CSC165 - Problem Set 3

Junaid Arshad, Sadeed Ahmed, & Frederick Meneses

March 18, 2022

1 Number Representation

(a) Let $(b_{k-1} \dots b_0)_2$ be a binary representation of a natural number, and a be a single bit. The following is a proof that $(b_{k-1} \dots b_0 a)_2 = 2(b_{k-1} \dots b_0)_2 + a$:

Proof. Want to prove: $(b_{k-1} \dots b_0 a)_2 = 2(b_{k-1} \dots b_0)_2 + a$. Let $(b_{k-1} \dots b_0)_2 = \sum_{i=0}^{k-1} b_i 2^i$. We will show the RHS = LHS. Let $k' = k + 1$ and $b'_0 = a$ and $\forall i \in \{1, 2, \dots, k\}$, $b'_i = b_{i-1}$

$$\begin{aligned}
2(b_{k-1} \dots b_0)_2 + a &= \sum_{i=0}^{k-1} b_i 2^{i+1} + a \\
&= \sum_{i=1}^{k} b_{i-1} 2^i + a \\
&= \sum_{i=1}^{k'-1} b'_i 2^i + a2^0 && (2^0 = 1) \\
&= \sum_{i=1}^{k'-1} b'_i 2^i + b'_0 2^0 && (b'_0 = a) \\
&= \sum_{i=0}^{k'-1} b'_i 2^i \\
&= (b'_{k'-1} \dots b'_0)_2 \\
&= (b'_k \dots b'_1 b'_0)_2 = (b_{k-1} \dots b_0 a)_2
\end{aligned}$$

□

(b) Let $n \in \mathbb{N}$ and let $(b_{2n-1} \dots b_0)_2$ be the binary representation of a natural number. The following is a proof by induction that $(b_{2n-1} \dots b_0)_2 - (b_1 b_0)_2 - (b_3 b_2)_2 - \cdots - (b_{2n-1} b_{2n-2})_2$ is a multiple of 3:

Proof. Let $n \in \mathbb{N}$ and $(b_{2n-1} b_{2n-2} \dots b_0)_2 = \sum_{i=0}^{2n-1} b_i 2^i$ be the binary representation of n. Let

$$P(n) : \exists k \in \mathbb{Z}, (b_{2n-1} b_{2n-2} \dots b_0)_2 - (b_1 b_0)_2 - (b_3 b_2)_2 - \dots - (b_{2n-1} b_{2n-2})_2 = 3k$$

Base Case. (n = 0) In this case, the binary representation of n is

$$\sum_{i=0}^{-1} b_i 2^i = 0 = ()_2$$

We want to show, $P(0) : \exists k_0 \in \mathbb{Z}, ()_2 - ()_2 - \ldots - ()_2 = 3k_0$
Let $k_0 = 0$

$$()_2 - ()_2 - \ldots - ()_2 = 0 = 3(0) = 3k_0$$

Inductive Step. WTS: $\forall m \in \mathbb{N}, P(m) \Rightarrow P(m+1)$
Inductive Hypothesis: Assume

$$P(m) : \exists d \in \mathbb{Z}, (b_{2m-1}b_{2m-2}\ldots b_0)_2 - (b_1b_0)_2 - (b_3b_2)_2 - \ldots - (b_{2m-1}b_{2m-2})_2 = 3d$$

Explicitly, we want to show:

$$P(m+1) : \exists d_2 \in \mathbb{Z}, (b_{2m+1}b_{2m}\ldots b_0)_2 - (b_1b_0)_2 - (b_3b_2)_2 - \ldots - (b_{2m-1}b_{2m-2})_2 - (b_{2m+1}b_{2m})_2 = 3d_2$$

We also know from the given hint that

$$\forall m \in \mathbb{N}, \exists y \in \mathbb{Z}, 4^m - 1 = 3y$$

Let $d_2 = 2y \cdot b_{2m+1} + y \cdot b_{2m} + d$
We will show that the LHS = RHS.

