all $n \geq 42$

The "42" above can be replaced by any integer (including some negative integer).

The above two induction techniques proves $P(n)$ are all true for $n \geq n_0$. Mathematical induction also allows you go "go backward". If you can do the following:

- Prove $P(n_0)$ is true
- Let $n \leq n_0$. Assume $P(n)$ holds and prove $P(n-1)$ holds as well.

then you can claim

- $P(n)$ is true for all $n \leq n_0$

This is also called weak mathematical induction. The strong induction going backward holds too. If you can achieve the following:

- Prove $P(n_0)$ is true
- Let $n \leq n_0$. Assume $P(n_0), P(n_0-1), ..., P(n)$ holds and prove $P(n-1)$ holds as well.

then you can claim

- $P(n)$ is true for all $n \leq n_0$

So induction allows you to prove $P(n)$ when n goes to infinity or when n goes to negative infinity.

There is another method that's important and does the same thing for you.

Sometimes, it is possible to prove $P(n)$ for all $n \geq 1$ by using the "proof by contradiction" method by using the well-ordering principle (WOP) which says that

- Every nonempty subset of $\mathbb{N} = \{0, 1, 2, ...\}$ has a least element, i.e., if X is a nonempty subset of $\mathbb{N}$, then there is some $m \in X$ such that $m \leq x$ for all $x \in X$.

(See class notes.) In this case, frequently, the proof involves an argument of the form:

"Suppose it's not true that $P(n)$ holds for all $n \geq n_0$". Then the set

$$X = \{n \mid n \geq n_0,\ \ P(n) \text{ does not hold}\}$$

is a nonempty subset of $\mathbb{N}$. By WOP, X has a least element, i.e., there is a smallest m such that $m \geq n_0$ and $P(m)$ is false. And you continue to prove that something goes wrong, i.e.,you attempt to arrive at a contradiction. This is frequently done in one of two ways. Here's one way to achieve this: Since m is the least element of X, all $n \in \mathbb{N}$ with $n < m$ must satisfy $P(n)$. From such n, you then show that in fact $P(m)$ holds, which clearly is a contradiction. The second method is this: Try to find some $m' < m$ such that $P(m')$ is also false. This would contradict the fact that m is the least elment of X.

(Aside. WOP is related to the proof method called **Fermat's infinite descent**. Applying the same argument above on k' and assuming $P(k')$ is false, you would arrive at another $k'' < k'$ such that $P(k'')$ is false, etc. This gives you infinitely many positive integers $k > k' > k'' > k''' > \cdots$. This is clearly impossible since there can only be finitely many positive integer from n_0 up to k.)

Until you know how to write induction proofs properly, you must follow these instructions for writing a proof that uses induction.

1. Paragraph 1: State you $P(n)$ and the range of values for n. If a problem involves proving multiple statements, you can also use $Q(n)$, $R(n)$, etc. State what method you are using (weak or strong induction). The default is weak induction, i.e., if you want you are using mathematical induction, it means you are using weak mathematical induction.
2. Paragraph 2: State you are proving the base case. Prove the base case.
3. Paragraph 3: State you are proving the inductive case. State your inductive hypothesis and state what you are going to prove. Then prove it. If the proof is long, state what you have proven. It's even a good idea to state it anyway. That's called good writing: State at the beginning of a paragraph what you want to do, do it, then remind the reader the goal at the beginning of the paragraph. (This is the longest part of the proof. If necessary, you might need more than one paragraph.)
4. Paragraph 4: State, quoting the method (i.e., induction), what you have proven.

Once you are done with writing about 50 induction proofs, you can use a freer form.

Here are two examples:

Theorem 0.1. *If $n \geq 0$, then*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

(Note that if $n = 0$, then the expression on the left-hand side of the above equation is 0 by definition. In other words an empty sum – sum of no terms – is defined to be 0.)

