Discussion Worksheet 1

1 Proof Methods Recap

1. **Proof Misconceptions.** For each of the following, determine what is incorrect about the proposed proof technique.

   (a) **Claim:** There are no even primes greater than 2.
   Proof: 3 is a prime that is greater than 2 and it is not even, so there must be no even primes greater than 2.

   (b) **Claim:** If n^2 is even, then n is even.
   Proof: If n is even, then $n = 2k$ for some integer k. Therefore, $n^2 = 4k^2 = 2 \cdot 2k^2$.

   (c) **Claim:** The sum of the first i positive odd integers equals the i^{th} square.
   Proof: $1 = 1^2$, $1 + 3 = 4 = 2^2$, $1 + 3 + 5 = 9 = 3^2, \ldots$. The pattern will continue, so the claim is proven.

   (d) **Claim:** 37 is the largest prime smaller than 41.
   Proof: 37 is prime since its only divisors are 1 and 37.

   (e) **Claim:** The sum of two even integers is even.
   Proof: Let n, m be two even integers. Since they are both even, then let $n = 2k$ and $m = 2k$ for some integer k. $n + m = 2k + 2k = 4k = 2(2k)$, therefore the sum is also even.

Solution:

(a) What is asked to be shown is that there are no primes greater than 2 that are even, however, this proof only provided a single counterexample. The main issue with this proof is that it attempts to prove a for all statement (for all primes greater than 2) using a counterexample. The proof would instead need to be general enough to apply to all primes greater than 2, not just one of them.

(b) The proof attempted to prove a statement of the form $p \to q$ by proving that $q \to p$. While it is possible that both $p \to q$ and $q \to p$ are true, $q \to p$ being true does not imply that $p \to q$ is true. Instead, this could be proven either directly or using the contrapositive.

(c) It is not sufficient to show a pattern but then not prove that the pattern continues. Noticing that there is a pattern and becoming convinced that the claim is true are critical to understanding the proof, however, they do not constitute the proof itself. One valid way to prove the given claim is through induction.

(d) This is not a complete proof because the proof did not demonstrate that 37 was necessarily largest prime smaller than 41, but rather only showed that 37 was prime. To complete the proof, one should also show that $38, 39$ and 40 are all composite (not prime).

(e) This proof is incorrect because it assumes that n and m are the same even number which is not necessarily true. Instead, the proof should assign $n = 2k_1$ and $m = 2k_2$ for integers k_1 and k_2 in order to be general enough to allow n and m to be distinct.

2. **Proof By Contradiction.** Prove by contradiction that $\sqrt{7}$ is irrational.

Solution: Since this proof is by contradiction, the first step is to suppose that the negation of the claim is true and then proceed to show that a contradiction is reached.

In this way, suppose that $\sqrt{7}$ is rational.

By definition of rational, this means that $\sqrt{7} = \frac{a}{b}$ for some integers a, b and such that a and b share no common factors greater than 1.

Then $7 = \frac{a^2}{b^2}$ and thus $7b^2 = a^2$. Since a^2 is divisible by 7 and since 7 is prime, then it must also be true that a is divisible by 7. Therefore, $a = 7k$ for some integer k.

Substituting $7k$ in for a, $7b^2 = (7k)^2 = 49k^2$. Dividing by 7, $b^2 = 7k^2$. This then implies that b^2 is divisible by 7 and thus also that b is divisible by 7 by the same argument as above.

While a and b are both divisible by 7, they also must not share any divisors greater than 1, therefore there is a contradiction and the original claim is prove true.

3. **Geometric Sums.** Let $a_1, a_1r, a_1r^2, \ldots, a_1r^n$ be a finite geometric sequence with common ratio r and initial term a_1 (notice the 1-indexing). Prove using induction that the sum of the i terms is equal to $S_i = \frac{a_1(1-r^i)}{1-r}$.

Solution:

Let the proposition $P(k)$ be true if and only if $S_k = \frac{a_1(1-r^k)}{1-r}$.

Base Case: $P(1) : \frac{a_1(1-r^1)}{1-r} = a_1 \cdot \frac{(1-r)}{1-r} = a_1$.