$$\begin{aligned}
&= (b_{2m+1}b_{2m}\ldots b_0)_2 - (b_1b_0)_2 - (b_3b_2)_2 - \ldots - (b_{2m-1}b_{2m-2})_2 - (b_{2m+1}b_{2m})_2 \\
&= \sum_{i=0}^{2m+1} b_i 2^i - (b_1b_0)_2 - (b_3b_2)_2 - \ldots - (b_{2m-1}b_{2m-2})_2 - (b_{2m+1}b_{2m})_2 \\
&= \sum_{i=0}^{2m-1} b_i 2^i + \sum_{i=2m}^{2m+1} b_i 2^i - (b_1b_0)_2 - (b_3b_2)_2 - \ldots - (b_{2m-1}b_{2m-2})_2 - (b_{2m+1}b_{2m})_2 \\
&= \left(\sum_{i=0}^{2m-1} b_i 2^i - (b_1b_0)_2 - \ldots - (b_{2m-1}b_{2m-2})_2\right) + \left(\sum_{i=2m}^{2m+1} b_i 2^i - (b_{2m+1}b_{2m})_2\right) \\
&= \big((b_{2m-1}b_{2m-2}\ldots b_0)_2 - (b_1b_0)_2 - \ldots - (b_{2m-1}b_{2m-2})_2\big) + \big(b_{2m+1}2^{2m+1} + b_{2m}2^{2m} - b_{2m+1}2^1 - b_{2m}2^0\big) \\
&= 3d + \big(b_{2m+1}2^{2m+1} - b_{2m+1}2\big) + \big(b_{2m}2^{2m} - b_{2m}2^0\big) && \text{(by Inductive Hypothesis)} \\
&= 3d + 2b_{2m+1}(4^m - 1) + b_{2m}(4^m - 1) \\
&= 3d + 2b_{2m+1}(3y) + b_{2m}(3y) && \text{(using the given hint)} \\
&= 3(d + 2y \cdot b_{2m+1} + y \cdot b_{2m}) && \text{(Factoring out 3)} \\
&= 3d_2
\end{aligned}$$

$\square$

(c) Let x be a natural number with a binary representation where the difference between the number of 1 bits with an even index and the number of 1 bits with an odd index is a multiple of 3. The following is a proof that x is a multiple of 3:

Proof. Let $x \in \mathbb{N}$. The binary representation of x can have an even *or* odd number of bits. If x has an even number of bits, then its binary representation is of the form $(b_{2n-1} \dots b_0)_2$. If x has an odd number of bits, then we can add a leading zero, in which case its binary representation is also $(0b_{2n-2} \dots b_0)_2$, which can be similarly be re-written as $(b_{2n-1} \dots b_0)_2$.

Given that the binary representation of x is $(b_{2n-1} \dots b_0)$, assume that the difference between the number of 1 bits with an even index and the number of 1 bits with an odd index is a multiple of 3, i.e.:

$$3 \mid \left(\sum_{i=0}^{n-1} b_{2i} - \sum_{i=0}^{n-1} b_{2i+1} \right),$$

or that:

$$\exists d_1 \in \mathbb{Z},\ \sum_{i=0}^{n-1} b_{2i} - \sum_{i=0}^{n-1} b_{2i+1} = 3d_1.$$

From **Part B**, we know that:

$$\exists d_3 \in \mathbb{Z}, (b_{2n-1} \dots b_0)_2 - (b_1 b_0)_2 - (b_3 b_2)_2 - \dots (b_{2n-1} b_{2n-2})_2 = 3d_3$$

Want to prove: $(b_{2n-1} \dots b_0)_2$ is divisible by 3, or that, $3 \mid \sum_{i=0}^{2n-1} b_i 2^i$, i.e.:

$$\exists d_2 \in \mathbb{Z}, \sum_{i=0}^{2n-1} b_i 2^i = 3d_2$$

Let $d_2 = d_1 + d_3 + \sum_{i=0}^{n-1} b_{2i+1}$.

