

TCSS 343 - Assignment 1

June 27, 2018

1 2.1 Understand

Prove the theorem below. Use a **direct proof** to find constants that satisfy the definition of $\Theta(n^2)$ or use the **limit test**. Make sure your proof is complete, concise, clear and precise.

Theorem 1. $n^5 - 64n^3 - n^2 \in \Theta(n^5)$

For the first theorem a limit test was used to ensure that polynomial given was $\Theta(n^5)$. For most limits of this nature it is best to factor the polynomial, this usually results in a short elegant solution.

$$\lim_{n \rightarrow \infty} \frac{n^5 - 64n^3 - n^2}{n^5} = \lim_{n \rightarrow \infty} \frac{n^5}{n^5} \left(\frac{1 - \frac{64}{n^2} - \frac{1}{n^3}}{1} \right) = \lim_{n \rightarrow \infty} 1 \left(\frac{1 - 0 - 0}{1} \right) = \lim_{n \rightarrow \infty} 1 = 1$$

Since the limit converged to 1, a positive constant value, we may say that theorem 1 is indeed true.

Prove Gauss's sum using induction on n . Make sure to include a base case for $n = 1$ and an inductive hypothesis and an inductive step for $n > 1$.

Theorem 2. $P(n) : \sum_{i=1}^n i = \frac{n(n+1)}{2} \forall n \in \mathbb{Z}_+$

For this proof I used the fundamental theorem of algebra to help assist me.

I hope that the steps are clear.

1. Base Case:

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

2. Inductive Hypothesis:

$$P(k) : \sum_{i=1}^k i = \frac{k(k+1)}{2} \forall k \in \mathbb{Z}_+$$

3. Inductive Step:

$$\begin{aligned} P(k+1) : \sum_{i=1}^{k+1} i &= \frac{(k+1)(k+2)}{2} \forall k \in \mathbb{Z}_+ \\ \sum_{i=1}^k i + (k+1) &= \frac{(k+1)(k+2)}{2} \\ \frac{k(k+1)}{2} + (k+1) &= \frac{(k+1)(k+2)}{2} \\ \frac{k(k+1)}{2} + \frac{2(k+1)}{2} &= \frac{(k+1)(k+2)}{2} \\ \frac{k(k+1) + 2(k+1)}{2} &= \frac{(k+1)(k+2)}{2} \\ \frac{(k+1)(k+2)}{2} &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

□

Prove Gauss sum using induction on n . Make sure to include a base case for $n = 1$ and an inductive hypothesis and an inductive step for $n > 1$.

Theorem 3. $P(n) : \sum_{i=1}^n i^5 = \left(\frac{n(n+1)}{2}\right)^2 \frac{2n^2+2n-1}{3} \forall n \in \mathbb{Z}_+$

For this proof I used the fundamental theorem of algebra to help assist me.

The last three steps of the inductive step to ensure $P(k+1)$ step I obtained those steps by expanding the right hand side and ensuring that each polynomial on the left hand side matched the right hand side. Those were included on the left hand side in reverse to ensure continuity.

1. Base Case:

$$\begin{aligned} P(1) : \sum_{i=1}^1 i^5 &= \left(\frac{1(1+1)}{2}\right)^2 \frac{2(1)^2 + 2(1) - 1}{3} \\ 1^5 &= \left(\frac{1(2)}{2}\right)^2 \frac{3}{3} \\ 1 &= 1 \end{aligned}$$

2. Inductive Hypothesis:

$$P(k) : \sum_{i=1}^k i^5 = \left(\frac{k(k+1)}{2}\right)^2 \frac{2k^2 + 2k - 1}{3} \forall k \in \mathbb{Z}_+$$