Inductive Step: Suppose that $P(k)$ is true for some positive integer k. We now want to show that $P(k+1)$ is also true. Note that the $k+1^{th}$ term equals a_1r^k rather than a_1r^{k+1}.

$$
\begin{aligned}
S_{k+1} &= S_k + a_1 \cdot r^k && (1)\\
&= \frac{a_1(1-r^k)}{1-r} + a_1 \cdot r^k && (2)\\
&= \frac{a_1 - a_1 \cdot r^k + a_1 \cdot r^k - a_1 \cdot r^{k+1}}{1-r} && (3)\\
&= \frac{a_1 - a_1 \cdot r^{k+1}}{1-r} && (4)\\
&= \frac{a_1(1-r^{k+1})}{1-r} && (5)
\end{aligned}
$$

Since $P(k) \to P(k+1)$ and since $P(1)$ was true, then by induction the original claim is also true.

4. **Number of Binary Strings.** Prove that the number of binary strings of length k is 2^k.

Solution: Let $P(k)$ be the statement: The number of binary strings of length k is 2^k.

Base case: There is only one binary string of length zero, i.e., the empty string ε, and $2^0 = 1$ so $P(0)$ is true.

Inductive step: Assume $P(j)$ is true for some j. Consider a string s of length $j+1$, denoted $s_0 s_1 \dots s_j s_{j+1}$. We can split s into $s_1 \dots s_j || s_{j+1}$. By IH, we know that there are 2^j possible strings for $s_1 \dots s_j$. For s_{j+1}, there are two possibilities: 0 or 1. Therefore, by multiplication rule from counting techniques, we have $2^j \cdot 2 = 2^{j+1}$ possible strings of length $j+1$.

5. **Strong Induction.** Suppose there is a pile of n stones that must be split into n piles of 1 stone each. Each split is characterized by taking a pile with > 1 stone and splitting the pile into 2 smaller piles each having at least 1 stone. Prove that no matter how the splits are performed over an initial pile of size n (i.e. any ordering, equal/unequal splits, etc.), the sum of the pairwise products of the splits will equal $\frac{n(n-1)}{2}$.

   As an example of the process, suppose there are 4 stones to start. One possible way to perform the splits is to have 3 splits as follows: $(2-2), (1-1)-2, 1-1-(1-1)$. This notation is intended to indicate first splitting into 2 piles of 2, then splitting 1 of the 2 piles of 2 into 2 piles of 1, and finally splitting the other pile of 2 into 2 piles of 1. Computing the sum of the pairwise products of the splits, we have $2 \cdot 2 = 4$ from the first split since the first split resulted in 2 piles of 2, then $1 \cdot 1 = 1$ from the second split since the second split resulted in 2 piles of size 1, and finally $1 \cdot 1 = 1$ for the third split. Summed together, we have $4 + 1 + 1 = 6 = \frac{4(4-1)}{2}$. The same process can be done by instead having the first split be $(3-1)$ and so on and the pairwise sum of splits will still be 6 (you can check!).

Solution: The claim can be proven using strong induction. As a minor note, strong induction differs from typical induction in that typical induction proves a claim during the inductive step of the form $P(k) \to P(k+1)$ whereas strong induction proves a claim of the form $P(1) \wedge P(2) \wedge \dots \wedge P(k) \to P(k+1)$.

Let the proposition $P(k)$ be true if and only if the sum of the pairwise product of splits of a pile of size k will equal $\frac{k(k-1)}{2}$ regardless of the way the splits are performed.

Base Case: $P(1)$: When starting out with a pile of size 1, there are no splits to be performed in order to reduce down to only piles of size 1 so the pairwise product of splits equals $0 = \frac{1(1-1)}{2}$.

Inductive Hypothesis: Suppose that $P(1) \wedge P(2) \wedge \dots \wedge P(k-1)$ is true.

Inductive Step: It is now the goal to prove that $P(k)$ is also true. The key insight it to perform a single arbitrary split on the pile of size k and then invoke the inductive hypothesis.

Given a pile of stones of size k, split the pile into one of size i and the other of size $k-i$ with $1 \leq i \leq k-1$. Also, let $SumOfSplits(n)$ be a function that maps pile size to the sum of splits of that pile size.