Using our result from **Part B**:

$$\begin{gathered}
(b_{2n-1} \dots b_0)_2 - (b_1 b_0)_2 - (b_3 b_2)_2 - \dots (b_{2n-1} b_{2n-2})_2 = 3d_3 \\
(b_{2n-1} \dots b_0)_2 - (b_1 \cdot 2^1 + b_0 \cdot 2^0) - (b_3 \cdot 2^1 + b_2 \cdot 2^0) - \dots - (b_{2n-1} \cdot 2^1 + b_{2n-2} \cdot 2^0) = 3d_3 \\
(b_{2n-1} \dots b_0)_2 - (b_1 \cdot 2 + b_3 \cdot 2 + \dots + b_{2n-1} \cdot 2) - (b_0 \cdot 1 + b_2 \cdot 1 + \dots + b_{2n-2} \cdot 1) = 3d_3 \\
(b_{2n-1} \dots b_0)_2 - 2(b_1 + b_3 + \dots + b_{2n-1}) - (b_0 + b_2 + \dots b_{2n-2}) = 3d_3 \\
(b_{2n-1} \dots b_0)_2 + 2\sum_{i=0}^{n-1} b_{2i+1} + \sum_{i=0}^{n-1} b_{2i} = 3d_3 \\
\sum_{i=0}^{2n-1} b_i 2^i = 3d_3 + 2\sum_{i=0}^{n-1} b_{2i+1} + \sum_{i=0}^{n-1} b_{2i}
\end{gathered}$$

From our assumption, we know that:

$$\sum_{i=0}^{n-1} b_{2i} - \sum_{i=0}^{n-1} b_{2i+1} = 3d_1 \Leftrightarrow \sum_{i=0}^{n-1} b_{2i} = 3d_1 + \sum_{i=0}^{n-1} b_{2i+1}$$

Plugging this value into our expression above:

$$\begin{aligned}\sum_{i=0}^{2n-1} b_i 2^i &= 3d_3 + 2\sum_{i=0}^{n-1} b_{2i+1} + 3d_1 + \sum_{i=0}^{n-1} b_{2i+1} \\ &= 3d_3 + 3d_1 + 3\sum_{i=0}^{n-1} b_{2i+1} \\ &= 3\left(d_3 + d_1 + \sum_{i=0}^{n-1} b_{2i+1}\right) \\ &= 3d_2\end{aligned}$$

Thus, we have proven that $(b_{2n-1} \ldots b_0)_2$ *is divisible by 3, or that,* $3 \mid \sum_{i=0}^{2n-1} b_i 2^i$ *when the difference between the number of 1 bits with an even index and the number of 1 bits with an odd index is a multiple of 3.* □

2 Induction

For $m, n \in \mathbb{Z}^+$, define $P(m, n)$ to be:

$$\text{the number of ways to write } n = x_1 + \cdots + x_m \text{ with } x_1, \ldots x_m \in \mathbb{N} \text{ is } \frac{(n+m-1)!}{n!(m-1)!}.$$

(a) We will prove the following statements:

i $\forall n \in \mathbb{Z}^+, P(1, n)$

Proof. Let $n \in \mathbb{Z}^+$. **WTS:** $P(1, n)$: The number of ways to write $n = x_1 + \ldots + x_m$ with $x_1, \ldots x_m \in \mathbb{N}$ when $m = 1$ is 1
Let $m = 1, n = n$. In this case, $x_m = x_1 = n$. Thus, we can see that the number of ways to write n is 1. We can also confirm this using the formula:

$$\frac{(n+1-1)!}{n!(1-1)!} = \frac{n!}{n!} = 1$$

□

ii $\forall m \in \mathbb{Z}^+, P(m, 1)$

Proof. Let $m \in \mathbb{Z}^+$. **WTS:** $P(m, 1)$: The number of ways to write $1 = x_1 + \cdots + x_m$ with $x_1, \ldots, x_m \in \mathbb{N}$ is m
Since $n = 1$ here, one of $x_1, \ldots, x_m \in \mathbb{N}$ must be 1 whereas every other digit must $= 0$, thus there are m ways to represent 1 this way since any one of the m digits can take on the value 1 and all others must be $= 0$. Conversely, if one of the m digits is 1 and all the others are 0, they must add up to $n = 1$. We can also show this using the given formula,

$$\frac{(1+m-1)!}{1!(m-1)!} = \frac{m!}{(m-1)!} = m$$

□

iii $\forall m, n \in \mathbb{Z}^+, P(m+1, n) \wedge P(m, n+1) \Rightarrow P(m+1, n+1)$