3. Inductive Step:

$$\begin{aligned} P(k+1) : \sum_{i=1}^{k+1} i^5 &= \left(\frac{(k+1)(k+1+1)}{2}\right)^2 \frac{2(k+1)^2 + 2(k+1) - 1}{3} \forall k \in \mathbb{Z}_+ \\ \sum_{i=1}^k i^5 + (k+1)^5 &= \left(\frac{(k+1)(k+2)}{2}\right)^2 \frac{2k^2 + 5k + 2}{3} \\ &= \left(\frac{k(k+1)}{2}\right)^2 \frac{2k^2 + 2k - 1}{3} + (k+1)^5 = \\ &= \left(\frac{1}{12}\right) [k^2(k+1)^2(2k^2 + 2k - 1) + 12(k+1)^5] = \\ &= \left(\frac{1}{12}\right) [(k^4 + 2k^3 + k^2)(2k^2 + 2k - 1) + 12(k+1)^5] = \end{aligned}$$

$$\begin{aligned}
& \left(\frac{1}{12}\right)(2k^6 + 6k^5 + 5k^4 - k^2 + 12k^5 + 60k^4 + 120k^3 + 120k^2 + 60k + 12)) = \\
& \left(\frac{1}{12}\right)(2k^6 + 18k^5 + 65k^4 + 120k^3 + 119k^2 + 60k + 12)) = \\
& \left(\frac{1}{12}\right)(k^4 + 6k^3 + 13k^2 + 12k + 4)(2k^2 + 6k + 3) = \\
& \left(\frac{1}{12}\right)(k^2 + 3k + 2)^2(2k^2 + 6k + 3) = \\
& \left(\frac{(k+1)(k+2)}{2}\right)^2 \frac{2k^2 + 5k + 2}{3} =
\end{aligned}$$

□

Prove by induction that for all natural numbers x and n , $x^n - 1$ is divisible by $x - 1$.

For this proof I decided to show that $(x^n - 1) \bmod x - 1 \equiv 0$ because that statement is equivalent to saying $x^n - 1 \mid x - 1$.

Show $\forall x, n \in \mathbb{Z}_+; P(x, n) : (x^n - 1) \bmod x - 1 \equiv 0$

1. Base Case:

$$P(1, 1) : (1^1 - 1) \bmod 1 - 1 \equiv 0 \quad \bmod 0 \equiv 0$$

This is assuming that we define $a \bmod 0 \equiv 0$ where a may be any integer. This answer depends on how we decide to define the modulus function. This is assuming we define the modulus to be the distance of any two integers from each other. In many modern programming languages and applications this operation is undefined. I see no other way to complete this proof without ignoring this limitation and using the more liberal definition.

2. Inductive Hypothesis:

$$P(a, b) : (a^b - 1) \bmod a - 1 \equiv 0 ; \forall a, b \in \mathbb{Z}_+$$

3. Inductive Step:

For this proof I made heavy use of the binomial theorem, specifically

the power expansion on $(1+x)^n$.

$$\begin{aligned}
P(a+1, b+1) : ((a+1)^{b+1} - 1) \bmod (a+1-1) &\equiv 0 ; \forall a, b \in \mathbb{Z}_+ \\
((a+1)(a+1)^b - 1) \bmod a &\equiv 0 \\
((a+1) \sum_{i=0}^b \binom{b}{i} a^i - 1) \bmod a &\equiv 0 \\
(\sum_{i=0}^b \binom{b}{i} a^{i+1} + \sum_{i=0}^b \binom{b}{i} a^i - 1) \bmod a &\equiv 0 \\
(\sum_{i=0}^b \binom{b}{i} a^{i+1} + \sum_{i=1}^{b-1} \binom{b}{i} a^i + \binom{b}{b} (a^b + 1) - 1) \bmod a &\equiv 0 \\
(\sum_{i=0}^b \binom{b}{i} a^{i+1} + \sum_{i=1}^{b-1} \binom{b}{i} a^i + (1)(a^b + 1 - 1) \bmod a &\equiv 0 \\
(\sum_{i=0}^b \binom{b}{i} a^{i+1} + \sum_{i=1}^{b-1} \binom{b}{i} a^i + a^b) \bmod a &\equiv 0 \\
((\sum_{i=0}^b \binom{b}{i} a^{i+1}) \bmod a + (\sum_{i=1}^{b-1} \binom{b}{i} a^i) \bmod a + (a^b) \bmod a) \bmod a &\equiv 0 \\
(0 + 0 + 0) \bmod a &\equiv 0 \\
0 \bmod a &\equiv 0 \\
0 &\equiv 0 \\
&\square
\end{aligned}$$

Prove by induction that $x^n - y^n$ is divisible by $x - y$ for all natural numbers x, y (with $x \neq y$), and n .

