

CSC236 Homework Assignment #1

The Principle of Simple, Strong, and Structural
Induction

Alexander He Meng

Prepared for September 30, 2024

Question #1

Let $P(n)$: For any set A , if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$

(a) **Claim:** $\forall n \in \mathbb{N}, P(n)$

Proof.

This proof explores the Principle of Simple Mathematical Induction.

Base Case $\{P(0)\}$:

Let $n = 0$.

Suppose an arbitrary set A has the property $|A| = n = 0$. Then, A is a set with 0 elements, so its power set, $\mathcal{P}(A)$, must have the null set as the only element; $|\mathcal{P}(A)| = |\emptyset| = 1 = 2^0$.

Thus, $P(0)$.

Induction Hypothesis:

Assume for some $k \in \mathbb{N}, P(k)$. Namely, for some $k \in \mathbb{N}$, assume for any set A , if $|A| = k$ then $|\mathcal{P}(A)| = 2^k$.

Induction Step:

The following intends to prove $P(k+1)$, which namely represents that for any set A , if $|A| = k+1$, then $|\mathcal{P}(A)| = 2^{k+1}$.

Consider A as a set with $k+1$ elements:

$$A = \{a_1, a_2, \dots, a_k, a_{k+1}\}.$$

Denote $\tilde{A} \subset A$ such that $a_{k+1} \notin \tilde{A}$:

$$\tilde{A} = \{a_1, a_2, \dots, a_k\}.$$

By the induction hypothesis, \tilde{A} has 2^k subsets; denote these subsets by $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{2^k}$.

Since $\tilde{A} \subset A$, $\mathcal{P}(A)$ can be expressed in terms of $\mathcal{P}(\tilde{A})$, because every subset of \tilde{A} is also a subset of A .

The remaining subsets for $\mathcal{P}(A)$ are expressed by adding a_{k+1} to the common sets between both power sets; denote these remaining subsets by $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_{2^k}$:

$$\begin{aligned}\mathcal{B}_1 &= \mathcal{A}_1 \cup \{a_{k+1}\} \\ \mathcal{B}_2 &= \mathcal{A}_2 \cup \{a_{k+1}\}, \\ &\dots \\ \mathcal{B}_{2^k} &= \mathcal{A}_{2^k} \cup \{a_{k+1}\}\end{aligned}$$

Altogether, \mathcal{A}_i and \mathcal{B}_j , for $i, j \in [0, 2^k]$, compose a complete list of the subsets of A .

Subsets not containing the element a_{k+1} are one of the \mathcal{A}_i , while subsets containing a_{k+1} are one of the \mathcal{B}_j . Hence, there is exactly one listing of every subset of A .

Lemma α :

Finally, consider that $\mathcal{A}_i \cap \mathcal{B}_j = \emptyset$, because $a_{k+1} \in \mathcal{B}_j$ but $a_{k+1} \notin \mathcal{A}_i$, for all $i, j \in [0, 2^k]$.

This means $|A_i \cup B_j| = |A_i| + |B_j| - |A_i \cap B_j| = |A_i| + |B_j| - |\emptyset| = |A_i| + |B_j| - 0 = |A_i| + |B_j|$.

Therefore, $\mathcal{P}(A) = \mathcal{A}_i \cup \mathcal{B}_j$, for $i, j \in [0, 2^k]$

$\implies |\mathcal{P}(A)| = |\mathcal{A}_i \cup \mathcal{B}_j|$, for $i, j \in [0, 2^k]$

$\implies |\mathcal{P}(A)| = |\mathcal{A}_i| + |\mathcal{B}_j|$, for $i, j \in [0, 2^k]$, by Lemma α

$\implies |\mathcal{P}(A)| = 2^k + 2^k$, there are 2^k subsets A_i and 2^k subsets B_j

$\implies |\mathcal{P}(A)| = 2^k \cdot 2$

$\implies |\mathcal{P}(A)| = 2^{k+1}$.