After performing the first split:

$$SumOfSplits(k) = SumOfSplits(i) + SumOfSplits(k-i) + i \cdot (k-i)$$

Then invoking the inductive hypothesis two times:

$$SumOfSplits(k) = \frac{i(i-1)}{2} + \frac{(k-i)(k-i-1)}{2} + i \cdot (k-i)$$

Performing algebra:

$$SumOfSplits(k) = \frac{i^2 - i + k^2 - 2ki + i^2 - k + i + 2ki - 2i^2}{2}$$

Canceling terms and simplifying:

$$SumOfSplits(k) = \frac{k^2 - k}{2} = \frac{k(k-1)}{2}$$

Therefore, $P(k)$ is true. This completes the proof by strong induction to prove the original claim.

2 Asymptotic Notation

1. **Time Complexity - Theoretical**
On the same computer with the same input, an algorithm having $O(n \log n)$ worst case time complexity runs in less time than **all/some/no** algorithms having $O(n^2)$ worst case time complexity.

> **Solution: Some**.
>
> Suppose that an algorithm A takes $376n \log n = O(n \log n)$ steps, where n is the input length. Suppose that another algorithm B takes $n^2 = O(n^2)$ steps. Then for small n (say, $n = 2$), algorithm B takes fewer steps than algorithm A does. Specifically for $n = 2$, A would take $376 \cdot 2 \cdot 1 = 752$ steps whereas B would take $2^2 = 4$ steps. In this case, the $O(n \log n)$-time algorithm takes more time than the $O(n^2)$-time algorithm.
>
> Now suppose that an algorithm A takes $n \log n = O(n \log n)$ steps, where n is the input length, and suppose that another algorithm B takes $376n^2 = O(n^2)$ steps. Then for *all* $n \geq 1$, algorithm A takes fewer steps than algorithm B does, because $\log n \leq 376n$. Specifically for $n = 2$, A would take $2 \cdot 1 = 2$ steps whereas B would take $376 \cdot 2^2 = 1504$ steps. In this case the $O(n^2)$-time algorithm takes more time than the $O(n \log n)$-time algorithm.

2. **Time Complexity - Applied**
For the following pairs of $f(n)$ and $g(n)$, is $f(n) = O(g(n))$? Justify your answer by applying the definition of big-O or by applying a limit argument.

   (a) $f(n) = 4^n$, $g(n) = 2^n$

   > **Solution:** No.
   >
   > $$\begin{aligned}\lim_{n\to\infty} \frac{g(n)}{f(n)} &= \lim_{n\to\infty} \frac{2^n}{2^n \cdot 2^n} \\ &= \lim_{n\to\infty} \frac{1}{2^n} \\ &= 0.\end{aligned}$$
   >
   > Thus, $g(n) = o(f(n))$, which implies that $f(n) \neq O(g(n))$.

   (b) $f(n) = \log_a n$, $g(n) = \log_b n$ with $a, b > 0$ and $a, b \neq 1$

Solution: Yes. Setting $c = \frac{\ln b}{\ln a}$ and $n_0 = 1$;

$$\begin{aligned} f(n) &= \log_a n \\ &= \frac{\ln n}{\ln a} \\ &= \frac{\ln n}{\ln a} \cdot \frac{\ln b}{\ln b} \\ &= \frac{\ln b}{\ln a} \cdot \frac{\ln n}{\ln b} \\ &= \frac{\ln b}{\ln a} \cdot g(n) \end{aligned}$$

3 Euclidean Algorithm

1. Which pair of numbers takes the greatest number of iterations to find the GCD when using the Euclidean Algorithm?

   ◯ $(800, 300)$
   ◯ $(100, 55)$
   √ $(29, 18)$
   ◯ $(1000, 999)$
   ◯ $(19, 11)$

Solution: $\gcd(29, 18)$ takes the most steps:

$\gcd(800, 300) = \gcd(300, 200) = \gcd(200, 100) = \gcd(100, 0) = 100$
$\gcd(100, 55) = \gcd(55, 45) = \gcd(45, 10) = \gcd(10, 5) = \gcd(5, 0) = 5$
$\gcd(29, 18) = \gcd(18, 11) = \gcd(11, 7) = \gcd(7, 4) = \gcd(4, 3) = \gcd(3, 1) = 1$
$\gcd(1000, 999) = \gcd(999, 1) = 1$
$\gcd(19, 11) = \gcd(11, 8) = \gcd(8, 3) = \gcd(3, 2) = \gcd(2, 1) = 1$