Proof. Assume $P(m+1, n)$: The number of ways to write $n = x_1 + x_2 + \cdots + x_{m+1}$ with $x_1, \ldots x_{m+1} \in \mathbb{N}$ using $m + 1$ terms is

$$\frac{(n+m)!}{n!m!}$$

and assume $P(m, n+1)$: The number of ways to write $n + 1 = x_1 + x_2 + \cdots + x_m$ with $x_1, \ldots x_m \in \mathbb{N}$ with m terms is

$$\frac{(n+m)!}{(n+1)!(m-1)!}$$

We want to show:

$$P(m+1, n+1) : \text{the number of ways to write } n + 1 = x_1 + x_2 + \cdots + x_{m+1}$$

$$\text{for some } x_1, x_2, \ldots, x_{m+1} \in \mathbb{N} \text{ is } = \frac{(n+1+m)!}{(n+1)!m!}$$

Since x_1 is a natural number, we know $x_1 \geq 0 \leftrightarrow x_1 = 0 \vee x_1 \geq 1$. Using this we can split up our domain of x_1 into two independent parts.

When $x_1 = 0$:
Starting with the LHS of **WTS:**
$n + 1 = x_1 + x_2 + \cdots + x_{m+1}$
Define x'_i such that $x'_i = x_{i+1}$ for $1 \leq i \leq m$.

$$n + 1 = 0 + x_2 + \cdots + x_{m+1} = x'_1 + x'_2 + \cdots + x'_m$$

Since there are m terms in this equation, by our assumption that $P(m, n+1)$ is True the number of ways to write $n + 1$ with m terms is

$$\frac{(n+m)!}{(n+1)!(m-1)!}$$

When $x_1 \geq 1$:
In this situation, we consider what we want to prove:

$$\begin{aligned}
n + 1 &= x_1 + x_2 + \cdots + x_{m+1} \\
n &= x_1 - 1 + x_2 + \cdots + x_{m+1} && \text{(subtracting 1 from both sides)} \\
n &= (x_1 - 1) + x_2 + \cdots + x_{m+1}
\end{aligned}$$

We know: $x_1 \geq 1 \leftrightarrow x_1 - 1 \geq 0 \; (\in \mathbb{N})$
We then define $x''_1 = x_1 - 1$ and x''_i such that $x''_i = x_i$ for $2 \leq i \leq m + 1$. Then, we have the equation

$$n = x'_1 + x'_2 + \cdots + x'_{m+1}$$

Since there are $m+1$ terms in this equation, by our assumption that $P(m+1, n)$ is True, the number of ways to write n using $m + 1$ terms is:

$$\frac{(n+m)!}{n!m!}$$

Therefore, the total number of solutions we have for the equation $n+1 = x_1+x_2+\cdots+x_{m+1}$ when $x_1 \geq 0$ will be the sum of the solutions to the same equation when $x_1 = 0$ and when $x_1 \geq 1$

$$\begin{aligned}
P(m, n+1) + P(m+1, n) &= \frac{(n+m)!}{(n+1)!(m-1)!} + \frac{(n+m)!}{n!m!} \\
&= \frac{(n+1)(n+m)! + m(n+m)!}{(n+1)n!m(m-1)!} \\
&= \frac{(n+1+m)(n+m)!}{(n+1)!m!} \\
&= \frac{(n+1+m)!}{(n+1)!m!} \\
&= P(m+1, n+1)
\end{aligned}$$

Which is exactly what we wanted to show. $\square$

(b) We will use the results from part (a) to prove $P(2,2) \wedge P(3,3)$.

Proof. From part a we know that $\forall n \in Z^+, P(1,n)$ and $\forall n \in \mathbb{Z}^+, P(m,1)$ are True. Using these two facts, we know that the following are true:

- $P(1,2)$
- $P(1,3)$
- $P(2,1)$

From iii) we know that $\forall m,n \in \mathbb{Z}^+, P(m+1,n) \wedge P(m,n+1) \Rightarrow P(m+1,n+1)$. Using this and the true statements from above we can conclude the following:

$$P(1,2) \wedge P(2,1) \Rightarrow P(2,2)$$
$$P(3,1) \wedge P(2,2) \Rightarrow P(3,2)$$
$$P(2,2) \wedge P(1,3) \Rightarrow P(2,3)$$
$$P(3,2) \wedge P(2,3) \Rightarrow P(3,3)$$

Thus, $P(3,3)$ is also True. This completes the proof. □

(c) For $t \in \mathbb{Z}^+$ with $t \geq 2$, define $Q(t)$ to be: $\forall m,n \in \mathbb{Z}^+, m+n=t \Rightarrow P(m,n)$. We will prove the following by induction: $\forall t \in \mathbb{Z}^+, t \geq 2 \Rightarrow Q(t)$.