Show $\forall x, y, n \in \mathbb{Z}_+; P(x, y, n) : (x^n - y^n) \bmod x - y \equiv 0$

1. Base Case:

$$P(1, 1, 1) : (1^1 - 1^1) \bmod 1 - 1 \equiv 0 \quad \bmod 0 \equiv 0$$

This is assuming that we define $a \bmod 0 \equiv 0$ where a may be any integer. This answer depends on how we decide to define the modulus

function. This is assuming we define the modulus to be the distance of any two integers from each other. In many modern programming languages and applications this operation is undefined. I see no other way to complete this proof without ignoring this limitation and using the more liberal definition.

2. Inductive Hypothesis:

$$P(a, b, c) : (a^c - b^c) \bmod a - b \equiv 0 ; \forall a, b, c \in \mathbb{Z}_+$$

3. Inductive Step:

$$\begin{aligned}
P(a+1, b+1, c+1) : ((a+1)^{c+1} - (b+1)^{c+1}) \bmod ((a+1) - (b+1)) &\equiv 0; \\
&\forall a, b, c \in \mathbb{Z}_+ \\
((a+1)^{c+1} - (b+1)^{c+1}) \bmod ((a+1) - (b+1)) &\equiv 0 \\
((a+1)(a+1)^c - (b+1)(b+1)^c) \bmod (a-b) &\equiv 0 \\
((a+1) \sum_{i=0}^c \binom{c}{i} (a^i - 1) - (b+1) \sum_{j=0}^c \binom{c}{j} (b^j - 1)) \bmod (a-b) &\equiv 0 \\
(\sum_{i=0}^c \binom{c}{i} a^{i+1} - \sum_{j=0}^c \binom{c}{j} b^{j+1} + \sum_{i=0}^c \binom{c}{i} a^i - \sum_{j=0}^c \binom{c}{j} b^j) \bmod (a-b) &\equiv 0 \\
(\sum_{i=0}^c \binom{c}{i} a^{i+1} - \sum_{j=0}^c \binom{c}{j} b^{j+1} + \sum_{i=1}^c \binom{c}{i} a^i - \sum_{j=1}^c \binom{c}{j} b^j + c - c) \bmod (a-b) &\equiv 0 \\
((\sum_{i=0}^c \binom{c}{i} a^{i+1} - \sum_{j=0}^c \binom{c}{j} b^{j+1}) \bmod (a-b) + & \\
(\sum_{i=1}^c \binom{c}{i} a^i - \sum_{j=1}^c \binom{c}{j} b^j) \bmod (a-b)) \bmod (a-b) &\equiv 0 \\
(((\sum_{i=1}^c \binom{c}{i} a^{i+1} - \sum_{j=1}^c \binom{c}{j} b^{j+1}) + (1-1) \bmod (a-b) + & \\
((\sum_{i=1}^c \binom{c}{i} a^i - \sum_{j=1}^c \binom{c}{j} b^j)) \bmod (a-b)) \bmod (a-b) &\equiv 0
\end{aligned}$$

$$(0 + 0) \equiv 0$$

$$0 \equiv 0$$

□

Some explanation is needed to explain how the summations on the last page are divisible by $a - b$. Due to the binomial theorem, any series of the nature $(a - b) + (a^2 - b^2) + (a^3 - b^3) + \dots$ has within it an $(a - b)$. So if the first term 1 is allowed to elapse from each term we can then say the summations are divisible.

Prove the following theorem using the definition of $\Omega(f(n))$ and $O(f(n))$, or else the limit test.

Theorem 4. Let $d \geq 2$ be an integer. Then $\sqrt[d]{n} \epsilon \Omega(\sqrt[2d]{n})$ and $(\ln n^d) \epsilon O(\sqrt{n})$

$$\lim_{n \rightarrow \infty} \frac{n^{\frac{1}{d}}}{n^{\frac{1}{2d}}} = \lim_{n \rightarrow \infty} n^{\frac{1}{d}} n^{\frac{-1}{2d}} \quad (1)$$

$$= \lim_{n \rightarrow \infty} n^{\frac{1}{d} - \frac{1}{2d}} \quad (2)$$

$$= \lim_{n \rightarrow \infty} n^{\frac{1}{2d}} \rightarrow \infty \quad (3)$$

Use the fact that for any $n \geq 1$ by the Cauchy-Sqwarz inequality

$$\ln n = \int_1^n \frac{dx}{x} \leq \sqrt{\int_1^n dx \int_1^n \frac{dx}{x^2}} = \sqrt{(n-1)(1-\frac{1}{n})} = \sqrt{n + \frac{1}{n} - 2}$$