Conclusion:

Therefore, $|A| = k + 1 \implies |\mathcal{P}(A)| = 2^{k+1}$ as needed. By the Principle of Simple Mathematical Induction, $P(n)$ holds for all $n \in \mathbb{N}$.

Citation:

This proof is inspired by pp. 105-106 from the textbook, “Shay Fuchs - Introduction to Proofs and Proof Strategies (Cambridge Mathematical Textbooks)-Cambridge University Press (2023).”

□

Let $Q(A, n) : |A| = n \implies |\mathcal{P}(A)| = 2^n$

(b) **Claim:** For any set A , $\forall n \in \mathbb{N}, Q(A, n)$

An attempted proof.

This proof explores the Principle of Simple Mathematical Induction.

Fix A to be an arbitrary set.

Base Case $\{Q(A, 0)\}$:

Let $n = 0$.

Suppose A has the property $|A| = n = 0$. Then, A is a set with 0 elements, so its power set, $\mathcal{P}(A)$, must have the null set as the only element; $|\mathcal{P}(A)| = |\emptyset| = 1 = 2^0$.

Thus, $Q(A, 0)$.

Induction Hypothesis:

Assume for some $k \in \mathbb{N}, Q(A, k)$. Namely, assume $|A| = k \implies |\mathcal{P}(A)| = 2^k$.

However, the proof breaks here for any values $k \neq 0$, as A has a fixed cardinality of 0 due to the base case.

Suppose the proof proceeds nonetheless...

Induction Step:

The following attempts to prove $P(k+1)$, which namely represents $|A| = k+1 \implies |\mathcal{P}(A)| = 2^{k+1}$.

Attempt to consider A as a set with $k+1$ elements; $|A| = k+1$:

$$A = a_1, a_2, \dots, a_k, a_{k+1}.$$

It is no longer relevant to the predicate, $Q(A, n)$, to denote $\tilde{A} \subset A$ such that $a_{k+1} \notin \tilde{A}$. This is because $Q(A, n)$ requires the arbitrary set A to be fixed.

Thus, consider A also as a set with k elements; $|A| = k$.

However, A is already established to have $k+1$ elements. If $|A| = k+1$ and $|A| = k$, then $k+1 = k \implies 1 = 0$, which is a contradiction.

Hence, A cannot also have k elements, so the Induction Hypothesis cannot be leveraged.

Therefore, the attempted induction proof fails. The failure occurs because the predicate, $Q(A, n)$, restricts A to be a fixed set, preventing the inductive property that requires another set with cardinality, $|A| + 1$, to show $Q(A, k+1)$.

Question #2

Let n, m be natural numbers. Let A and B be arbitrary finite sets of sizes m and n , respectively.

(a): Claim: There are n^m functions with domain A and co-domain B , where $|A| = m$ and $|B| = n$, $\forall m, n \in \mathbb{N}$.

Proof.

This proof explores the Principle of Simple Mathematical Induction.

Predicate:

Let S be the set of all functions $f : A \mapsto B$, where $|A| = m$ and $|B| = n$, for natural numbers n, m .

$$P(m) := |S| = n^m$$

Base Cases

Let $m = 0$.

Then, $|A| = m = 0 \implies A = \emptyset$, and f is a function which maps elements of A to elements of B .

Denote f_0 as the function that leaves no elements from A unmapped to B .

If $m \neq 0$ and $n = 0$, there is simply no element in B that any elements of A can map to. There are $0 = 0^m$ functions.

If $n \neq 0$, then a function is vacuously well-defined; there is $1 = n^0$ function.

Also, if $n = 0$, then a function is vacuously well-defined, and the number of functions is $1 = 0^0$.

With no elements in A , f_0 is vacuously a valid function, and also the only unique way to map A to B .

Hence, $S = \{f_0\}$

$$\implies |S| = |\{f_0\}|$$

$$\implies |S| = 1$$

$$\implies |S| = n^0$$

$$\implies |S| = n^m|_{m=0},$$

so $P(0)$.

Next, let $m = 1$.