Proof. **Base Case.** (t = 2)
The only possible values that m and n can have in this case are $m=1$ and $n=1$. We know that $P(1,1)$ is `True` using our results from **(1.a.i)**

Inductive Step. Let $t_1 \in \mathbb{N}$. Assume $t_1 \geq 2$ and also assume $Q(t_1)$: $\forall m_1, n_1 \in \mathbb{Z}^+, m_1+n_1 = t_1 \Rightarrow P(m_1,n_1)$
WTS: $Q(t_1+1)$: $\forall m_2, n_2 \in \mathbb{Z}^+, m_2+n_2 = t_1+1 \Rightarrow P(m_2,n_2)$

- Let $m_2, n_2 \in \mathbb{Z}^+$
- Assume $m_2+n_2 = t_1 \leftrightarrow m_2+n_2-1 = t_1$.
- Since by our assumption, $t_1 \geq 2$, the values that m_2 and n_2 can take on can be split up into 3 cases

  Case 1. $m_2 = 1 (\in \mathbb{Z}^+)$
  Since this is the smallest value that m_2 can have, in this case for the expression m_2+n_2-1 to be equal to t_1, it must stand that $n_2 \geq 2$.
  Since $m_2 = 1$ and $n_2 \in \mathbb{Z}^+$, we know from **(2.a.i)** that $P(m_2,n_2) = P(1,n_2)$ is `True`.

  Case 2. $n_2 = 1 (\in \mathbb{Z}^+)$
  Since this is the smallest value that n_2 can have, in this case for the expression m_2+n_2-1 to be equal to t_1, it must stand that $m_2 \geq 2$. Thus, we have that $n_2 = 1$ and $m_2 \geq 2$ in this case.
  Since $n_2 = 1$ and $m_2 \in \mathbb{Z}^+$, we know from **(2.a.ii)** that $P(m_2,n_2) = P(m_2,1)$ is `True`.

Case 3. $n_2 > 1 \wedge m_2 > 1$ In this case, the following statements are `True` using the induction hypothesis:

$$
\begin{aligned}
m_2 + (n_2 - 1) = t_1 &\Rightarrow P(m_1, n_1 - 1) && (m_2, (n_2 - 1) \in \mathbb{Z}^+) \\
(m_2 - 1) + n_2 = t_1 &\Rightarrow P(m_2, n_2 - 1) && ((m_2 - 1), n_2 \in \mathbb{Z}^+)
\end{aligned}
$$

Since both of these expressions are `True` in this case, by **(2.a.iii)**, we can conclude that:

$$P(m_2 - 1, n_2) \wedge P(m_2, n_2 - 1) \Rightarrow P(m_2, n_2)$$

□

(d) We will use the results from previous parts to prove $\forall m, n \in \mathbb{Z}^+, P(m, n)$.

Proof. Let $m, n \in \mathbb{Z}^+$. We know that $m + n \geq 2$, and from **(2.c)**, we know that this implies $Q(m + n)$, i.e.:

$$\forall m', n' \in \mathbb{Z}^+, m' + n' = m + n \Rightarrow P(m', n')$$

Consider the instance when $m' = n \wedge n' = n$. In this case, $P(m', n') = P(m, n)$, which is what we wanted to prove. □

3 Asymptotic Notation

The following facts may be referenced in this section:

$$\forall n \in \mathbb{Z}, n \leq 2^n \tag{Fact 1}$$

$$\forall x, y \in \mathbb{R}^+, x \leq y \Leftrightarrow log_2(x) \leq log_2(y) \tag{Fact 2}$$

$$\forall x, y \in \mathbb{R}, x \leq y \Leftrightarrow 2^x \leq 2^y \tag{Fact 3}$$

(a) We will **prove** that $log_2(k+n) \in \mathcal{O}(log_2 n)$, or that:

$$\exists c, n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow \log_2(k+n) \leq c \cdot \log_2(n)$$

Proof. Let k be an arbitrary $\mathbb{R}^+$. Let $c = 2$, where $c \in \mathbb{R}^+$. Let $n_0 = \left\lceil \frac{1+\sqrt{1+4k}}{2} \right\rceil$, where $n_0 \in \mathbb{R}^+$.