Proof. We will prove this by weak mathematical induction. For $n \geq 0$, we define

$$P(n) = \left(1 + 2 + \cdots + n = \frac{n(n+1)}{2}\right)$$

Base case. When $n = 0$, we have

$$1 + 2 + \cdots + n = 0 = \frac{0(0+1)}{2} = \frac{n(n+1)}{2}$$

Hence $P(0)$ holds.

Inductive case. Assume $P(n)$ holds where $n \geq 0$, i.e., we assume

$$P(n) = \left(1 + 2 + \cdots n = \frac{n(n+1)}{2}\right)$$

holds. We want to show $P(n+1)$ holds, i.e., we want to show

$$P(n+1) = \left(1 + 2 + \cdots n + 1 = \frac{(n+1)(n+1+1)}{2}\right)$$

is true. Since $P(n)$ holds, we have

$$\begin{aligned} 1 + 2 + \cdots n &= \frac{n(n+1)}{2} \\ \therefore \quad 1 + 2 + \cdots n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

i.e., $P(n+1)$ holds.

Therefore, by weak mathematical induction, $P(n)$ holds for all $n \geq 0$, i.e., for $n \geq 0$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

□

Theorem 0.2. *Let T be a tree wth at least one node, i.e., a connected simple graph with at least one node and no cycles. Then $e = v - 1$ where e and v are the number of edges and nodes of T respectively.*

(Note: A simple graph is a graph with no loops, i.e., no edge joining a node to itself and no multi-edges, i.e., no multiple edges joining the same two nodes. A graph is connected is for every pair of distinct vertices x, y, there is a path of edges from x to y.)

Proof. For a graph G, we will write v_G and e_G for the number of nodes and number of edges of G (respectively). For $n \geq 0$, we define the proposition $P(n)$ as follows:

$$P(n) = (\text{If } T \text{ is a tree with at least one node and with } n \text{ edges, then } e_T = v_T - 1)$$

We will prove $P(n)$ holds for all $n \geq 0$ by strong mathematical induction.

Base case. We will prove $P(0)$, i.e., we will prove that if T is a tree with at least one node and 0 edges (i.e., $e_T = 0$), then $e_T = v_T - 1$. If T has at least two distinct nodes, say x and y, then x and y are not adjacent since there are no edges in T. But T is connected. This is a contradiction. Hence T has exactly one node, i.e., $v_T = 1$. Therefore

$$e_T = 0 = 1 - 1 = v_T - 1$$

i.e., $P(0)$ holds.

Inductive case. Let $n \geq 0$. Assume $P(0), P(1), ..., P(n)$ holds. We will show that $P(n+1)$ holds, i.e., we will show that if T is a tree with at least one node and has $n + 1$ edges, then

$$e_T = v_T - 1$$

Let T be a tree with at least one node and $n + 1$ edges. Since $n \geq 0$, we have $n + 1 \geq 1$. Hence there is at least one edge in T, say e denote an edge in T joining node x and node y. Since T is simple, $x \neq y$. Construct the graph

$$G = T - e$$

i.e., G is the graph T with edge e removed. We have

$$v_G = v_T$$
$$e_G = e_T - 1$$

Note that G contains all the nodes of T and in particular contains x and y. We claim that G is made up of two disjoint trees.

First, we show that G has exactly two connected components, i.e., G is made up of two

maximal connected subgraphs. Suppose k is the number of connected components of G. Let $G_1, G_2, ..., G_k$ denote the connected components of G. There are no paths joining a node in G_i to a node in G_j if $i \neq j$. We will show $k = 2$ and furthermore each G_i is a tree.

The nodes x and y are in G. Therefore x is in some G_i and y is in some G_j. Note that $i \neq j$. Otherwise, if $i = j$, x and y are in the same connected component G_i which implies that there is some path p in G_i joining x and y. Since G_i is a subgraph of $G = T - e$ and G does not contain edge e, G_i cannot contain e. The path p (which is in G_i) therefore also cannot contain edge e. Hence p and edge e will form a cycle in T. This is a contradiction since T is a tree and cannot have a cycle. Hence we have shown that $i \neq j$, i.e., x and y are in two different connnected components of G.