Then, $|A| = m = 1 \implies A = \{a_1\}$, a_1 is an arbitrary element.

The lone element, a_1 , in A may map to any element of B .

Since B has n elements, a_1 can possibly map to n different elements.

So, there are n mappings possible, and thus, n possible functions.

Hence, $S = \{f_1, f_2, \dots, f_n\}$, where f_i for $i \in [1, n]$

$$\implies |S| = |\{f_1, f_2, \dots, f_n\}|$$

$$\implies |S| = n$$

$$\implies |S| = n^1$$

$$\implies |S| = n^m|_{m=1},$$

so $P(1)$.

Induction Hypothesis:

Assume for some $k \in \mathbb{N}$, $P(k)$. Namely, assume for some $k \in \mathbb{N}$, $|S| = n^k$.

Induction Step:

Suppose $|A| = k + 1$, where $A = \{a_1, a_2, \dots, a_k, a_{k+1}\}$.

Denote $\tilde{A} \subset A$ to be the set obtained by removing a_{k+1} from A ; so, $\tilde{A} = \{a_1, a_2, \dots, a_k\}$.

The induction hypothesis suggests that there are n^k unique functions which map \tilde{A} to B , where $|\tilde{A}| = k$ and $|B| = n$.

Next, A can be expressed in terms of \tilde{A} :

$$A = \tilde{A} \cup \{a_{k+1}\}$$

To show $P(k + 1)$, it is sufficient to see that there are n^{k+1} functions, $f : A \mapsto B$.

Notice that $A \mapsto B \Rightarrow \tilde{A} \cup \{a_{k+1}\} \mapsto B$.

\tilde{A} yields n^k unique function mappings to B (by the induction hypothesis), and a_{k+1} yields n unique function mappings B (as $|B| = n \Rightarrow a_{k+1}$ can map to n possible elements).

Since $a_{k+1} \notin \tilde{A}$, $A = \tilde{A} \cup a_{k+1}$ altogether yields $n^k \cdot n = n^{k+1}$ unique functions that map its elements to the elements of B .

Conclusion:

Therefore, if $|A| = k + 1$ and $|B| = n$, then there are n^{k+1} unique functions, $f : A \mapsto B$, as needed. By the Principle of Simple Mathematical Induction, $P(n)$ holds for all $n \in \mathbb{N}$. □

From *Question #1*...

Let $P(n)$: For any set A , if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$

(b) Claim: $\forall n \in \mathbb{N}, P(n)$

Proof.

This proof leverages the previous claim that has been proving, stating:

If $n, m \in \mathbb{N}$ and A, B are arbitrary finite sets of sizes m and n respectively,
then there are n^m functions with domain A and co-domain B . (1)

Let A be an arbitrary set such $|A| = n$.

Then, unique functions can $f : A \mapsto \{0, 1\}$ can map all subsets $\tilde{A} \subset A$ as follows:

$$\forall a \in A, a \in \tilde{A} \text{ yields } f(a) = 1; \text{ otherwise, } f(a) = 0$$

The claim from *Part (a)* concludes that there are 2^n different functions with domain A and co-domain $\{0, 1\}$.

Hence, there must also be 2^n subsets of A , meaning $\mathcal{P}(A) = 2^n$.

□

Question #3

The connectives \neg , \wedge , \vee , \rightarrow , and \leftrightarrow are prevalent in propositional logic.

Let $Q(P)$ denote:

P is equivalent to a proposition built only using $\{\neg, \rightarrow\}$.

Claim: For all propositions P , $Q(P)$

Proof.

Base Case:

Let P be a proposition $P_i(\text{connective}_1, \text{connective}_2, \dots, \text{connective}_k)$.

Then, P_i is equivalent a proposition constructed using only $\{\neg, \rightarrow\}$ (i.e. themselves).

Thus, $P_i(\text{connective}_1, \text{connective}_2, \dots, \text{connective}_k)$.

Induction Hypothesis:

Assume for some propositions X, Y $Q(X), Q(Y)$. Namely, assume that X is equivalent to a proposition built only using \neg, \rightarrow , and likewise for Y .