Assume that $n \geq n_0 \Leftrightarrow n \geq \left\lceil \frac{1+\sqrt{1+4k}}{2} \right\rceil$

Want to prove: $\log_2(k+n) \leq \log_2(n^2)$.

Since $k > 0$,

$$k > 0$$

$$1 + 4k > 1$$

$$\sqrt{1+4k} > 1$$

$$1 - \sqrt{1+4k} < 0$$

$$\frac{1-\sqrt{1+4k}}{2} < 0 \tag{4}$$

We also know that:

$$\frac{1+\sqrt{1+4k}}{2} > \frac{1-\sqrt{1+4k}}{2}$$

Using our assumption and **(4)**, we can conclude following:

$$n - \left(\frac{1+\sqrt{1+4k}}{2}\right) > 0$$

$$n - \left(\frac{1-\sqrt{1+4k}}{2}\right) > 0$$

Moreover, since the aforementioned terms are greater than 0, we can perform the following arithmetic:

$$\left(n - \left(\frac{1+\sqrt{1+4k}}{2}\right)\right) \cdot \left(n - \left(\frac{1-\sqrt{1+4k}}{2}\right)\right) \geq 0$$

$$n^2 - n \cdot \left(\frac{1-\sqrt{1+4k}}{2}\right) - n \cdot \left(\frac{1+\sqrt{1+4k}}{2}\right) + \left(\frac{1+\sqrt{1+4k}}{2}\right) \cdot \left(\frac{1-\sqrt{1+4k}}{2}\right) \geq 0$$

$$n^2 + \frac{-n + n\cdot\sqrt{1+4k} - n - n\cdot\sqrt{1+4k}}{2} + \frac{1^2 - (\sqrt{1+4k})^2}{4} \geq 0$$

$$n^2 - \frac{2n}{2} + \frac{1-1-4k}{4} \geq 0$$

$$n^2 - n - k \geq 0$$

$$n^2 - n - k \geq 0$$

$$n^2 \geq n + k$$

Using **Fact (2)**, we can also conclude that:

$$\begin{aligned} n^2 \geq n + k &\Leftrightarrow \log_2(n+k) \leq \log_2(n^2) \\ &\Leftrightarrow \log_2(n+k) \leq 2 \cdot \log_2(n) \\ &\Leftrightarrow \log_2(n+k) \leq c \cdot \log_2(n) \end{aligned}$$

Thus, we have proven that: $\log_2(k+n) \leq \log_2(n^2)$. □

(b) We will **disprove** that $n \in \Omega(n^{1+\epsilon})$, or that:

$$\forall c, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, n \geq n_0 \land n < c \cdot n^{1+\epsilon}$$

Proof. Let $\epsilon, c, n_0 \in \mathbb{R}^+$. Let $n = \left\lceil \frac{1}{c^{\frac{1}{\epsilon}}} + n_0 + 1 \right\rceil \in \mathbb{N}$.

Want to prove: $n \geq n_0$ and that $c < c \cdot n^{1+\epsilon}$.

<u>**Part 1:**</u> We will prove that $n \geq n_0$.

Since our choice of n depends on $\frac{1}{c^{\frac{1}{\epsilon}}}$, we will show that $\frac{1}{c^{\frac{1}{\epsilon}}} > 0$:

$$\epsilon > 0$$

$$\frac{1}{\epsilon} > 0$$

$$c^{\frac{1}{\epsilon}} > 1$$

$$0 < \frac{1}{c^{\frac{1}{\epsilon}}} < 1$$

Thus, since n *is the ceiling of the sum of positive real numbers (including* n_0*), we can conclude that* $n \geq n_0$.

Part 2: We will prove that $n < c \cdot n^{1+\epsilon}$.