Now suppose $k > 2$, i.e., suppose there are three connected components. Recall that x is in some G_i and y is in some G_j with $i \neq j$. Since there are at least three connected components, there is some k such that $k \neq i, k \neq j$. Let z be a node in G_k. Since T is a tree, there is a path p in T from x to z. There are no repeated nodes in p. Since x and z are in different connected components, the path p must leave G_i and must enter G_k. The only edge that leaves G_i is the edge e. Since y is in G_j, path p will leave G_i and enter G_j. Therefore on entering G_j, p contains x and y. However to arrive at G_k, which is not G_j, the path p has to leave G_j. The only edge leaving G_j is e, which means that the path p on leaving G_k will repeat x. This is a contradiction. We conclude that $k = 2$, i.e., there are two connected components in $G = T - e$.

We have now shown that there are two connected components G_1, G_2 in G.

We now show that the connected components G_1, G_2 in G are trees. Suppose there is a cycle C in G_1. Since G_1 is in $G = T - e$, the cycle C is also in G and is therefore in T. This is a contradiction since T is a tree. (This shows that every subgraph of a tree cannot have cycles.)

We have now shown that $T - e$ is made up of two disjoint trees, say T_1 and T_2.

Since T_1, T_2 are both subgraphs of G and G is a subgraph of T,

$$e_{T_i} \leq e_G = e_T - 1 < e_T = n + 1$$

for $i = 1, 2$. Therefore by induction hypothesis,

$$e_{T_1} = v_{T_1} - 1$$
$$e_{T_2} = v_{T_2} - 1$$

Adding these two equations, we get

$$\begin{aligned} e_{T_1} + e_{T_2} &= v_{T_1} - 1 + v_{T_2} - 1 \\ \therefore \quad e_{T_1} + e_{T_2} &= v_{T_1} + v_{T_2} - 2 \end{aligned} \tag{a}$$

Now note that since $T = G - e$, the only difference between T and G is an edge. Hence

$$e_T = e_G + 1 = e_{T_1} + e_{T_2} + 1 \tag{b}$$

$$v_T = v_G = v_{T_1} + v_{T_2} \tag{c}$$

Hence equations (a), (b), (c) gives us

$$\begin{aligned} e_T &= e_{T_1} + e_{T_2} + 1 \\ &= (v_{T_1} - 1) + (v_{T_2} - 1) + 1 \\ &= v_{T_1} + v_{T_2} - 1 \\ &= v_T - 1 \end{aligned}$$

We have now shown $P(n+1)$ holds if $P(0), P(1), ..., P(n)$ hold.

Therefore, by strong mathematical induction, $P(n)$ holds for all $n \geq 0$, i.e., we have shown that if T is a tree with at least one node then

$$e_T = v_T - 1$$

□

Template for induction proofs

A. Here is the template for weak induction proofs:

We will prove the above statemet by weak induction. For $n \geq ?$, let $P(n)$ be the statements

$$P(n) = \Big(n^2 \text{ is a prime}\Big)$$

Base case. We now prove the base case $P(?)$. [... your proof ...] Hence $P(?)$ holds.

Inductive case. We now prove the inductive case. Assume $P(n)$ holds where $n \geq ?$. [... your proof ...] Hence $P(n+1)$ holds.

Therefore, by weak mathematical induction, $P(n)$ is true for all $n \geq ?$, i.e., for any $n \geq ?$,

$$n^2 \text{ is a prime}$$

B. Here is the template for strong induction proofs:

We will prove $P(n)$ is true for all $n \geq ?$ using strong mathematical induction. For $n \geq ?$, let $P(n)$ be the statements

$$P(n) = \Big(n^2 \text{ is a prime}\Big)$$

Base case. We now prove the base case $P(?)$. [... your proof ...] Hence $P(?)$ holds.