Induction Step:

Denote Z, W as propositions constructed from only \neg, \rightarrow respectively.

Then, $X \equiv Z$ and $Y \equiv W$.

Now, consider the following five cases:

Case 1: $\neg X \equiv \neg Z$

Trivially, $Q(\neg X)$ holds.

Case 2: $X \rightarrow Y \equiv Z \rightarrow W$

Again, $Q(X \rightarrow Y)$ trivially holds.

Case 3: $X \wedge Y \equiv Z \wedge W$

Consider the following truth table:

Z	W	$Z \wedge W$	$\neg(Z \rightarrow \neg W)$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Because $X \wedge Y \equiv \neg(C \rightarrow \neg D)$, a proposition constructed by $\{\neg, \rightarrow\}$, $Q(X \wedge Y)$.

Case 4: $X \vee Y \equiv Z \vee W$

Consider the following truth table:

Z	W	$Z \vee W$	$\neg(\neg Z \rightarrow W)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Because $X \vee Y \equiv \neg(\neg C \rightarrow D)$, a proposition constructed by $\{\neg, \rightarrow\}$, $Q(X \vee Y)$.

Case 5: $X \leftrightarrow Y \equiv Z \iff W$

Consider the following truth table:

Z	W	$Z \leftrightarrow W$	$\neg((Z \rightarrow W) \rightarrow \neg(W \rightarrow Z))$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	T	T

Because $X \leftrightarrow Y \equiv \neg((Z \rightarrow W) \rightarrow \neg(W \rightarrow Z))$, a proposition constructed by $\{\neg, \rightarrow\}$, $Q(X \leftrightarrow Y)$.

Conclusion:

Therefore, by the Principle of Structural Induction, $Q(P)$ holds for all propositions P .

□

Question #4

Consider the following two-pointer style Python program which finds whether a given string s is a palindrome or not:

```
def check_if_palindrome(s):
    left = 0
    right = len(s) - 1
    while left < right:
        if s[left] != s[right]:
            return False
        left += 1
        right -= 1
    return True
```

Claim: The above program is correct and will terminate.

Proof.

This proof explores the Principle of Simple Mathematical Induction.

Proving Correctness...

Predicate:

Let s be an arbitrary string. Let $i \in \mathbb{N}$.

Define the loop invariant as follows:

$$P(i) := (0 \leq i \leq \text{len}(s)//2 + 1) \implies (\forall k > 0, k < i \implies s[k-1] = s[\text{len}(s) - k])$$

This proof intends to demonstrate that $P(\text{len}(s)//2 + 1)$ holds after the final iteration of the loop. As a result, this shows that, for the string s , the former half is equivalent to the reverse of the latter half.

Leveraging induction on i can demonstrate that for all $i \in \mathbb{N}$, $P(i)$ holds at the start of each i -th iteration.

Base Cases:

Let $i = 0$.

Then, for all $k \in \mathbb{N}, k > 0, k < 0$ is false, so $P(0)$ is vacuously true.

Let $i = 1$.

Likewise, for all $k \in \mathbb{N}, k > 0, k < 1$ is still false, so $P(1)$ is vacuously true.

Induction Hypothesis:

Assume that for some $i \in \mathbb{N}$, $P(i)$ holds at the start of each i -th iteration.

Induction Step:

Suppose $0 \leq i + 1 \leq \text{len}(s)//2$.

If $i + 1 \in \{0, 1\}$, then $P(i + 1)$ holds trivially (see base cases).

Hence, assume $1 \leq i + 1 \leq \text{len}(s)//2 - 1$

$\implies 0 \leq i \leq \text{len}(s)//2 - 2$.

This demonstrates the induction hypothesis.

The induction hypothesis accounts for all $k < i$.

Hence, it is sufficient to demonstrate that $k = i$ implies $s[\text{len}(s) - k]$ at the end of the i -th iteration, in order to show $P(i + 1)$ holds at the start of the $i + 1$ -th iteration.