Before continuing with the proof, we will prove that $\frac{c}{n^\epsilon}$ is a positive real number. Since ϵ is a positive real number, we can perform the following arithmetic operations:

$$\begin{aligned} \epsilon &> 0 \\ n^\epsilon &> 1 \\ 0 < \frac{1}{n^\epsilon} &< 1 \end{aligned} \qquad \textbf{(6)}$$

Moreover, since c is a positive real number and **(6)** is True, we can conclude that $\frac{c}{n^\epsilon} > 0$.

By our choice of n, and from our conclusion in **part 1** that n consists of positive terms $\Big($including $\frac{1}{c^{\frac{1}{\epsilon}}}\Big)$, we can perform the following arithmetic operations:

$$\begin{aligned} n &> \frac{1}{c^{\frac{1}{\epsilon}}} \\ n^\epsilon &> \frac{1}{c} && \text{(raise inequality to the power of } \epsilon) \\ c &> \frac{1}{n^\epsilon} && \text{(multiply by } \tfrac{c}{n^\epsilon} > 0) \\ c &> n^{-\epsilon} \\ c &> n^{1-1-\epsilon} \\ c &> n^{1-(1+\epsilon)} \\ c &> \frac{n}{n^{1+\epsilon}} \\ c \cdot n^{1+\epsilon} &> n && \text{(since } n^{1+\epsilon} > 0) \end{aligned}$$

Thus, we have proven that $n \geq n_0$ and that $n < c \cdot n^{1+\epsilon}$. $\square$

4 More Asymptotic Notations

(a) We will **prove** that if $f + g \in \mathcal{O}(h)$, then $f \in \mathcal{O}(h)$ and $g \in \mathcal{O}(h)$.

Proof. Let $f, g, h : \mathbb{N} \to \mathbb{R}^{\geq 0}$. Assume that $f + g \in \mathcal{O}(h)$, or that:

$$\exists c_0, n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow (f + g)(n) \leq c \cdot h(n)$$

We know that the definition of the sum of f and g is:

$$\forall n \in \mathbb{N}, (f + g)(n) = f(n) + g(n)$$

Want to prove:

$\boldsymbol{f \in \mathcal{O}(h)}$**:** $\exists c_1, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_1 \Rightarrow f(n) \leq c_1 \cdot h(n)$

and

$\boldsymbol{g \in \mathcal{O}(h)}$**:** $\exists c_2, n_2 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_2 \Rightarrow g(n) \leq c_2 \cdot h(n)$

Proof that $\boldsymbol{f \in \mathcal{O}(h)}$, i.e., $\exists c_1, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, f(n) \leq c_1 \cdot h(n)$.

From our assumption, we know that $f(n) + g(n) \leq c_0 \cdot h(n)$.

Let $c_1 = c_0$. Let $n_1 = n_0$. Let $n \in \mathbb{N}$.

Since $n \geq n_1 = n_0$, using our assumption we know that $f(n) + g(n) \leq c_0 \cdot h(n)$.

Since $g(n) \in \mathbb{R}^{\geq 0}$ (by the definition of the function), we know that if we subtract $g(n)$ from the left side, it would become even smaller and the inequality would still hold, i.e.:

$$\begin{aligned} f(n) + g(n) &\leq c_0 \cdot h(n) \\ f(n) &\leq c_0 \cdot h(n) && \text{(subtract } g(n) \text{ from the left side)} \\ f(n) &\leq c_1 \cdot h(n) && \text{(since } c_1 = c_0\text{)} \end{aligned}$$

Proof that $\boldsymbol{g \in \mathcal{O}(h)}$, i.e., $\exists c_2, n_2 \in \mathbb{R}^+, \forall n \in \mathbb{N}, g(n) \leq c_2 \cdot h(n)$.

From our assumption, we know that $f(n) + g(n) \leq c_0 \cdot h(n)$.

Let $c_2 = c_0$. Let $n_2 = n_0$. Let $n \in \mathbb{N}$.