Inductive case. We now prove the inductive case. Assume $P(?), P(?+1), ..., P(n)$ hold where $n \geq ?$. [...] Hence $P(n+1)$ holds.

Therefore, by strong mathematical induction, $P(n)$ is true for all $n \geq ?$, i.e., for any $n \geq ?$,

$$n^2 \text{ is a prime}$$

B. Here is a template for WOP proofs:

We will prove the above statement using the well-ordering principle. For $n \geq ?$, let $P(n)$ be

$$P(n) = \Big(n^2 \text{ is a prime}\Big)$$

Assume on the contrary that $P(n)$ does not hold for all $n \geq ?$. Then there is some n such

that $P(n)$ does not hold. Define

$$X = \{n \geq ? \mid P(n) \text{ does not hold}\}$$

[... now prove that X is a nonempty subset of $\mathbb{Z}$ that is bounded below, or a nonempty subset of $\mathbb{N}$.]

By the well-ordering principle X has a least element, say m. Since m is the least element of X, $P(n)$ holds for all $? \leq n < m$. [Now derive a contradiction. Warning: You usually have to use some n such that $? \leq n < m$. This means that you have to explain why $m >?$.] This is a contradiction because [...]

Therefore, $P(n)$ holds for all $n \geq ?$.

Q1. Using mathematical induction, give a complete proof of the following fact:

$$4(1^3 + 2^3 + \cdots + n^3) = n^2(n+1)^2$$

for $n \geq 1$.

SOLUTION.

□

Primes

Note that a number n is said to be a **prime** if it is a whole number that can only be divided by 1 and itself (i.e., n). The positive integer n is said to be **composite** if it is greater than 1 and is not a prime, which means that it is possible to write n as a product, $n = a \cdot b$, where a and b are positive integers such that $1 < a < n$ and $1 < b < n$. A positive integer n (positive means > 0) must fall into exactly one of the 3 cases:

- n is 1
- n is prime
- n is composite.

Note that if a and b are integers and $a > 0$, $b > 0$, then $a \leq ab$ and $b \leq ab$. And if $a > 1$, then $b < ab$.

Q2. Consider the following fact: Every positive integer $n \geq 1$ is a product of primes. For instance for $n = 20$, the ordered collection of primes involved are $(2, 2, 5)$ (in ascending order). We define the product of the empty collection of primes, i.e. (), to be 1. Of course the collection can have one single number: If the collection is (11), then the product is 11.

Define $P(n)$ to be the above statement, i.e.,

$$P(n) = \Big(\text{Every positive integer } n \geq 1 \text{ is a product of primes}\Big)$$

Give a complete proof of $P(n)$ for all $n \geq 1$ using strong or weak induction. Here, I'm giving you the $P(n)$ for free.

You can assume Euclid's lemma: If p is a prime dividing ab, then p divides a or p divides b.

(In fact not only is every positive integer n representable as a product of primes, it is represented as a product of primes in a *unique way*. In other words, the ordered collection of primes for n is unique. This can also be proven using induction. But you don't have to prove it.)

SOLUTION.

□

Q3. Consider the following statement: Every positive integer is a sum of distinct 2-powers. In other words, there is a set of distinct 2-powers whose sum is the given positive integer. For instance the number 10 can be expressed as

$$10 = 2^1 + 2^3$$

(a) Prove the above statement using strong or weak induction.

(b) Prove the above statement using the well-ordering principle.

(Note: This is the missing piece of information in CISS360. In CISS360, we assume that, for instance, all 32-bit unsigned int can be written as a binary sequence which is a sum of powers of 2 up to the power of 31. Also, the set of 2-powers adding up to n is unique. For instance $2^1 + 2^3 = 10$ and if you look at another sum of 2–powers such as $2^1 + 2^2$, you will not get 10. But you don't have to prove it.)

SOLUTION.