Notice that the left and right pointers start at 0 and $\text{len}(s)$ respectively, then increments and decrements by 1 respectively after each iteration.

This means for the i -th iteration, the left and right pointers have already incremented and decremented respectively $i - 1$ times.

Therefore, $left = 0 + (i - 1) = i - 1$ and $right = \text{len}(s) - 1 - (i - 1) = \text{len}(s) - i$, where $left, right$ represent the left and right pointers of the loop respectively.

There are now two cases, as follows:

Case 1: $s[left] \neq s[right]$

In this case, s is simply not a palindrome, so the program returns **False** and terminates. The program also never reaches the $i + 1$ -th iteration, so the post-conditions of the program are satisfied.

Case 2: $s[left] = s[right]$

Here, $s[i - 1] = s[\text{len}(s) - i]$, so the program increments $left$ and decrements $right$ without ever entering the body of the if-statement.

Thereafter, the program advances to the $i + 1$ -th iteration.

Because $s[k - 1] = s[\text{len}(s) - k]$ holds for $k \in [1, i]$, $P(i + 1)$ holds at the beginning of the $i + 1$ -th iteration.

Correctness Conclusion:

Therefore, by the Principle of Simple Mathematical Induction, $P(i)$ holds at the start of all iterations i for $i \in \mathbb{N}$.

Proving Termination...

Denote the loop invariant to be the value of the right pointer, which takes the initial value of $\text{len}(s) - 1$.

Because the right pointer decrements by 1 after each loop iteration, so does the loop invariant decrements likewise.

If the string is empty (i.e. $\text{len}(s) = 0$), then the value of the left pointer is smaller than that of the right pointer, and the loop does not run.

If the string is not empty, then the value of the right pointer is bounded (from below) by the value of the left pointer; the right pointer value decreases through each iteration.

Therefore, the loop terminates.

Conclusion:

Collectively, the correctness and termination of the program has been shown, as needed.

Thus, this proof is complete.

□

Question #5

(Note: Because n is a common variable between the claim of *Question #2* and the claim of *Question #5 (a)*, refer to n -ary as N -ary for the following claim.)

(a) Claim: $\forall n \in \mathbb{N}$, there are 2^{2^N} N -ary connectives.

Proof.

The claim from *Question #2* states that there are n^m functions with domain A and co-domain B , where $|A| = m$ and $|B| = n$, for natural numbers m, n .

Since a function with mapping, $\{T, F\}^N \mapsto \{T, F\}$, represents the N -ary connective, the claim from *Question #2* can be applied, as follows:

$$|A| = |\{T, F\}^N| = 2^N = m \text{ and } B = |\{T, F\}| = 2 = n.$$

Hence, there are $n^m = 2^{2^N}$ such functions, so there are 2^{2^N} N -ary connectives.

□

(b) Claim: Any truth table that can ever exist is the truth table of some proposition constructed using only $\{\neg, \wedge\}$.

Proof.

This proof explores the Principle of Simple Induction.

Predicate:

$P(n) :=$ If Z is an arbitrary n -ary truth table, there exists an equivalent truth table of some proposition constructed using only $\{\neg, \wedge\}$.

Base Case:

Let $n = 1$.

With an arbitrary predicate, p , there are four possible unary truth tables, Z :

p	Z	p	Z	p	Z	p	Z
T	T	T	F	T	T	T	F
F	T	F	F	F	F	F	T

The above truth tables represent T , F , p , and $\neg p$ respectively, which are constructed using only $\{\neg, \wedge\}$.

Thus, $P(1)$.

Induction Hypothesis:

Assume that for some $k \in \mathbb{N} \setminus \{0\}$, $P(k)$.

Induction Step:

Consider an arbitrary $n + 1$ -ary truth table Z . Let the inputs of Z be $p_1, p_2, \dots, p_n, p_{n+1} \in \{T, F\}$.

Denote Z_T and Z_F both as k -ary truth tables obtained by fixing p_{k+1} to be true and false respectively.