Since $n \geq n_2 = n_0$, using our assumption, we know that $f(n) + g(n) \leq c_0 \cdot h(n)$. Since $f(n) \in \mathbb{R}^{\geq 0}$ (by the definition of the function), we know that if we subtract $f(n)$ from the left side, it would become even smaller and the inequality would still hold, i.e.:

$$\begin{aligned} f(n) + g(n) &\leq c_0 \cdot h(n) \\ g(n) &\leq c_0 \cdot h(n) && \text{(subtract } f(n) \text{ from the left side)} \\ g(n) &\leq c_1 \cdot h(n) && \text{(since } c_1 = c_0\text{)} \end{aligned}$$

Thus, we have proven that $f(n) \leq c_1 \cdot h(n)$ and $g(n) \leq c_2 \cdot h(n)$. □

(b) For all functions $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$, we define the *product function* $f \cdot g : \mathbb{N} \to \mathbb{R}^{\geq 0}$ as follows:

$$\forall n \in \mathbb{N}, (f \cdot g)(n) = f(n) \cdot g(n).$$

Let $f, g, h : \mathbb{N} \to \mathbb{R}^{\geq 0}$. We will **disprove** that if $f \cdot g \in \mathcal{O}(h)$, then $f \in \mathcal{O}(h)$ and $g \in \mathcal{O}(h)$.

Want to prove: $\exists f, g, h : \mathbb{N} \to \mathbb{R}^{\geq 0}, f \cdot g \in \mathcal{O}(h) \wedge \big(f \notin \mathcal{O}(h) \vee g \notin \mathcal{O}(h)\big)$

Proof. Let $n \in \mathbb{N}$. Let $g(n) = n^2$. Let $h(n) = n$. Let $f(n)$ be the piece-wise function defined by:

$$\begin{cases} f(n) = 0 & \text{when } n = 0 \\ f(n) = \frac{1}{n} & \text{when } n \geq 1 \end{cases}$$

Want to prove: $f \cdot g \in \mathcal{O}(h) \wedge \big(f \notin \mathcal{O}(h) \vee g \notin \mathcal{O}(h)\big)$

Proof that $\boldsymbol{f \cdot g \in \mathcal{O}(h)}$, i.e., $\exists c_0, n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow (f \cdot g)(n) \leq c_0 \cdot h(n)$.

By definition of product functions, we know $(f \cdot g)(n) = f(n) \cdot g(n)$.

Let $c_0 = 1$. Let $n_0 = 1$. Let $n \in \mathbb{N}$.

From our assumption that $n \geq n_0$, we can infer the following:

$$\begin{aligned} & n \geq 1 \\ \Leftrightarrow 0 < & \frac{1}{n} \leq 1 \end{aligned} \tag{1}$$

Moreover, from our assumption:

$$n^2 \geq 1 > 0 \tag{2}$$

We can then conclude the following:

$$f(n) \cdot g(n) = \frac{1}{n} \cdot n^2 \geq 0 \qquad \text{(using } \mathbf{(1)} \text{ and } \mathbf{(2)}\text{)}$$

Want to prove: $f(n) \cdot g(n) \leq c_0 \cdot h(n)$.

We can perform arithmetic operations on the product functions to prove this:

$$\begin{aligned} f(n) \cdot g(n) &= \frac{1}{n} \cdot n^2 \\ &= 1 \cdot n^{2-1} \\ &= n \\ &\leq 1 \cdot n \\ &= c_0 \cdot h(n) && \text{(from our choice of } c_0 \text{ and } h(n)\text{)} \end{aligned}$$

Proof that $\boldsymbol{f \notin \mathcal{O}(h) \vee g \notin \mathcal{O}(h)}$:

Want to prove: $g \notin \mathcal{O}(h)$, i.e.,

$$\forall c_1, n_1 \in \mathbb{R}^+, \exists n \in \mathbb{N}, n \geq n_1 \wedge g(n) \geq c_1 \cdot h(n)$$

Let $c_1, n_1 \in \mathbb{R}^+$. Let $n = \lceil c_1 + n_1 + 1 \rceil$, where $n \in \mathbb{N}$.

Want to prove: $n \geq n_1 \wedge g(n) \geq c_1 \cdot h(n)$.

By our choice of n, we know that $n \geq n_1$ is $True$.

By our choice of n, we also know the following:

$$c_1 \leq n$$
$$c_1 \cdot n \leq n^2$$
$$c_1 \cdot h(n) \leq g(n)$$

Thus, we have proven that $f \cdot g \in \mathcal{O}(h)$ and that $g \notin \mathcal{O}(h)$. □