Producing a desired result of:

$$\ln n \leq \sqrt{n + \frac{1}{n} - 2}$$

Using the result of prior limit test and immediate results above (since $d \geq 2$), we may say that:

$$\ln n < \sqrt[2d]{n} < \sqrt{n + \frac{1}{n} - 2} < \sqrt{n}$$

Thus:

$$\lim_{n \rightarrow \infty} \frac{(\ln n)^d}{\sqrt{n}} \rightarrow 0$$

2 2.1 Understand

Place these functions in order from slowest asymptotic growth to fastest asymptotic growth. You will want to simplify them algebraically before comparing them. Give a short justification (a proof is not necessary) of how you came to this ordering.

According to Donald Knuth, in Concrete Mathematics page 426 and 427, hierarchy and asymptotics of functions was introduced by Paul du Bois-Reymond in 1871 with the following definition:

$$f(n) < g(n) \iff \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$$

Knuth continues on to give a what he calls, "asymptotic pecking order" (where $0 < \epsilon < 1 < c$) which I used to solve this problem:

$$1 < \log \log n < \log n < n^\epsilon < n^c < n^{\log n} < c^n < n^n < c^{c^n}$$

Using this pecking order, I made educated guesses as to which functions grew slower than others, then used Mathematica to check these guesses.

1. $f_7(n) = \log \log n - 1$
The above function is clearly smaller than the function below it. Applying a logarithm to another logarithm significantly slows down the asymptotic growth.
2. $f_6(n) = \log n - 1$
The above function is clearly smaller than the function below it once a simplification is applied to the below function. n dominates any logarithm.
3. $f_5(n) = \log n^n = n \log n$
The degree of the polynomial above is smaller than that below.

4. $f_3(n) = 4^{\log n} = n^2$

The degree of the polynomial above is smaller than that below.

5. $f_2(n) = (\frac{n}{\log n})^3 = n^3(\frac{1}{\log n})^3$

The degree of the polynomial above is same as that below but the function above has a division of logarithm which slows it down.

6. $f_0(n) = n^3 + n^2 + n + 1$

No simplification of the function below that I know of can be applied but by looking at Knuth's pecking order I can see that any function of the form c^n will be greater than n^c .

7. $f_8(n) = 100^{\sqrt{n}}$

By consulting concrete mathematics, when you have two different exponentials you need to compare the powers of the function inside the power. Since $\sqrt{n} < n$ the function above grows slower than that below.

8. $f_4(n) = 9^{\frac{n}{2}} = 3^n$

Since $n < 2n$ the function above grows slower than that below.

9. $f_1(n) = 3^{2n}$

Since all other cases have been exhausted this function above should grow the fastest.

With use of mathematica and the definition Knuth provided ($f(n) < g(n) \iff \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$), I obtained the following results, where the row corresponds the $f_i(n)$ and the column corresponds to $g_j(n)$:

$$\begin{bmatrix} 1 & 0 & \infty & \infty & 0 & \infty & \infty & \infty & 0 \\ \infty & 1 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\ 0 & 0 & 1 & \infty & 0 & \infty & \infty & \infty & 0 \\ 0 & 0 & 0 & 1 & 0 & \infty & \infty & \infty & 0 \\ \infty & 0 & \infty & \infty & 1 & \infty & \infty & \infty & \infty \\ 0 & 0 & 0 & 0 & 0 & 1 & \infty & \infty & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \infty & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \infty & 0 & \infty & \infty & 0 & \infty & \infty & \infty & 1 \end{bmatrix}$$

The rows with the most zeros or likewise the column with the most infinities in them should match to the ordering of what I obtained, which we see that it does. In the workplace and in the future I will make heavy use of technology to reduce errors and introduce best practices, so I felt like it was important to show this step.