By the induction hypothesis, there exists some truth table equivalent to Z_T and some other truth table equivalent to Z_F , both with propositions constructed using only $\{\neg, \wedge\}$.

Denote the propositions of the respective equivalent truth tables by $\Theta_T(p_1, p_2, \dots, p_k)$ and $\Theta_F(p_1, p_2, \dots, p_k)$.

With the $k + 1$ -ary truth function as

$$\Theta(p_1, p_2, \dots, p_k, p_{k+1}) := (\Theta_T(p_1, p_2, \dots, p_k) \wedge p_{k+1}) \vee (\Theta_F(p_1, p_2, \dots, p_k, p_{k+1}) \wedge \neg p_{k+1}),$$

there are two cases to consider in confirming the equivalence between the truth table of the above truth function and Z .

Case 1: $p_{k+1} = T$

$$\begin{aligned} & \text{This shows that } \Theta(p_1, p_2, \dots, p_k, p_{k+1}) \\ & \equiv \Theta(p_1, p_2, \dots, p_k, T) \\ & \equiv (\Theta_T(p_1, p_2, \dots, p_k) \wedge T) \vee (\Theta_F(p_1, p_2, \dots, p_k) \wedge \neg T) \\ & \equiv (\Theta_T(p_1, p_2, \dots, p_k) \wedge T) \vee (\Theta_F(p_1, p_2, \dots, p_k) \wedge F) \\ & \equiv \Theta_T(p_1, p_2, \dots, p_k). \end{aligned}$$

Thus, the truth table Z outputs $\Theta_T(p_1, p_2, \dots, p_k)$ when p_{k+1} is T . This means $\Theta(p_1, p_2, \dots, p_k, p_{k+1})$ matches the output of Z given that $p_{k+1} = T$.

Case 2: $p_{k+1} = F$

$$\begin{aligned} & \text{This shows that } \Theta(p_1, p_2, \dots, p_k, p_{k+1}) \\ & \equiv \Theta(p_1, p_2, \dots, p_k, F) \\ & \equiv (\Theta_T(p_1, p_2, \dots, p_k) \wedge F) \vee (\Theta_F(p_1, p_2, \dots, p_k) \wedge \neg F) \\ & \equiv (\Theta_T(p_1, p_2, \dots, p_k) \wedge F) \vee (\Theta_F(p_1, p_2, \dots, p_k) \wedge T) \\ & \equiv \Theta_F(p_1, p_2, \dots, p_k). \end{aligned}$$

Thus, the truth table Z outputs $\Theta_F(p_1, p_2, \dots, p_k)$ when p_{k+1} is F . This means $\Theta(p_1, p_2, \dots, p_k, p_{k+1})$

also matches the output of Z given that $p_{k+1} = F$.

Therefore, for $p_{k+1} \in \{T, F\}$, $\Theta(p_1, p_2, \dots, p_k, p_{k+1})$ matches the output of truth table Z . This implies that $\Theta(p_1, p_2, \dots, p_k, p_{k+1})$ yields an equivalent output to that of Z .

Finally, using De Morgan's Laws, consider that:

$$\begin{aligned}\Theta(p_1, p_2, \dots, p_k, p_{k+1}) &= (\Theta_T(p_1, p_2, \dots, p_k) \wedge p_{k+1}) \vee (\Theta_F(p_1, p_2, \dots, p_k, p_{k+1}) \wedge \neg p_{k+1}) \\ &= \neg(\neg(\Theta_T(p_1, p_2, \dots, p_k) \wedge p_{k+1}) \wedge \neg(\Theta_F(p_1, p_2, \dots, p_k, p_{k+1}) \wedge \neg p_{k+1}))\end{aligned}$$

Thus, Θ is a proposition constructed using only $\{\neg, \wedge\}$.

So, $P(k+1)$.

Conclusion:

Therefore, by the Principle of Simple Mathematical Induction, any truth table is the truth table of some proposition constructed using only $\{\neg, \wedge\}$.

□